Chapter 7: Malware Threats

Technology Brief

Malware

Malware is abbreviated from the term Malicious Software. The term malware is an umbrella term that defines a wide variety of potentially harmful software. This malicious software is specially designed for gaining access to target machines, stealing information and harm the target system. Any software is having malicious intention like damaging, disabling or limiting the control of the legitimate owner and providing control of the target system to the developer of malware or an attacker, or any other malicious intent can be considered as Malware. Malware can be classified into various types including Viruses, Worms, Keyloggers, Spywares, Trojans, Ransomware and other malicious software. Malware is the most critical, prominent, emerging problem now a day. Malicious software classified as Viruses and Worm have some older techniques whereas Malware has some new techniques which makes them more dangerous.

Malware Propagation ways

There are different ways that malware can get into a system. Users should be careful while interacting with these methods. Some of these methods that are popularly used to for the propagation of malware are: -

- ***Free Software***

When software is available on the internet for free, it mostly contains additional software and applications which may belong to the offering organization bundled later by any third party to propagate this malicious software. Most common example of free software is like downloading crack files usually contains additional malicious software, or sometimes it only contains a malware.

- ***File Sharing Services***

File sharing services such as torrent and Peer-to-peer file sharing services transfer the file from multiple computers. During the transfer, the file can be infected, or any infected file may additionally transfer with the transfer because there may be a computer having low, or no security policy.

- ***Removable Media***

Malware can also propagate through removable media such as USB. Various advance Removable media malware is introduced which can propagate through Storage area of USB as well as through Firmware embedded in the hardware. Apart from USB, External hard disk, CD, DVD can also bring malware along with them.

- ***Email Communication***

In an organization, email communication is the most popularly- used way of communication. Malicious software can be sent through email attachment, Email containing malicious URL.

- ***Not using Firewall and Anti-Virus***

Disabling Security Firewalls and Anti-virus programs or not using Internet security software can also allow the malicious software to be download on a system. Anti-virus and Internet security Firewalls can block malicious software from downloading automatically and alert upon detection.

Trojan Concept

Trojan Horse and Trojan are the malicious programs which mislead from its actual intentions. This term is actually derived from a Greek story of a great Wooden horse. This horse had soldiers hiding inside waiting to enter into the city. As this wooden horse reached in the city, soldiers came out and attacked the city.

With this philosophy, Trojan software misleads from its true intentions and wait for best time to attack. These Trojan may provide access to personal information, as well as unauthorized access to the attacker. The trojan can also lead to infection of other connected devices across a network.

Trojan

A Malicious Program misleading the user about its actual intention is classified as Trojan. Trojans are typically spread by Social Engineering. The purpose or most common use of Trojan programs are: -

- Creating back door
- Gaining Unauthorized Access
- Steal Information
- Infect Connected Devices
- Ransomware Attacks
- Using Victim for Spamming
- Using Victim as Botnet
- Downloading other malicious software
- Disabling Firewalls

Port Number	Port Type	Trojans
2	TCP	Death
20	TCP	Senna Spy
21	TCP	Blade Runner / Doly Trojan / Fore / Invisble FTP /

		WebEx / WinCrash
22	TCP	Shaft
23	TCP	Tiny Telnet Server
25	TCP	Antigen / Email Password Sender / Terminator / WinPC / WinSpy
31	TCP	Hackers Paradise / Masters Paradise
80	TCP	Executor
421	TCP	TCP Wappers Trojan
456	TCP	Hackers Paradise
555	TCP	Ini-Killer / Phase Zero / Stealth Spy
666	TCP	Satanz backdoor
1001	TCP	Silencer / WebEx
1011	TCP	Doly Trojan
1095-1098	TCP	RAT
1170	TCP	Psyber Stream Server / Voice
1234	TCP	Ultors Trojan
10000	TCP	Dumaru.Y
10080	TCP	SubSeven 1.0-1.8 / MyDoom.B
12345	TCP	VooDoo Doll / NetBus 1.x, GabanBus, Pie Bill Gates, X-Bill
17300	TCP	NetBus
27374	TCP	Kuang2 / SubSeven server (default for V2.1-Defcon)
65506	TCP	SubSeven
53001	TCP	Remote Windows Shutdown
65506	TCP	Various names: PhatBot, Agobot, Gaobot

Table 7-01 Known Ports used by Trojans

Trojan Infection Process

The infection process using a Trojan is comprised of some steps. This combination of steps is taken by an attacker to infect the target system.

1. Creation of a Trojan using Trojan Construction Kit.
2. Create a Dropper.
3. Create a Wrapper.
4. Propagate the Trojan.
5. Execute the Dropper.

Trojan Construction Kit

Trojan Construction Kit allow the attacker to create their own Trojans. These customized Trojans can be more dangerous for the target as well as an attacker if it is not executed properly or backfires. These customized Trojans created by using Construction kits can avoid detection from virus and Trojan scanning.
Some Trojan Construction Kits are: -

- Dark Horse Trojan Virus Maker
- Senna Spy Generator
- Trojan Horse Construction Kit
- Progenic mail Trojan Construction Kit
- Pandora's Box

Droppers

A dropper is a software or program that is specially designed for delivering a payload on the target machine. The main purpose of Dropper is to install malware codes on to the victim's computer without alerting and avoiding detection. It uses various methods to spread and install malware.

Trojan-Dropper Tools

- TrojanDropper: Win32/Rotbrow.A
- TrojanDropper: Win32/Swisyn
- Trojan: Win32/Meredrop
- Troj/Destover-C

Wrappers

It is a non-malicious file that binds the malicious file to propagate the Trojan. Basically, Wrapper binds a malicious file in order to create and propagate the Trojan along with it to avoid detection. Wrappers are often popular Executable file such as games, music and video files, as well as any other non-malicious file.

Crypter

A Crypter is software used while creating Trojans. The basic purpose of Crypter is it encrypt, obfuscate, and manipulate the malware and malicious programs. By using Crypter for hiding a malicious program, it becomes even more difficult for security programs such as anti-viruses to detect. It is popularly used by hackers to create malware which is capable of bypassing security programs by presenting itself as a non-malicious program until it gets installed.

Some of the available Crypter to hide malicious programs are: -

- Cryogenic Crypter
- Heaven Crypter
- Swayz Cryptor

Deployment of Trojan

The Deployment process to a Trojan is simple. An Attacker uploads the Trojan on a server where it can be downloaded immediately when the victim clicks on the link. After uploading the Trojan on the server, Attacker sends an email containing a malicious link. When the victim receives this spam email, which may be offering something he is interested in and clicks the link, it will connect it to Trojan Server and download the Trojan on victim PC. Once Trojan is installed on victim's PC, it will connect the attacker to the victim by providing unauthorized access or extract secret information or perform a specific action for which Trojan is designed for.

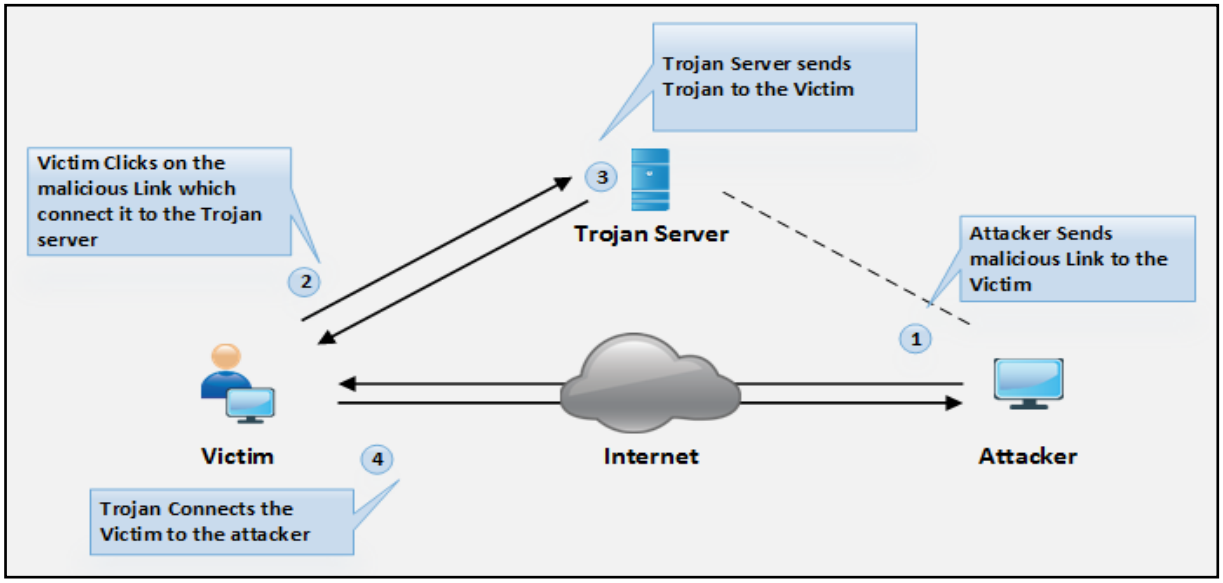


Figure 7-01 Linux Log Directory

Types of Trojans

- ***Command Shell Trojans***

Command Shell Trojans are capable of providing remote control of Command Shell of a victim. Trojan Server of Command Shell Trojan such as Netcat is installed on the target machine. Trojan Server will open the port for command shell connection to its client application, installed on attacker's machine. This Client Server based Trojan provide access to Command line.

- ***Defacement Trojans***

Using Defacement Trojan, Attacker can view, edit and extract information from any Windows program. Using this information attacker replaces the string, images, and logos often to leave their mark. Using User-Styled Custom Application (UCA), attacker defaces programs. Website Defacement is most popularly known; it is the same concept on applications running on the target machine.

- ***HTTP/HTTPS Trojans***

HTTP and HTTPS Trojans bypasses the firewall inspection and execute on the target machine. After execution, they create HTTP/ HTTPS tunnel to communicate with the attacker from victim's machine.

- ***Botnet Trojans***

A botnet is the large scale of the compromised system. These compromised systems are not limited to a specific LAN; they may be spread over the large geographical area. These Botnets are controlled by Command and Control Center. These botnets are used to launch attacks such as Denial of Service, Spamming and other.

