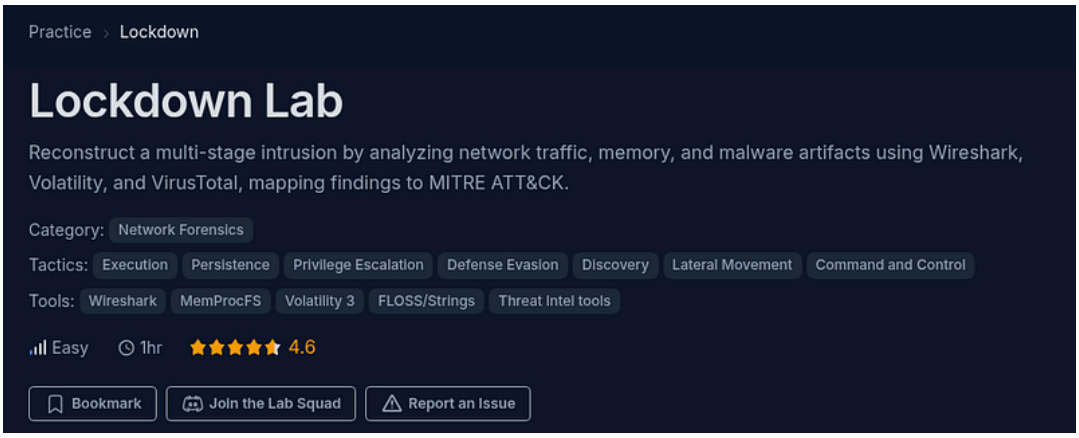
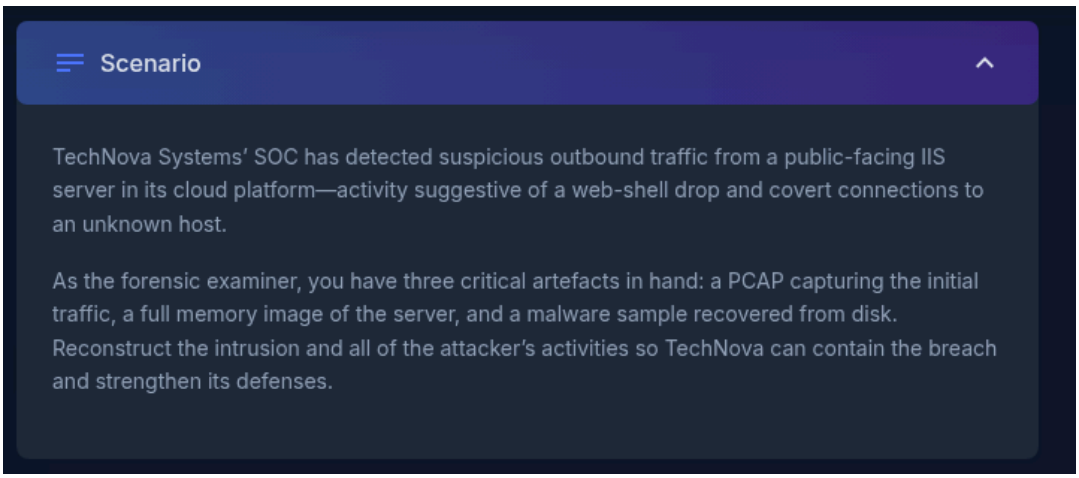
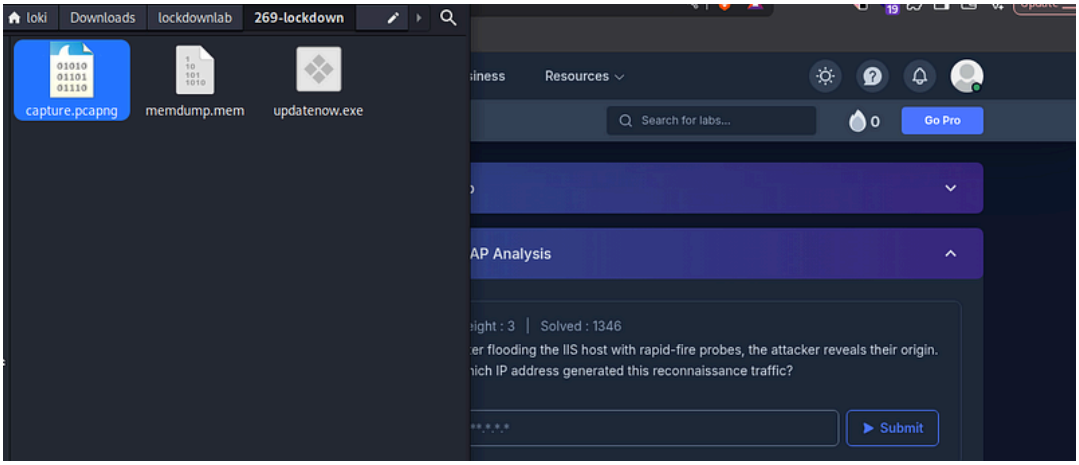
CyberDenders Write-up: Lockdown Lab







