

Malicious Applications on Android

By Abdisalan Mohamud

Mentor: Ming Chow

Abstract

Malicious applications on the android platform are ubiquitous and dangerous to many users. They can execute countless attacks that users never realize such as collect data through their camera, microphone, or even root their device. This paper seeks to explore how these malicious applications have come to be so popular, and how users can protect themselves from them.

Introduction

The android software environment has always been touted as an open platform where users have more control over their phones and application developers have more channels to circulate their apps, even allowing users to install them from a third party marketplaces. This, along with the affordable prices of android smartphones has enabled android to control almost 90% of the smartphone operating system marketplace in the first half of 2016 alone [1]. A platform so popular and open is convenient to users but also a ripe target for hackers.

The number malware applications reported on the android platform has been increasing at an alarming pace. In the Juniper Mobile Security Report of 2013, the number of mobile malware samples that were found from 2012 to 2013 jumped over 614%, where about 92% of those samples were targeting the android platform [2]. The malware comes in many different shapes depending on the vector of attack. If they want your bank account information or other login credentials, they can setup phishing screens that look very close the original product and masquerade as the real service recording your login credentials. This type of scam tricks even some of the most experienced security specialists.

Another vector is a type of malware called spyware. Spyware allows the malicious app to listen to the many different activities you perform on your phone such as making a call, sending text messages, and also track information like your exact GPS location and time spent in certain areas. And spyware can send all this data back to the developer without the knowledge of the user. Spyware can also be considered a bit of a grey area in “malicious activity” because many legitimate companies such as Facebook, Google, and Twitter collect that exact same information on users and more selling them to the highest bidding advertisers. Who’s to say that this “malicious app” isn’t just collecting the legally permissioned data for advertising purpose? Of

course many malicious applications are using this information to especially target users for criminal activities like find usernames and passwords to email and bank accounts.

Some malicious applications have no other desire than to attempt financial ruin on the user. These types of applications sign users up for premium SMS services which then have to be paid by the victim in their cell phone bill. There are many more vectors of attack using malicious applications, so it is becoming much harder for users to protect themselves. This paper seeks to contribute to the community by raising awareness on what permissions we give to our applications and how we can limit their powers.

To The Community

I choose this project because as mobile phones become more popular they will soon become a more popular hacking target than personal computers (though phones are slowly replacing those too). We need to have more users aware of the power they wield in protecting themselves and potentially their employer from hackers accessing their private information or sometimes even destroying your device.

This is important because there is currently too much trust in the system – the system of app approval in any marketplace of apps. If an application makes it to the Google Play Store, that does not guarantee that the app is safe to trust. Google has not released their process for reviewing applications published to the store, but we know that the process must be automated due to the sheer number of applications that are published per day. According to Statista, a site that collects statistical data on several industries and countries has shown that the number of apps on the Play store has grown exponentially – From December of 2009 to September of 2016, the number of applications on the Play Store has risen from a mere 16,000 to 2.4 million [3]. This

translates to about an average of 973 applications added to the store per day. In the automated application review process though, we would hope Google performs a static analysis on the application code for any violations of their terms because the average time for an application to be approved on the Play Store is usually less than a couple hours [4]. Who knows how many apps could fall through the cracks of their review system? The real answer may not be known but we can glimpse at it with recent discoveries made from independent researchers. In June of 2016, the Trend Labs Security Intelligence Blog posted about its discovery of “GODLESS” Malware found on the Play Store on several apps that allows the attacker to root the device without the user knowing and thus allowing remote commands to be executed on the device [5]. With more and more apps being published to the play store, the more potential there is for these malicious applications to fall through the cracks of Googles review system. This paper seeks to inform users more on how to protect themselves from applications like these that can be prevented with some preparation.

Defenses

There are many immediate actions one can take to defend themselves from malicious applications. These include, reviewing the applications you currently have installed, fine tuning the permissions on the applications you decided to trust, taking precautions to review the permissions of *every* application you install on your device, updating your android device to the latest operating system, and lastly authentically reviewing applications on the store. This is not a comprehensive list of actions one can take, but a starting point in which one can develop a distrust of all incoming applications no matter the source.