- ***Proxy Server Trojans***

Trojan-Proxy Server is standalone malware application which is capable of turning the host system into a proxy server. Proxy Server Trojan allows the attacker to use victim's computer as a proxy by enabling the proxy server on victim's system. This technique is used to launch further attacked by hiding the actual source of the attack.

- ***Remote Access Trojans (RAT)***

Remote Access Trojan (RAT) allows the attacker to get remote desktop access to victim's computer by enabling Port which allows the GUI access to the remote system. RAT includes a back door for maintaining administrative access and control over the victim. Using RAT, an attacker can monitor user's activity, access confidential information, take screenshots and record audio and video using a webcam, format drives and alter files, etc.

The following are the list of RAT tools: -

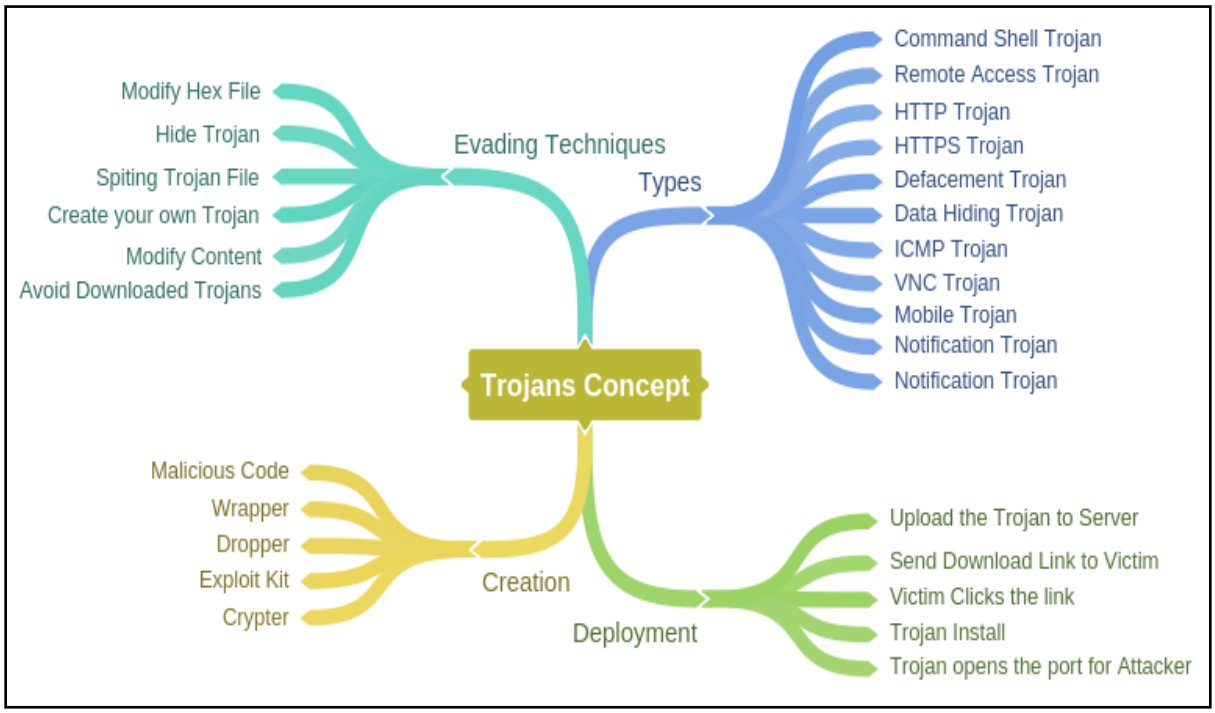
- Optix Pro
- MoSucker
- BlackHole RAT
- SSH-R.A.T
- njRAT
- Xtreme RAT
- DarkComet RAT
- Pandora RAT
- HellSpy RAT
- ProRat
- Theef

Some other types of Trojans are: -

- FTP Trojans
- VNC Trojans
- Mobile Trojans
- ICMP Trojans

- Covert Channel Trojans
- Notification Trojan
- Data Hiding Trojan

Mind Map

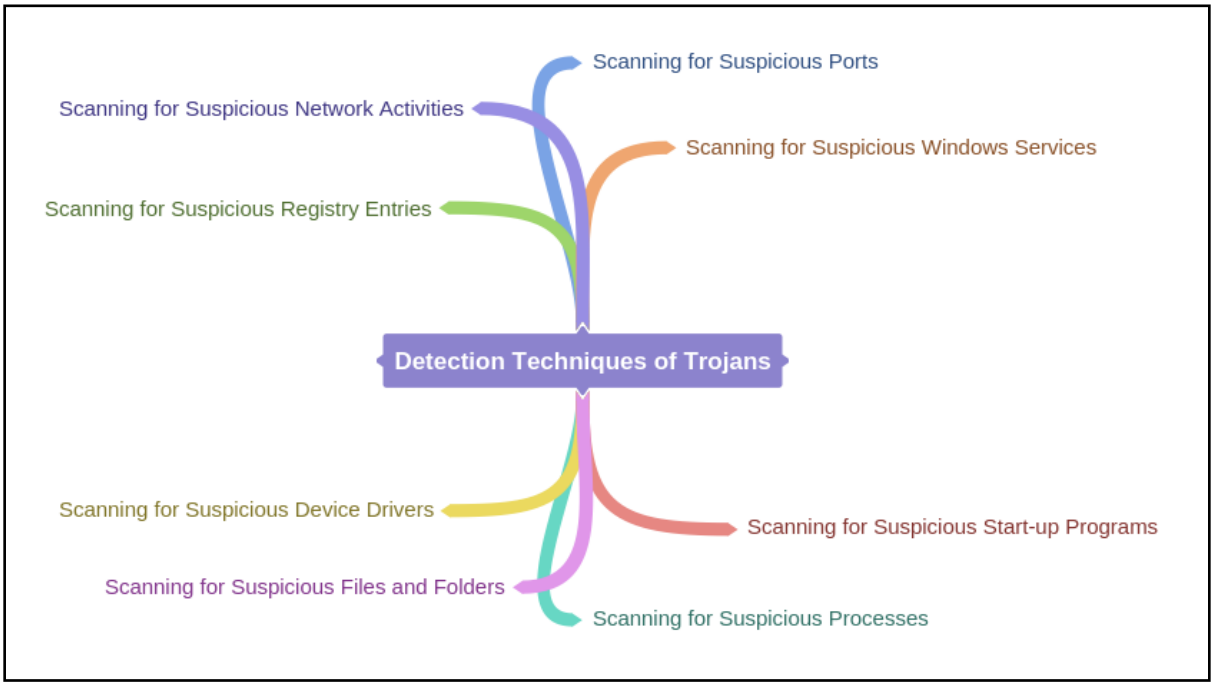


Trojan Countermeasures

A network or a system can be protected, or protected from most of the Trojans if it is following the countermeasures to prevent Trojan attacks. The following are some key countermeasure that are recommended to prevent these attacks and protect your system.

- Avoid to Click on Suspected Email Attachments
- Block unused ports
- Monitor Network Traffic
- Avoid Download from Untrusted Source
- Install Updated Security software and Anti-viruses
- Scan removable media before use
- File integrity
- Enable Auditing
- Configured Host-Based Firewall
- Intrusion Detection Software

Detection Techniques for Trojans



Virus and Worms Concepts

Viruses are the oldest form of the malicious program; it was first introduced in 1970. In this section, we will discuss the virus and worms, how viruses are classified to be different from other malicious programs, how to create viruses and how does virus infect the target.

Viruses

The virus is a self-replicating program; it is capable of producing multiple copies of itself by attaching with another program of any format. These viruses can be executed as soon as they are downloaded, it may wait for the host to execute them as well as be in sleep for a predetermined time. The major characteristics of viruses are: -

- Infecting other files
- Alteration of data
- Transformation
- Corruption
- Encryption
- Self-Replication

Stages of Virus Life

The process of developing a virus till its detection is divided into the following six stages. These stages include the creation of a virus program, its execution, detection, and anti-virus stages. The methodology of Developing a virus is classified as: -

- **Design**

In Designing phase, Virus is created. To design a virus, the developer can create its own virus code completely from scratch using programming languages, either he can use construction kits.

- **Replication**

In Replication phase when the virus is deployed, the virus replicates for a certain time period in a target system. After the certain period, the virus will spread itself. Replication of difference viruses may differ depending upon how the developer wants to replicate them. usually, this replication process is very fast to infect the target in short order.

- **Launch**

Launch stage is the stage when user accidentally launches the infected program. Once this virus is launch, it starts performing the action it is designed for. For example, a virus is specially designed for destroying the data; once the virus is activated, it starts corrupting the data.

- **Detection**

In the detection phase, the behavior of a virus is observed, and the virus is identified as a potential threat to systems. Typically, antivirus developers observe the behavior of a reported virus.

- **Incorporation**

Anti-Virus Software developer after identification, detection and observing the behavior of a virus, design a defensive code in term of anti-virus or an update to provide support to an older version of anti-viruses to detect this new type of virus.

- **Elimination**

The user, by installing the update of an anti-virus, or downloading the newer version of anti-virus capable of detecting advanced threats can eliminate the threat from its operating system.

Working of Viruses

Working on Virus is a two-phase process. in which virus replicates onto an executable file and attack on a system. Different phases of virus operation are defined below: -

1. ***Infection Phase***

   During Infection phase, virus planted on a target system replicate itself onto an executable file. By replicating into a legitimate software, it can be launch when a user runs the legitimate application for its use. These Viruses spread by reproducing and infecting the programs, documents, or e-mail attachments. Similarly, they can be propagated through e-mails, file sharing or downloaded files from internet. They can be entering into an operating system through CDs, DVDs, USB-drives and any other sort of digital media.

2. ***Attack Phase***

   In the Attack Phase, the Infected file is executed accidentally by the user, or by any other way. Viruses normally require a triggering action to infect a victim. This infection can be minimized to complete destruction and corruption of program files and data. Some Virus can initiate an attack when they are executed, but they can also have configured to infect upon certain predefined conditions.

