Mobile Malware: Analysis and Comparison Against Computer Based Malware

Author:

Yusuf Oaris

oaris@sheridancollege.ca

School:

Sheridan College

1430 Trafalgar Road, Oakville

Faculty Advisor:

Gurdeep Gill

gurdeep.gill@sheridancollege.ca

Signature:

Date:

July 22nd, 2022

Abstract **--- With the growth in popularity of mobile devices in modern times, malware authors have started to develop malware specific to mobile devices to gain another attack vector. Authors can develop malware that differentiate from computer based malware based on the mobile devices architecture with their own features and behaviors. While the malware differentiate from their computer based counterpart, they do still share many similarities such as needing to exploit a vulnerability that exist within the device to have a manner of executing its payload. The two platforms also share some of the same types of vulnerabilities but mobile devices have certain vulnerabilities specific to its unique features. In order to combat the rise in popularity of mobile based malware and its evolution, many companies that manufacture mobile devices have integrated some built-in features to protect the devices from being harmed by malware such as scanners and detection mechanisms.**

TABLE OF CONTENTS

I. Introduction and problem statement

Over the course of the Information System Security program, various topics are taught by various teachers, some directly relating to security topics and others acting as backbones to understand computer related topics and then be brought up again in later years. Some of these topics range from databases, programming, networking, cryptography, learning how to secure the different layers and the many types of threat that exist in the cyber world. Of the many types of threats that exist, the most famous one known by not only to people knowledgeable in computer related topics but also people who know little about computer related topics is that of malwares or commonly and incorrectly generalized as viruses.

While learning about the previously mentioned fields of topic, the topics were taught in a manner relating to computer devices as they are the most commonly used and most commonly attacked devices in modern era as well as the fact that computers allow more diversity in terms of program and software usage. This leads to a gap of knowledge leading into the real world as mobile devices as becoming more popular as the days go by, with not only adult and teenagers owning at least 1 mobile device, but also children being given a device to watch videos and play games. This rise in popularity gives malicious attackers another platform to target and exploit, especially with the fact that most mobile users do so recreationally or do not know about the dangers of the internet such as the younger children. To add to this, most people do not think about malware being made to target mobile devices as they are not covered on media outlets, leading some to believe that mobile devise do not experience malware threats.

Due to this, an analysis will be done on the different types of mobile malware that do exist, from how they are developed for the platforms to how they are distributed and eventually deliver its payload. To further fill in the knowledge gap, a comparison will be made between mobile and computer based malware to distinguish how they differ and what traits they share. Finally, to understand how cybersecurity is being handled against these mobile threats, an analysis of the security feature present on device will be done to see how it compares to computer protection procedures.

II. Prior work

Abdullahi et al.[1] discusses the appeal of mobile based malware and why they are as attractive as they are for malware authors. The paper goes over the threats found in these sorts of devices and touches on how they operate and then proposes a security solution to minimize the damage caused by mobile malware.

Mina et al.[2] and Abdulaziz [3] focuses on manners to detect mobile malware through various means such as machine learning or static and dynamic analysis. In doing so, the taxonomy of the different mobile malwares are given along with a short explanation for each.

Sevil et al.[4] and Mijoo et al.[5] discuss the manners in which mobile malware are evolving to prevent it from being detected easily. The paper focuses on evasion techniques used by mobile malware and how they are continuously evolving to further avoid detection.

Tae et al.[6] focuses more on mobile malware meant for android devices as most forms of mobile malware are developed for android devices. It gives and overview of the Android operating system and discusses how the apps are stored and managed within it.

Sethi et al.[7] and the paper published by DataTheorem [8] both perform threat modeling for mobile devices. The works analyze the threats found on mobile devices as well as explaining each type of threat and then suggests controls for them.

III. Mobile based malware

A. Development Process

In order to create malware for mobile devices, there are a few prerequisites that need to be completed and decided upon. These prerequisite are matters such as deciding:

- What type of malware is to be created?
- What platform/operating system will it be used against?
- What vulnerability will be exploited?
- How many concealment technique are going to be used?
- What language it will be written in?
- What protocols will be used for its networking aspects?

- What environment will be used to develop and test the malware?

