International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Fully Undetectable Remote Access Trojan: Android

[1]Akshitasinh Chauhan, [2]Dr. Ravi K Sheth
[1]*Student Master in Technology Cyber Security, Department of Information Technology and Telecommunication, Raksha Shakti University, Ahmedabad, India*
[2]*Assistant Professor Raksha Shakti University*

Abstract: ***Android is the one of the fastest growing and most popular operating system for all the smart phones. With over 80 percent market share, Android is the most prevailing player in the mobile platform and people are switching to it with its every update. As popularity and usability for Android is growing with every minute, cybercriminals are targeting android devices with malicious programs, as smart phones are often used as a tool to pay online, and for storing sensitive information about the user. Remote Access Tool (RAT) allows a potentially malicious user (intruder) to remotely control the system. A Remote Access Trojan is remote control software which installed on a smart phone, will allow a remote computer to take control of it. A RAT allows an attacker to remotely control a computing system and usually consists of a server unnoticeably running and listening to definite TCP/UDP ports on the victim's system as well as a client acting as the interface between the server and the attacker. The most common means of infection is through installing games, email attachments or downloading applications from unverified third party. The developer of the malware usually uses various fully undetectable techniques in order to make the malware unsuspicious to the users. These often implanted in lawful programs through RAT-endorsed procedures. They are stealthily planted and help gain access of victim's phone, through patches, games, E-mail attachments, or even in legitimate-looking binaries. Once installed, RATs perform their unpredicted or even unauthorized operations and use an array of techniques to hide their traces to remain undetectable and stay on victim systems for the long haul. In this paper, our objective is to demonstrate how we can create our own Remote Access Trojan software/Trojan followed by a detailed explanation of the construction, deployment and working of the RAT software, which can be used by law enforcement agencies to spy on suspicious people. The biggest advantage about creating your own RAT is that it is fully undetectable and you can add whichever features you desire.***

Keywords: ***Android, Remote Access Trojan, Trojan, third party applications, email attachments, malicious, compromised system***

I. INTRODUCTION

P=[;.32\[[ogram or file that is harmful either to a computer software or user. In Spanish, "mal" is a prefix that means "bad" overall making the term "bad ware". Malware includes worms, computer viruses, Trojan horses and spyware which are few examples of malware. These malicious programs can carry out a variety of functions, ranging from stealing, encrypting or deleting sensitive data, they might also alter or hijack core computing functions and monitor users' computer activity without users' permission or knowledge. One of the most common but dangerous Trojans is called Backdoor Trojans (also known as Remote Access Trojans or RATs). A computer with a sophisticated backdoor Trojan installed may also be referred to as a zombie or bot. These threats are almost invisible to the user and if they succeed in entering the system, the intruder has remote access to the system. The intruder/attacker, with the help of the Trojan, is now in control of the computer. Few abilities of backdoor Trojans are to gather information, terminate or run a task or process, download and upload files, reports to the attacker's machine, change critical setting in Windows, restart or shutdown the PC, and perform Denial of Service (DoS) attacks.

A shared B2B International and Kaspersky Lab survey conducted in 2014 found that 77% of the Internet users surveyed uses several devices to access the World Wide Web; alongside computers, they typically use smart phones and tablets.

According to the identical IDC report, the distribution of operating systems for mobile devices looks like this:

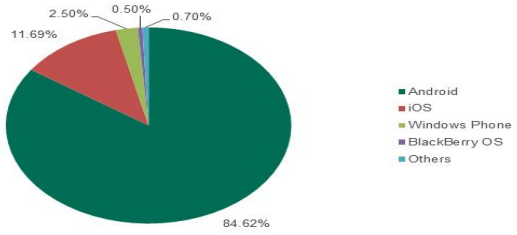

Fig. 1 Distribution of mobile operating systems in Q2 2014, according to IDC [7]

As the figure shows, nearly 85% of the mobile device market was occupied by Android in Q2 2014. These numbers are recognition of Android's undisputed leadership among mobile environments. This operating system is free for device manufacturers and can be easily modified to match various business needs, which has helped it achieve popularity among developers as well as consumers across the world. This also means that Android-based devices naturally attract the attention of cybercriminals who are creating and distributing malicious programs.

Kaspersky Lab experts evaluate that 98.05% of all existing mobile malware targets the users of Android devices. They have reported that in the first half of 2014 alone, 175,442 new unique Android malicious programs were detected. That is 18.3% (or 32,231 malicious programs) more than in the entire year of 2013. This makes it easy understand why cybercriminals make so many malicious programs targeting Android devices: as, smart phones are progressively more used as a tool to pay online for products and services.

