# Android Attacks Detection Techniques

Hugo Marques

Lusófona University of Porto, Portugal
hugomaarqz@gmail.com

**Abstract.** Nowadays, almost everyone has a mobile device, especially a smartphone. Most people who have a smartphone are constantly at risk, often due to the applications they install, and just the fact that they connect to the internet for various purposes, they get unprotected from malware attacks, even though technology is becoming increasingly advanced. It is true that there are several malware detection tools, which are extremely important on every mobile device to protect each user's personal data. But it's also true that these tools just work to a certain point, and the "intruders" can get around these tools through numerous techniques. This study summarizes the various malware detection techniques used in the Android OS, explaining the advantages and disadvantages of each.

**Keywords:** Malware Attacks, Detection Tools, Personal Data, Android, Security, Application, Signature

## 1 Introduction

With the increased use of Android smartphones [1], the amount of android malware attacks is growing very quickly, and this growth brings several associated problems because it catches the attention of major malware attacks. Android is an opensource system unlike iOS, which is a closed system where apps are constantly inspected by security experts, so it makes the first system more vulnerable to external attacks.
These attacks are increasingly in 2019, and according to the information collected, researchers at Check Point examined cyberattacks in the first half of 2019 and found that those targeting smartphones and other mobile devices have risen by 50% compared with last year. The findings have been outlined in the Cyber Attack Trends: 2019 Mid-Year Report and the report suggests one of the key reasons for the sharp rise is the increased use of homebanking applications. This has seen cybercriminals following the money and increasingly distributing malware designed to steal payment data, login credentials, and ultimately funds from victims' bank accounts. In many cases, the malware attacks follow similar distribution strategies to those targeting desktop users, with the applications silently running in the background without the victim being any the wiser [2]. Android is the most popular platform for smart-phone based malware authors and sometimes even trusted applications can leak user's location and phone's identity and share it without its consent. These days we must be very updated and informed in order to keep up with what we can be struck with, so it is very important to know what android attacks are, how to spot a potential one and protect ourselves.

10.11228/dpsc.02.01.011

This paper focuses on describing mobile-based android attacks and its counter detection techniques. It's going to be analyzed the android security enhancement, what are the vulnerabilities and how Google's providing tools to protect users.

## 2 Android Environment: Attacks and Types of Malware

A malware attack is a type of cyberattack in which malware or malicious software performs activities on the victim's computer system, usually without his/her knowledge. [3]. Malware attacks can occur on all sorts of devices and operating systems, including Microsoft Windows, macOS, Android, and iOS. At least one type of malware attack is growing. Mobile ransomware attacks increased by a third in 2018 from the previous year. Most of those attacks occurred in the United States [4].

### 2.1 Types of Attacks on Android

The entire development lifecycle of Android has been subject to a rigorous security program, but it doesn't invalidate that android is vulnerable to cyber-attacks and there are several cyber-attacks which cause lot of harm to users. These attacks can be isolated cyber-attacks or based upon use of malware as attack tool. Beyond that we can observe clearly that Android developers are keep improving the Android version by version, but in the other hand that shows that the older android versions had some security issues and vulnerabilities and that leads to malware and cyber-attacks. Patching these vulnerabilities prevents some attacks but there are always others which attackers discovers and forms attacks around these vulnerabilities.

| Attack type | MALWARE | Description | Impact |
|---|---|---|---|
| Data theft | SMS/Email | The users get a SMS or a email giving them big bounties with a link. When they click that they may be redirected to a malicious website giving away their sensitive information or may lead to financial loss. | The most innocent people can be fooled by these messages and their personal information is exposed. |
| Identity Theft | NFC/OTP | Attacker gets access of mobile device and impersonate the user using their smartphone running Android. | Loss can be very huge and only limited with the attacker though |
| Bloat-ware | Adware | Nasty form of bloatware that exists to pump ads to the user, via websites or via popups that come up directly on computer screen. | Adware can slow PC down - it can spy on user as well or expose user's system to other dangers. |

**Table 1.** Types of Android attacks [5]

### 2.2 Types of Malware

**Trojans:** A Trojan, often mistakenly thought of as a virus or a worm, is a malicious program that enters in a device, hidden in programs that seem harmless. It serves to open a door so that malicious users can break into a person's computer or device. A Trojan is a program that simulates some useful functionality that can harm computers and their users, such as hacking or stealing user passwords. Their main propagation is through the Internet, where they are offered as tools with useful - or even vital - functions for devices**.** The two most common types of Trojans are Keyloggers (which are commonly used to steal passwords) and Backdoors (files that allow door openings for intrusion) [6].