Working on these prerequisites can take some time as different tools can provide different results. An example of this would be how depending on the programming language used, the malware will have different strengths and weaknesses such as how Python is an easier language to program in which more advantages to its portability and scalability, but is easier to detect as it uses many libraries. Comparing this to Assembly language, it is much harder to develop a program, but by directly communicating with the registers, the malware will be much faster and a lot harder to detect. Apart from identifying which tools to use based on their advantages and disadvantages, properly identifying a vulnerability in the system is a crucial step, often considered the first step as without a vulnerability to exploit, the malware will not have a way to infect and attack the system itself.

After properly identifying all the prerequisites desired for the mobile malware, what many consider to be the actual development portion can now commence. In this step, the features desired for the malware to perform is decided such as if it wants to manipulate the files on the mobile device (whether that be creating new ones, deleting old ones, downloading files), any other feature such as attacking system resources like bandwidth, processor speed or features that will obtain private and sensitive information from the user interacting with the device. While deciding these, with the evolution and development of malware detection software, the malware author must integrate evasion and anti-analysis techniques. These techniques can be employed through the use of obfuscation and packing as has been previously known but also the use of techniques such as timing attacks which delays the start of its attack, hides its malicious behaviors during runtime and to launch the malicious behaviors in case it is detected [5].

B. Existing Mobile Vulnerabilities

When thinking about mobile devices in general, many only gravitate towards cellular phones and tablets, forgoing other devices such as smartwatches, portable gaming consoles or devices used for mobile medical care such as pacemakers which have had previous hacking incidents where its information was being monitored [9]. First and foremost, as with any cyber device, the weakest link in the security chain is the user and this stand even more firm when considering mobile devices as with the current societal norm, most people have at least one mobile device on them almost all day. To add to this, Abdullahi et al. states that “76 percent of mobile users depend on their mobile devices to access their most sensitive personal information, such as online banking or personal medical information” [1]. With the amount of people using mobile devices for various uses, the device is being exposed to more and more vulnerabilities as time goes on, endangering personal information due to something such as browsing on a website to read something.

To further discuss vulnerabilities that exist on mobile device, we can categorize them into 6 groups. These 6 groups are browser vulnerabilities, Man-in-the-Middle (MitM) attacks, application vulnerabilities, jailbreaking, vulnerabilities through SMS (Short Message Service) such as text messages and emails and vulnerabilities found in the device or operating system. Table 1 further elaborates on these 6 categories by giving an explanation for each vulnerability as well as an example.

Category	Explanation	Example
Browser Vulnerabilities	Since mobile browsers are only patched through their respective OS upgrades, they remain vulnerable to malicious websites for far longer.	Some mobile version of certain websites and if they are not properly hardened, the user can become victim to attacks such as Cross-Site Scripting (XSS) or SQL Injection.
Man-in-the-Middle (MitM) attacks	A third party or attacker intercepts network communication to either eavesdrop or modify transmitted data. This is more common for mobile devices as all communications are done wirelessly and rely on an access point.	Connecting to public Wi-Fi access point and having someone eavesdrop on the communication to then decide to interject and attempt to steal data.

Application vulnerabilities	Some application developed for the mobile device can introduce additional vulnerabilities into the device. The application developer can also intentionally make the app vulnerable to then exploit it themselves.	Downloading an app from the app store only for it to have been a Trojan and containing malware within it.
Jailbreaking	This process is done to gain administrator access to mobile devices by taking advantage in the root access of these devices.	Certain people will pay to jailbreak their own phone to have more control over the default apps on mobile devices but in doing so allow an attacker to have access to more data and cause more harm than if it were not jailbroken.
Vulnerabilities through SMS (Short Message Service	Using the additional feature found on mobile devices to directly message the user, fake messages are sent to trick the user to performing an action.	Phishing attacks are the most popular form of this category. Another example would be spam callers recording a call and waiting for the word "yes" to be said, thus making it seem like someone had agreed verbally to something they otherwise hadn't agreed to.
Device and Operating System (OS) vulnerabilities	Vulnerabilities found either on the device itself or on the underlying OS it operates with.	The "CVE-2022-22292" vulnerability found on Samsung devices in 2021 which allowed local apps to perform privileged operations without proper authorization [10]

