Aggravation of Mobile Banking Trojan in Android Platform and its Mitigation Techniques

Rincy Raphael[#1]

[#] Research Scholar, Department of Computer Science & Engineering,
Anna University, Chennai, India

Abstract: *As mobile banking and online banking services grow, the threat actors' interest in exploiting mobile platforms is also spreading. According to experts in data protection services, hackers have recently tried to develop banking malware capable of exploiting security vulnerabilities in the implementation of these services, increasingly widespread. This paper is reviewing the mobile malware threats and some measures that can strengthen the security of the user against mobile banking malware.*

Keywords: *Mobile Banking, Banking Trojan, Android Malware Trojan*

I. INTRODUCTION

According to data collected by various cyber security firms, between January and March 2019, banking malware in mobile devices grew by about 60%, which represents more than 300k mobile banking users infected with some malware variant, without mentioning that these attacks are also possible by infecting desktop equipment [11]. The main way of infection of mobile devices is the downloading of unreliable software/applications. Although nothing guarantees absolute protection against these attacks, the main security recommendation for the user is to download applications only from trusted sources (App Store, Google Play Store, etc). Application and system updates are also a fundamental protection measure, commented experts in data protection services. Banking malware can enter our devices by exploiting known security vulnerabilities, corrected by updates and security patches, so it is essential to keep our systems and applications always updated to their latest versions.

In 2016, cyber security researchers at ESET came across a malware, aka Android/Spy.Agent.SI, which could put millions of Australian customers' bank account details at serious risk [20]. The malware could copy popular banking apps from different countries such as CommonWealth Bank, NAB and ANZ banks in Australia. As a result, the malware would show an overlay screen on the infected apps, showing fake username and password fields for snatching these sensitive details. The malware was so potent that it could circumvent the two-factor authentication security of the app, thereby revealing the details to the hackers. Later the same year, security researchers at Kaspersky Lab also discovered a similar but modified Trojan malware that could bypass the Android 6's security features [9]. As a result, the hacker could be able to steal the bank account details of the online banking app users. Fast forward to 2017, a small group of Russian hackers used a malware to dupe Russian bank users, stealing over $800,000 [15]. The hackers deceived the unsuspecting users by showing them fake banking apps that were plagued with the malware that would steal their money.

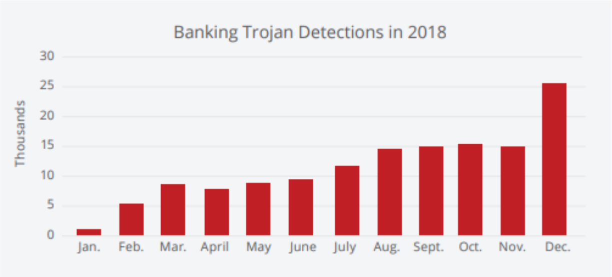


Figure 1: Mobile Banking Trojan Detection in 2018

Over the past month, banking trojans threatened users of Android devices. In late April Doctor Web virus analysts [24] detected new modifications of the *Android.Banker.180.origin* malware.These modifications were distributed under the guise of package tracking apps targeting Japanese users. Once installed, these Trojans delete their own icons and hide themselves from users. As per the McAfee mobile thread report in 2019 [23], nearly 25000 mobile banking Trojans are detected (refer Figure 1). Lack of security measures available in the android malware market always attract the attackers to inject vulnerability in such app store [4]. The Figure 2 shows that 98% of mobile malware targets Android platform because of the ease and flexibility of the Android open source operating system [22]. Mobile malware applications are added with unnecessary permissions to perform the unauthorised activities unknowingly by the users. It needs a strong and efficient mechanism to deal with such types of fraud Mobile banking applications [13].

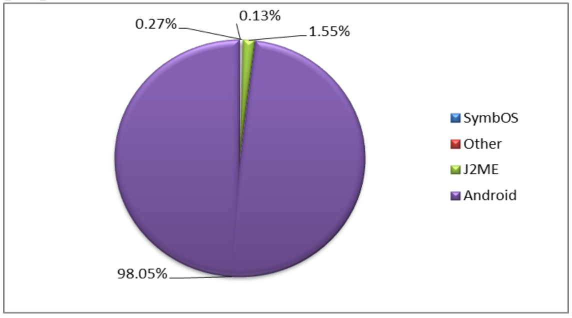


Figure 2: Mobile Banking Trojan Attacks to various Mobile Operating System

II. MOBILE MALWARE: A BRIEF HISTORY

Symantec Researcher shows that, in 2017, new mobile malware variants increased by 54 percent and an average of 24,000 malicious mobile applications were blocked every single day [10]. But it is difficult for finding and blocking the malicious apps in each and every day. Mobile malware had to begin somewhere, so let's take a look at a brief history of Mobile Malware.