Applications can be installed through Google Play as well as third parties such as Amazon App store. Third party applications present a security threat to users who enable the installation of applications from unverified sources. These unverified packages may transfer malware that would be installed on a device without the user's permission or knowledge.

Another risk is the possibility of an attacker gaining access to personal data such as the user's cloud storage accounts and associated email identifiers. This information can be used to access content that is stored in cloud base storage without the user's knowledge or permission. Smart phones can also be considered as a kind of mobile sensor, since they routinely collect a multitude of personal information about their owners. In other words, mobile devices users are a very valuable target for cybercriminals.

II. REMOTE ACCESS TROJAN

There are two programs required for this tool. A client program runs on the Attacker's computer, it listens for the server program on the specified port to make connection, implements a GUI and the attacker can send through various commands to carry out the attack. The server program runs in the background of the victim's machine, hidden from the user. It makes connection with client program whenever it's online and uses it to receive commands from the attacker and carries out the required function. A simple Network Program consists of 2 parts, a server and a client. The server program must be started first and waits or listens for the client program to connect. However, it is also possible to have the server connect to the client as in the case of Reverse-Connection-RATs that are used to bypass firewall or router limitations. The server program will usually be on one computer while the client program will be on another computer. Both can be on the same Local Area Network, or, on the Internet. After connection is established, the client will send a command to the server. Upon receiving the command, the server will execute it.

Remote Access Tool is a piece of software used to remotely access or control a device. This tool can be used legitimately by system administrators for accessing the client computers. Remote Access tools, when used for malicious purposes, are known as a Remote Access Trojan (RAT). They can be used by a malicious user to control the system without the knowledge of the victim. Most of the popular RATs are capable of performing key logging, screen and camera capture, file access, code execution, registry management, password sniffing etc.

A. Damage by Remote Access Trojan

Because a RAT enables administrative control, it makes it possible for the intruder to do about anything on the targeted victim's computer, including:

1) Observing user behavior through key loggers or other spyware.
2) Accessing confidential information, such as credit card.
3) Starting a system's webcam and recording video.
4) Taking screenshots.
5) Distributing viruses and other malware.
6) Formatting drives.
7) Deleting, downloading or modifying files and file systems.

B. Trojan Usage

1) DarkComet was in use by the Syrian government to spy on its citizens. The general population had taken to employing VPNs and secure chat applications to block government surveillance, so the spyware features of DarkComet enabled the Syrian government to avoid those security measures.
2) It can also be used to spy on suspicious targets by the government.

3) Intelligence agencies in Germany use malware to track computers of people under suspicion. The Trojan is able to track user chats and conversations on smart phones and PCs.
4) German agencies have mandatory authority to place Trojan horses on the hard drives of suspected criminals using email that would install key loggers, record webcams and microphones and scan infected hard drives for documents, diagrams and photography.
5) Chinese covert intelligence bodies have been associated with Trojan horse activity against both other governments and private industry.
6) NSA was spying on everyone living in US which were later disclosed by snowden.
7) A government Trojan is installed on a computer or network by a law enforcement agency for the purpose of capturing information relevant to a criminal investigation, it acts as a spyware. Depending on the prerequisite, government Trojan horses may interrupt email or VoIP traffic; scan hard drives for applicable digital media or even record conversations and video conferences. This type of software captures data and then sends it back to a central server for processing and analysis without a user's knowledge; it is generally called as a back door Trojan horse virus.
8) Swiss government agencies have reported to be working with Internet service providers to record speech on an infected PC's microphone, as opposed to of intercepting encrypted voice packets.
9) Government Trojans represent a step in turning the tables on cybercriminals by using a proven mechanism for capturing data secretly.

C. Effect Of Android Version On Malware

How much higher are the odds that your device will be exposed to malware if you download apps from outside Google Play or if you use one of Android's older versions? Potentially Harmful Application (PHA), which is Google's term for mobile malware.

