AndroRAT – a Simple Walkthough

Georgin John George and Sona Maria Sebastian

June 3, 2020

ANDRORAT – A SIMPLE WALKTHOUGH

[1]Georgin John George, [2]Sona Maria Sebastian

[1] PG Scholar of Amal Jyothi College Of Engineering, Kanjirappally, Kerala

[2] Asst. Professor of Amal Jyothi College Of Engineering, Kanjirappally, Kerala

[1] georginjohngeorge@mca.ajce.in, [2] sonasebastian@amaljyothi.ac.in

Abstract: In this journal paper, you can find a brief description about AndroRAT tool and its working, AndroRAT is one of the well known android RAT (Remote Administration Tool). AndroRAT can be used to exploits android smart phones and get complete remote control of the android device It is a simple graphical user interface and can create payloads with an existing apk file or build a customized apk for injecting payload.In AndroRAT was introduced in the year 2016.

Keywords: AndroRAT, Android Phones, payload.

I. INTRODUCTION

AndroRAT is a well known android RAT which has the ability to hack all the devices that have android. also, this software has a simple user interface which makes any user to use this software with relative ease. Moreover, using AndroRAT you can live stream front or main camera. This software makes penetrating android devices looks like child's play. Using AndroRAT you can crack even the latest version of android i.e, android pie.Using this software you can monitor the client mobile's all activities. 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.

The malware, dubbed AndroRAT, was first discovered in 2012.The malware was originally a university project meant to be an open-source application that provided remote control of an Android system. However, AndroRAT was eventually also discovered by cyber criminals, which in turn launched its malicious journey.According to security researchers at Trend Micro, who discovered the new version of the malware, it targets a vulnerability that was publicly disclosed in 2016. Exploiting the flaw allows hackers to hijack older Android devices, allowing them access to an extensive amount of data stored in the infected devices. Although Google already patched the vulnerability, older Android devices may still be vulnerable.

FEATURES

Bind APK Tool: Bind your server APK with any other Game or App. Encrypt APK using AES/DES/TDES/Blowfish algorithms. Rename APK package name. Remove unwanted features and permissions from APK.

File Manager: Explore files.Download file/folder. Delete files .Upload file/folder and Create folder

SMS Manager: Delete SMS, Read conversations. Write SMS and Send SMS.

Call Manager: Read call logs, Delete call logs, Make calls and Record call conversation.

Contacts Browser: Read contacts, Write contacts. Delete contacts and Add contacts.

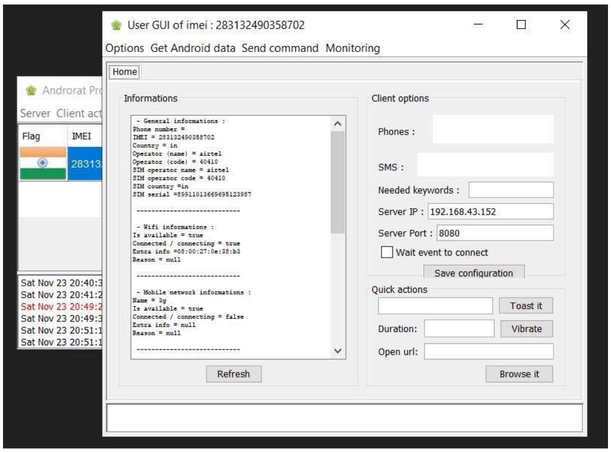
Remote Eyes: Take picture from front/back camera and Record video from front/back camera.

Remote Ears: Listen to mic lively, Record mic.

GPS Locator: Gets the last check in GPS location of the device, and shows it in Google maps.

Message Toaster: Toast a flash message on the device.