**Worm:** Worms is a type of malware that spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage. Worms can be transmitted via software vulnerabilities. Or computer worms could arrive as attachments in spam emails or instant messages (IMs). Once opened, these files could provide a link to a malicious website or automatically download the computer worm. Once it's installed, the worm silently goes to work and infects the machine without the user's knowledge [7].

**Adware:** Adware is an unwanted software designed to cause advertisement to appear on the screen, mostly within a browser. Usually it uses a discrete method to disguise itself as legitimate or it infiltrates in another program to trick the users into installing it on PCs, tablets or mobile devices [8].

**Ransomware:** A Ransomware is a type of malware that prevents users from accessing your system or personal files and requires them to pay a ransom to return the access. Those files are still on the device, but the malware has encrypted the device, making the data stored on computer or mobile device inaccessible. That malicious software comes in several different forms. The two most common variations are Crypto ransomware and Locker ransomware.[9]

**Rootkit:** A rootkit is a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence. The term rootkit is a connection of the two words "root" and "kit." Originally, a rootkit was a collection of tools that enabled administrator-level access to a computer or network. Root refers to the Admin account on Unix and Linux systems, and kit refers to the software components that implement the tool. Today rootkits are generally associated with malware – such as Trojans, worms, viruses – that conceal their existence and actions from users and other system processes [10].

**Botnet:** A botnet is a network of malware-infected computers that can be wholly controlled by a single command and control center operated by a threat actor. The network itself, which can be composed of thousands if not hundreds of thousands of computers, is then used to further spread the malware and increase the size of the network. [11] What happens is that botnets gain access to your machine through some piece of malicious coding. In some cases, your machine is directly hacked, while other times what is known as a "spider" (a program that crawls the Internet looking for holes in security to exploit) does the hacking automatically. [12]

### 2.3 Android Banking Malware: A Real Case of an Attack

The most prevalent type of Android banking malware is the fake banking apps, in this paper it will be explored the impact of that approach on potencial victims. Malware in both these categories is designed to achieve the same goal: steal credentials for, or money from, their victims. Malware in both these categories is designed to achieve the same goal: steal credentials for, or money from, their victims' bank accounts. To achieve that, both sophisticated banking Trojans and fake banking apps need to elicit sensitive banking information from their victims and, if direct theft is the aim typically also need to gain access to SMS messages received on the compromised devices. To lure the valuable information from potential victims, both types of malware make use of phishing and bogus login forms. However, despite the similarities in their objectives, sophisticated banking Trojans and fake banking apps differ significantly in their strategy for deceiving victims. The following section will explore that difference and offer a more detailed look into the modus operandi of each distinct malware type [13].

**Key features and strategy:** Fake banking apps bet everything on the success of impersonation – their whole operation stands or falls on how believably they can imitate a legitimate banking application, or stand in for a non-existent one, from the very first moment a potential victim comes across them, up to the point when the victim enters sensitive information. Their weapon of choice is therefore their presentation – from app name, through app description, to icon and preview images, the apps need to appear trustworthy to attract unsuspecting users [13].

**Modus operandi:** To reach their malicious goals, fake banking apps typically take the following steps: 1) Trick victims into installing malware by posing as a legitimate banking app; 2) Obtain needed permissions; 3) Upon launch, display a phishing screen mimicking a legitimate banking app and requesting login credentials or credit/debit card details; 4) Harvest credentials or credit/debit card details entered into the bogus form; 5) Display an error/thank-you message; offer no further functionality; 6) Optional: Use SMS permissions to intercept one-time password (OTP); 7) Carry out fraudulent transactions using the victim's account or sell credentials on the black market; [13]

**Distribution**: Fake banking apps are often spread across Google Play or unofficial app stores, where they represent legitimate banking apps or other financial apps. Attackers who spread these malicious counterfeits try to lure their victims by using legitimate-looking application [13].

