**Android Malware Literature Review**

Arran Mcfadyen, Lee Cruickshank, Scott Postlethwaite,

Mateusz Szatanik, Chris Clark, Giovanni Paolini.

Abstract

The research was to expose the security features in the different android OS versions and how they would affect the malware program we are creating. The goal of this research is to gain a better insight into Androids security features, or lack thereof, furthermore, it was to recreate such a malware program to capture specific data without the hosts permission.

This article presents an in-depth literature review on this matter focused on Androids Malware manipulation. The different versions of Androids OS system play a part into re-creating and using this malware, such as different security feature, what they have fixed with updates, and what is still left open. ‘Cloak and Dagger’ and ‘Toast’ attacks are thoroughly looked into as they mimic what our malware is wanting to accomplish. To capture how the host uses the android device, how they hold the device, how they interact with the screen, etc, without the hosts knowing.

**Table of Contents**

[**Introduction 3**](#_gjdgxs)

[**Android OS 3**](#_30j0zll)

[History of Androids OS 3](#_1fob9te)

[Androids OS system impact on project 4](#_3znysh7)

[**Malware 4**](#_2et92p0)

[What is Malware? 4](#_tyjcwt)

[Why introduce malware into Mobile Devices? 5](#_3dy6vkm)

[Recent Malware 6](#_1t3h5sf)

[**Cloak and Dagger 6**](#_4d34og8)

[Overview of Cloak and Dagger malware 7](#_2s8eyo1)

[Androids Response to lack of security 7](#_17dp8vu)

[**Touch Analytics 7**](#_3rdcrjn)

[Problem with current verification system 7](#_26in1rg)

[Continuous Authentication 8](#_lnxbz9)

[**Conclusion 8**](#_35nkun2)

[**References 8**](#_1ksv4uv)

## Introduction

With the current android updates and the phones are increasing their storage which means people are more vulnerable to attacks as more information is being stored on their mobile devices which are vulnerable to malware attacks such as the “Toast Attack” and “Cloak and Dagger”. The research brought interesting facts in which it showed that in Android versions from Android 8(Oreo) and later the devices were vulnerable to those attacks until the later update in which new updates concentrated on stopping these malware attacks. With those attacks the hackers would be able to gain an invisible overlay in which they would see what the users are pressing, in this case this would allow them to see what passwords the users were using for their private information. In section 2, we look into the different type of OS systems that android run on their devices, we look at their differing security features, how robust they are, and how well they react to malware attacks. In section 3, we will be looking at the characteristics of what make up a malware, and how these malwares are getting into devices to infect. In section 4, we look at the malware attack that our program is based on, we explore their findings, and thus gave us a better insight into our own malware program. In section 5, we examine the data that we are hoping to capture with our malware, we observe their findings and make judgment on how we can implement that into our program, we also look at the deeper understanding of what this data could be used for, to get the device to solve if the host is the correct occupant of the device or not, by how they interact with the device.

## Android OS

### History of Androids OS

Throughout the research, the intentions were to find out how vulnerable Androids OS system is on there devices. Most of the attacks that happened to Androids OS system, were when they were running the early version of Android 8 (Oreo) and prior versions as well were attacked, a lot of work had been done to Androids OS systems, to give their users a better sense of security with their sensitive information. [1] This slowed down the process of information theft, but the hackers found other methods to go through Android's new OS system. The understanding we got from looking into this new updated version gave us a clear awareness that the Android market has become a safer place, in which the user should feel more secure and safe, while also disabling a lot of troubling sources. The security features that was implemented onto the Androids OS system, it only aloud ‘toast’ notifications to be displayed for 3.5 seconds, by this simple security feature, it has managed to stop users being lured into these malware attacks. [2]

For all the versions prior to Androids Oreo OS, the androids play store was riddled with malware programs, experts fear that this threat had led to over 36 million Android devices being breached and infected by just 41 apps found on their play store. [3] However, users can also be tricked into installing malware, that can set overlay images atop of other apps and elements of the device’s controls and settings. This type of malware could cause harm to the users device, for instance, it can insert an innocent picture/tag showing “continue installation” or a simple “OK” button can be set, and when pressing this button, you are instead giving this malicious app more privileges, or silently installing a rogue app.

