Trojan Vs Rat Vs Rootkit

Mayuri More[1], Rajeshwari Gundla[2], Siddharth Nanda[3]
[1]U.G. Student, [2] Senior Faculty, [3]Senior Faculty
SOE, ADYPU, Lohegaon, Pune, Maharashtra, India[1]
IT, iNurture, Bengaluru, India[2,3]

Abstract **-** Malicious Software is Malware is a dangerous software which harms computer systems. With the increase in technology in today's days, malwares are also increasing. This paper is based on Malware. We have discussed TROJAN, RAT, ROOTKIT in detail. Further, we have discussed the adverse effects of malware on the system as well as society. Then we have listed some trusted tools to detect and remove malware.

Keywords **-** Malware, Trojan, RAT, Rootkit, System, Computer, Anti-malware

I. INTRODUCTION

Nowadays, this world is full of technology, but with the advantages of technology comes its disadvantages like hacking, corrupting the systems, stealing of data etc. These malpractices are possible because of malware and viruses that are created by hackers and attackers. There are also many tools to prevent these malwares. Let us discuss some malware, their effects and how to remove them.

What Is A Malware? Malware is a software which is malicious and intends to harm the other systems/devices, server, computer network, people, and important data belonging to any person or organisation. Malware is capable of disrupting the system's function and allowing an attacker to retrieve confidential and sensitive information. An attacker can spy on the host computer using a malware [1].

Malware can be classified as:

1. Viruses
2. Worms
3. Trojan
4. Rootkits
5. Ransomware
6. Keyloggers
7. Grayware
8. Botnet
9. Spyware
10. Adware

II. LITERATURE SURVEY

Author discussed in depth analysis of the rootkits that target the operating system and which uses various hooking techniques to hide themselves [8]. Konrad Rieck, Thorsten Holz, Carsten Willems, Patrick D¨ussel, and Pavel Laskov authors have proposed a method to classify different malware types based on behaviour of malware [9]. By installing Remote Access Trojan, attacker can monitor and control the victim's PC remotely to steal confidential information. Main issue is it is hard to prevent the intrusion of RATs completely and prevent confidential data being leaked. So Dan Jiang and Kazumasa Omote researchers have proposed an approach to detect RAT in the early stage [10].

III. CLASSIFICATION

Rootkit vs Trojan vs Rat

Rootkit - A rootkit is a malicious software that permits a legitimate user to have confidential access to a system and privileged areas of its software. A rootkit possibly contains a large number of malicious means for example banking credential stealers, keyloggers, antivirus disablers, password stealers and bots for DDoS attacks. This software stays hidden in the computer and allocates the remote access of the computer to the attacker[2].

Types of Rootkit:

1. Kernel rootkit: Kernel rootkit operates at the operating system making it difficult to spot and may also cause serious consequences on the operating system.
2. Firmware Rootkit: Firmware devices like network devices are affected by these kinds of rootkits. It is very difficult to detect as it is booted when machines get booted and stay in the device forever.
3. Application Rootkit: These rootkits infect the application files inside the computer. The application files are replaced by the rootkit files or the behaviour of the application is changed due to code injected.
4. Memory rootkit: These kinds of rootkits take shelter of the RAM to hide and operate from the computer memory.
5. Bootkit rootkits: These rootkits infect the authentic boot loader of the computer with the corresponding rootkit, enabling them to activate when the operating system is started.
6. Persistent Rootkit: These types of rootkits are able to restart the system activities after shutting down.
7. Library rootkits: These Rootkits are capable of altering the library files in the system library.

Trojan - A Trojan is a malicious program that seems to be legitimate but is capable of taking control of the host computer. The basic operations of trojan are damaging, disrupting, stealing, or perpetrating further harmful actions on the data or network [3].

Types of Trojan:

1. Backdoor Trojan: These types of trojan are capable of creating a "backdoor" on the computer. The attacker can access and control the computer. The data in the

device can be stolen by a third person and more malwares can be uploaded to the device.
2. DDoS (Distributed Denial of Service) attack trojan: These trojans perform DDoS attacks. The task is to deflate a network by inundating it with traffic coming from infected devices.
3. Downloader trojan: This Trojan makes the pre-infected computer as its target by downloading and installing new editions of malicious programs including adware.
4. Fake AV Trojan: These trojans acts like antivirus, but necessitates money to spot and remove threats.
5. Game-Thief Trojan: The account information of online gamers is stolen by game-thief trojans.
6. Info-stealer Trojan: As the name suggests, this trojan seeks for the data in the infected device.
7. Mail-finder Trojan: Stealing the email addresses present on the computer is done by this Trojan.
8. Ransom Trojan: This Trojan asks for a ransom to reverse the changes or damage it made to the computer by blocking data or worsening the computer's functioning.
9. Remote Access Trojan: An attacker can remotely access the device, also whipping any data and prying on anyone.
10. Rootkit Trojan: A Rootkit fleece or obscure a program on the infected device.
11. SMS Trojan: SMS Trojans intend to infect a mobile device by sending intercept text messages.
12. Trojan-Banker: Trojan banker targets the financial accounts of the host. It steals account information for which online transactions are done including credit card, bill pay data and online banking.
13. Trojan IM: This Trojan aims instant messaging, stealing the logins and password on IM platforms.