App Manager: Read installed apps, Open app Get currently running app, Detailed Info, Get IMEI number, Get WiFi Mac Address. Get Cellphone Carrier. Check whether device is rooted.



```
 - General informations :
Phone number =
IMEI = 283132490358702
Country = in
Operator (name) = airtel
Operator (code) = 40410
SIM operator name = airtel
SIM operator code = 40410
SIM country =in
SIM serial =89911013669695123987

 ----------------------------

 - Wifi informations :
Is available = true
Connected / connecting = true
Extra info =08:00:27:0e:38:b3
Reason = null

 ----------------------------

 - Mobile network informations :
Name = 3g
Is available = true
Connected / connecting = false
Extra info = null
Reason = null

 ----------------------------
```

Server IP : 192.168.43.152

Server Port : 8080

□ Wait event to connect

```
Sat Nov 23 20:40:3
Sat Nov 23 20:41:2
Sat Nov 23 20:49:2
Sat Nov 23 20:49:3
Sat Nov 23 20:51:1
Sat Nov 23 20:51:1
```

II. LITERATURE REVIEW

Praful Meshram at el [1] Smart phones are also portable computers as they provide many services needed in our day to day lives such as texts, calls, camera, Bluetooth, GPS and various other applications. Due to the attractive features of android smart phones, it‟s use is increasing tremendously. With the growing popularity of Android and it being one of the best players in mobile industry, knowing the best practices for its security becomes very crucial. Android is known as a platform that lends itself to hacking. Smart phones are prone to data leakage as they can easily exchange data over the Internet. Applications are made of four components namely Activity, Service, Broadcast receivers, and Content provider. This paper proposes the various threats and security risks Activity, Broadcast Receivers and Content Providers pose and how they can be responsible for sensitive data leakage without the user‟s knowledge. It also states the various attacks and the prevention mechanism and focuses on the prevention mechanism known as YASSE. This paper also states various other methods and technologies that are implemented for cloud based security that not only enhances the safety of the devices, but also reduces the system load of the devices.

Buthaina Mohammed AL-Zadjali at el [2]

The Android platform is an open source operating system, which is widely used on Smart phones. Android operating system usage and adaptation is rapidly increasing with a variety of applications. It also, allows developers to freely access and modifies source code. The open nature of the Android platform attracts attackers to do different types of criminal activities. The android users likely to install and download many applications which can be contain malicious code written by software hackers. The purpose of this paper is to explore the most significant security threats and vulnerabilities in the Android Operating System.

G. Delac at el [3] The proliferation of smart-phone devices, with ever advancing technological features, has brought the issue of mobile device security back into focus. Mobile devices are rapidly becoming attractive targets for malicious attacks due to significant advances in both hardware and operating systems. The modern mobile platforms, like Android, IOS and Symbian, increasingly resemble traditional operating systems for PCs. Therefore, the challenges in enforcing smart-phone security are becoming similar to those present in PC platforms. By installing malicious content, smart phones can be infected with worms, Trojan horses or other virus families, which can compromise user's security and privacy or even gain complete control over the device. Such malicious content can easily spread due to advances in mobile network technologies which provide smart-phones with capability of constant Internet connection over 3G or Wi-Fi networks. Additionally, the improvements in smart phone features introduce new types of security concerns. By compromising mobile OS, malicious applications can access voice-recording devices, cameras, intercept SMS messages or gain location information. Such security breaches severely compromise user's privacy. In this paper we present an analysis of contemporary mobile platform threats and give an in-depth overview of threat mitigation mechanisms built into state of the art mobile operating systems.

Kwame Ofosuhene Peasah at el [4] The intent of deletion, factory resetting as well as flashing of user's mobile device is to conceal sensitive data or information from a third party or anonymous user. However, if the application of these commonly used data wiping methodologies fails to achieve their intent, then the user may appear to be “naked” or vulnerable (susceptible to possible electronic related crime attack). Considering the Android OS design flaws in data erasure, and subsequent abundance and dominance of Android smart phones in recent years, the study assessed users' awareness and knowledge about Android smart phones security in Ghana. Adopting the cross-sectional design and simple random sampling technique, 1240 respondents aged 18 years and above were sampled for the study. Result indicates that majority of the study participants had previously owned an Android smart phone and were either keeping it or gave it out. Photos, videos, audios, office documents, notes and contacts were considered private data yet email, financial transactions, and health, academic and social information were information frequently accessed. Using the binary logic model, respondents' gender and age predicted their knowledge and awareness, respectively, on data encryption and data recovery. The vulnerability level of respondents to malicious attacks was rated as high and as such, the study recommends the need for awareness campaign among Smart phone users so as to reduce their tendencies to cyber crime and malicious attacks in the event of theft, misplaced and/or damaged phone

