Remote Access Tool Using Metasploit

Prakhar Ahlawat, Sushant Dhar, Samruddha Wagh, Amit Koppad
Student, Dept of Computer Engg
MCT’s Rajiv Gandhi Institute Of TechnologyMumbai, India
prakhar_ahlawat@yahoo.co.in, sushantdhar.sd@gmail.com, samruddhawagh@gmail.com, amit.koppad513131@gmail.com

Abstract—A Remote Access Trojan (otherwise known as a RAT) is a piece of software designed to provide full access to a remote client. Capabilities of such a software often include: keystroke logging, file system access and remote control of the client with all the peripheral devices it is connected to, such as microphones and webcams. RATs are designed as legitimate administrative tools, yet due to their extensive capabilities are often seen used with malicious intent. The most common means of infection is through email attachments. The server is cleverly disguised as a significant software and positioned in peer-to-peer file sharing networks, or unauthorized download websites. The developer of the virus usually uses various spamming techniques in order to distribute the virus to unsuspecting users. In this paper, our objective is to demonstrate how we can create our own RAT software/Trojan followed by a detailed explanation of the construction, deployment and working of the RAT software. The biggest advantage about creating your own RAT is that it is fully undetectable and you can add whichever features you desire.

Keywords--*RAT*

*****

I. Introduction

RATs (Remote Access Tools) are types of backdoor through which an attacker can take remote control of the system.These RAT applications are installed on the victim and attacker computer. The RAT server is installed on the victim and RAT client is present on the attacker’s computer, thus the attacker can connect to the server (victim). RAT Trojans can generally do the following: Block mouse and keyboards, downloads, processes, uploads, delete and rename files, format drives, play sounds, shutdown, restart, log-off monitor, etc. The log file created by the key logger can then be sent to a specified receiver.

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. But, both can

also reside on the same computer, for testing purposes. After connection is established, the client will send a command to the server. Upon receiving the command, the server will execute it.

The command could be, to display the message “Hello World” , beep, eject the CD, shutdown, reboot, activate a device on the parallel/serial port, and all commands that could ordinarily be executed by a user sitting in front of a computer. The server program can also send back messages to the client. Two-way communication can take place. A Remote Access Trojan (otherwise known as a RAT) is a piece of software designed to provide full access to a remote client. Capabilities of such a software often include: keystroke logging, file system access and remote control of the client with all the peripheral devices it is connected to, such as microphones and webcams. RATs are designed as legitimate administrative tools, yet due to their extensive capabilities are often seen used with malicious intent. The most common means of infection is through email attachments. The server is cleverly disguised as a significant software and positioned in peer-to-peer file sharing networks, or unauthorized download websites. The developer of the virus usually uses various spamming techniques in order to distribute the virus to unsuspecting users. In our project, our objective is to demonstrate how we can create our own RAT software/Trojan followed by a detailed explanation of the construction, deployment and working of the RAT software. The biggest advantage about creating your own RAT is that it is fully undetectable and you can add whichever features you desire. A **remote administration tool** (RAT) is a piece of software or programming that allows a **remote** "operator" to control a system as if they have physical access to that system. While desktop sharing and **remote administration** have many legal uses, "RAT" software is usually associated with criminal or malicious activity.

II. ANALYSIS

The proposed idea for infection of the malicious server program is by encapsulating it inside a deceivingly harmless game/music file or any executable file. This is done by attaching our server program as a payload to another file.Remote access tools (RATs) may be the hacker’s equivalent of training wheels.

Remote access tools (RATs) may be the hacker’s equivalent of training wheels, as they are often regarded in IT security circles. But dismissing this common breed of malware could

be a costly mistake. Despite their reputation as a software toy for novice "script kiddies," RATs remain a linchpin of many sophisticated cyber attacks.

Requiring little technical savvy to use, RATs offer unfettered access to compromised machines. They are deceptively simple—attackers can point and click their way through the target's network to steal data and intellectual property. But they are often delivered as key component of coordinated attacks that use previously unknown (zero-day) software flaws and clever social engineering.

Remote Access Tool is a piece of software used to remotely access or control a computer. 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.

RAT can also be called as a synonym for backdoor, which includes a client and server program. The server or the stub program, if installed in the compromised system unknowingly by the owner of that system, then it is called as a Remote Access Trojan.