- **Cabir**

Cabir, released in 2004, is considered the first real mobile malware. The worm spread via Bluetooth and targeted the Symbian operating system, which was the primary OS used on smartphones of the time. The malware was thought to be a proof of concept from a group of hackers known as 29A. The group sent Cabir to antivirus firms, likely in an effort to gain attention and prove that phones were not immune to malware. Cabir's main goal was to spread to other Bluetooth enabled devices. Once the malware had made it onto a device, it would display the word "Caribe" on the phone's screen every time the device was turned on. While Cabir was relatively harmless compared to mobile malware today, it did drain device battery power as it constantly scanned for nearby Bluetooth devices to spread to. Also, potential victims had to accept the Bluetooth file transfer request in order to become infected. Although the first version of Cabir wasn't considered much of a threat, later variants had the ability to steal data, such as information from the device's phonebook. While Cabir showed the world that mobile malware should be taken seriously, it would be a few years yet before smartphones were smart enough, i.e. were capable of processing and storing more information, for malware authors to see them as a worthwhile target.

- **Mosquitos\Trojan.Mos**

Soon after Cabir hit the scene, a Trojanized version of the popular Symbian game Mosquitos appeared. The game worked just like the legitimate version, the only difference was the addition of a malicious program known as Trojan.Mos that would send an SMS message to a premium-rate phone number every time the game was played. Mosquitos\Trojan.Mos made history as the first mobile malware to make money for its developers.

- **Skuller**

Skuller was a nuisance malware, designed to cause damage and hinder usage of the infected device. The threat was distributed through websites and internet forums disguised as a phone theme. Once it was installed on a device it replaced icons with a skull and crossbones logo. The malware also overwrote application files, making the phone practically unusable. Interestingly, Skuller used code from Cabir to enable it to spread over Bluetooth. Skuller did what it did purely to create chaos, however, its end goal of making devices unusable would later become a key facet in the world of mobile ransomware.

- **CommWarrior**

CommWarrior, emerging just a year after Cabir in 2005, was also a relatively harmless worm for Symbian devices. But while Cabir only had one infection vector, CommWarrior was the first mobile threat to spread via Multimedia Messaging Service (MMS) messages. The malware also attempted to spread using Bluetooth, but it was its ability to use MMS that made it stand out. The worm sent an MMS message to a random contact in the user's contact list. The message had a copy of the malware attached and was made to look like it was from someone the victim knew. Once the attachment was opened, the cycle would continue. With the added MMS infection vector, CommWarrior was more successful at spreading than it's cousin Cabir.

- **RedBrowser**

The 2006 was the year when the first multi-platform mobile malware arrived. RedBrowser could work on phones running the Java 2 Mobile Edition (J2ME) software. At the time, J2ME was running on phones made by Nokia, Motorola, Siemens, Samsung, and many others. The malware pretended to be a Wireless Application Protocol (WAP) browser but instead of browsing the internet it sent out premium-rate SMS messages from victim's devices. It wasn't long after RedBrowser that other platforms like Windows Mobile also became a target for mobile malware.

- **FlexiSpy**

In 2007, the first mobile spyware came along. FlexiSpy was advertised as a tool for people to spy on their partners. The malware could record phone calls and collect SMS messages and send the information to the attacker.

- **Ikee**

The 2007 was also when the first iPhone was launched, and with it the first iOS threats, although these would only be a problem for jailbroken devices up until 2015. However, if you were one of the people who decided you wanted Apple's software restriction removed from your iPhone, then the Ikee malware was the start of your problems. The worm spread between jailbroken iPhones that used the OpenSSH protocol to secure network traffic. The malware took advantage of unchanged default passwords to infect devices and, once it was in, stole the Apple ID and password and changed the phone's wallpaper to a picture of '80s singer and meme superstar Rick Astley. A year later, in 2008, the first Android devices hit stores. It wasn't long after the appearance of these devices that the Android operating system began attracting the majority of malware authors' attention. While it took a while, by 2010 Android was firmly in mobile malware's sights, but more on this later.