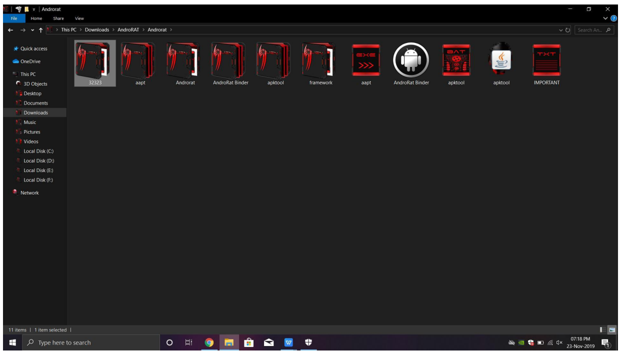
Taenam Cho at el [5] Smart phones are not just phones but also portable computers, providing diverse services needed in life including calls, texts, emails, GPS, camera, Wi-Fi and Bluetooth apps. These apps keep and manage diverse intrinsic data as well as sensitive private information such as address books. Smart phones enable swift and easy data exchange via 3G, 4G and Wi-Fi. Thus, personal information stored on Smart phones is prone to leakage. Particularly, Content Providers provided by Android to share data between apps are susceptible to illegitimate leakage of data. The present study analyzes the vulnerabilities of Content Providers and implements a malicious app to implicate risks related.

Karthik S at el [6] Android operating system uses the permission-based model which allows Android applications to access user information, system information, device information and external resources of Smart phone. The developer needs to declare the permissions for the Android application. The user needs to accept these permissions for successful installation of an Android application. These permissions are declarations. At the time of installation, if the permissions are allowed by the user, the app can access resources and information anytime. It need not request for permissions again. Android OS is susceptible to various security attacks due to its weakness in security. Android is most widely used mobile operating system. Improvising the security of an Android OS is very important to safeguard the user's privacy and confidential information. In this study, it was shown how to avoid misusing app permissions.

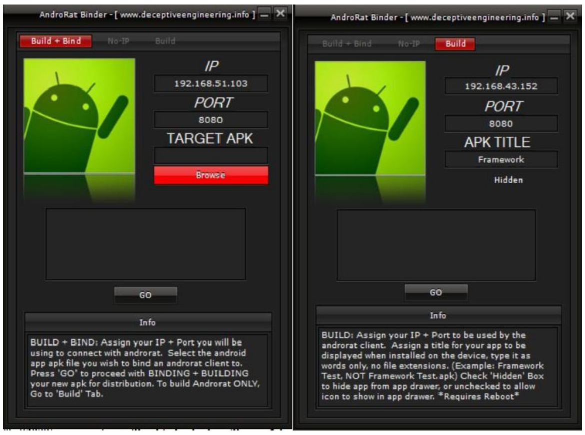
III. PROBLEM DEFINITION

Firstly, You need to download Java on your computer preferentially java version 8.0 works best. If you don't have Java installed in your system since java is one of the dependencies for AndroRAT.

First of all open AndroRAT Binder file. Its the application file that's in the picture below.



Now, you can see this type of interface.There you can find Build+Bind and build options you may select the one you prefer.Insert **your port number(recommend 8080)** in the field of port and **Host IP(if you don't know your IP address run ipconfig in command prompt)** address and click go if you prefer build option.