Ransomware

Ransomware is a malware program which restricts the access to system files and folder by encrypting them. Some type of ransomware may lock the system as well. Once the system is encrypted, it requires decryption key to unlock the system and files. Attacker demands a ransom payment in order to provide the decryption key to remove restrictions. Online payments using Digital currencies like Ukash and Bitcoins are used for ransoms which are difficult to trace. Ransomware is normally deployed using Trojans. One of the best examples of ransomware is WannaCry Ransomware attack.

The following are the most common, widely known types of ransomware family: -

- Cryptobit Ransomware
- CryptoLocker Ransomware
- CryptoDefense Ransomware
- CryptoWall Ransomware
- Police-themed Ransomware

Types of Viruses

- **System or Boot Sector Viruses**

  Boot Sector Virus is designed to move actual Master Boot Record (MBR) from its actual location. Boot Sector Virus responds from the original location of MBR when the system boots, it executes the virus first. Boot sector virus altered the boot

sequence by infecting the MBR. It infects the system causing boot problems, performance issues, instability and inability to locate directories.

- **File and Multipartite Viruses**

File or multipartite viruses infect systems in various ways. File viruses infect the files which are executed like executable file or BAT files. Multipartite Virus can infect boot sector and files simultaneously, hence the term multipartite. Attack targets may include boot sector and executable files on the hard drive.

- **Macro Viruses**

Macro Virus is a type of virus that is specially designed for the application of Microsoft Word, Excel and other application using Visual Basic for Application (VBA). Macro languages help to automate and create a new process which is used abusively by running on victim's system.

- **Cluster Viruses**

Cluster Virus dedicatedly designed for attack and modify the file location table or directory table. Cluster virus attacks in a different way. By altering the actual file located in the directory table, file entries point the viruses instead of an actual file. In this way, when a user attempts to run an application, the virus is executed instead.

- **Stealth/Tunneling Viruses**

These type of viruses uses different techniques to avoid detection by an anti-virus program. In order to evade detection, Stealth virus employs tunnel technique to launch under anti-virus via a tunnel and intercepting request from Operating System Interruption handler. Anti-virus uses their own tunnels to detect these types of attacks.

- **Logic Bombs**

A logic bomb virus is designed to remain in a waiting state or sleep mode until a predetermined period, event or action occurs. Fulfillment of condition triggers the virus to exploit, the payload detonates and perform its intended task. These Logic bombs are difficult to detect, as they are unable to detect in sleep mode and can cause destruction after triggering as it may be too late.

- **Encryption Virus**

Encryption viruses are the type of virus uses encryption, capable of scrambling to avoid detection. Due to this ability, these viruses are difficult to detect. They use new encryption to encrypt and decrypt the code as it replicates and infects.

Other types of viruses

Some other types of viruses are: -

- Metamorphic Viruses
- File Overwriting or Cavity Viruses
- Sparse Infector Viruses
- Companion/Camouflage Viruses
- Shell Viruses
- File Extension Viruses
- Add-on and Intrusive Viruses
- Transient and Terminate and Stay Resident Viruses

Writing a Simple Virus Program

Creating a virus is a simple process, although it depends upon the intention of the developer what is his intention. High profiled developer prefers to design code from scratch. The following are some steps to create a basic virus which can perform a certain action upon the trigger. To create a virus, you may have a notepad application and bat2com application, or you can create using GUI based virus creating an application.

Simple Virus Program using Notepad
1. Create a directory having bat file and text file. 2. Open Notepad Application 3. Enter the code as shown @echo off for %%f in (*.bat) do copy %%f + Virus.bat Del c:\windows*.* 4. Save the file in .bat format. 5. Convert the file using bat2com utility or bat to the .exe converter. 6. It will save an Exe file in the current directory which will execute upon click.

Virus Generating Tools

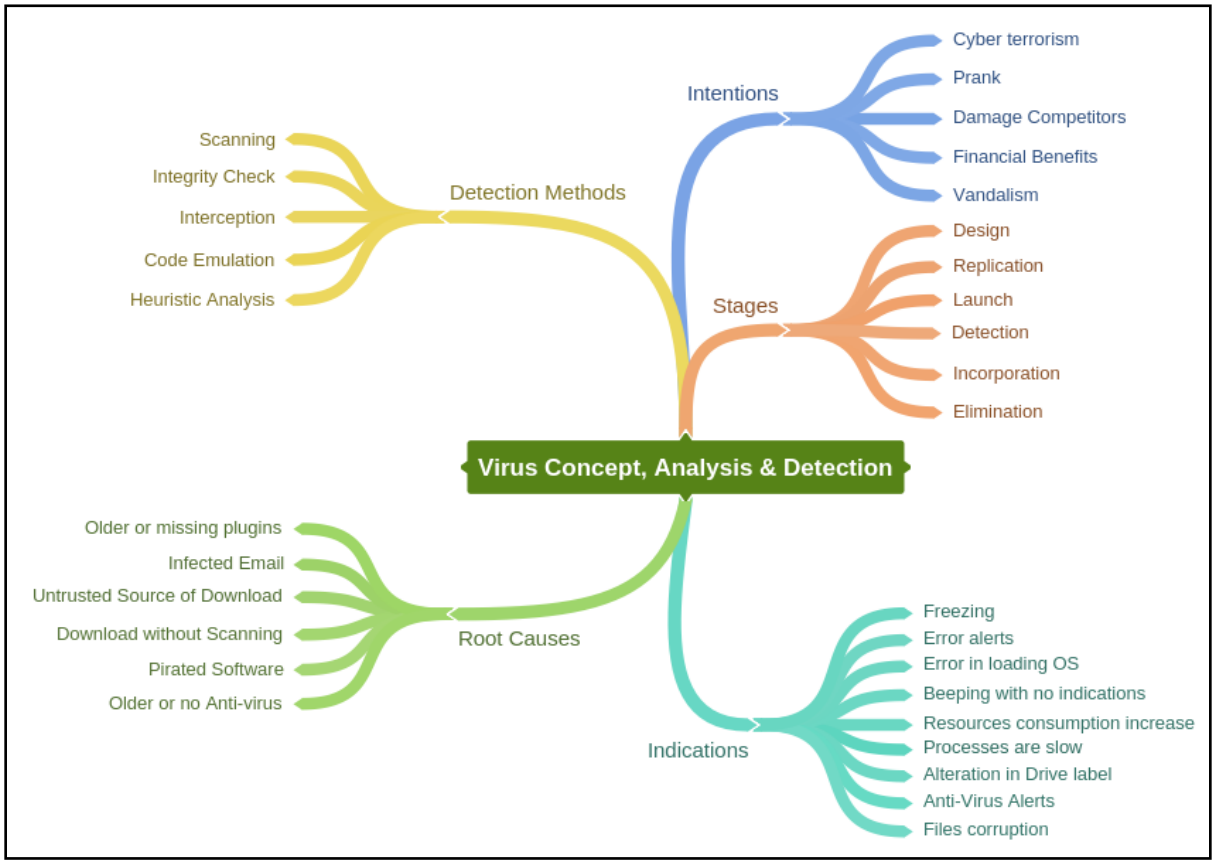
- Sam's Virus Generator and
- JPS Virus Maker
- Andreinicko5's Batch Virus Maker and
- DeadLine's Virus Maker
- Sonic Bat – Batch File Virus Creator and
- Poison Virus Maker

Computer Worms

Worms are a type of malware. Unlike viruses requiring a triggering event to perform intended tasks, Worms can replicate themselves but cannot attach themselves. The worm can propagate using File transport and spread across the infected network which virus is not capable of.

Virus Analysis and Detection Methods

Detection phase of virus initiate with scanning, Initially, the suspected file is scanned for the signature string. In the second step of the detection method, entire disk is checked for integrity. Integrity checker records integrity of all files on a disk by calculating Checksum usually. If a file is altered by a virus, it can be detected through integrity check. In an Interception step, Request from Operating system is monitored. Interception software's are used to detect virus resembling behaviors and generate a warning for users. Code Emulation and Heuristic Analysis include behavioral analysis and Code analysis of virus by executing it in a sophisticated environment.



Malware Reverse Engineering

Sheep Dipping

Sheep Dipping is the analysis of suspected file and packets against viruses and malware before allowing them to be available for users in an isolated environment. This analysis is performing on a dedicated computer. This is initial line of defense running, with highly secured computing along with port monitoring, file monitoring, anti-viruses and other security programs.

Malware Analysis

Malware Analysis is the process of identification of a malware till its verification that malware is completely removed, including observing the behavior of malware, scoping the potential threat to a system and finding other measures. Before explaining the malware analysis, the need for malware analysis and goal to be achieved by this analytics must be defined. Security analyst and security professional at some point in their career have performed malware analysis. The major goal of malware analysis is to gain detailed information and observe the behavior of malware, to maintain incident response and defense action to secure the organization.

Malware Analyses process start with Preparing the Testbed for analysis. Security Professional get ready a Virtual machine as a host operating system where dynamic malware analysis will be performed by executing the malware over the guest operating system. This host operating system is isolated from another network to observe the behavior of malware by quarantine the malware from the network.

After Executing a malware in a Testbed, Static and Dynamic Malware analysis are performed. Network connection is also setup later to observe the behavior using Process monitoring tools and Packet monitoring tools and debugging tools like OllyDbg and ProcDump.

Goals of Malware Analysis

Malware analysis goals are defined below: -

- Diagnostics of threat severity or level of attack.
- Diagnostics of the type of Malware.
- Scope the attack
- Built defense to secure organization's network and systems.
- Finding a root cause.
- Built Incident response actions.
- Develop Anti-malware to eliminate.

Types of Malware Analysis

Malware analysis is classified into two basic types.

- **Static Analysis**

Static Analysis or Code Analysis is performed by fragmenting the resources of the binary file without executing it and study each component. Disassembler such as IDA is used to disassemble the binary file.

- **Dynamic Analysis**

Dynamic Analysis or Behavioural Analysis is performed by executing the malware on a host and observing the behavior of the malware. These behavioral analyses are performed in a Sandbox environment.

