A Comparison Study of Remote Administration Tools

Alen James
Department Of Computer Application
Amal Jyothi College of Engineering
Kottayam, India
alenjames@mca.ajce.in

Paulin Paul
Asst. Prof. Department Of Computer Application
Amal Jyothi College of Engineering
Kottayam, India
paulinepaul@amaljyothi.ac.in

Abstract: **Remote Administration Tools are which has the ability to hack all the devices that have android. Also, these software has a simple user interface which makes any user to use this software with relative ease. In this paper, there is brief description and comparison about various RAT tools that are used for hacking android devices. In this will be discussing about the requirements needed for tools and what are the various features that are being provided by each tool. This process is done to find the best working remote administration tool.**

Keywords: **Android Phones, Payload, Port Forwarding.**

I. INTRODUCTION

A Remote Administration Tool (RAT) allows its user to perform many activities on the compromised device (e.g. control a device's camera, access its storage, intercept calls and text messages, etc.). This is all done via an easyto-use application hosted on a command and manipulated server. These RAT can gives the user access to the victim's system, just as if they had physical access to your device. With this access, the person can access your files, use your camera, and even turn on/off your device.

These tools are written in android and Java. The apk which we give to the victim helps to hack the device. In these tool there is an option to bind the payload apk with another apk where the payload can be hidden within that apk. After the installation the apk we can see the device using the java interface given in the tool. These tools can be used for taking your sensitive data and also can access the phone in real time that is they can track your calls, make calls, take messages from your phone eg:otp's from your phone, can sent messages etc..

Requirements:

- Java Installed PC
- RAT tool
- Dynamic IP
- Dynamic Update Client(such as No-IP)
- Victim

I. STEPS

Before you can use the tool there are some materials that are needed, as follows.

- Java must be installed on the computer.
- Router Port forwarder.
- Antivirus and firewall must be turned off.
- A computer desktop/laptop.
- An Android phone to deploy the client app.
- A wireless router.
- Fast internet connection

II. LITERATURE REVIEW

Saba Arshad at el [1] Android has surpassed iOS as the most widely used smartphone operating system. When compared to past years, the quick growth of Android has resulted in a huge increase in the number of infections. There are numerous antimalware and antivirus apps available that are meant to protect users' sensitive data on mobile phones from such attacks. There is a two-fold contribution. To begin, examine Android malware and the penetration techniques used to target systems, as well as antivirus products that protect Android devices from malware. Many of the most modern antimalware techniques can be classified based on how they detect malware. The goal is to provide a clear and comprehensive overview of malware detection and prevention systems, as well as to assess their pros and drawbacks. Second, we've predicted Android market trends for the year ahead, and we've developed a unique hybrid security solution that takes into consideration both static and dynamic analysis of an Android app.

Taenam Cho at el [2] Smart phones are more than just phones; they are also portable computers that provide a variety of services such as calls, texts, emails, GPS, camera, Wi-Fi, and Bluetooth apps. These apps store and handle a variety of internal information as well as sensitive information like address books. Through 3G, 4G, and Wi-Fi, smart phones allow for quick and easy data transfer. As a result, personal data kept on smart phones is subject to leakage. Content Providers, which are used by Android to transfer data between apps, are

DOI: 10.5281/zenodo.5091367
ISBN:978-93-5426-386-6@2021 *MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam*

particularly vulnerable to unauthorized data leaking. The current research examines the vulnerabilities of Content Providers and uses a rogue software to demonstrate the risks involved.

G. Delac at el [3] The adoption of mobile devices with an ever technological features has reintroduced the issue of mobile device security. Because of considerable advancements in both hardware and operating systems, mobile devices are quickly becoming desirable targets for malicious cyberattacks. Modern mobile platforms, such as Android, iOS, and Symbian, are becoming more and more like conventional PC operating systems. As a result, the issues of maintaining smart-phone security are beginning to resemble those of PC platforms. By downloading harmful contents, smart phones might become infected with worms, Trojan horses, and other virus families, compromising the security and privacy of users and even obtaining the entire control of the device. Because of developments in mobile network technologies, such malicious content can quickly propagate thanks to intelligence, ability to maintain a persistent Internet connection across 3G or Wi-Fi networks. Moreover, the advancements in smart phone features have led to the rise of new forms of security risks. Malicious programmes can gain access to voice-recording devices, cameras, intercept SMS messages, and obtain location information via compromising the mobile OS. Users' privacy is significantly threatened as a result of such security breaches. In this article, we examine current mobile platform risks and provide an in-depth look at threat mitigation techniques incorporated into current mobile operating systems.

Vikas Bhaskar Vooradi at el [4] Nowadays, every piece of information is priceless. The situation of security is terrible as a result of the widespread usage of the Internet. Hacking is a procedure in which a person attempts to exploit security flaws for personal gain or enjoyment. Some of them steal data for personal gain, while others ruin the identity of a legitimate company or business in order to gain market share. This paper briefly discusses ethical hacking, forms of hacking, preventive methods, and other facets of the subject.