PCAP Analysis

Q1
Weight : 3 | Solved : 1346

After flooding the IIS host with rapid-fire probes, the attacker reveals their origin. Which IP address generated this reconnaissance traffic?

flag: 10.0.2.4

Process:

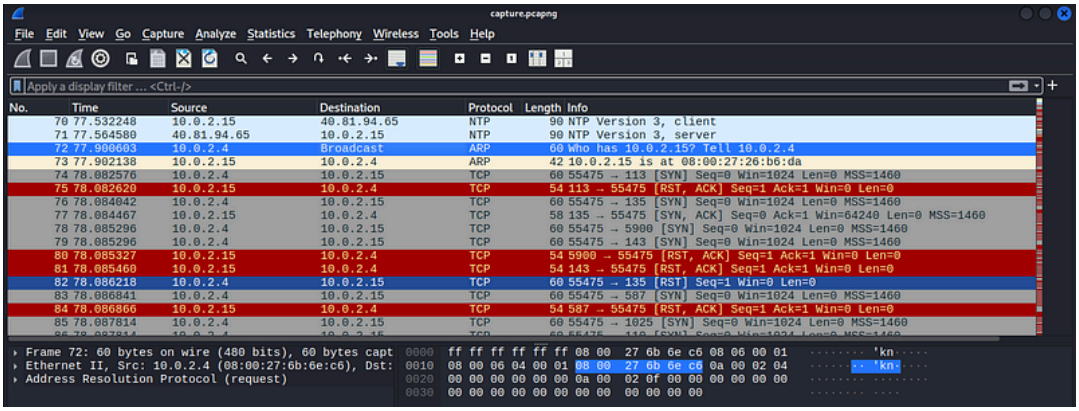
Source consulted: https://www.clrn.org/what-does-red-mean-in-wireshark/

Red packets can be indicative of an error or alert condition.

These packets were coming from the IP address **10.0.2.4**.

An ARP request originating from **10.0.2.4** was observed.

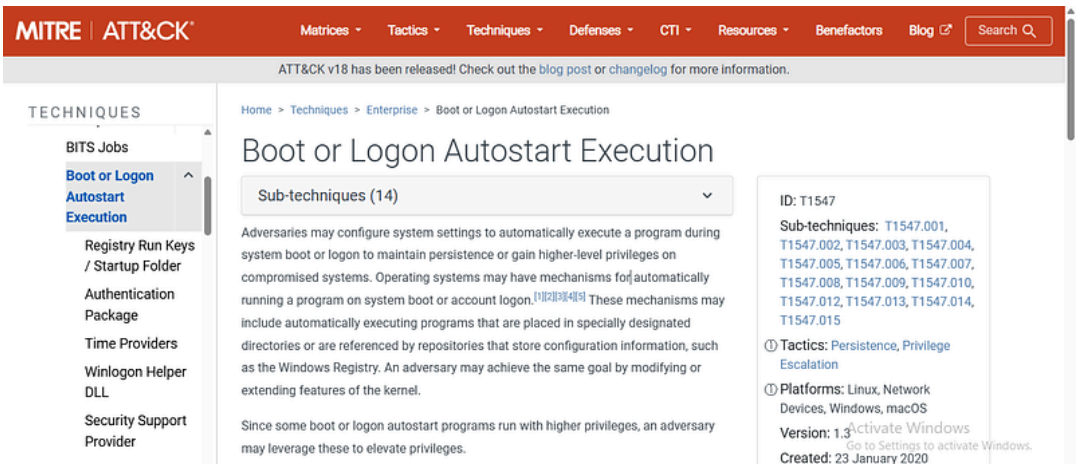
There was an increase in traffic coming from this IP address.