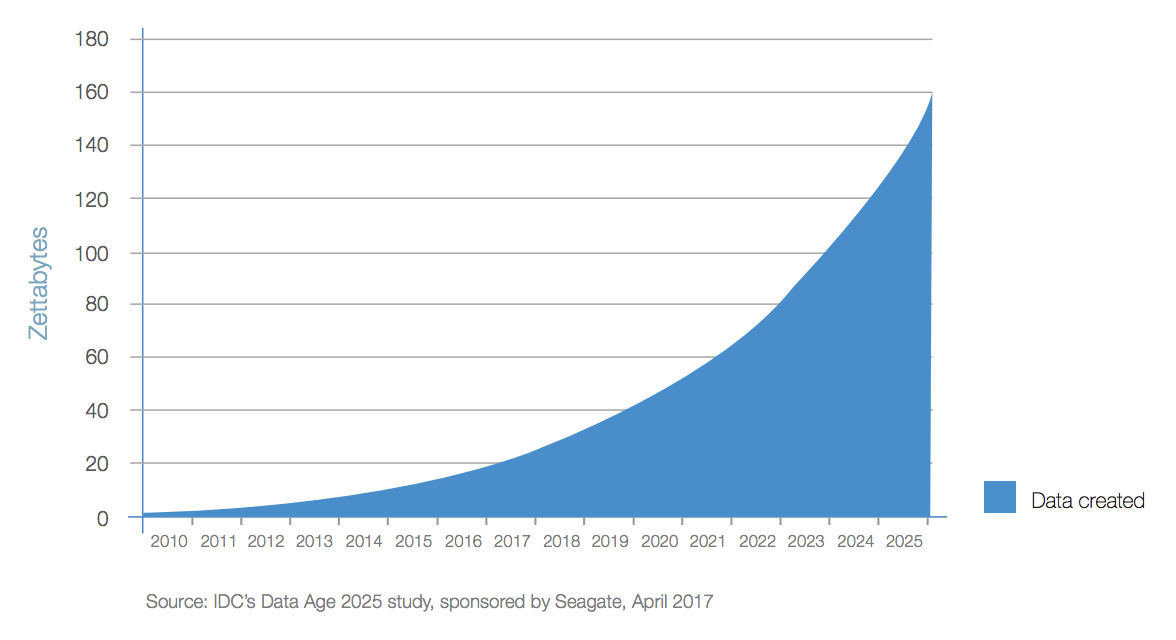
### Androids OS system impact on project

The project expected that our malware program is to capture valuable data from the user without their permission, this data is then observed to show similarities or differences on how people use their devices. With Android 8 at their early stage, people were still vulnerable to these malware attacks, but subsequently, with help from the Android market, the OS system Oreo was given a much more secure software system. The project was tested on Android 8, in which there are no proper security implementations to hinder our testing of our malware. The tests allowed us to gather valuable information, such as the users touch-input, the gyroscope of the device, etc, all this data is to then be place in a readable document in order to make it clear and simple to understand.

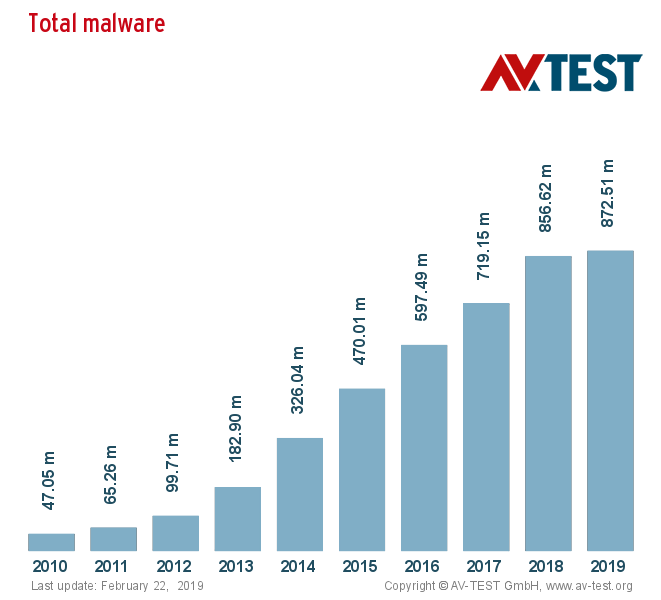
## Malware

### What is Malware?

Malware is a collective term used to describe software which has malicious intent. Malware can be ransomware, spyware, Trojan horses, worms and viruses. This kind of software is specifically designed by an attacker to complete specific malicious activities. The first serious piece of malware was found in 1982. This was a virus called Elk Cloner which was discovered on an Apple Mac 2, this malware spread through infected floppy discs. Over the year’s malware has adopted as our use for computing expanded. The amount of valuable data stored online has increased exponentially since the inception of computing. We now live in the era of “Big Data” as shown in (Figure 1) This new age in big data has also coincided with the rise of malware as shown in (Figure 2)



(Figure 1)