III. PROPOSED TOOLS

- AndroRAT
- Spymax
- Spynote
- DroidJack

A. AndroRAT

AndroRAT is a well-known android RAT which has the ability to hack all the devices which have android. Also, this software has a simple user interface which makes any user to use this software with relative ease. Client's mobile device can be monitored using this tool. AndroRAT is a client/server application which is developed using the basic java android for the client side and in java/swing for the server. In this tool a bind and build option is there which enables the user to inject payload to an existing app.
Features provided are can access and get contacts, call logs, messages. And also can track calls, make calls, send messages, access to camera and mic, get the location of user but it is not exact, and can get all details related to the victims mobile. Also user can toast messages to the victims mobile.

B. Spymax

It's the most superior and advanced version of SpyNote. SpyMax is a best android RAT (Remote Administration Tool). SpyMax is used to exploits Android smart phones and Get complete faraway control of the device. It provides a user-friendly Interface and make easier to work the environment by building yourself a customized apk for injecting payload. Its Server is written in Java, and the Client controller is written in Visual Basic .NET.
Features provided are can access and get contacts, call logs, messages. And also can track calls, make calls, send messages, access to camera and mic, get the location exactly, and can get all details related to the victims mobile. Also user can toast messages to the victims mobile. Moreover in this we live record camera in back or front mode. Can access to the files in the phone and also check the browse history

C. SpyNote

SpyNote is an android remote administration tool that allows a person to control another person's smartphone remotely. Using this software you can monitor the client's deivce all activities. SpyNote is precise as it does not need root access to the device in order to obtain these capabilities. SpyNote version 2 allows users to build their own application that can be used to communicate with C2 servers configured during the building process.

Features provided are can access and get contacts, call logs, messages. And also can track calls, make calls, send messages, access to camera and mic, get the location of user but it is not exact, and can get all details related to the victims mobile. Also user can toast messages to the victims mobile. Can access to the files in the phone.

D. Droidjack

DroidJack is an android RAT which offers you the power to set up and manipulate over your victim's Android devices with a smooth to apply GUI and all

DOI: 10.5281/zenodo.5091367
ISBN:978-93-5426-386-6@2021 *MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam*

the functions you need to monitor them. Features provided are can access and get contacts, call logs, messages. And also can track calls, make calls, send messages, access to camera and mic, get the exact location, and can get all details related to the victims mobile. Also user can toast messages to the victims mobile. Moreover in this we live record camera in back or front mode. Can access to the files in the phone and also check the browse history. In this tool it is also possible to take data from whatsapp.

IV. METHODOLOGY

In this project the aim is to recognize the best remote administration tool available from the above tools. For this we are installing the payload created from each of the tool into four different phones containing different android versions such as from lollipop to Nougat. The payload created from each tool is being installed to these four different mobile devices and the result is taken.

V. RESULT

As it mentioned there were different remote administartion tools from those droidjack and spymax are good for doing hacking since it supports on latest versions and also all the features which are given will work properly. Whereas in the other two spynote supports on older versions but doesn't work on new versions. In case of androRat many features doesn't work properly and also also supports on older versions.

Features	AndroRAT	Spymax	Spynote	DroidJack
Versions supported	Lolipop	Upto Nougat	Lolipop	Upto Mashmellow
Call, call logs and contacts	yes	yes	yes	yes
File manager	yes	yes	yes	yes
Send and read message	yes	yes	yes	yes
Toast message	yes	yes	yes	yes
Browser history	no	yes	no	yes
Location info	not accurate	Accurate	Less Accurate	Accurate
Camera access	yes	With live record	yes	With live record
Mic	Can talk	Can talk and record	Can talk	Can talk and record
Processing speed	slow	fastest	slow	fast

VI. CONCLUSION

Considering on the above project we have taken the result on installing the tools on different versions of android. According to it the best tools are droidjack and spymax where these two tools are giving us more performance and also all features are being working on these two.

RAT tools can be used for both good and bad intentions. This depends on the intention of user. For protecting our phone from bad people just keep play protect turned on and only download apps from trusted stores. "Users should refrain from downloading apps from third-party app stores to avoid being targeted by threats like AndroRAT," Trend Micro researchers warned.

VII. REFERENCES

[1] Saba Arshad, Abid Khan, Munam Ali Shah, Mansoor Ahmed "Android Malware Detection & Protection: A Survey"

[2] Taenam-Cho; Jae-Hyeong-Kim; Hyeok-Ju Cho ;Seung-Hyun-Seo ;Seungjoo-Kim"Vulnerabilities of android data sharing and malicious application to leaking private information"

[3] Goran Delac ; Marin silic "Emerging security threats for mobile platforms"

[4] Vikas Bhaskar Vooradi ; Lavina Jadhav "Ethical Hacking Techniques and its Preventive Measures for Newbies "

DOI: 10.5281/zenodo.5091367
ISBN:978-93-5426-386-6@2021 *MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam*