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: Windows

Hardik Vyas[1], Dr. Ravi Sheth[2]
[1]Student Master in Technology Cyber Security, [2] Assistant Professor Raksha Shakti University
[1]Department of Information Technology and Telecommunication, Raksha Shakti University

Abstract**: Remote Access Trojan (RAT) allowing a potentially malicious user to remotely control the system. RAT is remote control software that when installed on a computer allows remote computer to take control of it. RAT allows an attacker/intruder to remotely control a computing system and usually consists of a server silently running and listening to particular TCP/UDP ports on a victim machine as well as a client acting as the bridge between the server and the attacker. The most common (popular) means of infection is through email attachments. Malware developers use chat software as another way to distribute their Trojan horse viruses such as Yahoo Messenger and Skype. These developers usually use various spamming techniques in order to distribute the virus to unsuspecting users. Remote Administration Trojans are malicious (harmful) pieces of code often embedded in lawful programs through RAT-sanction procedures. They are stealthily planted and help achieve access of victim machines, through patches, games, E-mail attachments, or even in legitimate-looking binaries. Once installed, remote access Trojan perform their unexpected or even unauthorized operations and use an array of techniques to hide their traces to remain invisible and stay on victim systems for the long haul. In this paper we are going to discuss about how an antivirus detects a malware and how we will be designing a remote access Trojan which would bypass the antivirus which can be used by law enforcement agencies for spying on suspicious persons.
Keywords: Remote Access Trojan, Windows, Compromised System, Client, Server

I. INTRODUCTION

Malware or malicious software is any program 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.). A Trojan horse 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 capabilities of backdoor Trojans are to gather information, terminate or run a task or process, download and upload files. On Windows computers, three tools are commonly used by intruders to gain remote access to ones computer are: 1. BackOrifice, 2. NetBus, and Sub Seven.

Java combines both the approaches of interpretation and compilation. Firstly, java compiler compiles the source code into bytecode. At the run time, Java Virtual Machine (JVM) interprets this bytecode and generates machine code which will be directly executed by the machine in which java program runs. So java is both compiled and interpreted language.

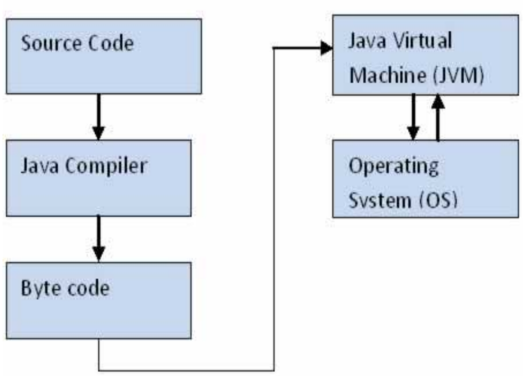

Fig. 1 Java Architecture

A. Java Virtual Machine (JVM)

It is a component which provides an environment for running Java programs. JVM interprets the bytecode into machine code which will be executed by the machine in which the Java program runs.

B. Java is Platform Independent

Platform independence is one of the most important advantages of Java language. In other words, java is portable because the same java program can be executed in multiple platforms without making any changes in the source code. One just needs to write the java code for one platform and the same program will run in any platforms. Java makes this possible by, first the Java code is compiled by the Java compiler and generates the bytecode. This bytecode will be stored in class files**.** Java Virtual Machine is exclusive for each platform. Though Java Virtual Machine is unique for each platform, all interpret the same bytecode and convert it into machine code required for its own platform and this machine code will be executed by the machine directly in which java program runs. This makes Java platform independent and portable.

II. TECHNIQUES USED BY ANTIVIRUS IN DETECTING MALWARE

A. Signature Based Detection

This uses key aspects of an examined file to create a static fingerprint of known malware. The signature would represent a series of bytes in the file. It would also be a cryptographic hash of the files. This method of detecting malware has been a necessary aspect of antivirus tools since their beginning; it remains a part of many tools to date, though its importance is withdrawing.

Restriction of signature-based detection is that, by itself, this method is unable to flag malicious files for which signatures have not yet been developed. With this in mind, modern attackers frequently mutate their creations to retain malicious functionality by modifying the file's signature.

B. Heuristic Based Detection

Heuristics-based detection aims at broadly detecting new malware by statically examining files for suspicious characteristics without an exact signature match. For example, an antivirus tool might look for the presence of rare instructions or junk code in the examined file. This may also emulate running the file to see what would happen if executed, attempting to do this without noticeably slowing down the system. A single doubtful attribute might not be enough to alter the file as malicious. However, several such individuality might exceed the expected risk threshold, leading the tool to classify the file as malware. The biggest downside of heuristics is it can often create false positives.

C. Behavioral Based Detection

Behavioral detection observes how the program executes, rather than just emulating its execution. It attempts to recognize malware by looking for malicious behavior's, such as modifying the hosts file or observing keystrokes. Observing such actions allows an antivirus tool to detect the occurrence of previously unseen malware on the protected system.

As with heuristics, each of these actions by itself might not be enough to classify the program as malware. However, taken together, they could be pinpointing of a malicious program. The use of behavioral techniques brings antivirus tools closer to the category of host intrusion prevention systems, which have traditionally existed.

D. Sandbox Detection

This is a behavioral based detection technique which executes the programs in a virtual environment, as contrasting to detecting its fingerprint at run time. Antivirus software that come with this type of detection abilities execute programs in a detach, virtual environment, and log the actions it performs to decide whether the programs are spiteful or not. If it is safe, then the given program is executed in the real environment. This technique is both slow and heavy, and its resource intensive nature means that it is rarely used in consumer antivirus solutions.

E. Cloud Based Detection

This identifies malware by gathering data from protected computers while analyzing it on the provider's infrastructure, instead of performing the analysis locally. This is usually done by gathering the relevant details about the file and the background of its execution on the endpoint, and providing them to the cloud engine for processing. The local antivirus agent only needs to carry out minimal processing. Moreover, the vendor's cloud engine can obtain patterns related to malware characteristics and behavior by correlating data from numerous systems. In distinction with other antivirus components base decisions mostly on locally observed attributes and behaviors. A cloud-based engine allows different users of the antivirus tool to benefit from the experiences of other members of the community.

III. JAVA BASED REMOTE ACCESS TROJAN

A. CrossRAT

CrossRAT is a cross-platform remote access Trojan which aims all four popular desktop operating systems, Windows, Linux, Solaris, and macOS, enabling remote attackers to take screenshots, manipulate the file system, and gain persistence on the infected systems.

According to researchers, Dark Caracal (hackers) don't depend on any "zero-day exploits" to share out its malware; instead, they uses basic social engineering via posts on (Facebook) groups and (WhatsApp) messages, cheering users to visit hackers-controlled fake websites and download malicious applications.

It is developed using Java programming language, making it easy for reverse engineers and researchers to decompile it.

CrossRAT 0.1 — Cross-Platform Persistent Surveillance Malware

Once it runs on the targeted system, the hmar6.jar first checks the operating system (OS) it is running on and then installs itself accordingly. Besides this, the CrossRAT embed also attempts to collect information about the infected system, including the installed OS version, kernel build and architecture. Moreover, for Linux systems, the malware attempts to query system files to determine its distribution, like Centos, Debian, Kali Linux, Fedora, and Linux Mint, among many more.

CrossRAT then implements OS specific perseverance mechanisms to automatically (re)executes whenever the tainted system is rebooted and register itself to the C&C server, allowing remote attackers to send command and exfiltrate data. As reported by Lookout researchers, CrossRAT variant circulated by Dark Caracal hacking group connects to '*flexberry(dot)com*' on port 2223, whose information is hardcoded in the 'crossrat/k.class' file.

This malware was planned with some fundamental surveillance capabilities, which gets activated only when received respective predefined commands from the (C&C) server.

Interestingly, CrossRAT has also been programmed to use 'jnativehook,' an open-source Java library to listen to keyboard and mouse events, but the malware does not have any predefined command to activate this keylogger

B. Adwind

The Adwind trojan, also referred as AlienSpy, Frutas, Unrecom, Sockrat, JSocket and jRAT, is a remote access tool (RAT) exposed as Frutas in 2012. The adwind backdoor is written in Java allowing it to run on numerous platforms including Windows, Mac OS, Linux, and Android. Adwind can allow an attacker to control the device remotely, exfiltrate data, gather data and move laterally in the network. Attackers can log keystrokes, steal credentials, take screenshots, take pictures and record from a web camera, record sounds from a microphone, transfer files, collect system information, steal cryptographic keys, manage SMS on Android, and steal VPN credentials. It is mainly used by cybercriminals in opportunistic attacks, distributed through spam. The trojan is not self-infecting or self-replicating, it requires victim interaction. Kaspersky estimated the number of total victims from 2013 to near the beginning of 2016 at about 443,000 located various countries, including the United States. JSocket RAT is currently available for purchase on its website for $30 for a one-month license and $200 for an unlimited license Adwind is written in Java.