AndroRat Binder - [www.deceptiveengineering.info]
Build + Bind
No-IP
Build
Browse
GO
Info
AndroRat Binder - [www.deceptiveengineering.info]
Build + Bind
No-IP
Build
GO
Info

IP
192.168.51.103
PORT
8080
TARGET APK

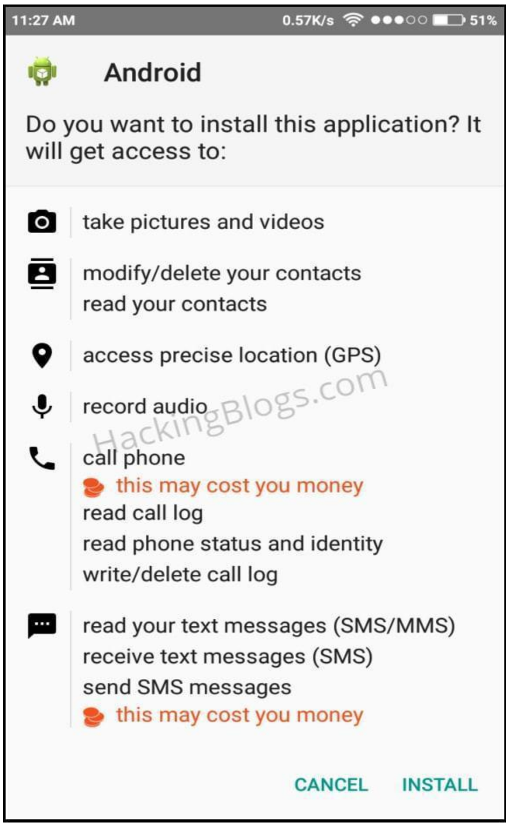
BUILD + BIND: Assign your IP + Port you will be using to connect with androrat. Select the android app apk file you wish to bind an androrat client to. Press 'GO' to proceed with BINDING + BUILDING your new apk for distribution. To build Androrat ONLY, Go to 'Build' Tab.

IP
192.168.43.152
PORT
8080
APK TITLE
Framework
Hidden

BUILD: Assign your IP + Port to be used by the androrat client. Assign a title for your app to be displayed when installed on the device, type it as words only, no file extensions. (Example: Framework Test, NOT Framework Test.apk) Check 'Hidden' Box to hide app from app drawer, or unchecked to allow icon to show in app drawer. *Requires Reboot*

The other option **Build+Bind** can be used if you want to Bind your Apk file to another Apk file then just type that Apk file path here and click on Bind it will bind both files. Otherwise, **click on go**.

That's it You created your payload apk file. The payload Apk file is present in the same folder where you find this software. The of the file will be the one you provided while creating payload Now, just send this file to the victim's device by doing social engineering. and Install this file on the victim's Device.



11:27 AM 0.57K/s 51%

Android

Do you want to install this application? It will get access to:

take pictures and videos

modify/delete your contacts
read your contacts

access precise location (GPS)

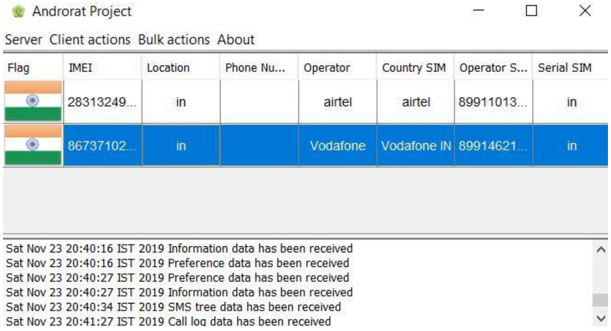
record audio

call phone
this may cost you money
read call log
read phone status and identity
write/delete call log

read your text messages (SMS/MMS)
receive text messages (SMS)
send SMS messages
this may cost you money

After Successfully Installing application when victim's click this button option then you will successfully get your victim's session on your system

Now, Click **Device** option in the tool and you can see where you got the victim's device



Androrat Project

Flag	IMEI	Location	Phone Nu...	Operator	Country SIM	Operator S...	Serial SIM
🇮🇳	28313249...	in		airtel	airtel	89911013...	in
🇮🇳	86737102...	in		Vodafone	Vodafone IN	89914621...	in

```
Sat Nov 23 20:40:16 IST 2019 Information data has been received
Sat Nov 23 20:40:16 IST 2019 Preference data has been received
Sat Nov 23 20:40:27 IST 2019 Preference data has been received
Sat Nov 23 20:40:27 IST 2019 Information data has been received
Sat Nov 23 20:40:34 IST 2019 SMS tree data has been received
Sat Nov 23 20:41:27 IST 2019 Call log data has been received
```

Just Right Click on the device and then you will see there is a lot of options is present which you can use.