Remote Administration Trojans (RATs) are malicious pieces of software and infect the victim's machine to gain administrative access. They are often included in pirated software through patches, as a form of cracked game or E-mail attachments. After the infection, it may perform unauthorized operations and hide their presence in the infected system. An attacker can remotely control the system by gaining the key logs, webcam feeds, audio footage, screen captures, etc.This paper presents a general overview on evolution of concealment methods in computer viruses and defensive techniques employed by anti-virus products. In order to stay far from the anti-virus scanners, computer viruses gradually improve their codes to make them invisible. On the other hand, anti-virus technologies continually follow the virus tricks and methodologies to overcome their threats victim gets infected without his/her knowledge and avoid any further suspicions or be ultimately detected. Since the program is coded by ourselves, 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-servers may be named as software patches or games with the corresponding binders, tricking users into downloading, un-bundling, and finally, executing such malicious programs.

III. PROPOSED SYSTEM

Proposed system for remote access trojan will have a wide range of functions like downloading a file, uploading, deleting files, formatting drives, opening CD-ROM tray, accessing various other peripherals and other endless utilities. The system will be using a reverse connection which will help in establishing connection between the Server and Client programs. Various infection methodology will be used for infecting the victim's machine with server program. Some of these methods are; a java driveby, sending the server program over the mail, downloading a game infected with the server program as the payload or even sending a link through an Instant Messaging service or even with the help of a rubber ducky USB drive.

IV. METHODOLOGY

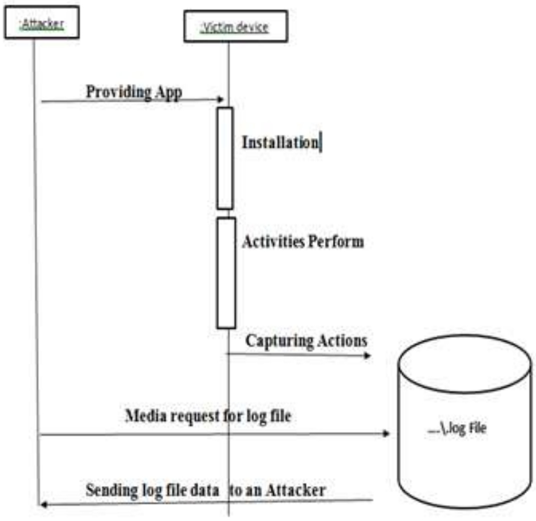

Figure 1. Activity Diagram

For the implementation of this tool we mainly require Kali Linux 2016.2 , Metasploit, IExpress.

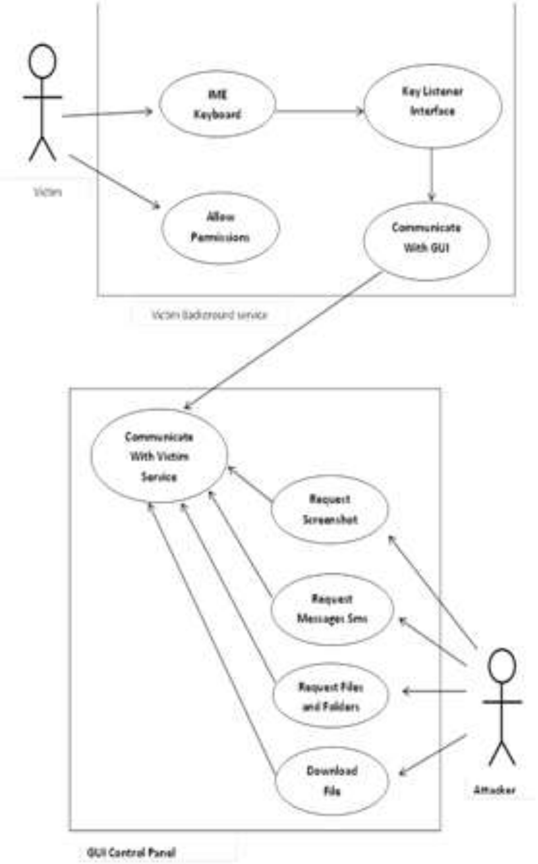

Figure 2. Use Case Diagram

Phase 1 includes coding the two programs required for the project, namely- Client and Server programs. The Client program has functionalities which include listening for connection for active servers, relaying the appropriate commands to the server and implementing a Graphical User Interface for the attacker's convenience. The Server program's functionalities include trying to establish connection with the client whenever the computer is connected to the internet, 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 using different machines, the victim's computer and the attacker's. To prevent being blocked by the firewall, we use reverse connection methodology to establish connection.