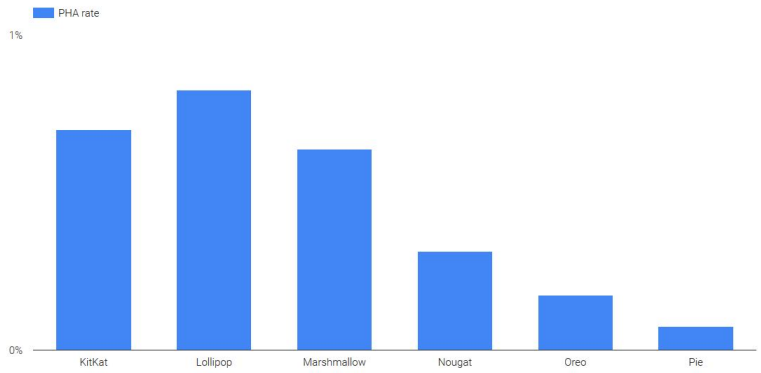

Fig. 2 Potentially harmful application rate by Android version [16]

After going through this research, we came to know Trojan horse is widely used malware, which disguises itself as a normal program to trick users into installing the malware. It can give remote access of an infected system be it computer or mobile. In recent times mobile malware are getting popular, majorly targeting android devices as it's one of the most used mobile operating system. In android if you are using any application you have to accept the permissions which the application needs in order to run. This is where many hackers find the loophole and try to exploit the ignorance of the user by tricking them into either installing the application or by linking unwanted links, which would give them the access of their device. There are many government Trojans available for windows system, monitoring any illegal activities done by someone whom the law enforcement agencies think is suspicious, but there isn't any for android devices known till now, given the increase in the usage of android devices.

III. PROPOSED SYSTEM: ANDROID REMOTE ACCESS TROJAN

Phase one includes coding the two programs required for the project, namely- Client and Server programs. The Server program has functionalities which include listening for connection for active clients, relaying the appropriate commands to the client and implementing a Graphical User Interface for the attacker's convenience. The Client program's functionalities include trying to establish connection with the server whenever the mobile phone is connected with the network; carry out the necessary functions as per the user's commands.

In second phase, having finished the client and the server programs, we now test the connection between the two programs, the victim's device and the attacker's.

The client, which runs in the background of the victim's device, sends a connection request to the attacker, whenever the victim's machine is online and connected with the network. The server (attacker) is constantly online, listening for active clients. The phase is successfully completed when a connection is established between the attacker and the victim; the attacker is notified of the victim's presence and is successfully able to send through commands which are executed on the victim's device. Phase 3 involves devising a proper, foolproof way to make sure that our victim gets infected without his/her knowledge and avoid any further suspicions or be ultimately detected. Since the program is coded by us, it is less likely to be detected by any Antivirus as its signature will not be present in the Database of the Antivirus. Prior to being delivered, RAT clients may be named as software patches or games with the corresponding binders, tricking users into downloading, unbundling, and finally, executing such malicious programs

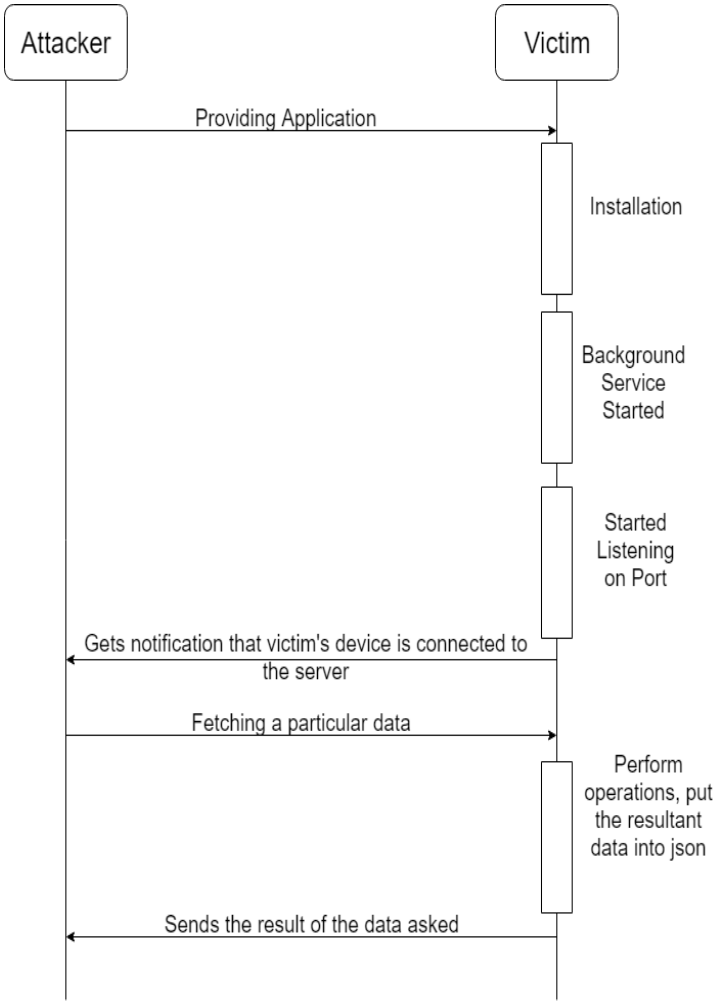

Fig. 3 Sequential Diagram of Remote Access Trojan

The purpose of our project (application) is to steal information stored on the device. Here is the list of stolen information: Call Logs, Contacts, Read SMS, Send SMS, and Read SD card details, Capture pictures, Location of the device.

