ANDROID MALWARE

Mohammed Tarwala[1], Munwar Hussain Shelia[2], Nazmuddin Mavliwala[3], Shabana Tadvi[4]

[1]Student, Computer Engineering, MHSSCOE, Maharashtra, India
[2]Student, Computer Engineering, MHSSCOE, Maharashtra, India
[3]Student, Computer Engineering, MHSSCOE, Maharashtra, India
[4] Assistance Professor, Computer Engineering, MHSSCOE, Maharashtra, India

Abstract

Now a day's android devices are so common that they are used by everyone in the world. But with the commonness of the android OS and Android based devices there comes a threat to these android devices. This paper will implement some of the threats to the Android device and will also present their counter measures. First of all it will implement trivial malware attack on android device and android OS like message stealing and contact stealing, files stealing from SD card and also their solutions to prevent it. Secondly this project will perform more sophisticated attacks like whatsapp message stealing, using twitter as command and control in android devices and using Web Based Remote Exploration and Control System, denial of convenience attacks using fake access point, phishing attacks.

Keywords: *Android Malware, Mobile Malware, Flaws in android Security Model, Web based exploitation, Application phishing in android.*

---***---

1. INTRODUCTION

Android is everywhere Phones Tablets. TVs and set-top boxes powered by Google TV. Soon, Android will be in cars and all sort of other places as well. However, the general theme of Android devices will be smaller screens and/or no hardware keyboard. And, by the numbers, Android will probably be associated mostly with smart phones for the foreseeable future. For developers, this has both benefits and drawbacks, as described next. This chapter also describes the main components in an Android application and the Android features that you can exploit when developing your applications.

Android powers hundreds of millions of mobile devices in more than 190 countries around the world. It's the largest installed base of any mobile platform and is growing fast. Every day another million user's power up their Android devices for the first time and start looking for apps, games, and other digital content Android gives you everything you need to build best-in-class app experiences. It gives you a single application model that lets you deploy your apps broadly to hundreds of millions of users across a wide range of devices from phones to tablets and beyond.

People with mobile phones tend to get very irritated when those phones do not work. Similarly, those same people will get irritated if your program "breaks" their phones by

1. Tying up the CPU such that calls can't be received.
2. Not quietly fading into the background when a call comes in or needs to be placed, because the program doesn't work properly with the rest of the phone's operating system.
3. Crashing the phone's operating system, such as by leaking memory like a sieve.

As with increase in popularity of this platform it has become attractive target for the hackers. Attackers have shifted their interest to this platform because it not only gives access to victim's files and personal details but also gives information regarding victim's location. Attackers can intercept victim's phone calls and messages.

The purpose of undertaking this project is to understand the android framework and the framework's weakness and what type of attack could be done on this platform and also to secure it by proposing feasible and proper patches for the corresponding attacks thus making the system more secure and safe to use. Also this project could help the security organizations to identify the irrational activities and could take appropriate efforts to avoid them.

2. PROPOSED SYSTEM

As most of the spyware uses different types of command and control servers which can be easily traceable will be using the twitter as our command and control and also use public service like pastebin.com to upload file and response to command.

The features of android malware application can be briefly summarized as follows:

2.1 Command and Control Centre (C&C)

Once the mobile device is infected with the malware the next thing we are looking for is to control the device which is done from a control centre which uses a channel to communicate to the infected system. In this design twitter is used as channel for communication. Attacker will use a web based command panel which will tweet command using attackers twitter account, this will be the command to be executed on compromised phone on the other end i.e. infected phone will read the tweet from the attacker and follow the order. Tweet may include the configuration command which changes the configuration of the malware like replaying channel. The infected phone will communicate back using other twitter account, so both attacker and compromised phone are using different twitter account. All infected devices will be using same twitter account.

We will be using the Hash tag to send the commands from the web interface. The hash tag will be dynamically generated by our own algorithm for every single day.The algorithm consists of a string array which has the code for the numbers from one to ten.

hashGeneratingStr[]={"ps","dk","rn","dh","kw","su","ql","ox" ,"zr"};