Reviewing the applications, you currently have installed can be done by going to the setting app, selecting Apps or Application Manager and then the app you want to update, and lastly tap Permissions to see a list of permissions the app currently holds. This alone is a great deterrent to all the spyware android applications out there.

As a part of the android community, and to further its prosperity from malicious attackers, users should make a more conscious effort to review applications asking for too many permissions or attempting to phish their information. If malicious applications are honestly reviewed and appropriately reported, then the moderators of the Play Store would be able to remove these apps much quicker, minimizing the damage done to the community.

Updating your android device can add significant improvements to the security of your device. Each major update carries with it patches to exploits that have accumulated over the years. Most hackers target the large body of android users that have not updated their OS because common exploits can still be performed. According to Juniper Mobile Threat Report, 77% of all android vulnerabilities and exploits can be defended against by having the latest version of android – currently only 4% have the latest version [2]. This can also be a controversial topic because not every android device is supported in the latest version. This leaves the question for the user: Pay for a new phone, or accept the security vulnerabilities of your current one? The answer is not easy, but if one decides to take the cheaper route, they should be more careful about the applications they install.

Conclusion

Malicious applications are still growing in number every year. Most of these apps are on android, because most people own android smartphone devices and users can install any

application no matter where it came from. These malicious applications can come from anywhere including the Google Play Store, so no source should be trusted without being vetted by other members of the community through strict reviewing. Malicious applications make it to the store because there are so many applications added that Google cannot manually review every one of them. This is a convenience for many developers who want to ship out updates to users within hours, but compromises by allowing malicious applications onto the market at a much larger volume. Users can defend themselves from these malicious applications by being more conscious about what reviews have come from the application, what permissions it asks for, as well as updating to the latest version of android.

Supplementary Material

In order to understand more about what a hacker can do when creating a malicious application, I decided to also attempt to create one. Creating one is relatively easy with free tools found in the Metasploit Penetration Test Software. Disclaimer: Using the penetration software to hack any hardware that you do not own is illegal and I do not condone those actions. The target device in my case was an amazon fire tablet, that was lent to me from my mentor Ming Chow. I used the Metasploit Penetration Test Software to create a payload that made a reverse TCP connection back to my computer if the user installs and runs the application. For the application to work, both the attacker and the victim had to be on the same network. Once the connection is made there was virtually nothing I couldn't do with the device. A short list of actions I could take were to record the microphone, take videos and photos, send and receive text messages, and more. All these actions were able to be executed without any notification of the device holder. This proved a scary outcome as I was terrified of how easily it was to create such an application.

That's not all though. I noticed that the application was called "Main Activity" and the icon was just a default android icon, so I decided to see if I could edit it to look more like a familiar app. After some research, I was able to find an open source tool called Apktool that reverse engineers android APK files [6]. With this tool, I was able to decompile the malicious app, and edit the application icon to be a copy of Flappy Bird, and the name to Flippy Bird (The apk for Flappy Bird was already on the device so I gave this one a different name). Lastly, I was able to recompile and sign the apk and it still performs the same exploit. The apk for Flippy Bird is included in the report.

Sources

[1] IDC - Smart Phone OS Market Share, 2016 Q2 from

<https://www.idc.com/prodserv/smartphone-os-market-share.jsp>

[2] "Juniper Networks Third Annual Mobile Threats Report" from

<http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2012-mobile-threats-report.pdf>

[3] "Number of available applications in the Google Play Store from December 2009 to September 2016" from <https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/>

[4] Claude SG (August 4, 2016) "App review times for Google Play, aka how fast will your app be published" from <http://www.androidb.com/2016/08/app-review-times-for-google-play-aka-how-fast-will-your-app-be-published/>

[5] Veo Zhang (June 21, 2016) "GODLESS Mobile Malware Uses Multiple Exploits to Root Devices" from <http://blog.trendmicro.com/trendlabs-security-intelligence/godless-mobile-malware-uses-multiple-exploits-root-devices/>

[6] "A tool for reverse engineering apk files" from <https://ibotpeaches.github.io/Apktool/>