Table 1: Mobile Device Vulnerabilities Categories

C. Mobile vs. Computer Malware

When looking at the previous sections involving the development process and the existing vulnerabilities for mobile malware, many comparisons can be made against their computer based brethren. Both share similarities in there general steps such as identifying what vulnerability to exploit and determining what type of malware to use. The biggest difference would be their infection vectors, computer based malware mainly targets browser vulnerabilities while mobile based malware mainly targets the vulnerabilities present in the mobile device itself and its operating system. Other difference would be in the features to implement inside of a malware. While some features are similar across both platforms such as file manipulations, some are exclusive to one platform compared to the other such as command line arguments on computer based malware. Other difference would be how some vulnerability categories are exclusive to only one side such as SMS and jailbreaking being vulnerabilities for mobile devices. Perhaps one of the vastest differences between the two would be the amount of variation that mobile malware can has as mobile devices are not limited to only cellphones but encompass any device that can be used on the move.

When looking at the difference purely by using numbers, a few differences (around 5 to 10) differences does not seem like a lot. However, upon delving into the sub categories for those differences, there is a lot more laying underneath which can amount to a different development or attack procedure. Table 2 compares computer based malware and mobile based malware, showing what they have in common and where they differ.

Similarities	**Differences**

Both have the same general development process	They have different attack vectors - Mobile Device and OS vulnerabilities - Computer Web browser vulnerabilities
File manipulation features that can be implemented into the malware	Some features that are exclusive to one platform such as command line arguments
Both share similar vulnerability categories such as: - Browser vulnerabilities - Man-in-the-Middle attacks - Application vulnerabilities	Jailbreaking is exclusive to mobile devices, therefore is only exploited in mobile malwares
	SMS vulnerabilities and are exclusive vulnerabilities for mobile malwares
	Bigger variety of devices when considering mobile devices that mobile malware can be made for: - Cellphones - Portable gaming consoles (ex: Nintendo Switch) - Mobile medical devices (ex: pacemaker)
	Both types of malware have different evolution rates and processes

Table 2: Comparison between mobile malware and computer malware

D. Protection Features

Due to the amount of risk coming from mobile based malware and its many methods of distribution, many mobile devices have integrated built in malware protection applications and systems within them. Mobile devices started off their security features by relying on OS hardening and relying on Wi-Fi security protocols such as WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) but as technology and malware have continued to evolve, so to have the protection systems. The first proper malware protection feature added onto mobile devices was a virus scanner which operates like any normal virus scanner, scanning the files on the device and trying to find anything malicious. This feature continues to be a staple on devices but additional features have been added to expand its protection range. The scanners now perform a more in depth search of the devices and are able to detect a wider range of the type of malware such as worms, spyware and potentially ransomware if it hasn't fully executed and encrypted the device, and after discovering them, will remove them from the device to restore its health. Some mobile device companies have also developed their own software such as Android using Google Play Protect for its malware protection.

Apart from malware protection systems, some companies also have systems in place to protect their devices from spam calls and SMS which aids to reduce the amount of phishing attacks that make it to the users. Android devices alert their users with an on text message to alert the user that a call or SMS that it is "Suspected Spam". Other companies such as Apple and Huawei also have more protection features against malware than just the typical scanner although they are incorporated in a different manner. Huawei features simply need to be enabled in the settings menu which is similar to Apple products as well with the only one major difference. As Apple focuses on having a very secure system due to it being a closed system and not releasing any of its information, the system itself is already secured and can further be hardened by downloading security apps from the app store. This could lead to one of the vulnerabilities categories previously mentioned, that off application vulnerabilities, but do to the nature of the system itself, this tends to not be too great a concern for Apple as much as Android devices as most mobile malware are designed for Android due to its open nature.

IV. Conclusion

The purpose of this paper is to research more about the mobile based malware and develop more of an understanding on them and then comparing them to computer based malware to see how they differ. From the research and analysis performed, that goal has been achieved, discovering more about mobile malware and their characteristics, especially in recent times where mobile devices are

the most used devices and only continue to increase in popularity. As has been shown, while mobile malware share many traits in common with computer malware, the differences make a big impact in the world of cybersecurity and this is further backed up with the fact that mobile malware are evolving in a different way than computer malware and at a different rate.