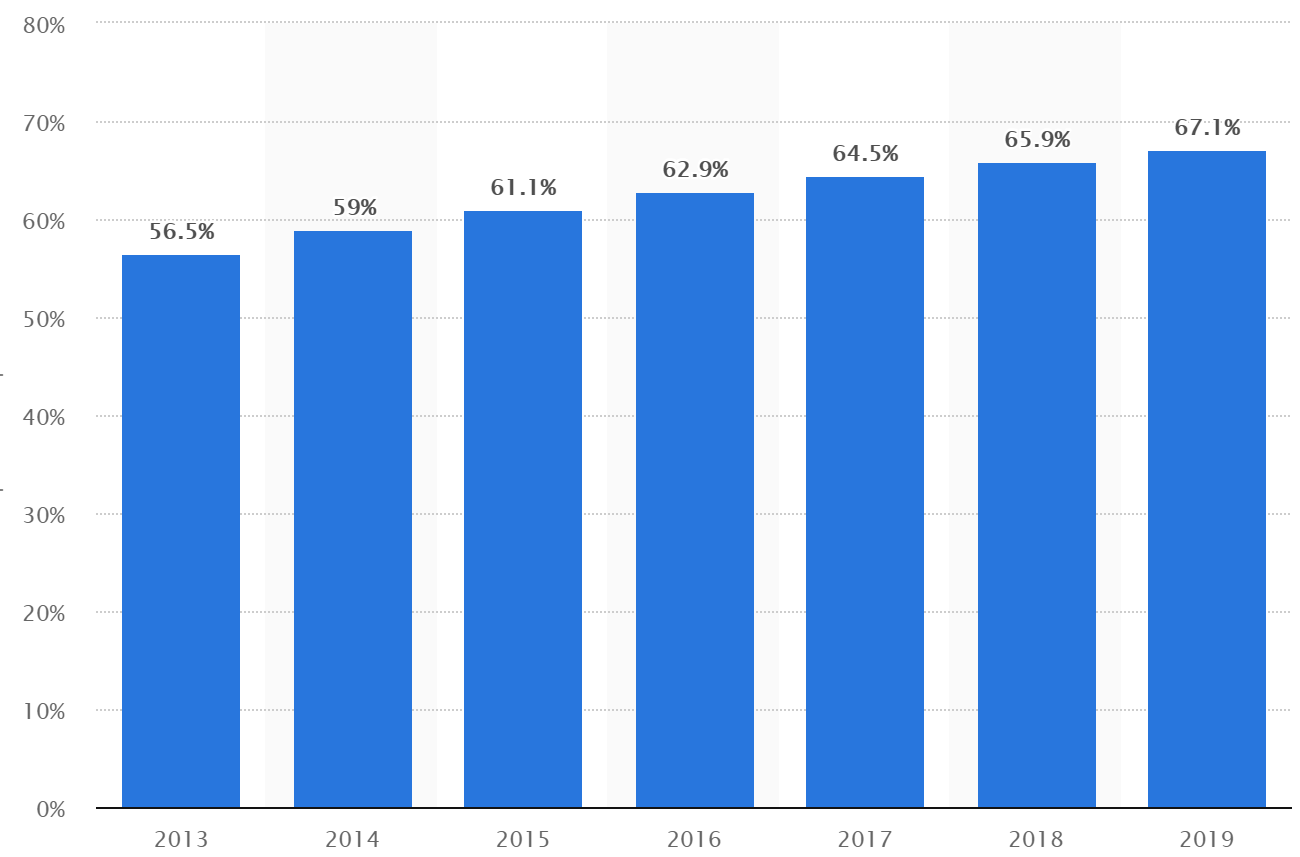


(Figure 2)

As we live in the digital age our online data has become our most valuable asset to companies & cybercriminals alike. Malware is designed to steal this data then profit from it.

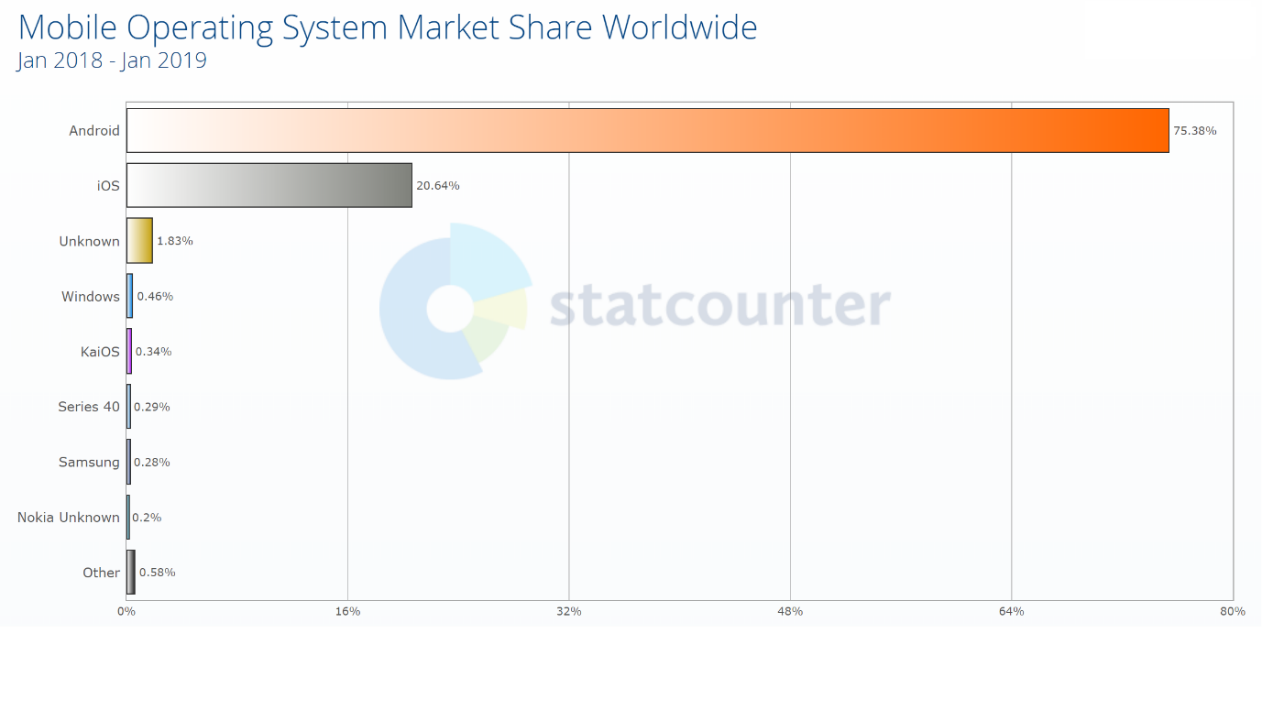
### Why introduce malware into Mobile Devices?