Q2
Weight : 2 | Solved : 1231

Zeroing in on a single open service to gain a foothold, the attacker carries out targeted enumeration. Which MITRE ATT&CK technique ID covers this activity?

flag: T1046



Process:

Network Service Discovery was identified, as the attacker was already within the network based on the initial analysis.

Reference: https://attack.mitre.org/techniques/T1046/

Q3
Weight : 2 | Solved : 1213

While reviewing the SMB traffic, you observe two consecutive Tree Connect requests that expose the first shares the intruder probes on the IIS host. Which two full UNC paths are accessed?

flag: \\10.0.2.15\Documents,\\10.0.2.15\IPC$

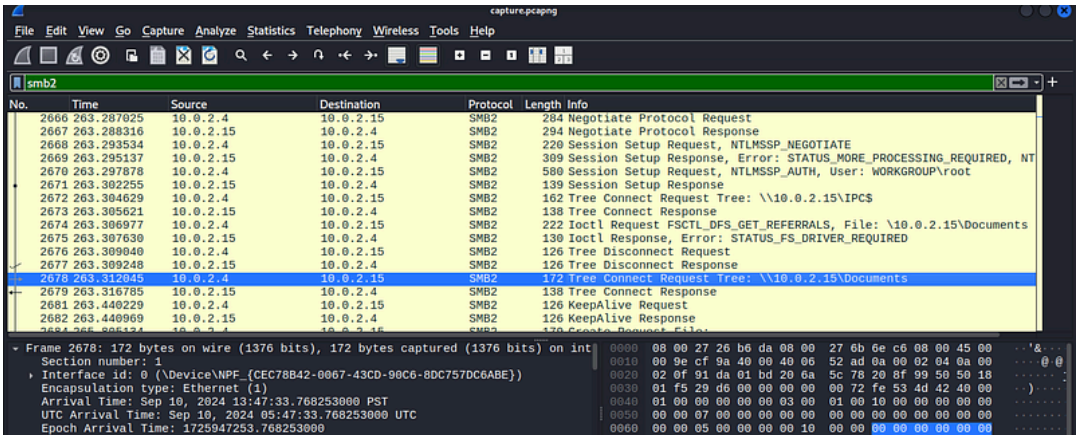
process:

WireShark filter search : smb2

found:

A.) 2629 240.778552 10.0.2.4 10.0.2.15 SMB2 162 Tree Connect Request Tree: \\10.0.2.15\IPC$

B.) 2678 263.312045 10.0.2.4 10.0.2.15 SMB2 172 Tree Connect Request Tree: \\10.0.2.15\Documents



Q4
Weight : 3 | Solved : 1189

Inside the share, the attacker plants a web-accessible payload that will grant remote code execution. What is the filename of the malicious file they uploaded, and what byte length is specified in the corresponding SMB2 Write Request?