**Targeting:** Fake banking applications often focus on targeting customers from just one financial institution or service - the one they practice. In choosing their destination, some malware authors take advantage of the absence of an official mobile app for the destination bank or service, while others try to mislead users by impersonating existing official applications. Occasionally, counterfeits are intended to offer additional and compelling functionality to existing legitimate applications, such as bank rewards or offers to increase credit card limits (Figure 1) [13].

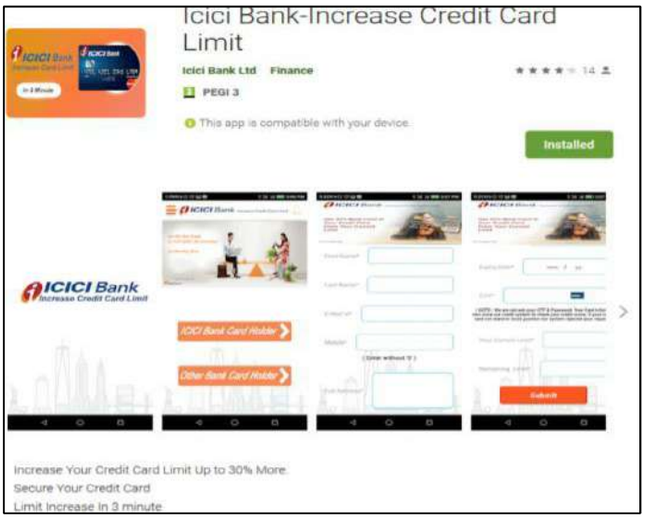


**Fig. 1.** Malicious app impersonating Indian Icici bank and claiming to increase credit card limit for its customers [13]

**Functionality and permissions:** These apps functionality come down to displaying bogus login screens and harvesting credentials entered into the fake forms. After the credentials are stolen, some apps display generic messages with a promise to get back to the victim, as a cover for not offering any real functionality. Optionally, depending on permissions gained during and after installation, fake banking apps can also intercept and redirect SMS messages to bypass SMS-based 2-factor authentication. As users install these apps believing they are installing real banking applications, they are likely to grant the apps SMS permissions without thinking twice about it [13].

### 2.4 Google Services for Android Security

Google try to give extra security to Android devices and protect users by offering various services like Google Play Protect, which provides high security for users in many ways.

**Data Protection:** Google Play keep apps and data safe [14].

**Scanning:** Every day, it automatically scans all the apps on Android phones and works to prevent harmful apps from ever reaching them. This tool checks all app developers on Google play, so even before downloading an app, the user knows that it has been verified and approved [14].

**SafetyNet:** Offers a set of services and APIs that help protect an app from security threats, including device tampering, incorrect URLs, potentially harmful apps, and fake users. There are four types of SafetyNet that will be presented next.

**SafetyNet Attestation:** Provides services for determining if a device running your app satisfies Android compatibility tests [15].

**SafetyNet Safe Browsing:** Offers services to determine if a URL has been marked as a known threat by Google [15].

**SafetyNet reCAPTCHA:** Protects apps against malicious traffic [15].

**SafetyNet Verify Apps:** Protects the devices against potentially harmful apps [15].

## 3 Malware Attacks Techniques

**Attack Targeting and Inception:** Cybercriminals will determine the method of initiating your attack. If profit is the primary objective, such as ransomware attacks, attackers will attack as many users as possible using spear-phishing attacks, in which recipients are urged to open the message attachment, which launches the malware program. Other comprehensive targeting methods involve using sites where attacks start through hidden redirects and drive-by-downloads. Attackers typically prefer public websites that run vulnerable web or application servers that they can take advantage of. Attacks targeting specific individuals can also leverage exploits and different types of social engineering techniques to entice an insider to inadvertently install malware inside an organization's firewall [16].