- **Zitmo**

Malware follows an evolutionary process, with each new threat learning from or using pieces of the threats that have come before. Mobile malware isn't any different and, in 2010, a threat came along that had built upon the success of an infamous PC threat. ZitMo, or Zeus-in-the-Mobile, was the little brother of the Zeus banking Trojan. ZitMo stole internet banking transaction authorization numbers and was first spotted targeting Symbian devices but was soon seen on Windows Mobile, Blackberry, and eventually Android.

- **DroidDream**

One of Android's appealing features is that it is, unlike Apple's tightly controlled App Store and iOS, an open platform, but this is also one of its problems. Google's Play Store (previously called Android Market) has, since its earliest days, been plagued with dodgy apps that manage to make their way past security checks. In 2011, an Android threat known as DroidDream, which had been downloaded thousands of times, was discovered packaged inside more than 50 seemingly legitimate applications on Android Market [8]. The malware stole sensitive information from compromised devices and could also install other apps. DroidDream, together with other early Android threats, represented the beginning of a long battle, that continues today, between Google and malware authors trying to get their wares onto the Play Store.

- **FakeDefender**

In 2013, FakeDefender [10], arguably the first mobile ransomware threat, targeted Android devices and displayed fake security alerts in an effort to get the user to buy an app to remove the fake threats. In some cases, the malware prevented users from uninstalling it and from launching other apps. FakeDefender also changed operating system settings and users were unable to carry out a hard reset. While FakeDefender merely locked up aspects of the device's features while it tried to get the user to pay to get access back, it would be the use of encryption that helped mobile ransomware really take off.

- **Simplocker**

The first mobile ransomware to encrypt files and hold them for ransom was Simplocker. Appearing in 2014, just a year after FakeDefender, the threat would be the first in a long line of similar threats targeting Android. Simplocker initially pretended to be legitimate apps on fake Google Play websites aimed at Russian-speaking users. The malware encrypted document, picture, and video files stored on the device's SD card. It then displayed a message saying the phone had been locked due to the presence of child pornography and that the only way to unlock the device was by paying a fee. This message appeared every time the user attempted to open an app.

- **YiSpecter**

Just in case Apple was feeling left out, in 2015 the first iOS malware for non-jailbroken devices emerged. YiSpecter basically created a backdoor on compromised devices that allowed attackers to install and uninstall apps, download files, and display advertisements, among other things. The threat was mostly targeting devices in China and Taiwan and was spread through third-party app stores, forum posts, social media, and hijacked internet service provider traffic that redirected users to download the malware.

As the number of smartphone user's increase each and every year, the malware authors continue to develop and improve their techniques and attacking strategies. Android is the one of interesting platform for most the attackers where it is easy to develop and deploy android applications. The flexibility and availability if android applications are attracting both legitimate users as well as intruders [1].

III. THE EVOLUTION OF MOBILE BANKING TROJAN

Visiting the bank to perform banking transactions is almost a thing of the past. These days, most banks aim to deliver a seamless banking experience to their users, all without having to step foot inside a bank. This concept of "bringing the bank closer to you" is done via online banking carried out on PCs or, more than not, smartphones. A tradeoff for this convenience is often security, with one of the contributing factors being the existence and evolution of so-called banking Trojans.

The mobile banking Trojan *Android.Fakebank*, for example, was first detected by Symantec in July 2013 and since then has impacted banking customers across the globe, including those from some of the world's top banks, using creative and resourceful tactics. There are thousands of fake mobile apps on the web that are actually banking Trojans in disguise, and the number is still increasing. The motivation behind banking Trojans is money, and they usually aim to steal the victim's login credentials and/or private banking information in order to gain full access to the victim's account [5]. The evolution of mobile banking Trojans and discuss some of the methods and tactics used by different threats over the years.

- **Fake login pages**

Banking Trojans often rely on impersonation. Upon launching, the Trojan shows a seemingly legit login page for the banking app it is masquerading as, requiring the victim to enter their banking credentials and/or credit card details, which will then be sent to the attacker's remote server. To target multiple banking apps at once, some malware authors hardcode copies of multiple popular bank login pages into one banking Trojan. Once one of the legitimate banking apps is launched, the Trojan displays the relevant login page to the victim.

A more advanced tactic used by some Trojans involves login pages dynamically loaded from a remote server based on whatever legitimate banking apps are installed on the device. As such, the attacker only needs one banking Trojan to infiltrate a victim's device, giving them the ability to steal credentials from a range of banks.

