REMOTE ADMINISTRATION TOOL (RAT)

[1]Shubham, [2]Chandan Acharya, [3] M. Prabu
[1]*UG Scholar, CSE, SRM University, Tamil Nadu, India*
[2]*UG Scholar, CSE, SRM University, Tamil Nadu, India*
[3]*Assistant Professor, CSE, SRM University, Tamil Nadu, India*

ABSTRACT

Remote Administration Tools are programs used to remotely gain control of the computer that it is attacking and giving the attacker unhindered access to the system resources and thereby compromising the privacy of the victim. These RATs can be injected in a computer via E-mail, application, games, links, updates etc. A backdoor can be created from which payload is inserted into the target computer. Once installed these RATs can give the root access of the computer. RAT hides the process running in the background to cover the tracks so that the anti-virus installed in the system cannot detect it. Through RATs the host can control the webcam, keyboard, and the running processes and can install any malicious software in the system.

Keyword: - *LAN, WAN, TCP/UDP, Trojans, Payload, Backdoor etc.*

1. INTRODUCTION

Remote administration means any method of controlling a computer or computers from a remote location. Any system with an Internet connection, TCP/IP or on a Local Area Network (LAN) can be remotely administered. Remote administration can be used for a number of activities and can span multiple servers. RATs are stealthily planted and help gain access of victim machines, through patches, updates, games, E-mail attachments, or even in legitimate-looking binaries. RAT can be made into FUD that is fully undetectable so that the antivirus in the victim's computer cannot detect it. RATs can give the attacker access to the directories, webcams, keyboard etc. The attacker can find out what victim is typing on his/her computer using key-loggers. The attacker can also control the keyboard leaving victim unable to type on their own computer and can install many other malicious programs. These RATs can be injected via pen drives, hard drives or any other external storage devices. These devices are called "bash bunny". A Bash Bunny can install the RAT, backdoor and payload just by inserting the drive in victim's computers. The RAT creates processes to hide its activities and injects running tasks with malicious code which go unnoticed by the system. They can cause Distributive Denial of Service (DDoS) attacks, obtain sensitive information, and record the actions of the current session of the system such as screen preview, keystrokes. They redirect traffic to other systems for obtaining specific services.
The characteristics of the RAT:

→Manipulate processes in task manager.
→Hinders mouse movement randomly.
→Files are deleted, moved, downloaded without permission.
→Infect system with viruses, malwares and worms
→Keyboard stops working.
→Anytime access to victim's computer is provided.

2. LITERATURE SURVEY

Remote administration is important for improving efficiency in managing and maintaining computer systems across communication networks in a cost-effective manner. Contemporary remote access tools support versatile features for controlling remote systems through a wide range of attractive. Remote control software allows you to take control of another PC on a LAN, WAN or dial-up connection so you see the remote computer's screen on your monitor and all your mouse movements and keystrokes are directly transferred to the remote machine. It lets you save hours of running up and down stairs between computers but if the remote administration is unauthorized it can cause a lot of damage to the machine. Absolute manage is a remote administration tool. It's system's communication protocol suffers from serious design flaws and fails to provide adequate integrity, confidentiality, or authentication. Attackers can exploit these vulnerabilities to issue unauthorized commands on client systems and execute arbitrary code with administrator privileges. RAT Catcher reliably detects and ultimately blocks RAT malicious activities even when Trojans use multiple evasion techniques. Employing network-based methods and functioning in inline mode to inspect passing packets in real time, our RAT Catcher collects and maintains status information for every connection and conducts session correlation to greatly improve detection accuracy.

There are many remote administration Trojans. Some of them are:

2.1. Dark comet:

DarkComet is a remote access Trojan (RAT) developed by Jean-Pierre Lesueur (known as DarkCoderSc), an independent programmer and computer security coder. DarkComet allows a user to control the system with a Graphical User Interface (GUI). It has many features which allows a user to use it as remote administration tool however, DarkComet has many features which can be used maliciously. It is mostly used to spy on someone's computer by taking screenshots, cracking password, and key-logging.

2.2. Blackshades:

Blackshades is a malicious Trojan horse used by hackers to control computers remotely. It targets computers using Microsoft's Windows -based operating systems. Over 500,000 systems was infected with this software worldwide. It was sold for $40, and it generated $350,000 in sales.

2.3. JSPY:

It is a good RAT as it is undetectable by many of the anti-viruses, but it was not a secure RAT as it was not stable possibly now they've improved their product in stability. It is a free RAT.

2.4. NJRAT:

NjRAT, is also called Bladabindi, is a Remote Access Tool or Trojan which allows the host to control the end user's computer. It was first found in June 2013. It was made by Arabic criminals and was used against targets in the Middle East. It can be spread through phishing and infected drives. It is rated "severe" by the Microsoft Malware Protection Center.

2.5. Cybergate:

CyberGate is a powerful, fully configurable and stable Remote Administration Tool. It is coded in Delphi. Using cybergate you can log the target's passwords and can also get the screen shots of their computer's screen. You can connect to multiple targets in single time. One should not know what the ip-address of the target computers is. That is the main advantage. You have to spread the server file to the target computers. Using file manager utility you can explore the data of the target computer.

3. EXECUTINON OF RAT

Before the RATs are installed they are customized that is the default TCP/UDP ports the listener/host IP, changing them to executables (.exe) such as apk's or games or any software or to make it more believable they are attached with a genuine apk or game or software.