A reverse connection is usually used to bypass firewall restrictions on open ports. A firewall usually blocks incoming connections on open ports, but does not block outgoing traffic. In a normal forward connection, a client connects to a server through the server's open port, but in the case of a reverse connection, the client opens the port that the server connects to. The most common way a reverse connection is used is to bypass firewall and router security restrictions.[7]

The server, which runs in the background of the victim's machine sends a connection request to the attacker, whenever the victim's machine is online and connected to the internet. The client (attacker) is constantly online, listening for active servers.

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 machine.

Phase 3 involves devising a proper, foolproof way to make sure that our victimgets infected without his/her knowledge and avoid any further suspicions or beultimately detected. Since the program is coded by ourselves, it is less likely tobe detected by any Antivirus as its signature will not be present in the Database of the Antivirus. Prior to being delivered, RAT-servers may be named as software patches or games with the corresponding binders, trickingusers into downloading, un-bundling, and finally, executing such malicious programs.The proposed idea for infection of the malicious server program is byencapsulating it inside a deceivingly harmless game/music file. This is done by attaching our server program as a payload to another file.

V TEST RESULTS

We tried making the payload FUD (Fully undetectable) but it was detected and eradicated by Windows defender 9/20 times. Once the payload is breached into the system, the success rate of setting up a session is 15/15. Once a the session is set up, the keylogging worked 8/9 times and the shutdown command worked 11/11 times.

VI CONCLUSION

We simply described a method that can be used to break the security provided any Operating system. These operating systems provided different permissions so any application can access machine data and access, but normally no one reads all permissions nor safeguards their machine. So using this mentality we implemented this Ratin Linux, it 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, hence we suggest users, please be careful and safe.

VI ACKNOWLEDGEMENT

We wish to express our sincere gratitude to Dr. U. V. Bhosle, Principal and Dr. Satish. Y. Ket, H.O.D of Computer Department of RGIT for providing us an opportunity to do our project work on "Remote Access Tool".

This project bears on imprint of many people. We sincerely thank our project guide Mr. Gautam M. Borkar for his guidance and encouragement in successful completion of our project work.

We would also like to thank our staff members for their help in carrying out this project work.

Finally, we would like to thank our colleagues and friends who helped us in completing the project successfully

REFERENCES

[1] Rad, BabakBashari, Maslin Masrom, and Suhaimi Ibrahim. "Evolution of computer virus concealment and anti-virus techniques: a short survey." *arXiv preprint arXiv:1104.1070* (2011).

[2] Thimbleby, H., Anderson, S. and Cairns, P., 1998. A framework for modelling trojans and computer virus infection. *The Computer Journal*, *41*(7), pp.444-458.

[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] Paul Chin. "How to Write Your Own Remote Access Tools in C#"

[5] Areej Mustafa Abuzaid ,MadihahMohd Saudi, Bachok M Taib and ZulHilmi Abdullah. "An Efficient Trojan Horse Classification (ETC)". IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 3, March 2013

[6] Provos, Niels, Dean McNamee, Panayiotis Mavrommatis, Ke Wang, and Nagendra Modadugu. "The Ghost in the Browser: Analysis of Web-based Malware." HotBots 7 (2007): 4-4.

[7] Gordon, Sarah, and David Chess. "Attitude Adjustment: Trojans and Malware on the Internet."

[8] Bishop, M., ―An Overview of Computer Viruses in a Paper Environment‖, p. 1-32, Technical Report: PCS-TR91-156-1999.

[9] Danchev, D. ,‖The Complete Windows Trojans‖, cited; Available from: http://www.windowsecurity.com/whitepapers/The_Complete_Windows_Trojans_Paper.html. Aug 29, 2005.

[10] Trojan Programs. cited; Available from: http://www.viruslist.com/en/virusesdescribed?chapter=152540521, Oct 20,2010.