One can make any android based application, be it any gaming application or photo editing application (Just make sure to develop an application which is being used by many). In this we would create a basic photo editor android application in which we would be asking users' permission for read contacts (for contacts), read and write external storage (for SD card), internet and access fine location state (for geo location of the device), read and send SMS (for SMS), camera (for using camera hardware), read call logs (for call logs)

TABLE 1
PERMISSION USED FOR MALWARE

Permissions	
android.permission.INTERNET	Allows applications to open network sockets
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.READ_SMS	Allows applications to read SMS messages
android.permission.READ_CONTACTS	Allows applications to read the user's contacts data
android.permission.READ_CALL_LOG	Allows applications to read the user's call log.
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.WRITE_EXTERNAL_STORAGE	Allows applications to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	Allows applications to read from external storage.
android.permission.RECEIVE_BOOT_COMPLETED	Allows applications to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting
android.permission.SEND_SMS	Allows an application to send SMS messages.
android.permission.CAMERA	Required to be able to access the camera device.
android.permission.ACCESS_FINE_LOCATION	Allows applications to access fine(e.g., GPS) location

These permissions would be added in the manifest of the android application which we have already created. For Android version lesser than 6, these permission would be given by default when the application is installed (as these would be installed time permission without which the application won't run), and for android version greater than 6, users will give runtime permission to each of them individually. With all the permission in place we would add background service in our application, which would work even when the user closes the application. For this we would be using service for starting ASYNC task (this would start listening to the IO socket).

Now in client side of the application, we would just be adding activities (java classes) of all the permission we have taken from the victim. For server side coding, we would be using Node JS in combination of "Electron", which is an open-source framework developed and maintained by GitHub. Electron allows for the development of desktop GUI applications using web technologies: It combines the Chromium rendering engine and the Node.js runtime. The way server and client would be get connected is by socket programming. In client side we would be adding a java class naming it as connection, in which we would be passing the IP address (URL) of the server and the port number on which the server would be listening. While in the server side we would just be listening

on the same port number which we have mentioned on the client side. Basically what it will do is that, the server will listen on the port number for all the devices which are present on that network.

Once the user installs the application and gives the permission (depending on the android version which the user, for version lesser than 6 (marshmallow) these permission would be taken during installation itself and if the version is higher than 6, then user would be giving runtime permission), on the server side we would open the command prompt and enter npm start which is used to launch the server.

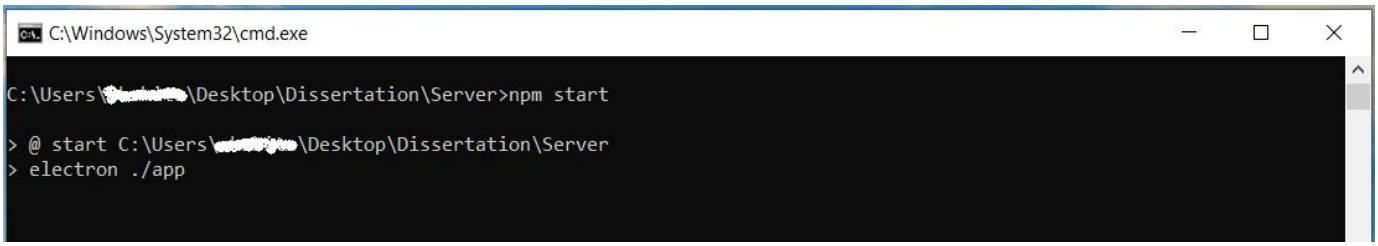

Fig. 4 launching the server

This would launch the server and open the control panel, where we would get the list of victim devices which have installed our application and in the network. By selecting which victim device we want to access remotely, all we need to do is open the device and start with the remote access.

The victim won't even notice that some background services are being taken place and users' data is being monitored and being accessed by third party. The victim would think that this is just a normal photo editing application which would help them edit the photo, but the application itself acts like a remote access Trojan to get users data from user without their knowledge. Below two figures shows, how message is sent from victim's device to third person.