Sandboxing technology helps in detection of threat in a dedicated manner in a sophisticated environment. During Sandboxing of a Malware, it is searched in the Intelligence database for the analysis report. It might be possible that diagnostics details are available if the threat is detected previously. When a threat is diagnosed before, its analytics are recorded for future use; it helps to diagnose now. If a match found is in the database, it helps in responding quickly.

Lab 7-1: HTTP RAT Trojan

Case Study: Using HTTP RAT Trojan, we are going to create an HTTP Remote Access Trojan (RAT) server on Windows 7 machine (10.10.50.202). When an executable Trojan file is executed on the remote machine (in our case, Windows Server 2016, having IP address 10.10.50.211), it will create remote access of Windows Server 2016 on Windows 7.
Topology:

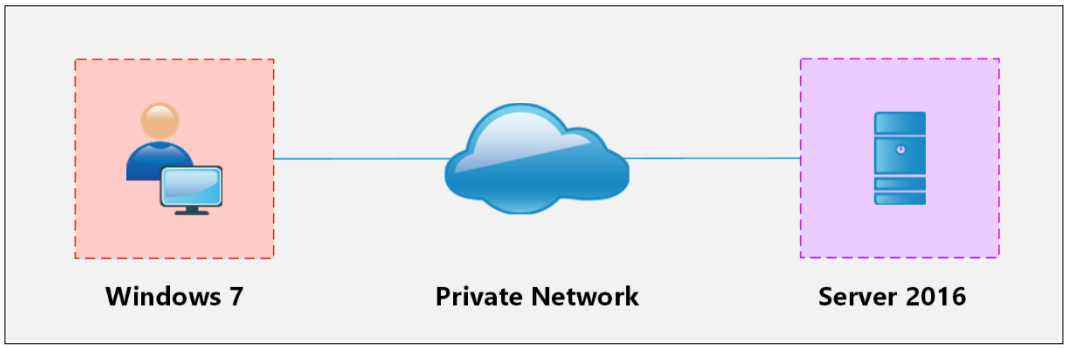


Figure 7-02 Topology Diagram

Configuration and Procedure:
Go to Windows 7 machine and run the HTTP RAT Trojan. 1. Uncheck Notification with IP address to mail 2. Configure Port 3. Click Create

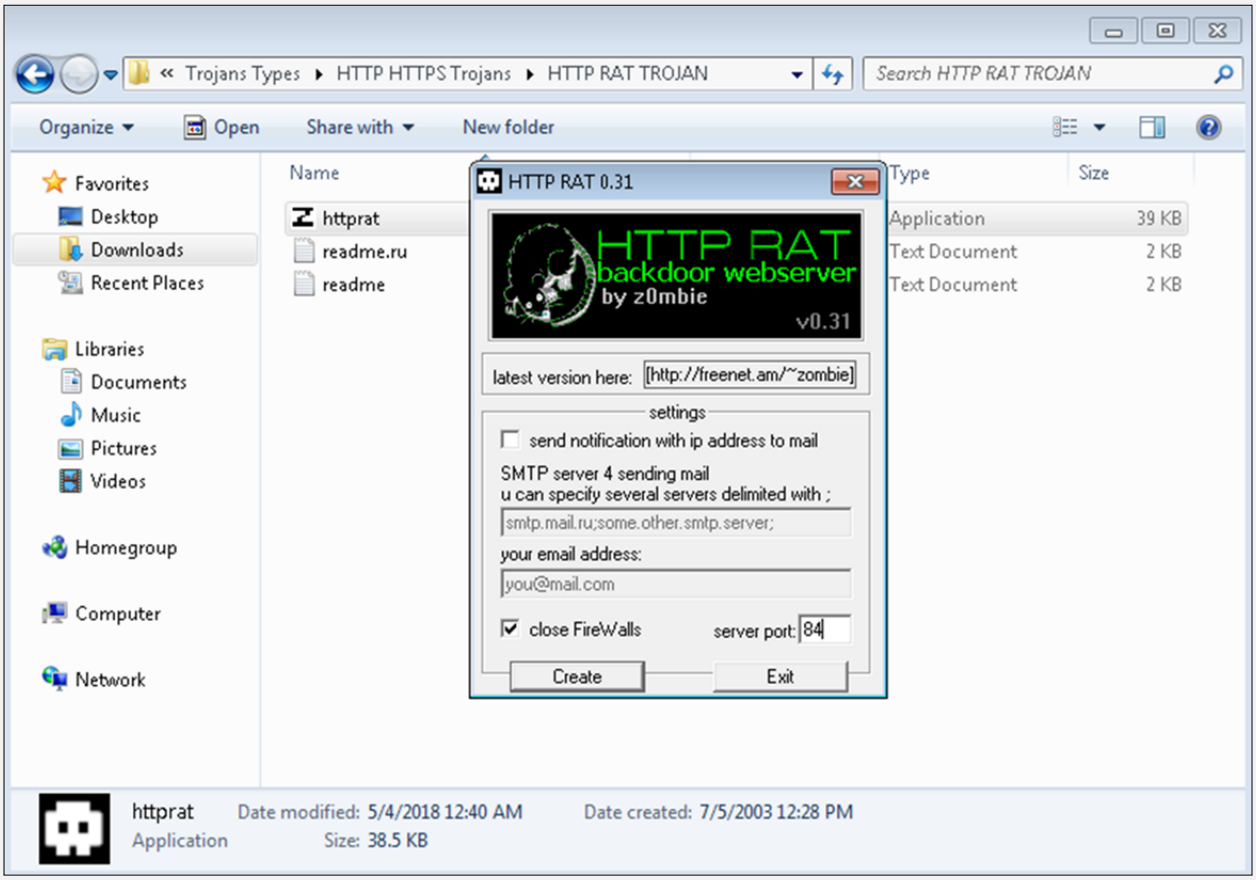


Figure 7-03 HTTP RAT Trojan

In the default directory where the application is installed, you will see a new executable file. Forward this file to the victim's machine.

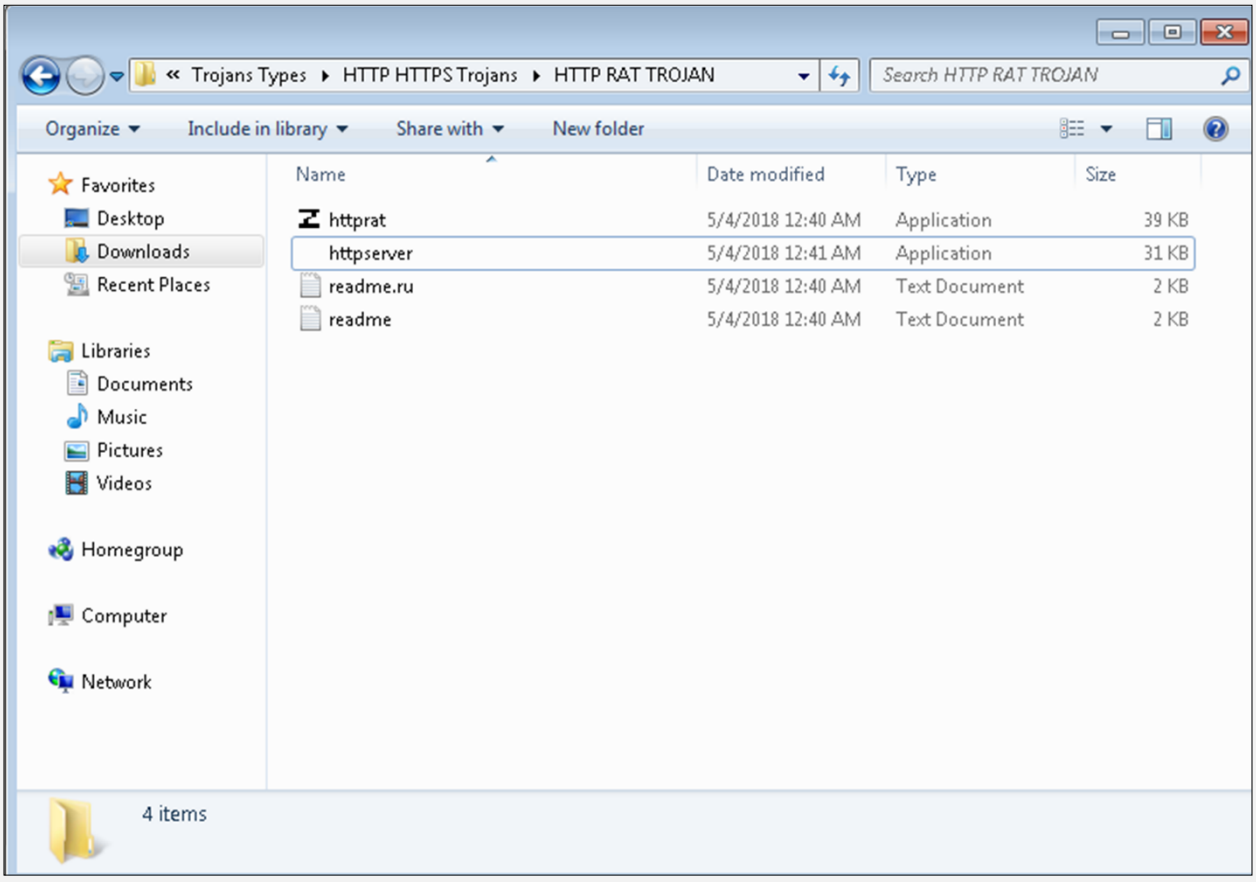


Figure 7-04 Trojan EXE file created

4. Log in to victim's machine (In our case, Windows Server 2016) and run the file.
5. Check task manager for a running process; you will see an HTTP Server task in the process.

