RAT: Remote Administrative Trojan

Sourabh Singh [1], Dr. Latika Kharb [2]
[1] Student(MCA), JIMS, Sector-5, New Delhi.
[2] Professor, Department of IT, JIMS, Sector-5, New Delhi.

I. INTRODUCTION

A RAT or remote administration tool, is software that gives a person full control a tech device, remotely. The RAT gives the user access to your 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. RAT is used to remotely connect and manage single or multiple computers. RAT is one of the most dangerous Trojan because it compromises features of all types of Trojans. It provides an attacker with nearly unlimited access to host computer along with Screen Capture, File management, shell control and device drivers control. RATs uses reverse connections to connect remote system and hence are more likely to remain undetected. They can hide themselves in process space of legitimate program and hence never appear in task manager or system monitors. A Trojan generally has two parts Client and Server or Master and Slave. We can say Server is Slave and Client is Master. So a server side is installed on a remote host and the attacker manipulates it with client software.

II. THREATS

RAT allows an attacker to gain access to the following items on a compromised computer:
• Files
• Processes
• Services
• Clipboard
• Active network connections
• Registry
• Printers
• Remotely control the compromised desktop
• Take screenshots
• Record webcam footage
• Record audio
• Log keystrokes
• Steal passwords
• Download files
• Open Web pages
• Display onscreen messages
• Play audio messages using the text-to-speech function
• Restart the compromised computer
• Hide the taskbar
• Hide desktop icons
• Cause system failure/blue screen of death

□ COMMON TYPES OF TROJAN MALWARE

• ***Backdoor Trojan:***
This Trojan can create a "backdoor" on your computer. It lets an attacker access your computer and control it. Your data can be downloaded by a third party and stolen. Or more malware can be uploaded to your device.

• ***Distributed Denial of Service (DDoS) attack Trojan:***
This Trojan performs DDoS attacks. The idea is to take down a network by flooding it with traffic. That traffic comes from your infected computer and others.

• ***Downloader Trojan:***
This Trojan targets your already-infected computer. It downloads and installs new versions of malicious programs. These can include Trojans and adware.

• ***Fake AV Trojan:***
This Trojan behaves like antivirus software, but demands money from you to detect and remove threats, whether they're real or fake.

• ***Game-thief Trojan:***
The losers here may be online gamers. This Trojan seeks to steal their account information.

• ***Infostealer Trojan:***
As it sounds, this Trojan is after data on your infected computer.

• ***Mailfinder Trojan:***
This Trojan seeks to steal the email addresses you've accumulated on your device.

• ***Ransom Trojan:***
This Trojan seeks a ransom to undo damage it has done to your computer. This can include blocking your data or impairing your computer's performance.

• ***Remote Access Trojan:***
This Trojan can give an attacker full control over your computer via a remote network connection. Its uses include stealing your information or spying on you.

• ***Rootkit Trojan:***
A rootkit aims to hide or obscure an object on your infected computer. The idea? To extend the time a malicious program runs on your device.

• ***SMS Trojan:***
This type of Trojan infects your mobile device and can send and intercept text messages. Texts to premium-rate numbers can drive up your phone costs.

• ***Trojan banker:***
This Trojan takes aim at your financial accounts. It's designed to steal your account information for all the things you do online. That includes banking, credit card, and bill pay data.

• ***Trojan IM:***
This Trojan targets instant messaging. It steals your logins and passwords on IM platforms.

SEVEN MOST COMMON RATS/ATTACKS IN USE TODAY:

• ***SAKULA:***
Sakula is believed to be associated with the recent OPM attack. It is signed, looks like benign software, and provides the attacker with remote administration capabilities over the victim machine. Sakula initiates simple HTTP requests when communicating with its command and control (C&C) server. The RAT uses a tool called "mimkatz" to perform "pass the hash" authentication, which sends the hash to the remote server instead of the associated plaintext password

• ***KjW0rm:***
KjW0rm is believed to be associated with the recent breach of TV stations in France. KjW0rm was written in VBS, which makes it even harder to detect. The Trojan creates a backdoor that allows the attacker to take control of the machine, extract information, and send it back to the C&C server

• ***Havex:***
Havex targets industrial control systems (ICS). It is very sophisticated and provides the attacker with full control over the infected machine. Havex uses different variants (mutations) and is very stealthy. The communication with its C&C server is established over HTTP and HTTPS. Its footprint inside the victim machine is minimal.

• ***Agent.BTZ/ComRat:***
Agent.BTZ/ComRat is one of the most notorious and well known RATs. Believed to be developed by the Russian government to target ICS networks in Europe, Agent.BTZ (also known as Uroburos) propagates via phishing attacks. It uses advanced encryption to protect itself from analysis, provides full administration capabilities over the infected machine, and sends extracted sensitive information back to its C&C server. Agent.BTZ uses advanced anti-analysis and forensic techniques.