**Exploit Discovery:** Many attackers favor packaging malware into exploit kits that they covertly place on legitimate websites or host the malware on a fake website designed to look like a legitimate site. When a potential victim's browser connects with a website hosting an exploit kit, the kit probes the visitor's system and extracts information like OS version, browser type, and installed applications, in order to find vulnerabilities to exploit. Exploits and malware go hand in hand. All types of enterprise and consumer applications have vulnerabilities that can potentially be exploited, paving the way for malicious programs to find their targets. [16]

**Payload Delivery:** The malicious program will download and install a "payload" to the target endpoint device. This payload could be the piece of malware itself, or it could be a hidden downloader which then creates a backdoor through which multiple types of malware can be downloaded, allowing different attacks to be executed. [16]

**Execution of Attack:** The malicious program has reached its target and begins to run on the system, carrying out the attacker's intent. In the case of ransomware, the program will begin to encrypt the user's files or block critical system operations, thus locking the user out. More sophisticated attack code can be designed to trigger off of specific system events, or stealthily steal data over an extended period of time [16].

**Malware Propagation:** If a malware attack goes undetected or unmitigated, it will likely spread laterally, infecting other endpoints or even launching further targeted attacks via the network. As the malware persists, it communicates back to the attacker's back end, or to other command & control servers. Lateral spread is often the goal of attacks leveraging RATs (Remote Access Trojans). RATs are malware programs designed to establish administrative control over the host computer through back doors. Once such control is gained by an attacker, they can distribute RATs to other vulnerable computers on the network, establishing a botnet [16].

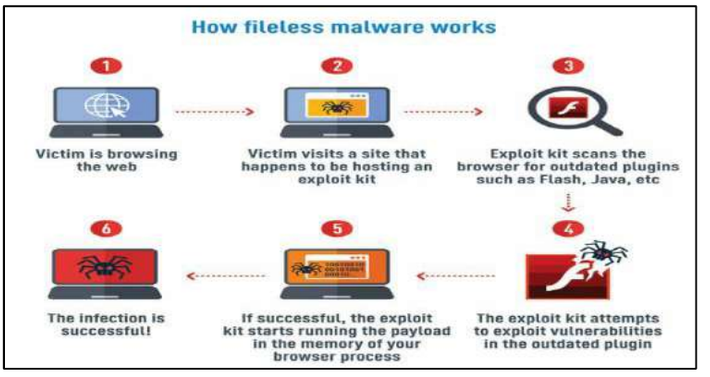


**Fig. 2.** Spreading process of a malware [17]

## 4 Malware Detection Techniques

In this section will be analyzed the types of android malware detection techniques that exist. That techniques can be categorized in three main groups: 1) Signature-based detection, 2) Anomaly-based detection and 3) Specification-based detection. These three based detection tools can also be group on the based-on type of analysis static, hybrid or dynamic analysis. Static analysis is done without running an application while dynamic analysis deals with features that were extracted from the application while running. The following explains the analysis of these techniques more deeply.

**Signature-Based Detection:** Signature-based detection is a process where a unique identifier is established about a known threat so that the threat can be identified in the future. In the case of a virus scanner, it may be a unique pattern of code that attaches to a file, or it may be as simple as the hash of a known bad file. If that specific pattern, or signature, is discovered again, the file can be flagged as being infected. Suspected files are typically quarantined and/or encrypted in order to render them inoperable and useless. Clearly there will always be new and emerging viruses with their own unique code signatures, so the library of known code signatures is updated by the anti-virus software provider and if a new viral signature is detected, the updates are pushed out to users immediately and zero-day vulnerabilities are avoided [18][19][20].

| ADVANTAGES | DISADVANTAGES |
|---|---|
| They are very efficient to detect without generating a large number of false alarms. | These types of detectors can only detect known attacks, which are included in the signature set that IDS has, so we must always be updating this set. |
| They can diagnose the use of a specific attack tool or technique. | Most of these detectors have very specific signatures, not detecting variants of the same attack. |

**Table 2.** Advantages and disadvantages of Signature-based detection [23].

**Anomaly-Based detection(behavior-based):** Anomaly based analysis is based on watching the behavior of the device by keeping track of different parameters and the status of the components of the device. A key advantage of anomaly-based detection is its ability to detect zero-day attacks Anomaly-based detection generally needs to work on a statistically significant number of packets, because any packet is only an anomaly compared to some baseline. This need for a baseline presents several difficulties. For one, anomaly-based detection will not be able to detect attacks that can be executed with a few or even a single packet. While signature-based detection compares behavior to rules, anomaly-based detection compares behavior to profiles. These profiles still need to define what is normal, like rules need to be defined. However, anomaly-based

profiles are more like white lists, because the profile detects when behavior goes outside an acceptable range. This analysis can be static, dynamic or hybrid [20][21][22].