➢ **Impersonating legitimate banking apps**

Some banking Trojans go a step further by persuading victims to replace their legitimate banking app with a fake malicious version. This is done by showing the user an alert informing them that they need to update the legitimate banking app because it's outdated. When the victim agrees, or is forced to agree, the Trojan downloads the fake version from the attacker's remote server. As such, the attack is still active even if the original Trojan is removed.

Trojan targets a list of specific legitimate banking apps to prepare for its bogus pop-up dialog. The Trojan alerts victim to update their legitimate banking app. Fake banking app containing another variant of the Trojan is downloaded from a remote server once the victim agrees with the update alert.

➢ **Interception and exploitation**

To strengthen the security of banking apps, most banks use two-factor authentication (2FA) when transactions are being made. In turn, banking Trojans have evolved to adapt to this security feature and many can still steal victims' credentials. They do this by intercepting the user's incoming text messages, which contain the 2FA code, and relaying all bank-related SMS messages to the attacker's remote server in real time. The attacker can then use the code to authenticate and carry out financial transactions on the victim's account.

There are also some banking Trojans that target phone calls on the compromised device made to and from financial institutions. The Trojan can intercept and record the victim's calls to and from the bank, which can then be used to retrieve sensitive banking information, such as identity verification details. To make matters worse, some Trojans actively hijack calls made to banks and redirect the victim to a phoneline belonging to the attacker [18]. By doing so, the attackers can talk directly to the victim and obtain sensitive financial information, saving them the trouble of recording and listening to voice calls. These Trojans can also spoof the attacker's caller ID to make it appear that the legitimate bank is calling. To prevent the victim from reporting any suspicious activity to the bank, the Trojan also blocks the bank's phone number on the compromised device.

➢ **Advanced interception technique**

Since 2016, many Android threats began making use of Android's Accessibility Service to monitor all events on the device's user interface (UI). Not to be left out, authors of banking Trojans latched on to the trend as well. Once the permission has been granted by the device's owner, these Trojans don't need to customize bogus login pages to steal login credentials. They can just grab this information on-the-fly as the Trojan can now monitor all UI events. With the Accessibility Service enabled, the Trojan can perform transactions all by itself, including transferring money to the attacker's bank account. If 2FA is set up, the Trojan can either hijack the SMS, as mentioned earlier, or bypass 2FA by abusing Android's Accessibility Service. All these steps can be done within a few seconds, making it extremely hard for the victim to stop it in time.

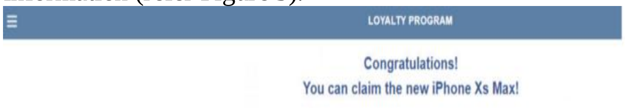
➢ **Impersonation of non-banking apps**

Other than impersonating banking applications, banking Trojans can also be found masquerading as other legitimate applications that enable in-app purchases, such as the Google Play Store app [6]. When installed, they are able to intercept the execution of legitimate apps and present a bogus page that requests the victim's credit card information.

These Trojans are malicious and powerful as they are designed to scam victims on multiple apps. In addition to banking apps, other finance related apps, and even mobile wallet apps, are targeted by these Trojans. While the behavior of these Trojans is similar to those targeting just banking apps, the amount of money the attackers can gain is significantly greater.

➢ **Other variants**

Stealing banking information can also be done in other ways. Instead of mimicking a legitimate bank or intercepting phone calls, some banking Trojans display scam and phishing websites, telling victims they have won a prize. In order to redeem the prize, victims are required to enter their credit card information (refer Figure 3).

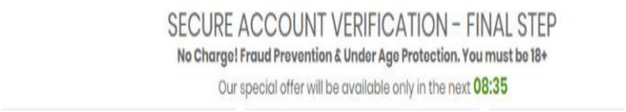


LOYALTY PROGRAM

Congratulations!

You can claim the new iPhone Xs Max!

Figure 3: Victims congratulated for winning an iPhone



SECURE ACCOUNT VERIFICATION - FINAL STEP

No Charge! Fraud Prevention & Under Age Protection. You must be 18+

Our special offer will be available only in the next 08:35

Figure 4: Attacker asking for Account information

Victims told to complete one more step to get their prize and the Credit card information is requested to claim the non-existent prize (refer Figure 4).

➢ **Infiltrating Google Play**

To impact a larger number of victims, banking Trojans also try and sneak their way onto the Google

Play Store, with this activity increasing significantly since 2018. The Trojans that manage to do this successfully are usually not embedded in apps, as more often than not, the app will get rejected by Google [7]. Instead, once an app is installed, the malware is downloaded from a remote server and tends to hide under a legitimate looking app. Once the initial app is installed from the Google Play Store and executed, the banking Trojan is dynamically loaded and installed to the victim's device.

