INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

REVIEW ON ANDROID REMOTE ADMINISTRATION TOOL (ANDROID RAT)

AMIT DESHMUKH[1], DR. H. R. DESHMUKH[2]

1. Department of Computer Science & Engineering, IBSS COE Amravati (MH) India.
2. Department of Computer Science & Engineering, IBSS COE Amravati (MH) India.

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: Android being the most used Mobile operating system and having the number of users in the world lead to evolve monitoring/administering tool. Android remote administration tool (RAT) is a piece of software that allows a remote "operator" to control a system as if he has physical access to that system. While mobile sharing and remote admin have many legal uses, "RAT" software is usually associated with criminal or malicious activity. Malicious R.A.T software is typically installed without the victim's knowledge, often as payload of a Trojan horse, and will try to hide its operation from the victim and from security software. The goal of the app is to give the control over android system remotely and retrieve information from it. This paper provides the information regarding building and using Android RAT.

Keywords: RAT, APK-Binder, Trojan, TCP, IP, UDP, AndroRAT

Corresponding Author: MR. AMIT DESHMUKH

Access Online On:

www.ijpret.com

How to Cite This Article:

Amit Deshmukh, IJPRET, 2015; Volume 3 (9): 463-468

PAPER-QR CODE

INTRODUCTION

AndroRAT is an open-source tool that was created and published on the Internet in November 2012, it's RAT for Android OS and exactly as any other RAT, it allow remote attacker to control the victim. Usually the RAT have a user friendly control panel that makes possible the control of victims, in the same way AndroRAT can control, make phone calls and send SMS messages of infected devices, it is also able to get its GPS coordinates, access to files stored on the handset and activate and use the microphone and camera. The fact that Android OS has increased its popularity has had as consequences an increase of malicious code developed for the Google's platform, *"The RAT comes in the form of an APK which is application format for Android. When used in conjunction with the AndroRAT APK binder easily allows an attacker with limited expertise to automate the process of infecting any legitimate Android application with AndroRAT, thus Trojanizing the app. When the Trojanized of the legitimate app is installed on the device, the user unsuspectingly i*nstalls *AndroRAT alongside the legitimate app they intended to install. This allows the attacker to circumvent elements of the Android* security m*odel through deception. To* date*, Symantec has counted 23 cases of popular legitimate apps being Trojanized in the wild with AndroRAT." Symantec report* Android Rat allows users to send remote commands to their Android devices through any web browser. Android Rat can be used for a variety of purposes, such as remote administration and control of your own devices or as a child monitoring tool. Android Rat works internationally on any carrier and only requires an internet connection through either Wi-Fi or a 3G/4G data connection. Android Rat works completely in the background. Even when sent commands from your the Control Centre (where you control and monitor your devices), no popup messages or notifications are generated by the mobile application (unless you use the "send notification" function). No logs are stored on the device of any commands sent to it, which leaves little chance of a user identifying the

software if you are using it for monitoring purposes. In short, Androrat is a mix of Android and RAT (Remote Access Tool). Androrat is a client/server application developed in Java Android for the client side and in Java/Swing for the Server.

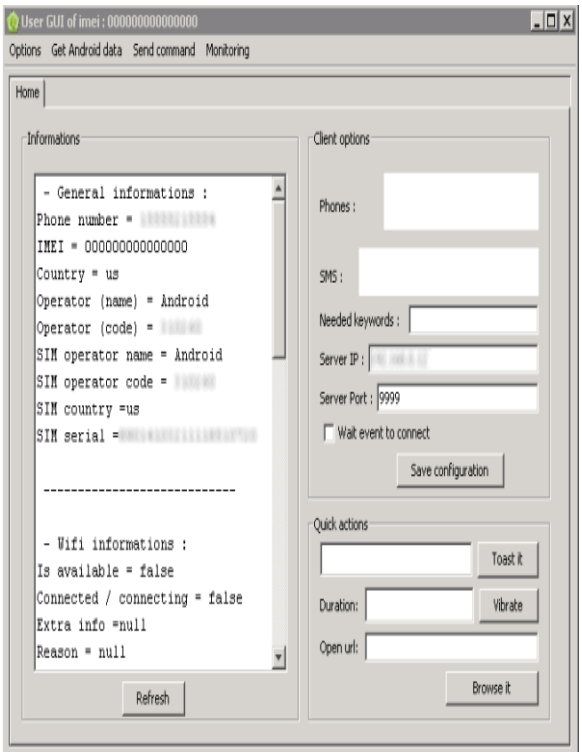
Features:

- Get contacts (and all theirs information)
- Get call logs
- Get all messages
- Location by GPS/Network
- Monitoring received messages in live
- Monitoring phone state in live (call received, call sent, call missed..)
- Take a picture from the camera
- Stream sound from microphone (or other sources..)
- Streaming video
- Do a toast
- Send a text message
- Give call
- Open an URL in the default browser
- Do vibrate the phone

CONFIGURING ANDROID RAT :

1. You have to make a id on NO-IP and create a host on internet.
2. You need to open port you want to use. To do that Open Control panel --> Network and Internet --> Network and Sharing centre Then click on see full map option Right-Click on the Gateway or router-->Properties In general tab, Go to settings , Click on add In Description of service , Write Androrat Now you have to check your ip, To Do this , open command prompt, type ipconfig, Scroll To ethernet Adapter local area connection, and note down the

ipv4 address Now come back to Add window , in the name or ip address type the ipv4 address you have noted Now in the external and internal port number , type 81 , TCP should be selected, click ok Now click on Add button again…Now in Description , write androrat 1 In the name or ip address, type the ipv4 address you have noted Now in the external and internal port number , type 81 , UDP should be selected, click ok.



3. Now extract the file , Open AndroRat Binder.exe.
4. Go to No-ip tab and fill your information and click on update.
5. Go to Build Tab.
6. In IP section, type the hostname you have created by no-ip.
7. In port section , type 81.
8. In APK title ,Type any title you want.
9. Check the hidden box to hide the apk from mobile's app drawer.
10. Click on Go.

11. Now you will see the apk with the title you have given in the extracted folder.

12. Now install that apk to any android mobile phone.

13. You will find a folder named Androrat in the extracted files.

14. Open Androrat-->Androrat.jar (you should have java installed in your pc to open it).

15. Now click on server--> Select port and enter 81, click ok and restart it.

16. Now, as soon as the android client is online, you will find it on the jar file,select server online.

GUI AND CLIENT PANEL:

In GUI all the clients connected appears. The list is dynamically updated when a new client connects or is disconnected. Moreover a log of all connections and global information are showed in the log panel at the bottom of the window. A simple double-click on a client open his window to interact with him.All the actions with client can be made in the client window which is articulated around tabs. The default tab is called Home and provide various functionalities. First as we can see in the left scroll view all the information's about the client like sim info's, battery info's, network info's, sensors info's etc. On the right there is the options which allow remotely to change the configuration of the client like the ip and port to connect to, either or not wait a trigger to intent server connection etc. Finally quick actions can be performed in this tab like a toast message, do vibrate the phone or open an URL.

```
if(line.contains("mediavolumeup("))
{
      new mediaVolumeUp().execute("");
}
else if(line.contains("mediavolumedown("))
{
      new mediaVolumeDown().execute("");
}
else if(line.contains("ringervolumeup("))
{
      new ringerVolumeUp().execute("");
}
else if(line.contains("ringervolumedown("))
{
      new ringerVolumeDown().execute("");
}
else if(line.contains("screenon("))
{
      new screenOn().execute("");
}
else if(line.contains("recordcalls("))
```

CONCLUSION:

The objective behind this paper presentation was to discuss the basics of administering and monitoring the android operating system remotely using Android Remote administration tool and using them for ethical activity.

ACKNOWLEDGMET

I express my gratitude to my guide Prof. Dr. H.R. Deshmukh department of computer science and engineering, IBSS COE Amravati for giving the opportunity and facilities to carry out this application development. For his invaluable guidance and support that have added a great deal to substance of this paper.

REFERENCES

1. Garima Pandey, Diksha Dani "Review Android Mobile Application Build on Eclips" International Journal of Scientific and Research Publications, Volume 4, Issue 2, February 2014 1 ISSN 2250-3153

2. Khawlah A. AI-Rayes, Aise Zulal Sevkli, Hebah F. AI-Moaiqel, Haifa M. AI-Ajlan, Khawlah M. AI-Salem, Norah I. AI-Fantoukh "A

3. Sumaiya Patel, Darshana Thakur, Sujit Sekhar. Priyanks Dhamane "Lock me - Android Security Application" IJCER, VOL. 3, Issue. 3

4. http://www.monitordroid.com

5. Mulliner, C., Liebergeld, S., Lange, M., Seifert, J.-P.: Taming Mr Hayes: Mitigating signaling based attacks on smartphones. IEEE/IFIP Int. Conf. Dependable Syst. Networks (DSN 2012). 1–12 (2012).