Remote Access Trojan (RAT) - Remote Access Trojan is a malware program including a backdoor, enabling an administrative control on the targeted computer or device. RAT is mostly downloaded unknowingly due to email attachments or games, compromising the host system. The intruder then distributes RATs to other vulnerable devices and establish a botnet. It monitors the behaviour of users with the help of keyloggers, access confidential information, activate a system's webcam and record videos, take screenshots, distribute malwares (generally viruses), format drivers and delete, download or alter files [4].

Types of RATs [5]:

1. Sakula: This RAT is endorsed, seems benevolent software and grants the permission of remote handling throughout the host device, to the attacker. It instigates HTTP requests while imparting with C&C (command and control) server.
2. KjWorm: It is very difficult to detect as it is written in VBS. The attacker can control the machine through the backdoor, extracting information and sending it to recede the C&C server.
3. Havex: Industrial Control Systems (ICS) is targeted by Havex. Being very erudite, it gives the attacker, full control of the infected machine. HTTP and HTTPS, helps it to communicate with its C&C server.
4. Agent.BTZ/ComRat: This RAT is a well known and infamous RAT created by the Russian government in order to target ICS networks in Europe. It is proliferated through phishing attacks. It cannot be easily detected in an analysis as it avails advanced encryption. Enhanced anti-analysis and forensic methods are used by Agent.BTZ.
5. Dark comet: It provides ample administration proficiencies across the infected device. It is difficult to detect because of Crypters used to veil its existence from antivirus. It carries out several administrative tasks maliciously, for example disabling windows firewall, Task manager and windows UAC.
6. AlienSpy: It is designed to target Apple OS X platforms. It indulges in collecting information, activating webcams, connecting to C&C server securely, providing control for victim machine. It detects the presence of virtual machines by anti-analysis techniques.
7. Heseber: This RAT operates to deploy Virtual Networking Computing (VNC). It cannot be detected by antivirus as VNC is an authentic isolated administration tool. It also provides control over the infected system and transfer files.

Adverse effects of malware

1. **Increase in network traffic -** Increase in network traffic illustrate the malware attacks on the computer. The malware works at the backend of genuine looking software and simultaneously increase the network traffic.
2. **Loss of critical system elements -** The malwares are designed to damage or steal user information. Some hackers intentionally erase the crucial elements of the system.
3. **Crashing of the operating system -** Computers get shut down whenever the user tries to remove the infection. A fake Blue screen of Death might be experienced which imitate a crashing computer.
4. **Hardware failure -** A Trojan may carry out recurring actions like opening and closing the CD/DVD tray. The repeated action causes the failure of the CD/DVD drive.
5. **Data loss or data theft -** Most of the attackers intend to whip data for their personal interests which results in forfeiting of important data [6].
6. **Financial losses due to bankrupting -** Banking related information is stored in computers or online payment methods which can be easily hacked. Attackers try to collect as much as possible data to steal money.
7. **Compromised privacy -** Many malwares succeed in opening the webcam of the personal computers which may result in compromising the privacy of the person.
8. **Annoying Ads open randomly on a computer or mobile screens -** Spywares are designed to collect and steal sensitive data without the user's knowledge. The

spyware creates unexpected popups on the screen, installs other malwares if the link is opened and then infects the whole system.

How to prevent malware attacks?

1. **Update operating system, browsers and plugins -** Always update the operating system of phones and computers. Cybercriminals get a chance to find vulnerabilities in the apps which are not updated and the updates are often released to remove vulnerabilities found in the app.
2. **Do not click on the ads -** The ads that pop up on the screen contains malware which infects the system. Enabling click to play plugins prevent these malicious ads being played directly.
3. **Remove the software which is no longer needed -** Do not use any outdated software as it does not have any patch for vulnerabilities and attacking can be easy.
4. **Do not open spam emails -** Always read emails with an eagle's eye, that means one needs to pay attention before opening any mail. Never trust an email containing any offers from banks or online shopping sites.
5. **Never contact fake tech support members -** Fake companies offer help regarding malware infection and charge money to remove the infections. Do not trust these popup messages as a real security company never offer help through advertisements.
6. **Do not trust the cold callers -** Many people are involved in social engineering, they try to fool people and most of them succeed to gather information or money from innocent people. Never trust a caller claiming he/she is from a bank, Ngo, any trusted company.
7. **Use strong passwords -** Always use those passwords which do not contain any personal information like birthdays or phone numbers. Easy passwords or passwords with personal information can be guessed easily by a hacker. It is best to use difficult passwords and keep changing the passwords.
8. **Log out of websites after use -** Always log out of a website after use. Your account may be vulnerable if it is left logged in, especially in public computers. An attacker can retrieve passwords from session cookies.
9. **Use anti-virus and firewalls -** A firewall can detect malware and make a person aware of it. Therefore, firewalls and anti-virus must be used in any personal computers.
10. **Use secure connections only -** The padlock icon on the left side of the URL indicates that the connection between the person and the server is secure. Make sure that the URL reads "https" and not only "http".