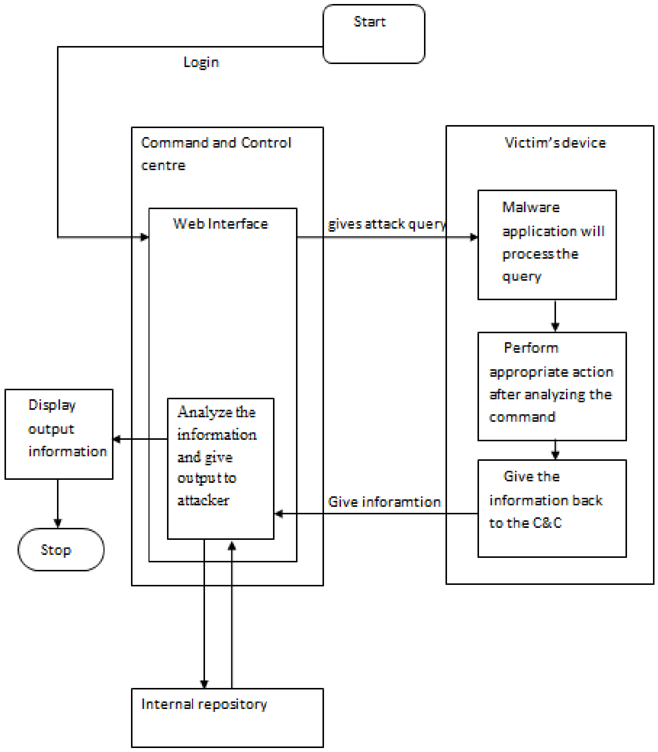
Start
Login
Command and Control centre
Web Interface
gives attack query
Victim's device
Malware application will process the query
Perform appropriate action after analyzing the command
Give the information back to the C&C
Give inforamtion
Analyze the information and give output to attacker
Display output information
Stop
Internal repository

Fig 1: Block diagram of android malware

So the hash tag will be generated as follows:

If today date is (01 – 03 – 2014)

0	ps
1	dk
0	ps
3	dh
2	rn
0	ps
1	dk
4	kw

Then the hash will be #psdkpsdhrnpsdkkw.

The command generated by web interface will include the hash tag along with the attack command to perform a specific attack on the victim phone.

Sample Command generated by the web interface #psdkpsdhrnpsdkkw sms-relay <attackers phone no> <victimsphone no>.

The following command consist of the hash tag as well as the attack name that is the sms relaying attack along with other attributes of the sms relaying attack. The following command will be twitted on the twitter account using the hash tag generated by the algorithm. Also the result file or snapshot will be twitted by the malware using the same algorithm. If the file is big in size it will be uploaded on pastebin.com.

2.2 Application Phishing

After receiving the attack command from the twitter command and control the malware will scan the foreground activity to see which application is running. After scanning the malware will use the phished application to activity to get the victims credentials and will upload it to the pastebin.com.

2.3 SMS Relaying

Attacker will send SMS to infected phone which will be relayed to other phone number, when the phone number will reply to compromised phone it will reply to the attacker this way attacker will remain stealth.

2.4 Stealing WhatsApp Chat:

After receiving the command from the attacker the malware in the device firstly gets the external storage rights to access the external storage. After getting the rights the malware access the Whatsapp message database stored in the external storage of the device. After accessing the database the malware then attaches the database file to the mail via a attach mail command and then sends it to the attacker via mail or it can simply upload it to the pastebin.com. The command and center will give the URL of the database to the attacker. The attacker can then decrypt the database file and see the content in it.

3. CONCLUSIONS

The Android OS can be improved further for: To use the same feature in an authenticated manner so this can be used for surveillance against perpetrator, thus preventing it to fall under wrong hands or person with malicious intent. This system can also be used to monitor the phone to prevent it to install cracked or pirated software thus preventing the piracy. User must be informed properly why particular permission is used (Android have a security permission model), proper justification has to be provided that why software needs to use certain feature of mobile device like for example why does it require phones GPS location.

REFERENCES

[1]. Mark Murphy and Apress, “Beginning android 3”.
[2]. Wei Meng Lee and Wrox, “Beginning Android tablet Application Development”.
[3]. James Steele and Nelson,”The android developer’s cookbook”
[4]. Md. Ashraful Alam Milton and Ainul Anam Shahjamal Khan, “Web Based Remote Exploration and Control System Using Android Mobile Phone”, IEEE/OSAIIAPR International Conference on Informatics, Electronics & Vision.
[5]. Earlence Fernandes and Bruno Crispo, “FM 99.9, Radio Virus: Exploiting FM Radio Broadcasts for Malware Deployment”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 6, JUNE 2013.
[6]. Dino A. Dai Zovi and Alexander Sotirov,” Mobile Attacks and Defense”
[7]. Marius Cristea and Bogdan Groza, “Fingerprinting Smartphones Remotely via ICMP Timestamps”, IEEE COMMUNICATIONS LETTERS, VOL. 17, NO. 6, JUNE 2013.
[8]. http://c0defreak.blogspot.in/2014/02/android-malware-detecting-emulator.html.

BIOGRAPHIES

Name: Mr. Mohammed Tarwala
Designation: Student
Department: Computer Engineering
Qualifications: B.E (comp)Pursuing

Name: Mr.Munwar Hussain Shelia
Designation: Student
Department: Computer Engineering
Qualifications: B.E (Comp)Pursuing

Name: Mr.Nazmuddin Mavliwala
Designation: Student
Department: Computer Engineering
Qualifications: B.E (Comp)Pursuing

Name: Mrs. Shabana Tadvi
Designation: Assistant Professor
Department: Computer Engineering
Qualifications: B. E. (Comp.) M. E. (Comp.), PhD. (Pursuing)