• ***Dark Comet :***
Dark Comet provides comprehensive administration capabilities over the infected machine. It was first identified in 2011 and still infects thousands of computers without being detected. Dark Comet uses Crypters to hide it existence from antivirus tools. It performs several malicious administrative tasks such as: disabling Task Manager, Windows Firewall, and Windows UAC.

• ***AlienSpy :***
AlienSpy targets Apple OS X platforms. OS X only uses traditional protection such as antivirus. AlienSpy collects system information, activates webcams, establishes secure connections with the C&C server, and provides full control over the victim machine. The RAT also uses anti-analysis techniques such as detecting the presence of virtual machines.

• ***Heseber BOT:***
Heseber BOT deploys Virtual Networking Computing (VNC) as part of its operation. Since VNC is a legitimate remote administration tool, this prevents Heseber from being detected by any antivirus software. Hesber uses VNC to transfer files and provide control over the infected machine.

• ***Emotet banking Trojan:***
After a long hiatus, Emotet's activity increased in the last few months of 2017, according to the Symantec 2018 Internet Security Threat Report. Detections increased by 2,000 percent in that period. Emotet steals financial information, among other things.

• ***Rakhni Trojan :***
This malware has been around since 2013. More recently, it can deliver ransomware or a cryptojacker (allowing criminals to use your device to mine for cryptocurrency) to infected computers. "The growth in coin mining in the final months of 2017 was immense," the 2018 Internet Security Threat Report notes. "Overall coin-mining activity increased by 34,000 percent over the course of the year."

• ***ZeuS/Zbot:***
This banking Trojan is another oldie but baddie. ZeuS/Zbot source code was first released in 2011. It uses keystroke logging — recording your keystrokes as you log into your bank account, for instance — to steal your credentials and perhaps your account balance as well.

EXECUTION 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.

III. 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.

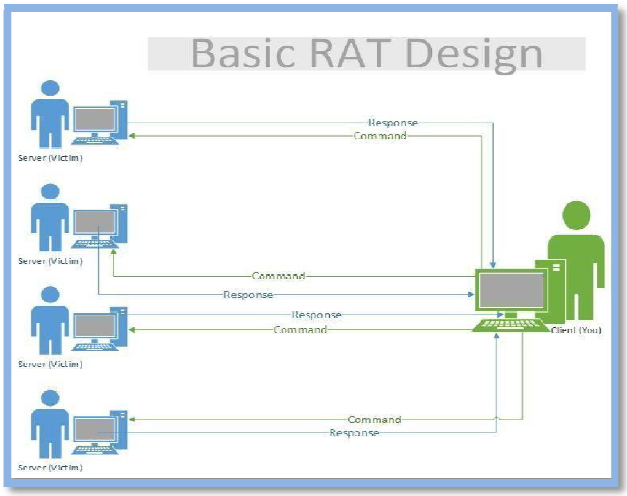

Figure 1: Basic RAT Design

How to detect and remove a Remote Access Trojan?

• *View the running processes:*
Open your Task Manager by right clicking the taskbar and selecting Task Manager. Click the Processes tab, and scroll down to see if there are any processes with strange names (or abnormal CPU usage) running in your system. If you find one but can't make sure whether it is a RAT' process, you can search for it on Google. You may get the answer.

• *Check the startup programs:*
A RAT often adds itself to system startup directories and registry entries so that it can start automatically each time you boot your computer. Press Windows key + R key together. When a box appears, type msconfig.exe into it and click OK. When a window opens, click the Startup tab and check whethre there is any suspicious startup item. If there is, then Google it.

• *View the list of installed programs:*
You can access Control Panel first, and then click Add or Remove Programs or Uninstall a program option. A window will open and show all programs installed on your computer. If you notice any odd program, then it could be malicious. Similarly, if you are unable to recognize it, please type it into Google.

• *Check Internet connection:*
Another indication of the RAT infection should be the inexplicably slow network speed. If your computer is infected by a RAT, your Internet connection would be extremely slow, since the hackers will use the bandwidth to download or upload something. Surely, it cannot be directly inferred you must have a RAT on your PC when your network connection becomes slow, but you should pay attention to it. More early you find the problem, less loss you would suffer from.

• *Firewall and Antivirus Software(easy):*
Firewall software blocks incoming and outgoing port connections, so they are your number one defense against RATs. Firewalls combined with antivirus software catches most threats, but you're not 100% safe. Even with these two defenses, new malware is always created to avoid detection. Always use common sense before installing an executable from an unknown source.

REFERENCES

[1] Bhagat, B. B., & Kharb, L. (2008). Phishing and Its Indian Perspective. The Internet Journal of Medical Informatics, 3(2).
[2] https://www.linkedin.com/pulse/remote-access-trojansrat-hamad-al-quait

[3] https://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan
[4] Garg P, Kharb L (2018), Bugs in Silicon, International Journal of Engineering Research in Computer Science and Engineering, 5(1).
[5] https://www.symantec.com/connect/blogs/creepware-who-s-watching-you
[6] https://en.wikipedia.org/wiki/Remote_access_trojan
[7] https://gbhackers.com/gravityrat-remote-access-trojan/