flag: shell.aspx, 1015024

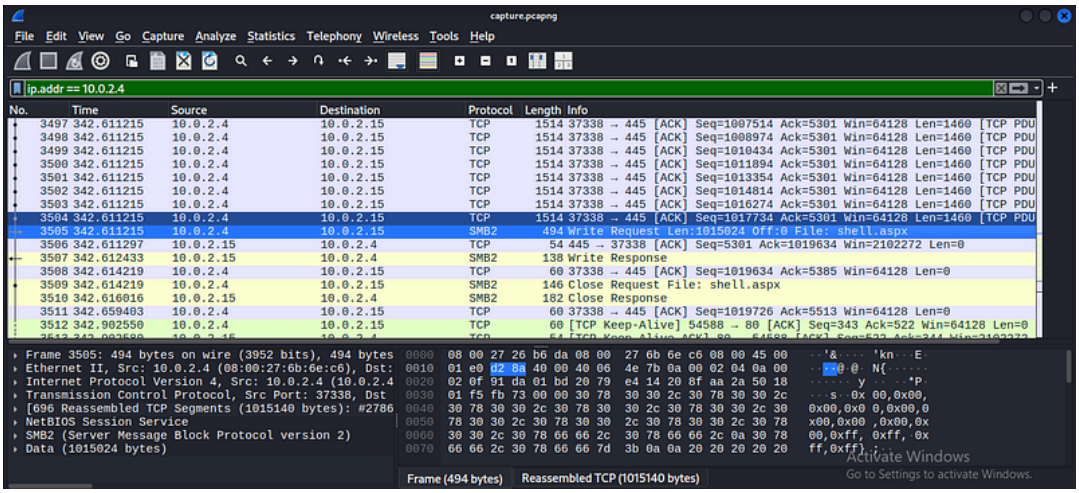
Process:

Filter applied: smb2

Next, all traffic from **10.0.2.4** was examined using the filter:

ip.addr == 10.0.2.4

A packet was found showing an **SMB2 Write Request** from **10.0.2.4**, which contained **shell.aspx**.



Q5
Weight : 2 | Solved : 1169

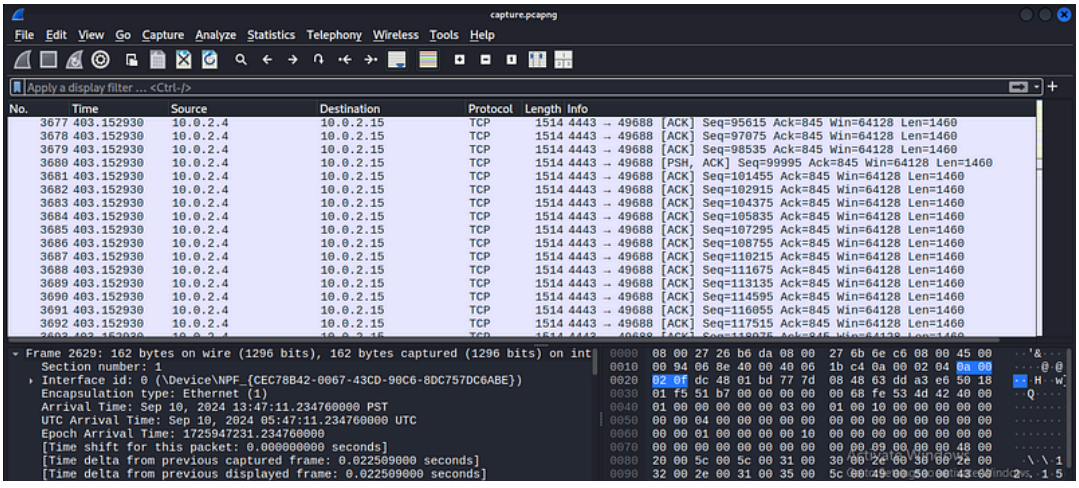
The newly planted shell calls back to the attacker over an uncommon but firewall-friendly port. Which listening port did the attacker use for the reverse shell?

flag:4443

Process:

Traffic between the two IP addresses was analyzed, from the attacker IP to **10.0.2.15**.

The connection was using **port 4443**, which was identified as the port used for the reverse shell.



Memory Dump Analysis

Q6
Weight : 3 | Solved : 952

Your memory snapshot captures the system's kernel in situ, providing vital context for the breach. What is the kernel base address in the dump?