| ADVANTAGES | DISADVANTAGES |
|---|---|
| Detect usually behaviour and thus have the ability to detect symptoms of attacks without specific knowledge of details. | Usually produces a large number of false alarms due to the unpredictable behaviors of users and networks.. |
| Can produce information that can be used to define signatures for misuse detectors | Often require extensive "training sets" of system event records in order to characterize normal behavior patterns. |

**Table 3.** Advantages and disadvantages of Anomaly-based detection [23]

**Specification-Based Detection:** Specification-Based Detection is the derivate of anomaly- based detection and is much more complex than the others detection techniques cause its analysis can be performed at the layers below the Internet Protocol stack application layer or at the operating system control level. In specification-based system there exists a training phase which attempts to learn the all valid behaviour of a program or system which needs to inspect. The main limitation of specification-based system is that it if very difficult to accurately specify the behaviour the system or program. One such tool is Panorama which captures the system wide information flow of the program under inspection over a system and checks the behaviour against a valid set of rules to detect malicious activity. Specification based detection makes use of certain rule set of what is considered as normal in order to decide the maliciousness of the program violating the predefined rule set. Thus, programs violating the rule set are considered as malicious program. This type of detection is considered lower level. This analysis can be static, hybrid or dynamic too [20][21][22].

All malware scanners, essentially, utilize signature and anomaly -based techniques for perceiving personalities of programs.

**a) Dynamic methods:** Dynamic analysis is the testing and evaluation of a program by executing data in real-time. The objective is to find errors in a program while it is running, rather than by repeatedly examining the code offline. It is a detection technique which aims at evaluating malware by executing the application and the main advantage of this technique is that determines the application behavior during runtime and loads target data. The resource consumption in this analysis technique is more as compared to static analysis. Dynamic behavioral detection method constructs operation environment by using a sandbox, virtual machine, and other forms, and simulates the execution of the application to acquire the application's behavior model [24].

**b) Static methods:** In the static analysis, the analysis of the applications is done, and the features are extracted without executing the application on an emulator or device. In comparison to other analysis techniques for android malware detection, static analysis consumes fewer resources and time as it does not involve execution of the application. The major disadvantage of this analysis is code obfuscation because of which detecting the malicious behavior of the application becomes difficult as pattern matching is not possible. This analysis can detect runtime errors, logical inconsistencies, and possible security violations. The most commonly used static features are the Permission and API calls [24].

**c) Hybrid methods:** Hybrid Analysis is a combination of static and dynamic analysis. It is a technology or method that can integrate run-time data extracted from dynamic analysis into a static analysis algorithm to detect behavior or malicious functionality in the applications. The hybrid analysis method involves combining static features obtained while analyzing the application and dynamic features and information extracted while the application is executed. Though it could increase the accuracy of the detection rate, it makes the system cumbersome and the analysis process is time consuming. [24].

| **Factors** | **Static Analysis** | **Dynamic Analysis** | **Hybrid Analysis** |
|---|---|---|---|
| Time required | Less | More | More |
| Input | Binary files, scripting language file etc. | Memory snapshots, runtime API data | Data obtained from both static and dynamic analysis |
| Code obfuscation | Yes | No | No |
| Resource Consumption (power & memory) | Less | More | More |
| Effectiveness and Accuracy | Less as compared to dynamic analysis | Better than static analysis | Better than static and dynamic analysis |
| Target code execution | Not possible | Possible | Possible |
| Advantages | Low cost and requires less time for analysis | Provides deep analysis and higher detection rate with unknown malware detection | Extracts features of static and dynamic analysis both, providing more accurate results |
| Limitations | Limited signature database and can detect only known malware types | More time and power consumption | High Cost |

**Table 4.** Comparison between static, dynamic and hybrid analysis [24]

## 5 Conclusion

It's so obvious that a good part of people is still outdated when we talk about technologies and the pros and cons of their advancements. People need to informate themselves about all what involves technology and not only about the "good part" of that. In this case we talk about a very known technology, the Android SO. The attacks on android by hackers are increasingly and the security remains compromised.
In this paper is presented all the android environment referring all the vulnerabilities despite the strict security program that Android has been subjected to. Within the Android Environment theme, is referred the 3 most known android attacks and what impact these produce. Are also mentioned the main types of malware and is chosen a real case of a malware attack. The way how Google provides her services to give extra security to Android devices and protect users is focused as well as the techniques of malware attacks, that is, how malware spreads and what are the stages until the end goal is reached. The main point of this paper in presented in point 4 where with searches done it was concluded that there are three main detection techniques which are all divided in static, dynamic or hybrid analysis.