In March, 2017 Kaspersky Lab reported more than 1,500 organizations in over 100 countries and territories were infected with the Adwind trojan. The retail and distribution sectors make up the majority of those targeted at 20.1 percent. Attackers sent victim's phishing emails purportedly from HSBC Advising Service, from the mail.hsbcnet.hsbc.com domain, with a "payment advice" attachment. If the ZIP file is opened, the Adwind trojan installs itself and attempts to communicate with its command and control (C2) server. If the machine is successfully compromised, the attacker gains roughly complete control over the device and can send sensitive data collected back to its C2 server.

C. Infection Chain of Adwind:

Adwind RAT used to extend via spam campaign containing malicious URL and distribution of the malware increased by 107% since the starting of 2017.

Trend Micro Researchers Detected this RAT as JAVA_ADWIND and its has Many sophisticated aliases functions including jRAT, Universal Remote Control Multi-Platform (UNRECOM), AlienSpy, Frutas, and JSocket.

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

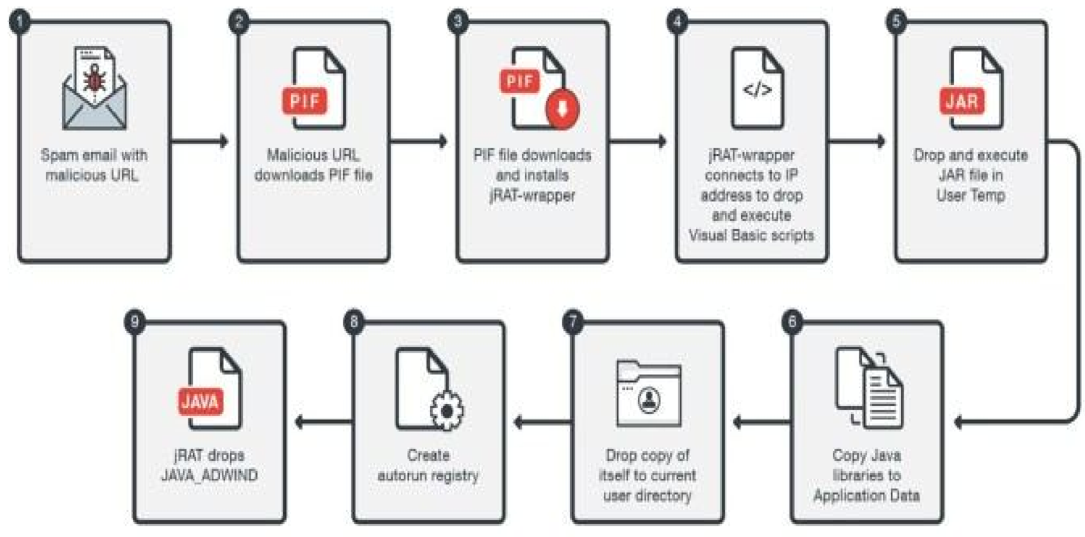

Fig. 2 Infected Chain

Adwind identified by two waves, first one contains malware equipped with spyware capabilities which divert the Victims using a different URL. Second one uses a dissimilar domains that hosted their malware and command and control (C&C) servers which were identified in June 14, 2017.

The malicious URL will drop a Program Information file (PIF). PIFs enclose information on how Windows would run MS-DOS applications, and can be started normally like any executable (EXE). This file is written in .NET and serves as a downloader. The process by the file kicks off the infection chain by first changing the system certificate.

While on initial stage of infection, it checks the systems internet access. The end of the process was a particularly useful feature in Java that enables developers to dynamically inspect, call, and instantiate attributes and classes at runtime. In cyber criminal hands, it can be ill-treated to evade static analysis from traditional antivirus (AV) solutions.