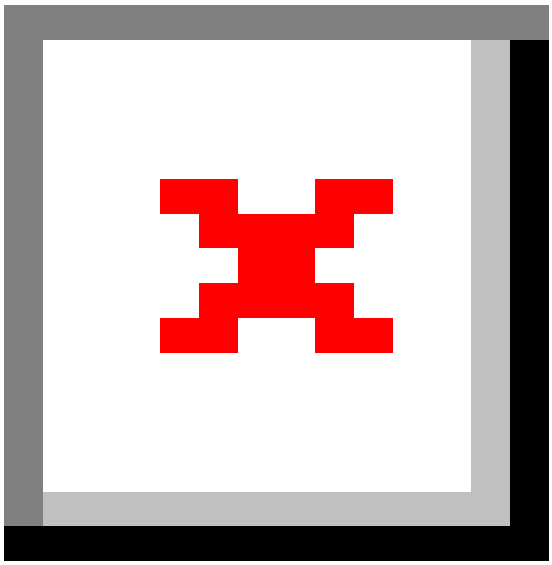


Figure 7-05 Trojan process on Victim machine

6. Go back to Windows 7.
7. Open Web browser
8. Go to IP address of victim's machine; in our case, 10.10.50.211

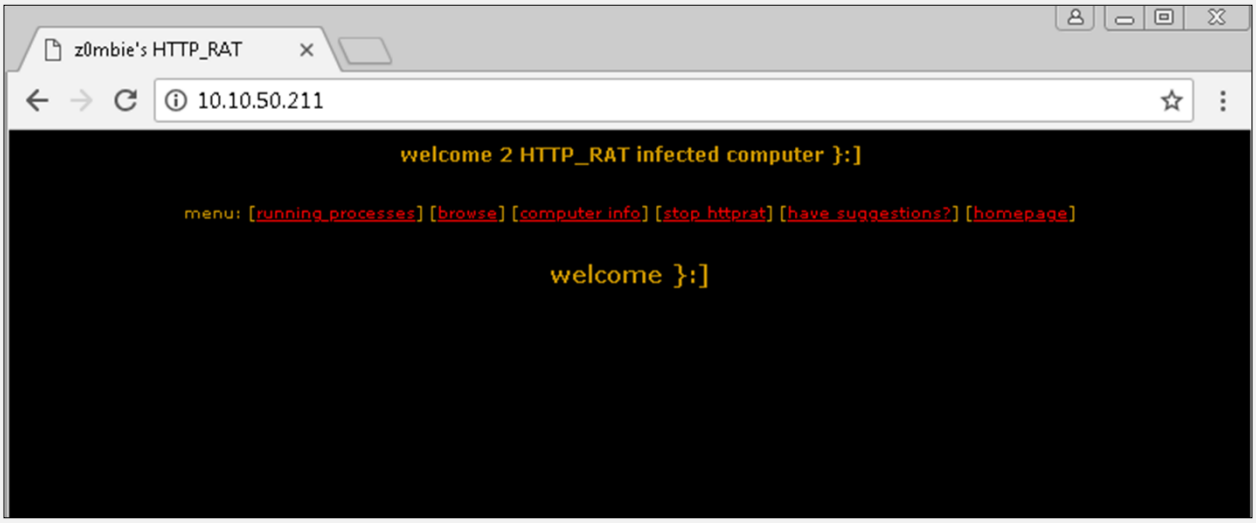


Figure 7-06 Accessing Victim using HTTP

HTTP connection is open from victim's machine. You can check running process, browse drives, check computer information of victim using this tool

9. Click **Running Processes**

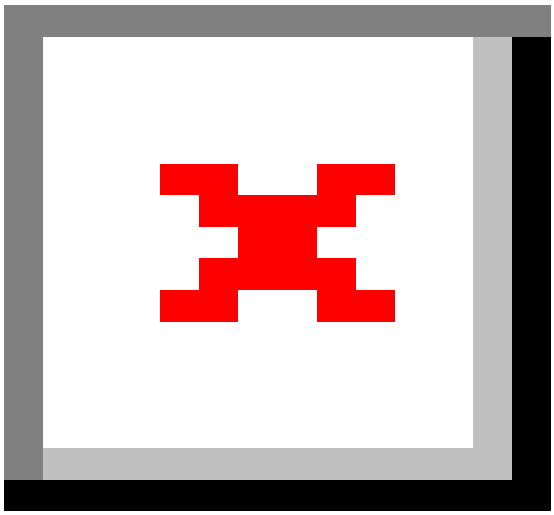


Figure 7-07 Running Process on Victim

Above output is showing running process of victim's machine.

10. Click **Browse**

Figure 7-08 Browse Drives of Victim

The output is showing drives.

11. Click **Drive C**

Figure 7-09 C drive of Victim

Output showing C drive

12. Click **Computer Information**

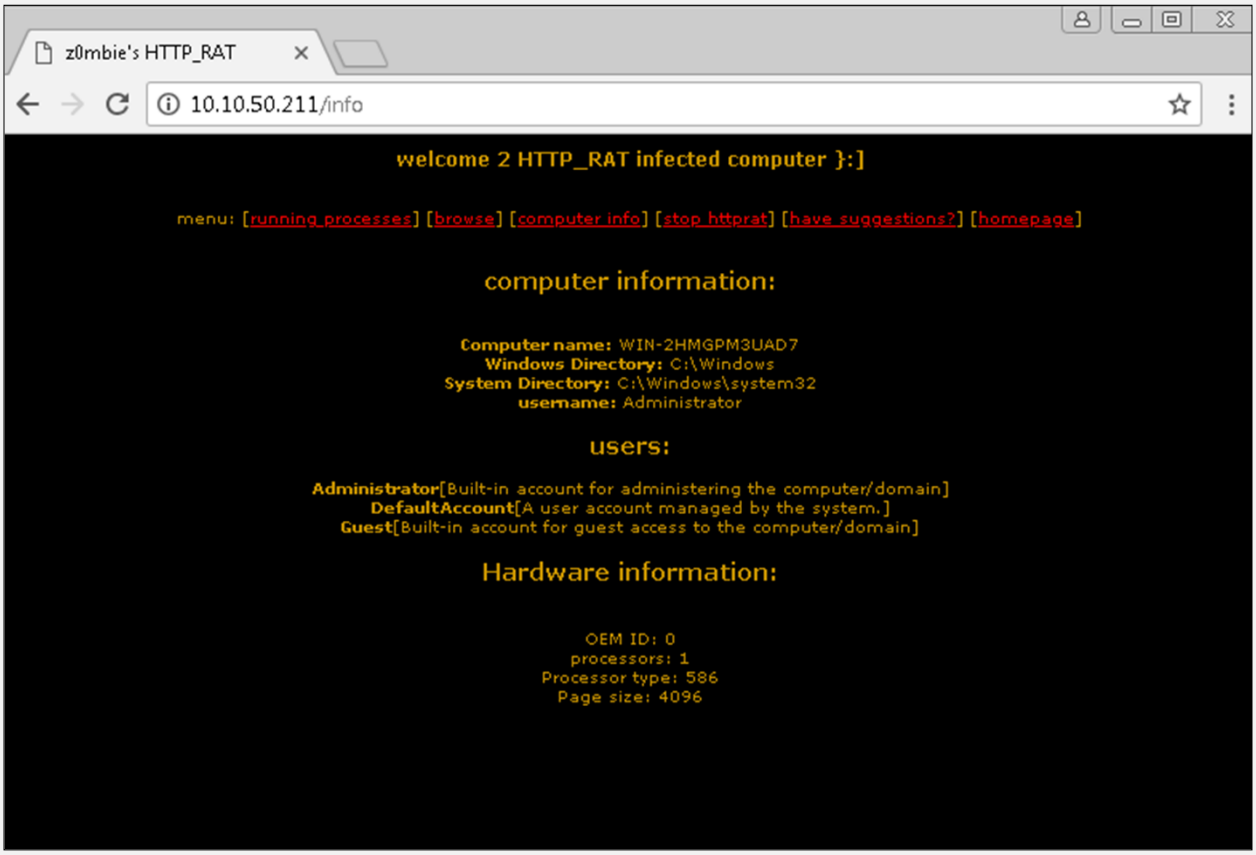


Figure 7-10 Computer's information of Victim

The output is showing computer information.

13. To terminate the connection, Click **Stop_httpRat**

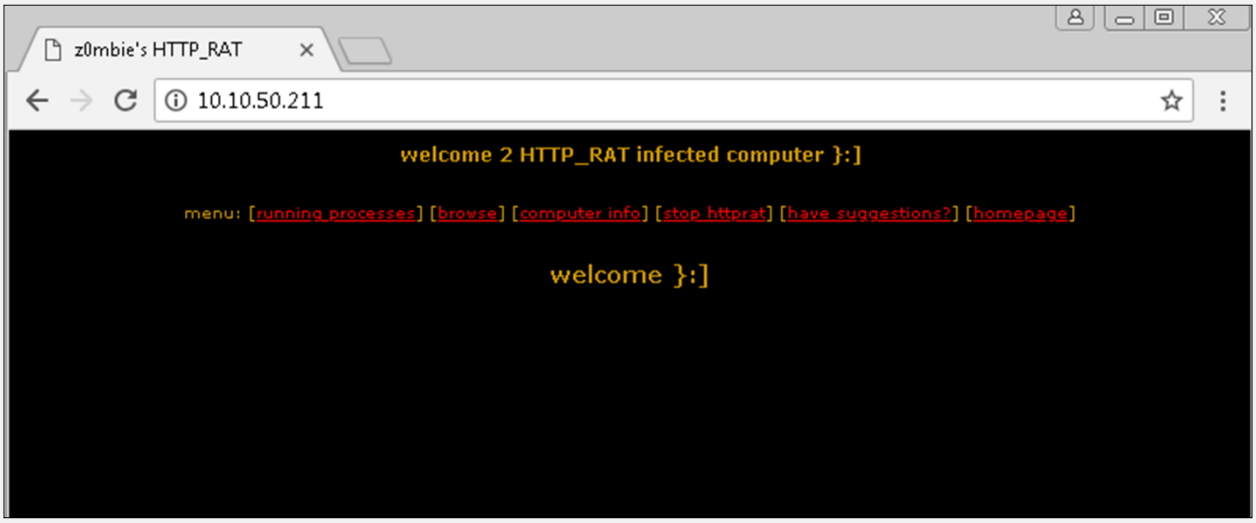


Figure 7-11 Stop HTTP Connection

14. Refresh the browser

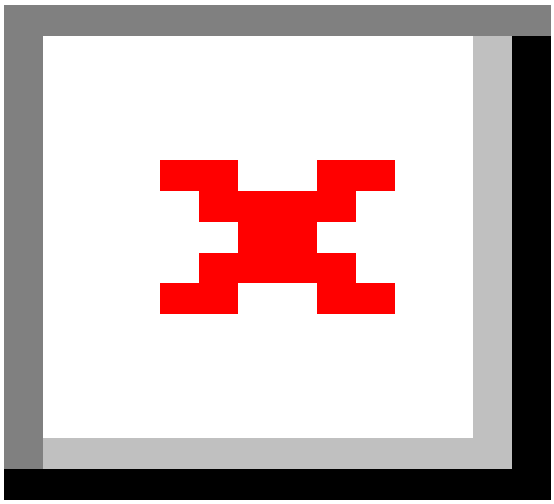


Figure 7-12 Connection terminated

The connection is successfully terminated.