These are just some of the tricks, tactics, and techniques employed by mobile banking Trojans. These threats have continued to evolve since they first arrived on the scene shortly after mobile banking started to become popular with users, and there's no doubt that this evolution will continue well into the future. As long as there is money to be stolen, cyber crooks will continue to try and find new and resourceful ways to steal it.

IV. TRACK AND MINE PERSONAL INFORMATION BY MOBILE APPS

While malware still remains to be a major concern for mobile devices a new study suggests that there are more severe threats lurking within your mobile apps. There are a number of mobile apps that exhibit risky behavior when it comes to sharing personal information - that includes accessing user's contacts, calendars, locations and more [17]. The unwarranted data mining from apps is more of a threat to users than any malware. It is important to take care of our personal credentials from unauthorised access from the apps because this unprotected flow of user data over unprotected networks could mean that more than just marketing companies are sniffing around for your personal info. Consider a flashlight app might need your location, calendar or address book. That is, an app is collecting more information than required. This information may not always be created securely and may become the target for criminals and illegal activities.

Major risks that enterprises need to be aware of:

(i). With the emerging trend of BYOD (Bring Your Own Devices), the problem of data mining is becoming even more important.

(ii). Enterprises need to be more careful when it comes to mobile device management.

(iii). Adequate security features can ensure that sensitive information does not get into wrong hands.

(iv). Strong passwords, network encryption and limiting the types of apps that can be downloaded on devices are some key measures to be implemented.

Above all, it is important to remember that data always flows two ways and it is important to keep your professional data separate from your private data. Never leave your devices open and be careful what you download on your mobile devices.

V. PROTECT ANDROID BANKING APPS FROM MALWARE

Be it a ransomware attack or a malware attack, these cyber threats are not going to go away anytime soon. Fortunately, there are some ways to prevent these attacks and the ensuing calamities.

1. **Install Latest Security Patch:** More often than not, attackers carry out successful hacks by exploiting security vulnerabilities in the system software, and Android is no exception. By exploiting a security hole in your Android, a hacker or snooper can inject a malware or any other malicious tool that could result in GPS hijacking, data theft, and identity theft, to name a few. Therefore, it is imperative to install security patches as soon as they are released by the vendor.
2. **Avoid Pirated Apps:** There are many Android users who readily root their devices so they can have more control on the OS. In fact, in most cases, users end up rooting their devices so they could install a new version of the OS that is not officially available for the specific device. Keep in mind that APK files are easily hacked. Any individual with the wrong intention of stealing your personal data can install a malware into the APK and leak your data without your knowledge. The best way to prevent such malware is by avoiding pirated apps altogether [21].
3. **Checkout Permissions:** Before you download an app from Google Play Store, you may have noticed that the Play Store asks for certain permissions. It is important that you read the permissions thoroughly to ensure that the app isn't asking for any unnecessary permissions [2]. For instance, a recipe app would not require permission for your GPS. If it does, it is most likely an unreliable app. In such situations, avoid downloading the app and report it as well [3].
4. **Use Security Tools:** Be it a computer or an Android device, installing the right security tool can help users avert the calamity caused by cyber-attacks. Especially, if you are a savvy online banking app user, it is important that you use some kind of security tool, or best yet encryption tool. With encryption in place, you can have a safe environment to make online transactions.
5. **Digital privacy and security** are getting weaker with every passing year. As more and more cyber-attacks continuously invade different sectors, it won't be too long before cybercriminals freely roam the digital space. However, by implementing the security tips mentioned above, not only can you protect your device but also take a firm stand against the rising plague of cyber threats.

VI. CONCLUSION

The ever-increasing popularity and most probably the open-source nature of the Mobile operating system is perhaps what attracts cybercriminals to make relentless efforts to hack into the device and salvage the personal data of users. Android is one of the interesting environments to implement Mobile banking Trojans. Cybercriminals use specialized malware to carry out the hacks and achieve their ulterior motives.

Always stay protected from online threats and risks by taking some precautions such as keep your software up to date and do not download apps from unfamiliar sites where as only install apps from trusted apps stores. Pay close attention to the permissions requested by apps as well as memory usage of your device. Always try to install a suitable security app to protect your device and data. The frequent backups of important data are also necessary as per the users working environment.

REFERENCES

[1]. H. Wang, Z. Liu, Y. Guo, X. Chen, M. Zhang, G. Xu, and J. Hong, "An explorative study of the mobile app ecosystem from app developers' perspective," in Proceedings of the 26th International Conference on World Wide Web (WWW 2017), pp. 163–172.