In Linux systems softwares like metasploit, Armitage are used to create an executable RAT while in windows softwares like PandoraRAT, Prorat, Sub seven etc. are used to create RAT executables but still the most efficient method of creating a RAT is to code it yourself via terminal and convert it into an executable. The most basic way of injecting a RAT is through E-mail, apk, games, software, or anything which is executable. For DDos the RATs are spread on many computers for this the easiest way for an attacker is to go on chat platforms and select from the active user at random and inject the RAT in their system.

Once the RAT is injected in the computer it can outlive reboots system, crashes evade Anti viruses. It edits registry and files like win.ini and system.ini and can be triggered during every reboot transparently.

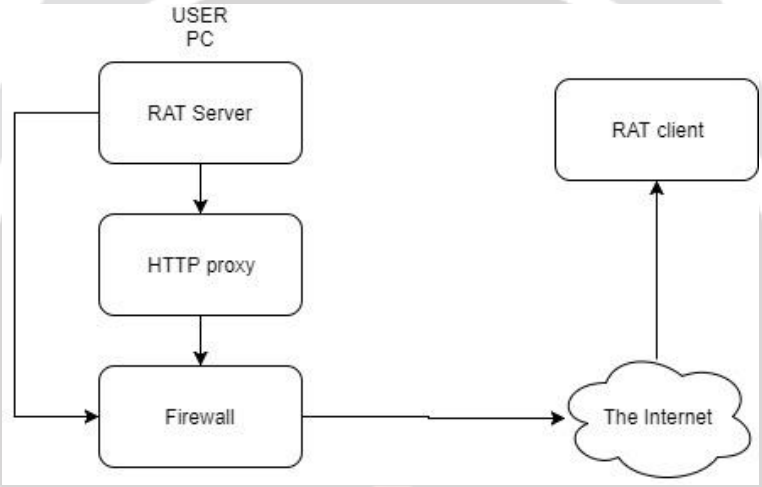

Fig 1: Architecture of RAT

4. WORKING OF RAT

A Remote Access Trojan enters a focused on PC through diversion applications, freeware or email connections in which digital assailants have hided the executable documents. Once a client runs the executable records unconsciously, this RAT introduces itself in the framework memory. The real program can utilize a system to join RAT with genuine executable projects so that the RAT executes out of sight while the real projects run, leaving the computer unknown from the malicious processes running.

4.1. ALGORITHM FOR CREATING A RAT

→Search for the root drive.
→Navigate to the following location on the root drive.
%systemroot%\Windows\System32
→Create the file named "ABC.dll".
→Start dumping the junk data onto the above file and keep increasing its size until the drive is full.
→Once the drive is full, stop the process

5. DETECT AND REMOVE A RAT

Open your Task Manager. Click the Processes tab, and check for any procedures with unusual names or irregular CPU use running in your framework. On the off chance that you discover one yet can't ensure whether it is a RAT' process.

5.1. CHECK YOUR PROGRAM START UP

A RAT adds itself to framework startup catalogs and registry sections so that it can begin consequently every time you boot your PC. Press Windows key + R key together. When a dialog box shows up, sort msconfig.exe into it and snap OK. When a window opens, tap the Startup tab and check if there are any suspicious startup thing.

5.2. VIEW LIST OF INSTALLED PROGRAMS

Go Control Panel, then click Add or Remove Programs. A window will open which will have all the programs installed in on your PC. On the off chance that you see any odd software or program, then it could be malicious. Uninstall it, if you are unable to uninstall it reboot your PC in safe mode then uninstall it from control panel.

6. FLAWS OF REMOTE ADMINISTRATION TOOLS

Remote administration tools have mechanisms to allow remote users to gain access of a machine. The machine user is always at a risk of abuse by authorized users.

If the encryption keys of the Remote Access Tool are decoded from a copy of the software the authentication of the messages and functions may be compromised. The data may get altered by this third party which can send partially or completely changed messages to the host and client servers. This is the problem one usually faces when infusing hardcoded keys into the security mechanism of the Remote Administration tool.

If a third party is accessing a machine it is necessary that the third party be authorized. Every server have a unique seed value whenever a command is given to client, it checks for the seed value if it isn't the expected value the command isn't executed. So if the client-server authentication isn't strong the commands given by server won't be executed and remote access won't be possible.

7. FUTURE SCOPE OF RAT

Already a lot of research is going on in the field of cybersecurity. In future work can be done to improve the efficiency of algorithms. The work of the different algorithms can be extended further in order to increase the security and speed of Remote Administration Tool. A major open issue for future work about the stability of the RAT and the behaviour of its components.

8. CONCLUSION

In this paper we revealed about the properties, execution, Security issues and vulnerabilities of remote administration tool.
Remote administration of devices helps to connects devices remotely which can be efficient in managing systems tasks like system updates, virus-removal, system scanning can be done remotely without actually being on the console.
Remote administration can be dangerous but also very useful this evaluation let customers choose their need of remote administrator tools carefully.

9. REFERENCES

[1] Manjeri N. Kondalwar and C.J Shelke for "Remote Administrative Trojan/Tool(RAT)", (2014)
[2] Zhongqiang Chen, Peter Wei and Alex Delis for "Catching Remote Administration Trojans(RATS)", (2002)

[3] Jay Novak, Jonathan Stribley, Kenneth Meagher, and J.Alex Halderman "Absolute Pwnage: A Short Paper About The Security Risks of Remote Administration Tools", (2011)
[4] Rupal D.bhatt, D.B. Choksi, "A Comparative Evaluation of Remote Administration Tools", (2013)
[5] Anis Ismail, Mohammad Hajjar, Haissam Hajjar, "Remote Administration Tools: A Comparative Study"(2012)