Since the inception of the mobile phone in 1973, they have become widely accessible, cheaper, faster and include more features. All these reasons have caused the adoption of mobile phones to increase exponentially with just under 70% of the world’s population owning a mobile phone as shown in (Figure 3)



(Figure 3)

With the invention of the smartphone in 1992 coupled with the rapid technological inventions since then, smartphones have grown to be very powerful machines. Most smartphones today are more than capable than some desktop computers. However; unlike desktop computers, mobile security hasn’t been at the forefront of people’s minds until very recently. The rise in smartphone adoption plus the big data society we live in today has caused mobile phone marked to become a hotbed for malware.



(Figure 4)

As shown above, in (Figure 4) Android & IOS operating systems account for most of the smartphone market share and as such have become the preferred platforms of choice for malware.

### Recent Malware

One of the most recent and significant form of attacks has been the cloak and dagger method CVE-2017-0752**.** This type of attack allows malicious code to completely take over a user’s device controlling the user interface. If downloaded from Google’s own play store the app requires no permissions to be accepted by the user, so the app could take over full control after being installed directly from a trusted source. This type of attack looks to exploit the SYSTEM\_ALERT\_WINDOW & BIND\_ACCESSIBILITY\_SERVICE functions. This attack allows for user input data such as keylogging, phishing, clickjacking. All android versions below Oreo (Android OS 8) are vulnerable. During testing of this application, the attackers found that none of the participants could tell their devices were compromised this makes it very dangerous. This attack was patched in Oreo when android implemented a 3.5 second timer onto the UI elements so they couldn’t run in the background indefinitely.

## Cloak and Dagger

In [4], Yanick Fratantonio sets out to show that some permissions on the android system, when used in combination with others, have the capacity to be very dangerous to end user’s privacy. Users who do not have proper grasp on how giving certain permissions to applications, without their knowledge, pose a great threat to the safety and security of there devices, ultimately leading to a sort of malicious attack.

### Overview of Cloak and Dagger malware

The research paper Cloak and Dagger: From two permissions to complete control of the UI feedback loop, was written specifically with the SYSTEM\_ALERT\_WINDOW and the BIND\_ACCESSIBILTY\_SERVICE permissions in mind, how with just these two permissions any application can take control of the UI feedback loop and create complex and stealthy attacks.

Throughout the paper, the author's intent was to demonstrate how an application, using these permissions, could launch a variety of attacks and successfully, and covertly, steal user’s login credentials, security pins, or even silently install an application that enabled all permissions without the user’s knowledge.

The practicality of the various attacks was tested via a user study. The 20 users that took place in the experiment were completely unaware that an attack had even been carried out on their devices. Further, the researchers also created a proof-of-concept application and found to get this malicious application on the official Play store, went through with ease, while still requiring these two permissions to be in use, SYSTEM\_ALERT\_WINDOW and BIND\_ACCESSIBILTY\_SERVICE.

### Androids Response to lack of security

The researchers disclosed their findings to google, however, as the vulnerabilities found were related to the core design of the OS system, the problems were left unaddressed, only to be resolved when the fixes were distributed through an over-the-air update. Finally, a defence was proposed that could be implemented as an extension to the current android API, which would safeguard developers and users from the potential threats that were uncovered over the course of the research. The defence recommended that whenever a user is interacting with an application that embeds a secure widget, no other application should be allowed to interfere with the user’s interaction with the device, by being able to create overlays on top of the screen. The OS system should take into account the effects of overlays, meaning that if there was an overlay present in the past few seconds, that no input from the user should be accepted, adding to that, that there should be on direct or indirect mechanisms in use, to leak information stored in secure widgets.