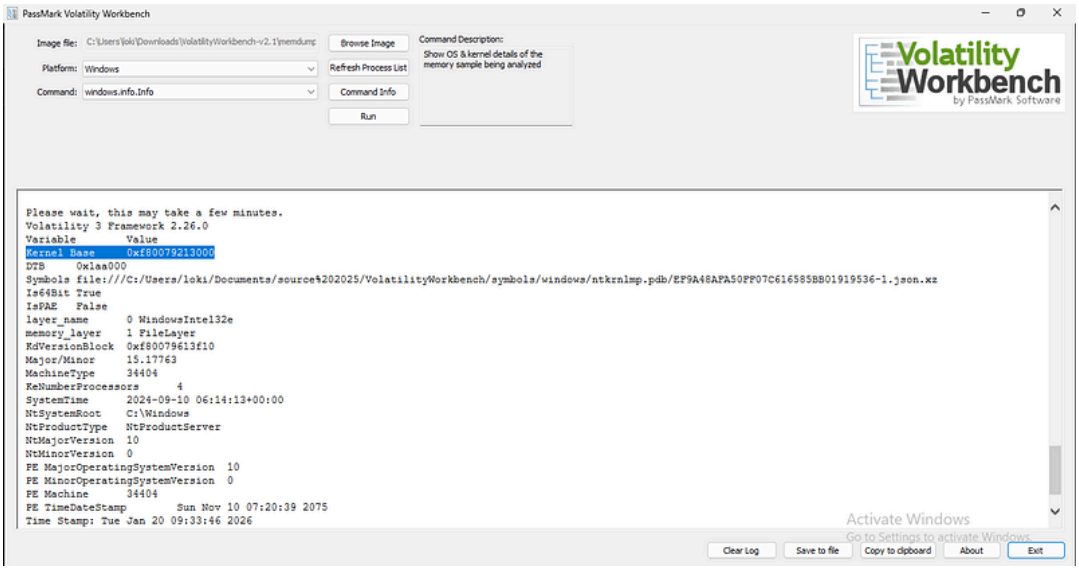
flag: 0xf80079213000

Process:

Volatility Workbench was used.

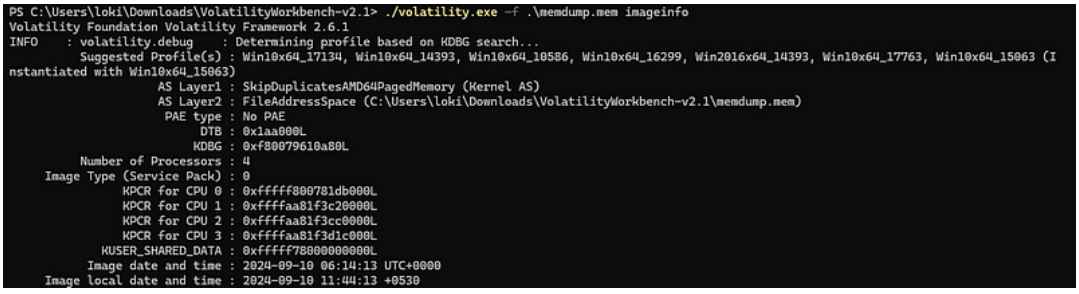
Command executed: windows.info.Info

This command displays the OS and kernel details of the memory sample being analyzed.



In the CLI, the equivalent command is:

./volatility.exe -f .\memdump.mem imageinfo



Q7
Weight : 2 | Solved : 875

A trusted service launches an unfamiliar executable residing outside the usual IIS stack, signalling a persistence implant. What is the final full on-disk path of that executable, and which MITRE ATT&CK persistence technique ID corresponds to this behaviour?

flag: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\updatenow.exe,T1547

Process:

Since the PID of the executable was identified in **Q8**, the analysis was continued in more depth.