15. Go to Windows Server 2016 and check running processes.

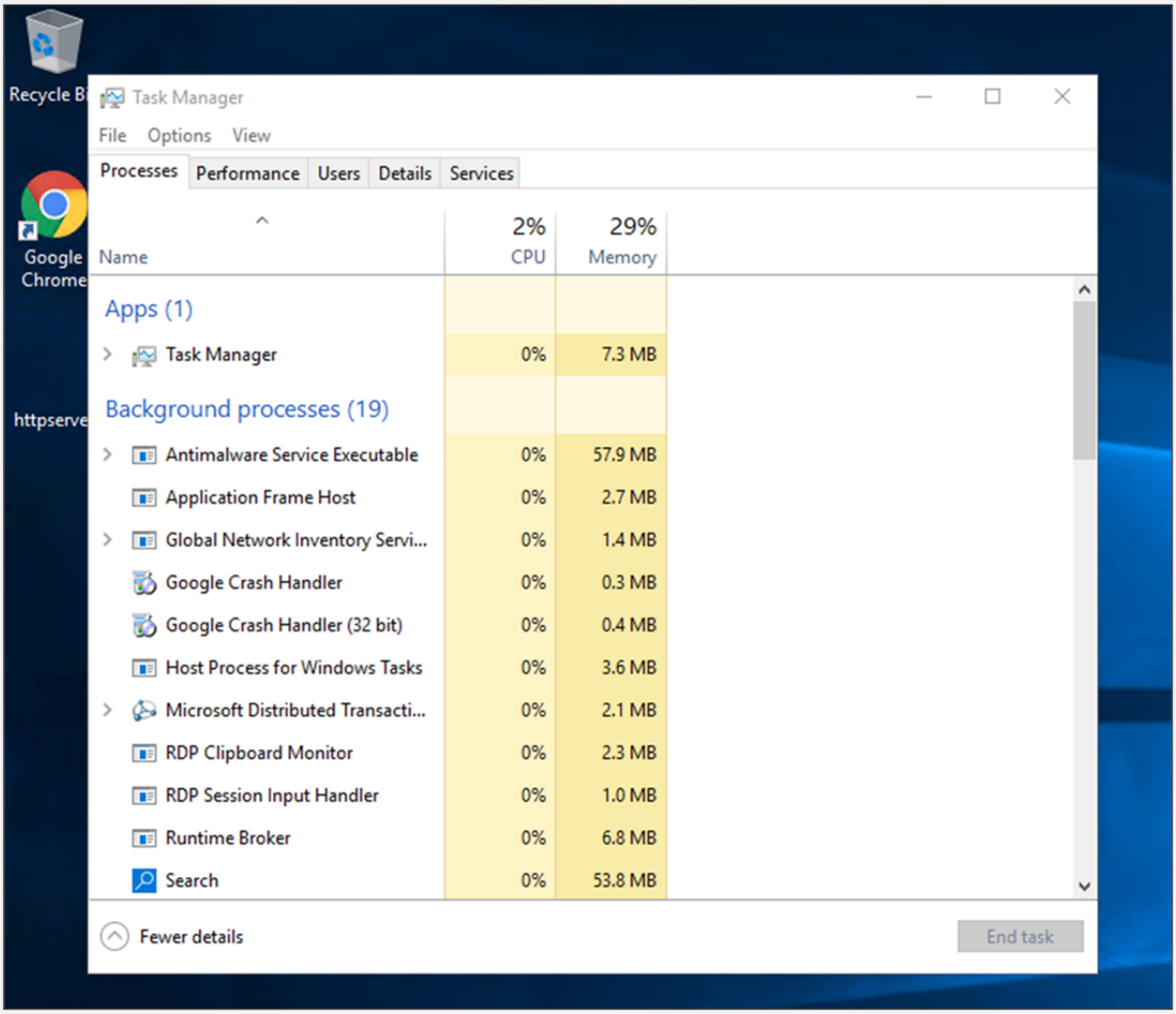


Figure 7-13 Verifying Process

HTTP Server process terminated.

Lab 7-2: Monitoring TCP/IP connection using CurrPort tool

Case Study: Using the Previous lab, we are going to re-execute HTTP Remote Access Trojan (RAT) on Windows 12 machine (10.10.50.211) and observed the TCP/IP connections to detect and kill the connection.

Topology:

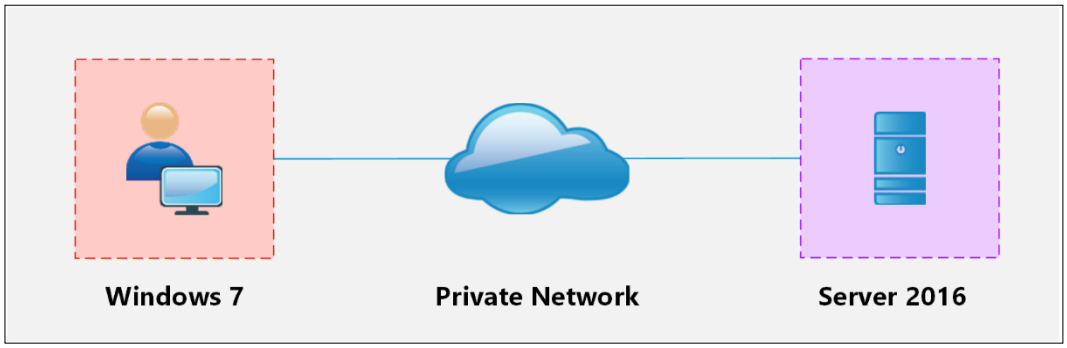


Figure 7-14 Topology Diagram

Configuration:

1. Run the application **Currports** on Windows Server 2016 and observe the processes.

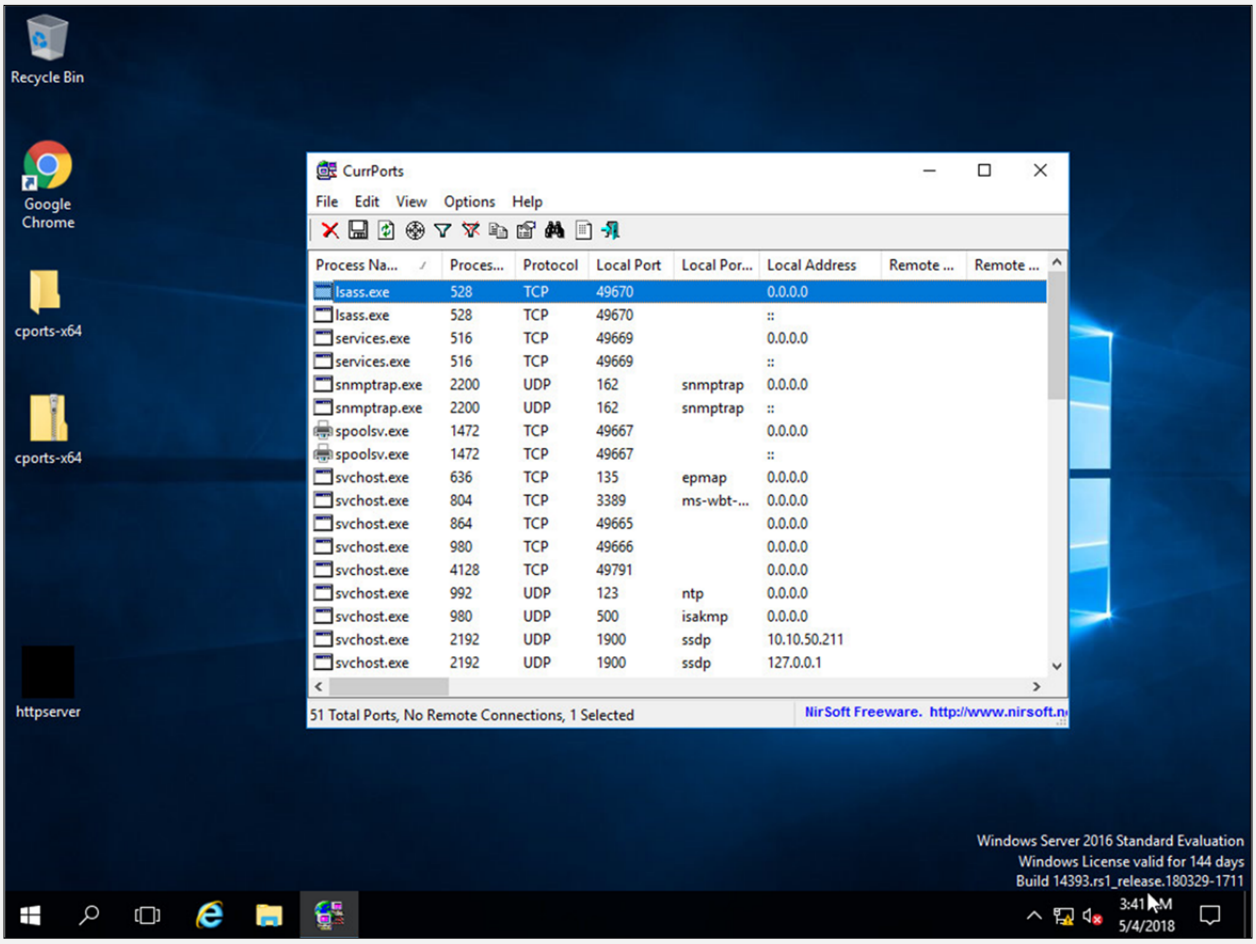


Figure 7-15 Currports Application showing Running processes

2. Run the HTTP Trojan created in the previous lab.

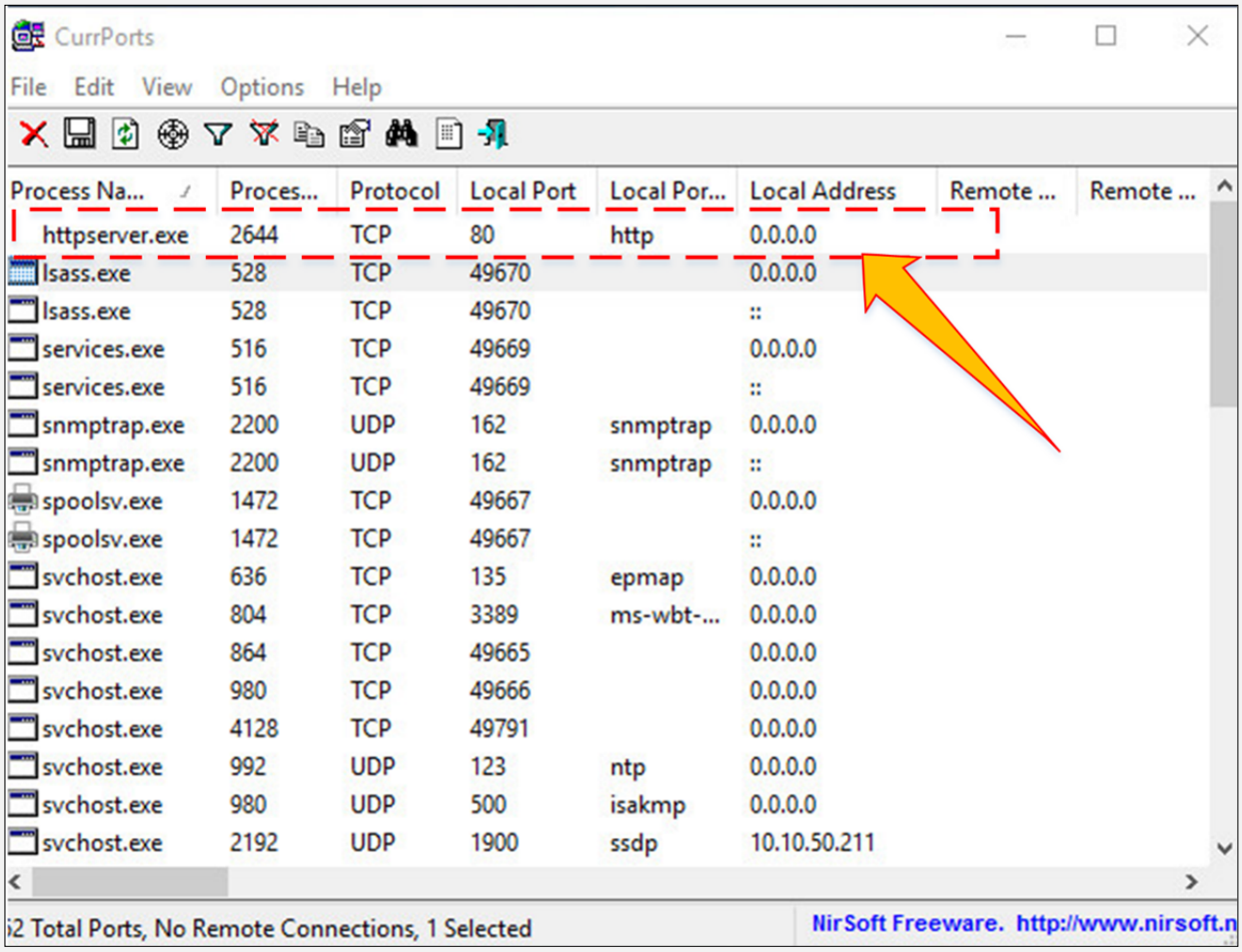


Figure 7-16 Trojan Connection

The new process is added to the list.

You can observe the process name, Protocol, Local and remote port and IP address information.

3. For more detail, right click on httpserver.exe and go to properties.

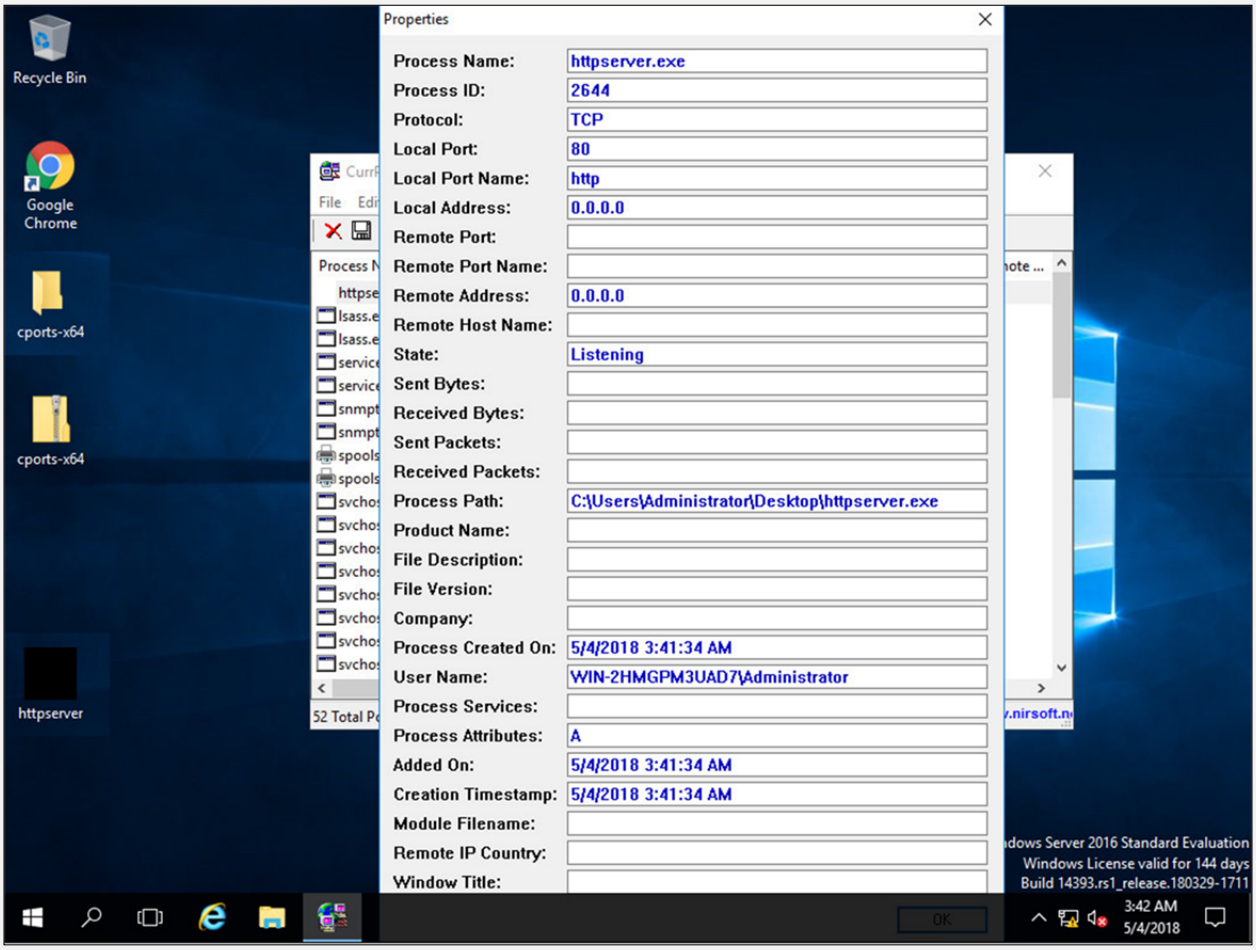


Figure 7-17 TCP connection properties

Properties are showing more details about tcp connection.