## Touch Analytics

In this day in age, when using a mobile device, we are met with inputting our passwords to gain access to our devices. However, this mundane task of repeatedly inputting your password, which may be a pin number, or gesture, to briefly use your mobile phone has started to make users lazy in having a secure pin or weak password, or even deactivate the unlock system. Mobile phones have a higher probability on being lost or stolen than that of a desktop computer.

### Problem with current verification system

Data was collected at the error rate of different types of verification systems that are being used on mobile phones to this day. One of the most common forms of this is the PIN number, where it only has between a 5% to 15%. When it comes to the task of face verification system, which is becoming increasingly used due to the fact that it’s easy to input, or lack thereof, the error rate increases to a staggering 28%, almost a third of times, the face recognition fails to register the users face, however the error rate of voice verification is 5% and signature verification 8%. Combining the voice & signature verification with the PIN based password, dramatically reduces the error rate down to 2%, however, it would be very troublesome for the user to input all three forms of verification to quickly and easily use their mobile device.

### Continuous Authentication

With the data we are hoping to collect from our malware program, this data can be used to create a sort of continuous authentication system for your mobile devices. In [5], the authors point out two forms of authentication systems, physiological and or behavioural biometrics, physiological relies on fingerprints, face recognition, hand geometry, or DNA. Behavioural biometrics look at how the mobile device is being used and handled, this is where the data we collect from our malware plays a part. We are continuously mapping and capturing keystrokes of the user, the gyroscope of the phone, so we can get a clearer understanding on the way the user holds the device.

## Conclusion

The purpose of this review was to help us gain a better insight as to what malware program we are creating. We looked at each aspect of the program and thoroughly researched each of these, with looking at what our program will be running, we were able to deduce what version would be most suitable to run it on, while also seeing the flaws, but also the strives, that androids OS system has. We carefully looked into what defines a malware, ad what affects it has had on the mobile device community, with looking at this we were able to understand how our program could affect these devices. Past papers were published that related a great deal to what we were creating, thanks to the generosity of the authors of the cloak and dagger paper, they answered our questions and gave us insight as to how they created their own program, from this, we could look at creating our malware from a different view, even implementing some of what they suggested. Furthermore, looking at how the data we captured can be used positively, to keep these devices more secure, giving us another way of feeling safe of our sensitive information, this helped us to understand why we were collecting this data, giving meaning to it, to also understand how we should present this data. Overall, all of the research we have done has affected and helped in creating our malware program.

## References

* G, M. (2019). *These Galaxy devices will be updated to Android 8.0 Oreo (updated: May 9)*. [online] SamMobile. Available at: <https://www.sammobile.com/samsung-galaxy-android-8-o-update>.
* Greenberg, A., Greenberg, A., Newman, L., Staff, W., Graff, G., Baker-Whitcomb, A., Graff, G. and Greenberg, A. (2019). *Patch Your Android Phone To Prevent an Evil ‘Toast’ Attack*. [online] WIRED. Available at: <https://www.wired.com/story/hack-brief-patch-your-android-phone-to-block-an-evil-toast-attack/>.
* Dassanayake, D. (2019). *Android WARNING: These Google Play Store apps steal YOUR pictures, are you affected?*. [online] Express.co.uk. Available at: <https://www.express.co.uk/life-style/science-technology/1081647/Android-warning-Google-Play-Store-apps-sinister-secret>.
* Dassanayake, D. (2019). *Android WARNING: These Google Play Store apps steal YOUR pictures, are you affected?*. [online] Express.co.uk. Available at: <https://www.express.co.uk/life-style/science-technology/1081647/Android-warning-Google-Play-Store-apps-sinister-secret>.
* Fratantonio, Y. (2017). *Cloak and Dagger: From two permissions to complete control of the UI feedback loop*.