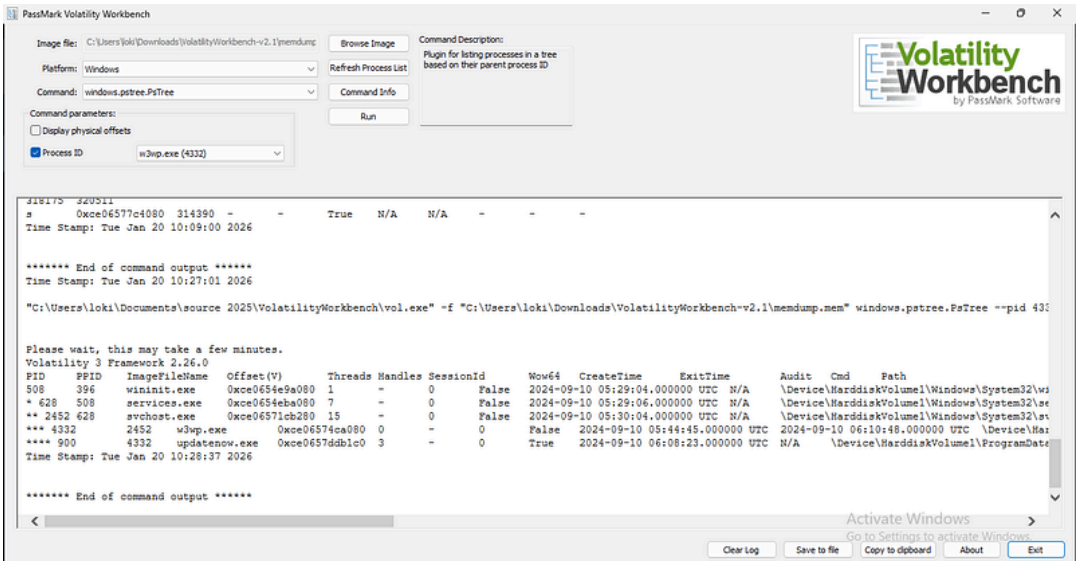
The following command was used to inspect the process tree:

Command: windows.pstree.PsTree

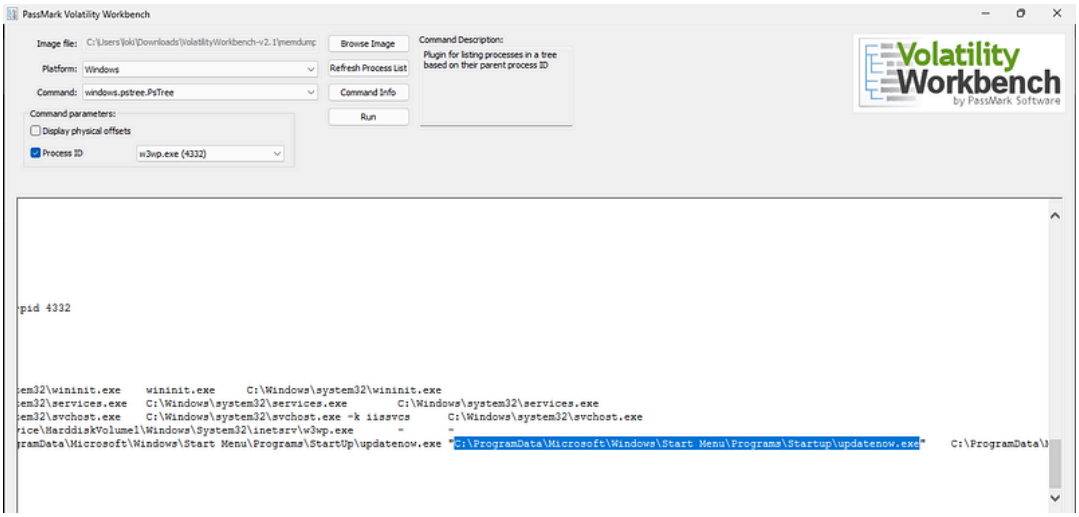
PID specified: **4332**

Findings:

**** 900 4332 updatenow.exe 0xce0657ddb1c0 3–0 True 2024–09–10 06:08:23.000000 UTC N/A \Device\HarddiskVolume1\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\updatenow.e "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\updatenow.exe"



The executable **updatenow.exe** was located in the **Startup** directory, indicating that it is configured to run automatically on system startup. This behavior is commonly used to maintain persistence within a compromised system.



A quick search for the corresponding MITRE ATT&CK technique identified this behavior as **Boot or Logon Autostart Execution**.