Adwind has the ability to:

1) collect keystrokes
2) take screenshots
3) record sound from a microphone
4) transfer files
5) collect general system and user information
6) steal VPN certificates

Manage SMS (for Android devices)

IV. PROBLEM STATEMENT

After going through various malware, we came to know Trojan horse is widely used malware. It disguises itself as a normal program to trick users into installing the malware. It can give remote access of an infected system computer. We even came to know that there are various Trojan developed using java language, but none of them are Fully Undetectable.

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 all of them have been detected by the antivirus.

V. PROPOSED METHOD

We are going to develop a Remote Access Trojan using java language, as with java we can target any operating system, but in this case we would particularly target windows operating system. We would be developing a fully undetectable remote access Trojan which would bypass the windows defender, along with the antivirus. This Remote Access Trojan which we are creating would compromise any existing rat and our addition to that rat making it bypass the windows defender and the antivirus. This Trojan which we are creating can be used by law enforcement agencies to spy on people whom they find suspicious.

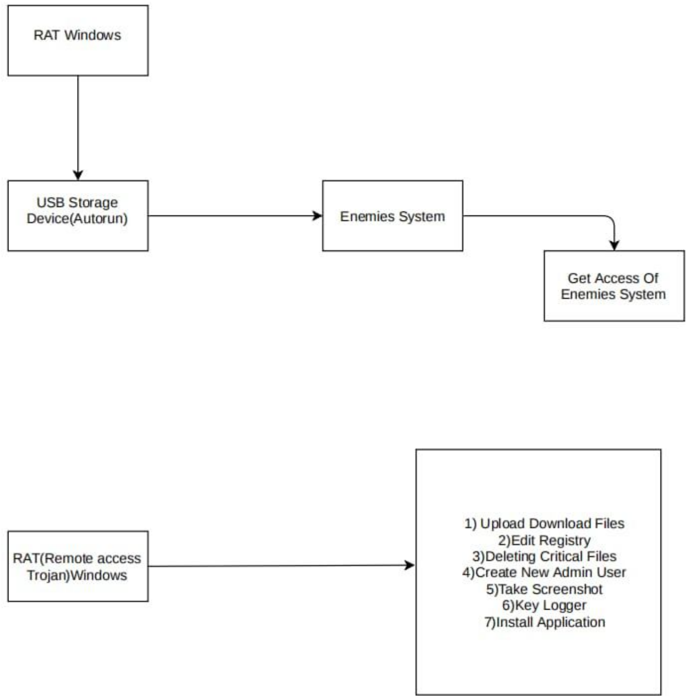

Fig. 3 Flowchart

VI. CONCLUSION

We have described a method of creating a Remote Access Trojan in windows using Java language 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. We see many people tend to click on links or tend to download content from third party without verifying them. So using this mentality we have implemented this remote access Trojan, which creates the security issue, best solution for this issue is that user updates its system regularly, don't click on any unknown links, regular patches should be done by the user, along with that user should scan his/her system regularly.

REFERENCES

[1] Common Malware Types: Cybersecurity 101. URL: https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101
[2] Malware. URL: https://searchsecurity.techtarget.com/definition/malware
[3] Malware. URL: https://en.wikipedia.org/wiki/Malware
[4] Manjeri N Kondalwar, Prof. C.J.Shelka. "Remote Administrative Trojan/Tool (RAT)". International Journal of Computer Science and Mobile Computing, Vol.3 Issue.3, March- 20114, pg 482-487
[5] Java Architecture. URL: https://www.careerbless.com/java/basics/JavaArchitecture.php
[6] CrossRAT. URL: https://thehackernews.com/2018/01/crossrat-malware.html
[7] Cross-platform Remote Access Trojan "Adwind" Steal Credentials, Record and Harvest keystrokes the Aerospace Industries Data. URL: : https://gbhackers.com/cross-platform-remote-access-trojan-adwind-targeting-steal-credentials-record-harvest-keystrokes-aerospace-industries/
[8] What it can do? URL: https://www.kaspersky.co.in/resource-center/threats/adwind
[9] Adwind. URL: https://www.cyber.nj.gov/threat-profiles/macos-malware-variants/adwind?rq=adwind