The Dissemination of Mobile Malware in Today's Society

Samantha Mallari
Taguig City, Philippines
sgmallari@student.apc.edu.ph

Faith Ballesteros
Taguig City, Philippines
fiballesteros@student.apc.edu.ph

Eva Samillano
Pasay City, Philippines
vrsamillano@student.apc.edu.ph

Maria Chrisva Landig
Taguig City, Philippines
mclandig@student.apc.edu.ph

Abstract--- There is an inevitable, increasing growth in the mobile market today. Moreover, concurrent with this rapid growth of mobile phones, personal digital assistance (PDA) and other integrated devices is the development of a more intelligent cyber-criminal operations and dissemination of mobile malwares. [1] ***The first malware that can infect phones began in 2004. By 2005, mobile malware was already diving into the realms of stealing confidential information from the targets.*** [2] ***Thus, mobile devices are becoming the target of cybercriminals.*** [3] ***This paper will provide an initial background about the indispensable growth of mobile malware (MM). It examines on the infection strategy, infection routes, threats, damage, and methods used by attackers to enter, control, and exploit the mobile devices. Lastly, this paper will provide useful tips, indicating what to do when a mobile malware infects a device and how to prevent it.***

Keywords: Mobile Malware, Threats, Mitigation, Security

I. Introduction

There are numerous mobile devices available in the market today. Parallel to this increasing growth is the development of different mobile malware set loose to attack them. [4] Mobile malware (MM) is defined as a malicious software that is built to attack mobile platforms by damaging or disrupting it. [5].The first MM was created purposively to exploit Symbian devices. However, as time passes, the developers of these MM are becoming more intelligent by also infecting devices running on Android OS and iOS. The researchers were able to ascertain that Android OS are more prone to MM threats than iOS because it allows their users to install apps using third-party sources. [6] According to the research in Kaspersky laboratory, Android has become the top target for malicious attacks which started in 2010, wherein the first Trojan for Android was discovered, called "ANDROIDOS_DROIDSMS". It is a fraud SMS app that sent messages to premium rate numbers. Another Trojan was uncovered in the same month, called "DROIDSMS.A," It poses as a Tap Snake game that will eventually transmit the GPS location of an infected phone over HTTP, this location data could then be queried by another phone using the GPS Spy app. Also in the same year, the first malware for iOS based devices was discovered, called "Ikee". Ikee worm can only infect jailbroken phones and those who have installed SSH.

Nowadays, criminals are developing mobile malware for financial gain. The attackers are looking forward in exploiting new areas of opportunity in the mobile platform and some of their primary reasons are remote controlling of mobile devices, identity theft, and stealing personal information. There is a rapid growth of cybercrimes nowadays and one of its common forms, is through deploying a mobile malware.

II. Statement of the Problem

Threats came into existence since 2000 but it outgrew when the source code for Cabir was disseminated in 2004. In 2000, a VBScript worm called, "Timofonica (Telefonica)" subsisted. The creator of Timofonica programmed the virus to send SMS-messages, saying in Spanish "Information for you: Telefonica is fooling you" to GSM mobile phones through Internet SMS-gate of the MoviStar mobile operator. It cannot infect phones, additionally, it only spams the phone with annoying messages. It was perceived to be the first experienced of a security incident with regards to MM. In 2004, the dissemination of Cabir's source code occurred. It uses Bluetooth and SMS to spread the infection. It's constant Bluetooth scanning drains phone's battery. Aside from Cabir and Timofonica, there are other mobile viruses made through the years; these are Skulls, CommWarrior, Blankfont, CardTrap, Doomed, and others. These mobile malwares originated in different countries and each has unique ways of attacking the users.

A taxonomy was created to provide a background about the increasing growth of MM. It will focus on infection strategy, distribution, and payload. These methods are most used by attackers to enter, control, and exploit the devices' systems. The current new virus wave targeting mobile devices has evolved at a much faster pace than viruses for desktop computers.