Reference: https://attack.mitre.org/techniques/T1547/

Q8
Weight : 2 | Solved : 889

The reverse shell's outbound traffic is handled by a built-in Windows process that also spawns the implanted executable. What is the name of this process, and what PID does it run under?

flag: w3wp.exe, 4332

Process:

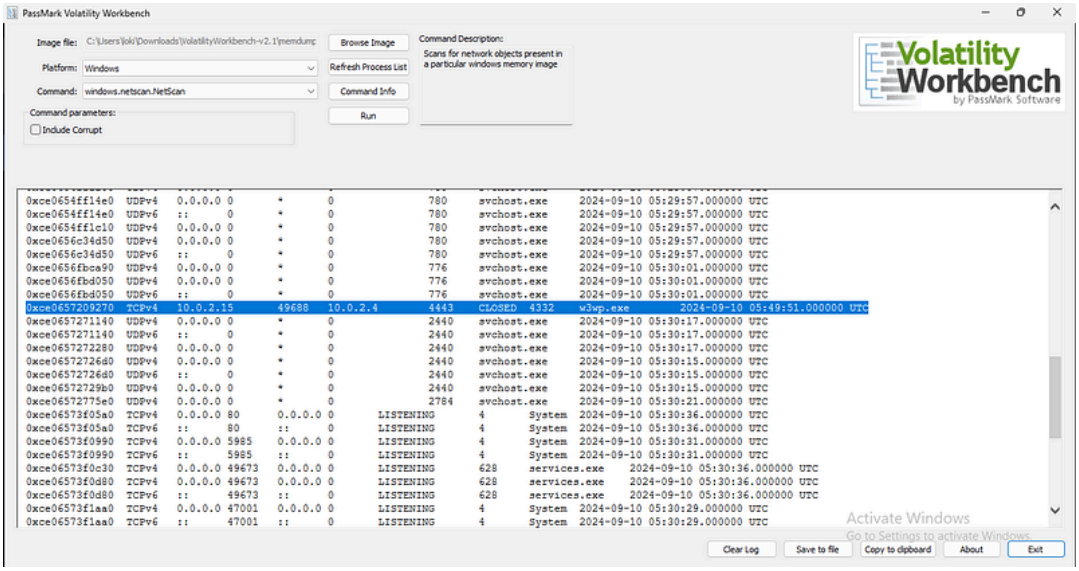
Revisiting the earlier network analysis, the threat actor's IP address **10.0.2.4** and the port **4443** were identified as being used within the internal network.

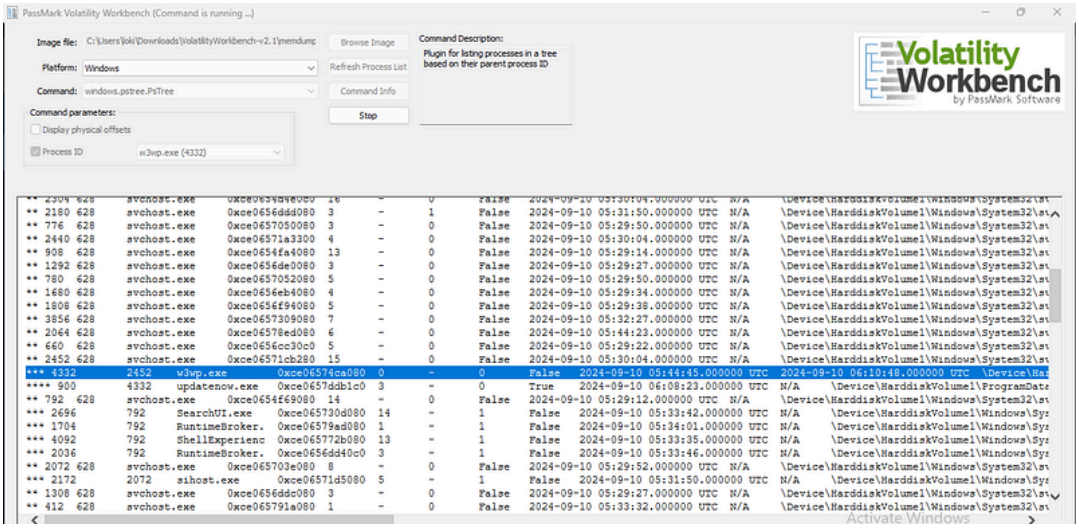
At this stage, the captured memory image was analyzed to inspect active and historical network connections.

Volatility Workbench Command:

windows.netscan.Netscan

This plugin scans for network objects present in a Windows memory image.





Findings:

0xce0657209270 TCPv4 10.0.2.15 49688 10.0.2.4 4443 CLOSED 4332 w3wp.exe 2024–09–10 05:49:51.00(

This entry shows a TCP connection from **10.0.2.15** to the attacker IP **10.0.2.4** over **port 4443**, associated with **PID 4332 (w3wp.exe)**, consistent with the previously identified reverse shell activity.