Fig.5 Sending SMS from victim's device to third person

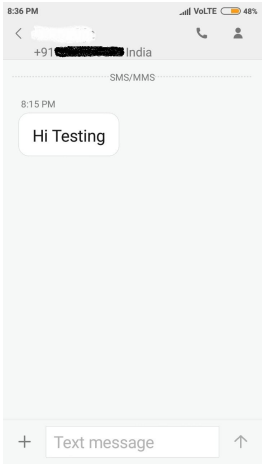

Fig.6 Person receiving message from victim

IV. CONCLUSION

Malware comes under top 5 cyber threat attack. When read about malware in depth we came to know that mobile malware are increasing day by day and android devices are being targeted the most. Trojans is a type of malware and they are mostly used for illegal activities likes stealing sensitive information from the infected system or devices, but there are many Trojans used by law enforcement agencies for spying on people whom they find suspicious. These Trojans are made for windows systems or they work for desktop based application, there isn't any Trojan used for android devices as of now.

For this reason, we have simply have described a method in android that can be used by law enforcement agencies for spying on people whom they find suspicious, as this breaks the security provided by the operating system. Android operating system provides different permissions so any application can access machine data, but no one reads all permissions nor safeguards their device. So using this mentality we have implemented this android remote access Trojan, which creates the security issue, best solution for this issue is user should be aware with this type of mechanism and user should read all the permission before installing any application from the internet as well as from any other source.

REFERENCES

[1] Common Malware Types: Cybersecurity 101. URL: https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101
[2] Malware (or malicious software). URL: https://searchsecurity.techtarget.com/definition/malware
[3] Manjeri N. Kondalwar, Prof. C.J. Shelke. "Remote Administrative Trojan/Tool (RAT)." International Journal of Computer Science and Mobile Computing, Vol.3 Issue.3, March- 2014, pg. 482-487
[4] Prakhar Ahlawat, Sushant Dhar, Samruddha Wagh, Amit Koppad. "Remote Access Tool Using Metasploit". International Journal on Recent and Innovation Trends in Computing and Communication, Volumne:5 Issue:4, April 2017
[5] Android/Mobile Security Status. URL: https://www.av-test.org/fileadmin/News/Documents/2016/AV-TEST_Security_Report_2015-2016.pdf
[6] Distribution of malware under windows. URL: https://www.av-test.org/fileadmin/_processed_/a/f/csm_AV-TEST-_Distribution_of_malware_under_Windows_2018_3462cfad3f.png
[7] Kaspersky Labs: Mobile malware detected in 2013 by platform and category. URL: https://images.techhive.com/images/idge/imported/article/ctw/2014/02/24/kaspersky_labs_mobile_malware_detected_in_2013_by_platform_and_category-100388097-orig.gif
[8] Mobile cyber threats: a joint study by Kaspersky Lab and INTERPOL. URL: https://securelist.com/mobile-cyber-threats-a-joint-study-by-kaspersky-lab-and-interpol/66978/
[9] Rooting your Android: Advantages, disadvantages and snags. URL: https://www.kaspersky.com/blog/android-root-faq/17135/
[10] 10 million Android phones infected by all-powerful auto-rooting apps. URL: https://arstechnica.com/information-technology/2016/07/virulent-auto-rooting-malware-takes-control-of-10-million-android-devices/
[11] DroidJack RAT. URL: https://www.symantec.com/connect/blogs/droidjack-rat-tale-how-budding- entrepreneurism-can-turn-cybercrime
[12] Android. Sandorat. URL: https://www.symantec.com/security_response/earthlink_writeup.jsp?docid=2014-110720-2146-99
[13] Androrat. URL: https://androratapk.com/
[14] Attackes are distributing OmniRAT via SMS messages. URL: https://news.softpedia.com/news/omnirat-lets-hackers-control-android-phones-windows-mac-and-linux-pcs-495779.shtml
[15] OmniRat variant in the wild. URL: https://blog.avast.com/2015/11/05/droidjack-isnt-the-only-spying-software-out-there-avast-discovers-that-omnirat-is-currently-being-used-and-spread-by-criminals-to-gain-full-remote-co
[16] Fake AV Investigation Unearths KevDroid, New Android Malware. URL: https://blog.talosintelligence.com/2018/04/fake-av-investigation-unearths-kevdroid.html
[17] Out with the old, in with the new? URL: https://www.welivesecurity.com/2018/11/12/googles-data-avoiding- malware-on-android/
[18] Malware. URL: https://en.wikipedia.org/wiki/Malware