[2]. K. W. Y. Au, Y. F. Zhou, Z. Huang, and D. Lie, "Pscout: Analyzing the android permission specification," in CCS 2012, pp. 217–228.

[3]. H. Wang, J. I. Hong, and Y. Guo, "Using text mining to infer the purpose of permission use in mobile apps," in The 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp 2015), pp. 1107–1118.

[4]. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in Proceedings of SPSM 2011, pp. 3–14.

[5]. R. Stevens, C. Gibler, J. Crussell, J. Erickson, and H. Chen, "Investigating user privacy in Android ad libraries," in MoST 2012.

[6]. N. Viennot, E. Garcia, and J. Nieh, "A measurement study of google play," SIGMETRICS Perform. Eval. Rev., vol. 42, no. 1, pp. 221–233, Jun. 2014.

[7]. H. Wang, H. Li, L. Li, Y. Guo, and G. Xu, "Why are Android apps removed from google play? a large-scale empirical study," in 15th International Conference on Mining Software Repositories (MSR 2018).

[8]. Y. Zhou, Z. Wang, W. Zhou, and X. Jiang, "Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets," Proc. 19th Annu. Netw. Distrib. Syst. Secur. Symp., no. 2, pp. 5–8, 2012.

[9]. "Riskware | Internet Security Threats." [Online]. Available: http://usa.kaspersky.com/internet-security-center/threats/riskware#.Vm-5IUp97IU. [Accessed: 15-Dec-2015].

[10]. "Android.Fakedefender.B | Symantec." [Online]. Available: https://www.symantec.com/security_response/writeup.jsp?docid=2013-091013-3953-99. [Accessed: 15-Dec-2018].

[11]. "2018 malware forecast: the onward march of android malware,"https://nakedsecurity.sophos.com/2017/11/07/2018-malware-forecastthe-onward-march-of-android-malware/, 2018.

[12]. "contagio mobile: Backdoor.AndroidOS.Obad.a." [Online]. Available: http://contagiominidump.blogspot.in/2013/06/backdoorandroidosobada.html. [Accessed: 28-Oct-2015].

[13]. "Number of available Android applications - AppBrain." [Online]. Available: http://www.appbrain.com/stats/number-of-android-apps. [Accessed: 28-Oct-2015].

[14]. "Gartner Says Annual Smartphone Sales Surpassed Sales of Feature Phones for the First Time in 2013." [Online]. Available: http://www.gartner.com/newsroom/id/2665715. [Accessed: 28-Oct-2015].

[15]. "Eric Schmidt: „There Are Now 1.3 Million Android Device Activations Per Day."" [Online]. Available: http://techcrunch.com/2012/09/05/eric-schmidt-there-are-now-1-3-million-android-device-activations-per-day/. [Accessed: 28-Oct-2015].

[16]. C. a Castillo, "Android Malware Past, Present , and Future," McAfee White Pap. Mob. Secur. Work. Gr., pp. 1–28, 2011

[17]. You and K. Yim, "Malware obfuscation techniques: A brief survey," Proc. - 2010 Int. Conf. Broadband, Wirel. Comput. Commun. Appl. BWCCA 2010, pp. 297–300, 2010.

[18]. W. Enck, D. Octeau, and P. Mcdaniel, "A Study of Android Application Security," no. August, 2011.

[19]. F. Wu, H. Narang, and D. Clarke, "An Overview of Mobile Malware and Solutions," J. Comput. Commun., vol. 2, no. 2, pp. 8–17, 2014.

[20]. "Trojan: Android/DroidKungFu.C Description | F-Secure Labs." [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_droidkungfu_c.shtml. [Accessed: 15-Dec-2015].

[21]. R. Raveendranath, V. Rajamani, A. J. Babu, and S. K. Datta, "Android malware attacks and countermeasures: Current and future directions," 2014 Int. Conf. Control. Instrumentation, Commun. Comput. Technol., pp. 137–143, 2014.

[22]. "Mobile Banking Trojans on Android OS", https://www.computerworld.com/article/2475964/98--of-mobile-malware-targets-android-platform.html [Accessed: 27-Nov-2018].

[23]. "McAfee Mobile Thread Report 2019", https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf [Accessed: 12-July-2019].

[24]. "Dr. Web Anti-Virus", https://news.drweb.com/show/review/?lng=en&i=13278, [Accessed:4-March-2019].