The attacker may use wired connections, wireless connections, and other infection strategy to spread the malware throughout the organization. Although, wireless connection is more popular than wired connections, there are still few necessities that are best accomplished with the use of a wired connection. Wired connections are often used to perform system backups, updates, and synchronization of data through ports and memory cards. Wireless connection, on the other hand, refers to the protocols such as Bluetooth, Multimedia Messaging Service (MMS), HTTP, and SMS. One of the most popular attack through wireless connection is known as, SMS phishing (SMSishing) wherein the victim receives a short message and lured into clicking the URL associated with the message to download the malware.

Payload refers to the damage associated with the inflicting malware. It can be classified as nuisance or devious. Nuisance payloads is simply an invasion of privacy but it is not as harmful as devious payload. It is purposively made to annoy the target. Some examples of these payloads are file deletions, e-mail deletions, disabling Internet connections, defacing background picture and icons, and uninstalling software. A devious payload are meant to exploit the information stored in a target for several reasons such as financial gain, distribution of personal data, identity theft, and others. [8] The most popular known example of devious payload is Phishing wherein the attacker is “fishing” for sensitive user credentials by sending an SMS message or an E-mail which contains links to phishing web pages or application. It comes in form of wireless communication. Now, Phishing also comes in form of a mobile application. Pharming is another type of phishing, wherein the attacker acquires a domain name for a Web site which redirects to a phishing Website, thus serves as a pathway to steal information. Vishing, on the other hand, is defined as a combination of phishing techniques and the use of a telephone. Traditional Vishing methods involve sending e-mails to users, prompting them to call a number to enter sensitive information. In comes in form of spam messages, which lures the user to call an interactive voice management system on a VoIP server. [9]

Mobile malware cannot be simply ignored because it compromises the privacy and confidential information of the user. As time passes, the threats inflicted with MM are increasing and even existing models of security are failing to account for the scale, complexity and intelligence of these threats that are present today.

III. Results and Discussion

Mobile malware continues to infect phones in every part of the globe. Security companies, cellular operators and phone makers are trying to address these issues before they become unstoppable by developing antivirus software and new security models. [10] Despite the risks and threats associated with MM, some preventive measures can be done by the users in order to protect their phone from this contagious infection.

Second, mobile users must only allow installation of apps from trusted sources, such as Google Play and App Store. Some apps located outside the trusted zone can accesses the user's personal information and send it to cybercriminals. Some apps can even leave users with expensive charges on their mobile bill. Malicious app can be a ransomware or a fake app. A ransomware app simply mimics a legitimate app to trick users into installing it. After the installation process, the app locks the device and forces the user to pay a ransom to unlock the device. Fake apps, on the other hand, can steal your personal information or trick user into paying for a useless app. [12] so the next time the user will download an application, he will proceed with caution and decide which apps are allowed on his device and which ones he will allow access to his personal information. [13]

Third, as tempting as it sounds, the user must never click on a link in an email or message from someone they do not know. These links might lead them to phishing Web sites. Also, they must never respond to text or voicemail with personal information. They must first verify the identity of the user before responding to any of their messages or calls.

Fourth, the user must turn off Bluetooth and other wireless connections when not in use. Not only because it can drain phone’s battery but also to protect their phone from possible threats that can occur such as blue jacking, wherein it allows the attacker to obtain unauthorized personal data from the target. [14]

Fifth, the user must keep the operating system of their mobile devices up to date. The older the operating system is, the more vulnerable the device can be to harmful attacks. In order to remove bugs and prevent mobile malware attacks, Apple and Android have to keep updating their mobile operating systems. [15]

Lastly, the user can download security apps such as Norton mobile security and McAfee mobile security to heighten the security of their mobile phones. Such apps give the user the ability to locate their phone, remote lock and wipe or restore the information they have stored on their devices.

IV. Conclusion and Recommendation

Mobile malware poses a threat to mobile platforms by collecting and distributing a user's confidential information stored on their devices without their consent. [16] Mobile malware inevitably mutates into new species that attack the mobile device in numerous ways. As time passes, it gets worse. All mobile devices are prone to the peril caused by MM. However, mobile manufacturers and mobile users must make a concerted action before MM degrades the utility and value of smartphones. One of the best ways to immunize and disinfect smartphones is through an Antivirus application. However, not everyone uses it because they do not know the relevance of security apps. They often misunderstood the concept of MM. Mobile malware awareness might just be the best solution to lessen the cases of MM. With sufficient knowledge and understanding about the threats and dangers of MM, people will be more responsible with their actions.