Tools to detect and remove Malwares - There are huge number of anti-malware software in the market but all cannot be trusted as some of them are fake and introduced by fake tech support companies. We have investigated and listed below the most reliable anti malware software [7].

1. **Hitman pro -** Hitman pro belongs to Sophos Security and is famous as second opinion scanner. It uses its personal database with some popular antiviruses like Kaspersky, Emisoft and Bitdefender. Hitman pro is very fast with scanning power of 4 scanners. It detects and scans the suspected files by scanning through cloud technology.
   It provides 30 days free usage and after that demands money for use. It is a portable scanner or can be installed in the computer. It is compatible with any antivirus protection pre-installed on the computer. It effectively removes Malware, Adware, Virus and any unwanted programs. Hitman pro is the best option for real time protection.
2. **Malware bytes Antimalware -** Malware bytes is a free of cost Antimalware software. It also provides option for paying for real time protection where it works in the background defending the system from any malware trying to enter the system. New version of Malwarebytes 3 includes some features like Ransomware protection, Web protection, exploit protection etc. and is compatible with any existing antivirus software in the system.
3. **Zemana Antimalware -** Zemana Antimalware is a new version of Zemana Antilogger. It is effective against malware and adware. It is a powerful cleaner with AV scanning based on Cloud. It is a tough competition for Hitmanpro and Malwarebytes. It offers 15 days free trial for cleaning the infections and a paid subscription for real time protection.
4. **Emisoft Antimalware -** Bitdefender and Emisoft's own AV engine database are used by Emisoft antimalware for scanning and blocking malicious programs, making it a good behavioral blocking software. Surf protection, Behavior blocker, Real time file guard etc are the features of Emisoft antimalware. It offers 30 days free trial. It is costlier than Hitmanpro and Malwarebytes antimalware but has an advantage of becoming cheaper while renewing reward points. Promos given by the company can be used time to time.
5. **Malicious Software Removal tool by Microsoft -** Microsoft's Window's Software removal tool is effective in removing popular malwares but it lacks behavioral based protection. It is updated in every month to remove newly detected malwares.
6. **Nortan Power Eraser by Symantec -** Norton Power Eraser can scan deeply and remove any malware, adware, crimeware etc. which cannot be detected by any traditional antivirus. It is mainly designed for scam-ware ads. It can remove some legitimate programs because of its aggressive nature, but has an option to undo changes.

IV. CONCLUSION

Malwares can harm the systems very badly, but we need to protect our systems and data from these malwares. In order to prevent from malwares, we must use antimalware and antiviruses and safeguard our devices as well as confidential data stored in our devices. Other than the tools, we should

spread awareness and follow some basic rules to avoid these malwares.

V. REFERENCES

[1]. Definition of malware, https://en.wikipedia.org/wiki/Malware
[2]. Rootkit, https://antivirus.comodo.com/blog/computer-safety/what-is-rootkit/
[3]. Trojan, https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html
[4]. RAT Definition, https://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan
[5]. Types of RAT,https://www.darkreading.com/perimeter/the-7-most-common-rats-in-use-today-/a/d-id/1321965
[6]. Effects of malware, https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/#scenario5
[7]. Best antimalware, https://www.techsupportall.com/best-free-effective-anti-malware-software/
[8]. Lobo, D., Watters, P., Wu, X.W. and Sun, L., 2010, July. Windows rootkits: Attacks and countermeasures. In *2010 Second Cybercrime and Trustworthy Computing Workshop*(pp. 69-78). IEEE.
[9]. Rieck, K., Holz, T., Willems, C., Düssel, P. and Laskov, P., 2008, July. Learning and classification of malware behavior. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 108-125). Springer, Berlin, Heidelberg.
[10]. Jiang, D. and Omote, K., 2015, March. An approach to detect remote access trojan in the early stage of communication. In *2015 IEEE 29th International Conference on Advanced Information Networking and Applications* (pp. 706-713). IEEE.