To do this paper, was consulted many other selected papers of different authors to collect authentic information based on different knowledge. To resume I hope people get more informed about this subject to be more protected and prevented to these attacks.

## References

1. Android tem mais de 2,5 bilhões de usuários, https://www.tecmundo.com.br/dispositivos-moveis/141038-android-tem-2-5-bilhoes-usuarios.htm, 2019/12/16
2. Mobile Malware attacks are booming in 2019: These are the most common threats, https://www.zdnet.com/article/mobile-malware-attacks-are-booming-in-2019-these-are-the-most-common-threats/, 2019/12/16
3. What is a Malware Attack, https://enterprise.comodo.com/what-is-a-malware-attack.php, 2019/12/16
4. Malware attacks: What you need to know, https://us.norton.com/internetsecurity-malware-malware-101-how-do-i-get-malware-complex-attacks.html, 2019/12/16
5. Khan, M.; Tripathi, R.; Kumar, A.; "A Malicious Attack and Defense Techniques on Android-Based Smartphone Platform", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume 8, Issue-8S3, June (2019)
6. Backdoor, https://www.malwarebytes.com/backdoor/, 2019/12/16
7. What is a computer worn, and how does it work, https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html, 2019/12/16
8. Adware, https://www.malwarebytes.com/adware/, 2019/12/16
9. Ransomware, https://www.malwarebytes.com/ransomware/, 2019/12/16
10. Rootkit: What is a Rootkit?, https://www.veracode.com/security/rootkit, 2019/12/16
11. What is a Botnet?, https://www.checkpoint.com/definitions/what-is-botnet/#, 2019/12/17

12. What is a Botnet", https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html, 2019/12/17
13. Štefanko, L.; "Android Banking Malware: Sophisticated trojans vs. Fake banking apps", ESET Malware Researcher, January (2019)
14. "Google Play Protect: Securing 2 billion users daily", "https://www.android.com/play-protect/", 2019/12/19
15. Protect against security threats with SafetyNet, https://developer.android.com/training/safetynet, 2019/12/19
16. Malware & Exploit Attacks Explained, https://newtecservices.com/malware-exploit-attacks-explained/, 2019/12/19
17. Fileless malware: Invisible threat or scaremongering hype, https://blog.emsisoft.com/en/29070/fileless-malware-attacks/, 2019/12/19
18. Limitations of Signature-Based Detection, https://bricata.com/blog/signature-detection-vs-network-behavior/, 2019/12/19
19. Sistema de Deteção de Intrusão – Artigo Revista infra Magazine 1, https://www.devmedia.com.br/sistema-de-deteccao-de-intrusao-artigo-revista-infra-magazine-1/20819, 2019/12/20
20. Sawle, P.; Gadicha, A.; Analysis of Malware Detection Techniques in Android, International Journal of Computer Science and Mobile Computing, Vol.3, Issue 3, March (2014)
21. Amro, B.; Malware Detection Techniques for Mobile Devices, International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol.7, No.4/5/6, December (2017)
22. Mohata, V.; Dakhane, D.; Pardhi, R.; Mobile Malware Detection Techniques, International Journal of Computer Science & Engineering Technology (IJCSET), Vol 4, April (2013)
23. Cherrier, S.; Doudane, Y.; Fault-Recovery and Coherence in Internet of Things Choreographies, International Journal of Information Technologies and Systems Approach, Vol 10, Issue 2, December (2017)
24. Rao, V.; Hande, K.; A Comparative study of static, dynamic and hybrid analysis techniques for android malware detection, International Journal of Engineering Development and Research, Volume 5, Issue 2, (2017)