Even the largest mobile manufacturers are taking necessary precautions in dealing with the MM. They are heightening their security to prevent the possible attacks of MM. The new Symbian operating system does not allow installation from third party sources. Unless it was disabled by a user, the system effectively excludes all mobile malware discovered to date. [17]

This case study therefore concludes that it is impossible to annihilate mobile malware. It will continue to exist throughout the century as attackers will continue to develop more intelligent ways to attack the user for their benefits. However, as the old saying goes, “Prevention is always better than cure”, the user can always take some precautions to protect their devices from getting infected by a malware. With the right knowledge and understanding, people can prevent the dissemination of a mobile malware. Having a mobile phone comes with great responsibility and application security is one of the most critical component that the user holds. [18]

V. References

[1] Yiang, X. & Yajin, Z. (2013). Android Malware. USA: North Carolina State University.

[2] Zorabedian, J. (2015, May 15). *Check out this infographic showing the history of mobile threats, 2004-2015*. Retrieved February 24, 2016 from https://blogs.sophos.com/2015/05/19/check-out-this-infographic-showing-the-history-of-mobile-threats-2004-2015/

[3] Kapersky Lab. (5 February 2016) *Mobile devices become a new target for spam and malware attacks*. Retrieved February 23, 2016 from http://www.kaspersky.com/about/news/spam/2016/Mobile-devices-become-a-new-target-for-spam-and-malware-attacks

[4] Bach, O. (13 July 2015) *Mobile Malware Threats in 2015: Fraudsters Are Still Two Steps Ahead.* Retrieved February 23, 2016 from https://securityintelligence.com/mobile-malware-threats-in-2015-fraudsters-are-still-two-steps-ahead/

[5] Rondeau, L. (2014) *Mobile Device Vulnerabilities & Securities.* (Unpublished senior honors thesis). Eastern Michigan University, Ypsilanti Michigan, USA.

[6] Bose, A. (2008) Propagation, Detection and Containment of Mobile Malware. (Unpublished thesis). University of Michigan, Ann Arbor Michigan, USA

[7] Bickford, J.E (January 2012) Rootkits on smart phones: attacks, implications and energy-aware defense techniques. (Unpublished thesis). New Brunswik Rutgers. New Brunswik, New Jersey.

[8] Dunham, K. (April 2004) Mobile Malware Attacks and Defense. Syngress Publishing, Inc. Burlington, MA.

[9] Fortinet Inc. (N.D) *Happy Birthday, Mobile Malware*! Retrieved February 23, 2016 from www.fortinet.com

[10] Trend Micro (N.D) The History of Mobile Malware. Retrieved February 24, 2016 from www.trendmicro.com

[11] Stratecast (October 2013). *The many shades of mobile app risk: Understanding and mitigating mobile threats effectively*. Retrieved February 24, 2016 from www.frost.com

[12] Van Der Veen, V. (2013). Dynamic Analysis of Mobile Malware (Unpublished Thesis). VU University Amsterdam.

[13] Sophos (N.D). *When Malware goes Mobile.* Retrieved February 23, 2016 from https://www.sophos.com/en-us/security-news-trends/security-trends/malware-goes-mobile/10-tips-to-prevent-mobile-malware.aspx

[14] Shabtai, A. Kanonov, U. Elovice, Y. Andromaly: A behavioral malware detection framework for android devices

[15] Security Awareness Company (17 September 2015) *Protect Yourself from Mobile Malware with these 6 Easy Tips*. Retrieved February 24, 2016 from http://blog.thesecurityawarenesscompany.com/protect-yourself-from-mobile-malware-with-these-6-easy-tips/

[16] Dupaul, N. (2 October 2013) *Common Mobile Malware Types: Cybersecurity 101*. Retrieved February 23, 2016 from https://www.veracode.com/blog/2013/10/common-mobile-malware-types-cybersecurity-101

[17] Hyponnes, M. (November 2006) Malware goes Mobile. *Scientific American Inc.*

[18] Worcel, E. (23 February 2016) *Mobile Application Security: Risks and Responsibilities*. Retrieved 26 February 2016 from https://securityintelligence.com/mobile-application-security-risks-and-responsibilities/