V. Areas for further study

As this paper focused on the characteristics of mobile based malware, from their development stage to their attack venues and comparing them to computer based malware, there are multiple areas which will require further study to be conducted. The first area would be in the way mobile malware are detected followed by methods for mitigating them altogether in order to prevent them as much as possible as to reduce the number users who fall victim. All of these can also be compared to computer malware methods as to provide a better understanding to people researching the topic.

VI. Bibliography

[1] A. Arabo and B. Pranggono, "Mobile Malware and Smart Device Security: Trends, Challenges and Solutions," 2013 19th International Conference on Control Systems and Computer Science, 2013, pp. 526-531, doi: 10.1109/CSCS.2013.27.

[2] M. E. Zadeh Nojoo Kambar, A. Esmaeilzadeh, Y. Kim and K. Taghva, "A Survey on Mobile Malware Detection Methods using Machine Learning," 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), 2022, pp. 0215-0221, doi: 10.1109/CCWC54503.2022.9720753.

[3] A. Alzubaidi, "Recent Advances in Android Mobile Malware Detection: A Systematic Literature Review," in IEEE Access, vol. 9, pp. 146318-146349, 2021, doi: 10.1109/ACCESS.2021.3123187.

[4] S. Sen, E. Aydogan and A. I. Aysan, "Coevolution of Mobile Malware and Anti-Malware," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 10, pp. 2563-2574, Oct. 2018, doi: 10.1109/TIFS.2018.2824250.

[5] M. Kim, T. J. Lee, Y. Shin and H. Y. Youm, "A study on behavior-based mobile malware analysis system against evasion techniques," 2016 International Conference on Information Networking (ICOIN), 2016, pp. 455-457, doi: 10.1109/ICOIN.2016.7427158.

[6] T. Oh, H. S. Moon, Y. H. Kim, J. N. Kim and B. Stackpole, "Android malware analysis and conceptual malware mitigation approaches," 2016 International Conference on Information and Communication Technology Convergence (ICTC), 2016, pp. 684-693, doi: 10.1109/ICTC.2016.7763562.

[7] A. Sethi, N. Bergman, J. Kozyrakis, C. gagnon, J. Scambray, The Developer's Guide to Securing Mobile Applications, San Francisco: Synopsys Inc., 2020, Accessed: Jul 8, 2022. [Online]. Available: https://www.synopsys.com/content/dam/synopsys/sig-assets/ebooks/developers-guide-securing-mobile-applications-threat-modeling.pdf

[8] Threat Model for Mobile Applications Security & Privacy, California: DataTheorem, 2013, Accessed: Jul 8, 2022. [Online]. Available: https://www.ten-inc.com/presentations/DataTheorem-Mobile-App-Threat-Model.pdf

[9] UR, A. and Simon, S., 2022. Can pacemakers be hacked? 'CBI' stirs debate. [online] The New Indian Express. Available at: https://www.newindianexpress.com/cities/kochi/2022/jun/23/can-pacemakers-be-hacked-cbi-stirs-debate-2468549.html#:~:text=Dr%20Vinod%20Thomas%2C%20chief%20cardiologist,do%20so%20with%20assistive%20devices.%E2%80%9D [Accessed 10 July 2022].

[10] Prospero, M., 2022. *Major security vulnerability found in Samsung phones — what to do now*. [online] Tom's Guide. Available at: https://www.tomsguide.com/news/major-security-vulnerability-found-in-samsung-phones-what-to-do [Accessed 11 July 2022].

[11] Nayak, C., 2018. *Malware Development – Welcome to the Dark Side: Part 1*. [online] Network Intelligence. Available at: https://niiconsulting.com/checkmate/2018/02/malware-development-welcome-dark-side-part-1/ [Accessed 11 July 2022].

[12] Check Point Software. 2022. *Top 6 Mobile Security Threats and How to Prevent Them*. [online] Available at: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-mobile-security/top-6-mobile-security-threats-and-how-to-prevent-them/ [Accessed 11 July 2022].