4. Go to Windows 7 machine and initiate the connection as mentioned in the previous lab using a web browser.

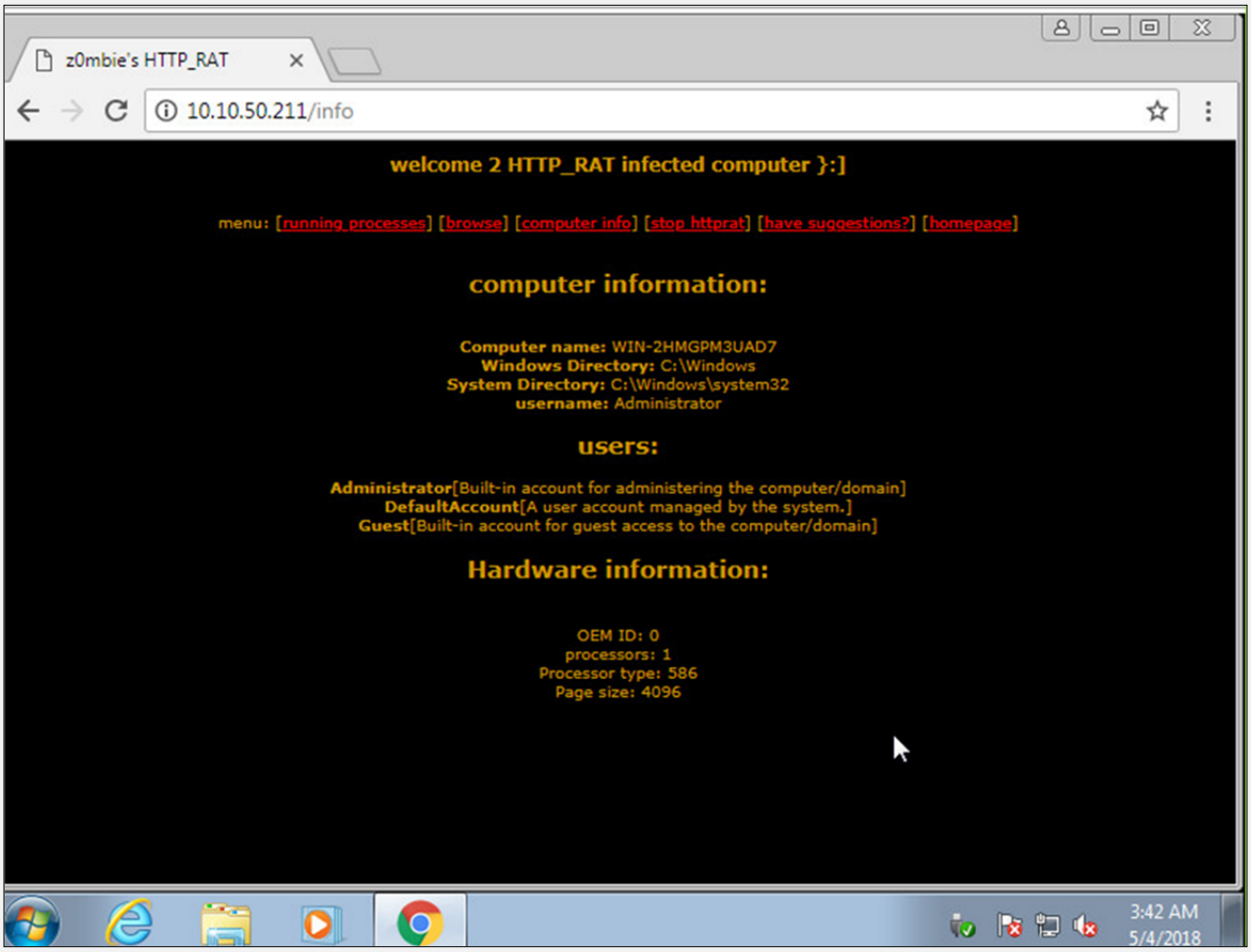


Figure 7-18 HTTP RAT Connection

Connection successfully established.

5. Back to Windows Server 2016, Kill the connection.

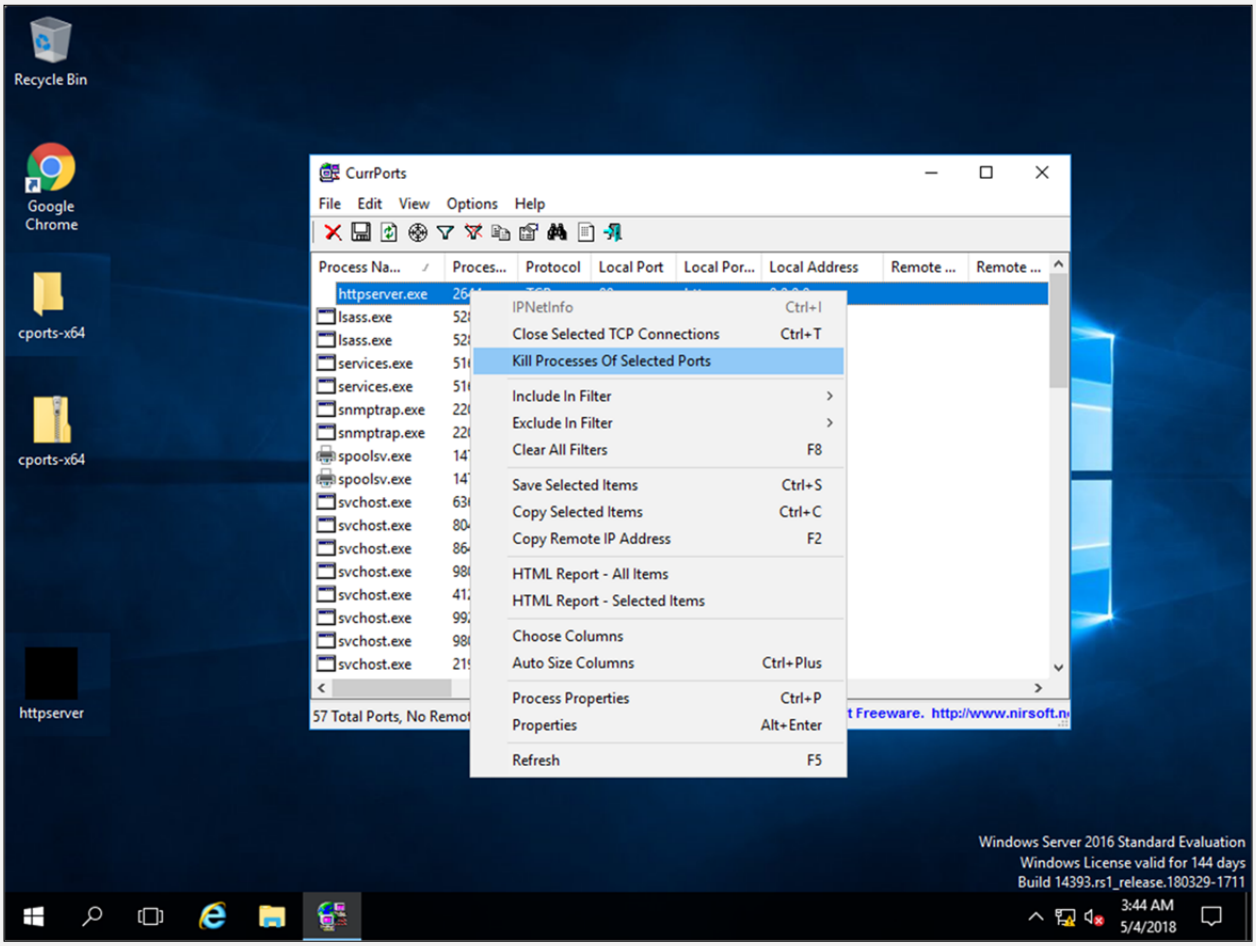


Figure 7-19 Killing TCP connection properties

6. To verify, retry to establish the connection from windows 7.

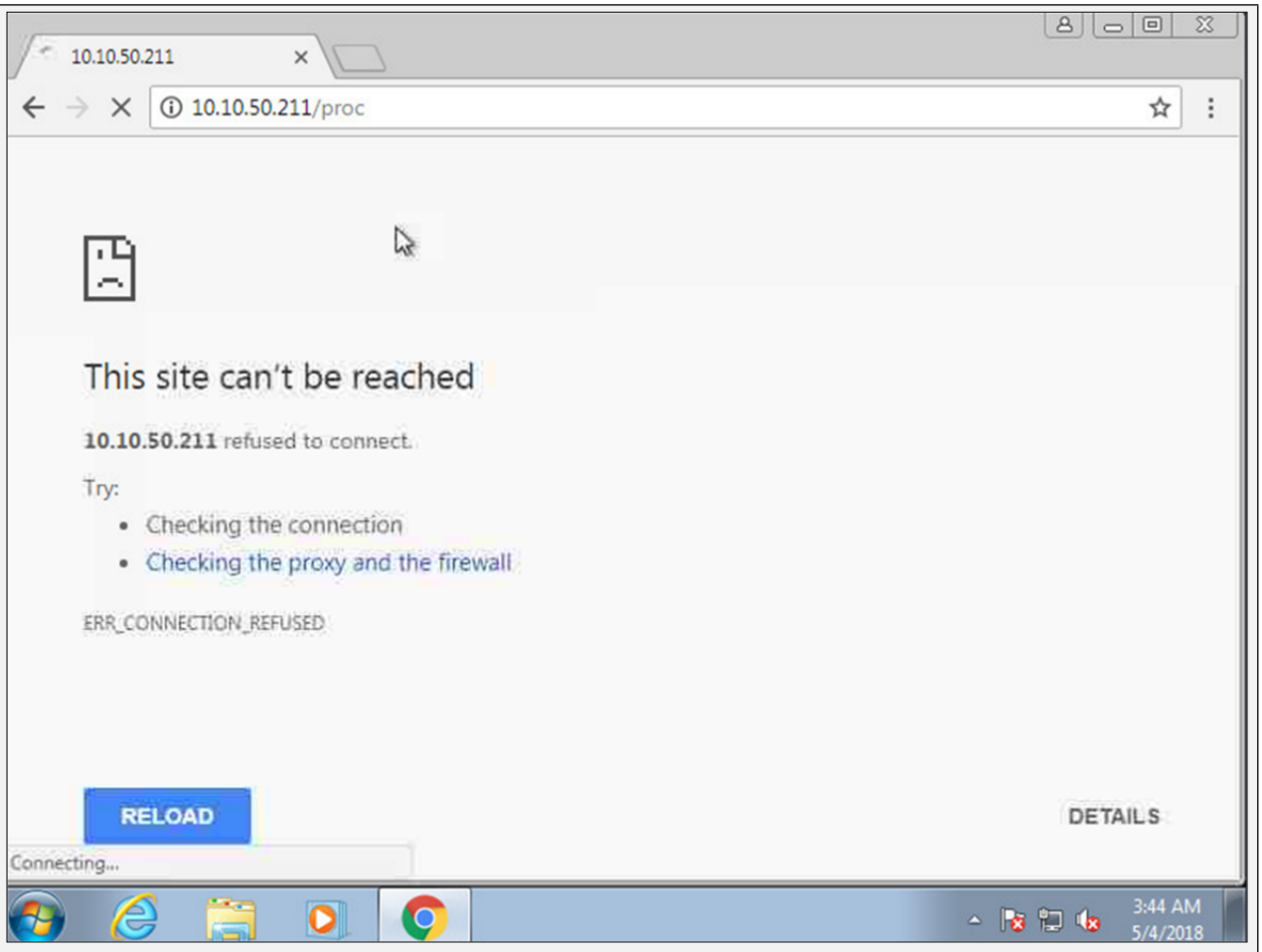


Figure 7-20 TCP connection terminated