Advantages & Disadvantages

Advantages:

- Open Source
- Simple and easy to use
- Router Port Forwarder - To mask our IP

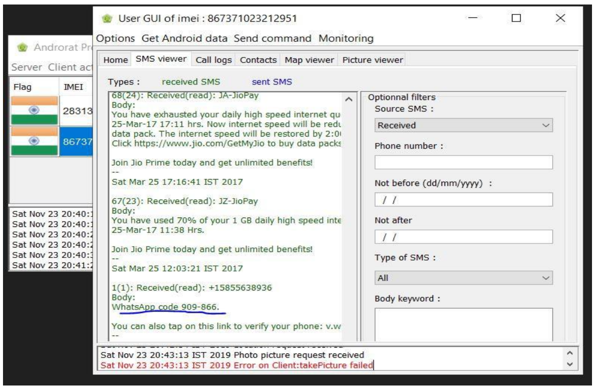
Disadvantages

- Used only in Android Phone.
- Devices should be in same network.
- Java Platform is required to run AndroRAT jar file.

IV. IMPLIMENTATION

Using manage SMS option, retrieve all messages in the device . In this retrieved data important information like OTP, username , password etc are contained. Using this OPT password the attacker can easily bankrupt the victim if attacker feels like it.

Retrieved message details



User GUI of imei : 867371023212951

Options Get Android data Send command Monitoring
Home SMS viewer Call logs Contacts Map viewer Picture viewer
Androrat Pr
Server Client ac
Flag IMEI
28313
86737

Types : received SMS sent SMS

```
68(24): Received(read): JA-JioPay
Body:
You have exhausted your daily high speed internet qu
25-Mar-17 17:11 hrs. Now internet speed will be redu
data pack. The internet speed will be restored by 2:0
Click https://www.jio.com/GetMyJio to buy data packs

Join Jio Prime today and get unlimited benefits!
--
Sat Mar 25 17:16:41 IST 2017

67(23): Received(read): JZ-JioPay
Body:
You have used 70% of your 1 GB daily high speed inte
25-Mar-17 11:38 Hrs.

Join Jio Prime today and get unlimited benefits!
--
Sat Mar 25 12:03:21 IST 2017

1(1): Received(read): +15855638936
Body:
WhatsApp code 909-866.

You can also tap on this link to verify your phone: v.w
--
```

Optionnal filters
Source SMS : Received
Phone number :
Not before (dd/mm/yyyy) : / /
Not after / /
Type of SMS : All
Body keyword :

```
Sat Nov 23 20:40:1
Sat Nov 23 20:40:1
Sat Nov 23 20:40:2
Sat Nov 23 20:40:2
Sat Nov 23 20:40:3
Sat Nov 23 20:41:2
```

```
Sat Nov 23 20:43:13 IST 2019 Photo picture request received
Sat Nov 23 20:43:13 IST 2019 Error on Client:takePicture failed
```

The one shown in the above picture is whatsapp's OTP code to authorize your phone number. This is just one of the many options like vise we can get all the OPT related content and an attacker can exploit the client all they want.

V. RESULT

You are authorized as the original phone user and can exploit the clients whatsapp all you want .

VI. CONCLUSION

AndroRAT is a remote administration tool, with a good spread of features and modules for nearly any type of penetration test.. It does not use metasploit framework for penetration. Android device have given a lot of power to its user. Whether you can have smart phone or a tablet, you can perform immense number of activities on it.

“Users should refrain from downloading apps from third-party app stores to avoid being targeted by threats like AndroRAT," Trend Micro researchers warned. "Downloading only from legitimate app stores can go a long way when it comes to device security. Regularly updating your device's operating system and apps also reduce the risk of being affected by exploits for new vulnerabilities.”

The AndroRAT was originally a university project for study purpose and so This walk-through is for study purpose as well.

VII. REFERENCES

https://www.ibtimes.co.uk/

https://hackingblogs.com/

https://www.apkmart.net/app/androrat/

https://www.youtube.com/watch?v=AALrtcqbsEI&t=204s