Volatility Workbench Command:

windows.pstree.PsTree

This plugin lists processes in a hierarchical tree based on parent process IDs.

Process Identified:

*** 4332 2452 w3wp.exe 0xce06574ca080 0–0 False
2024–09–10 05:44:45.000000 UTC 2024–09–10 06:10:48.000000 UTC
\Device\HarddiskVolume1\Windows\System32\inetsrv\w3wp.exe

The process **w3wp.exe** (IIS Worker Process) was confirmed as the executable associated with the network connection, further linking the malicious activity to the compromised web service process.

Malware Analysis

Q9
Weight : 2 | Solved : 917

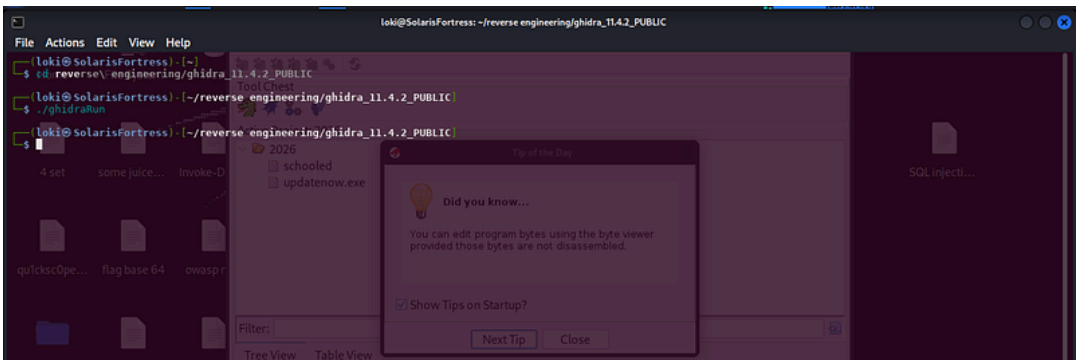
Static inspection reveals the binary has been packed to hinder analysis. Which packer was used to obfuscate it?

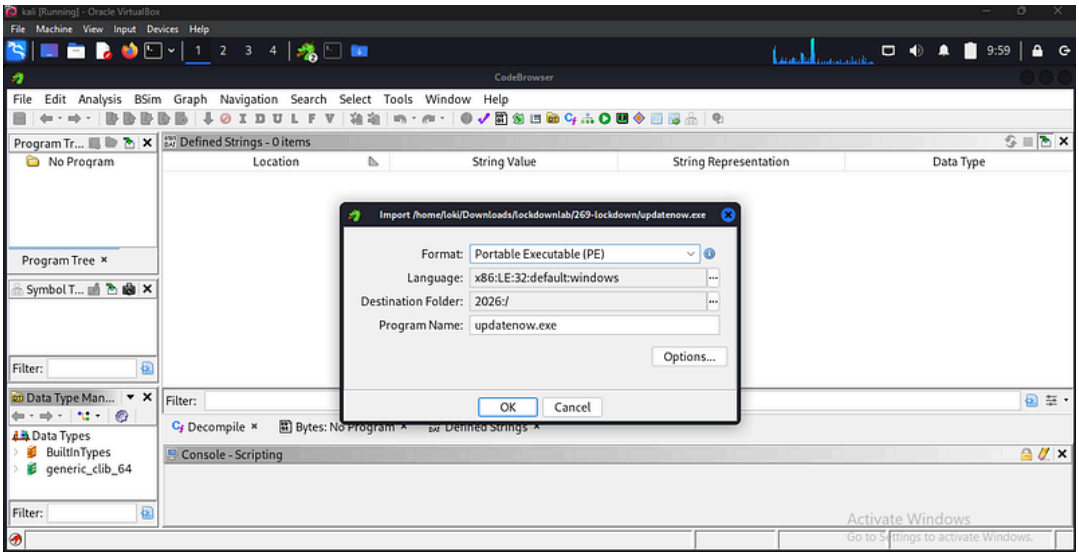
flag: UPX

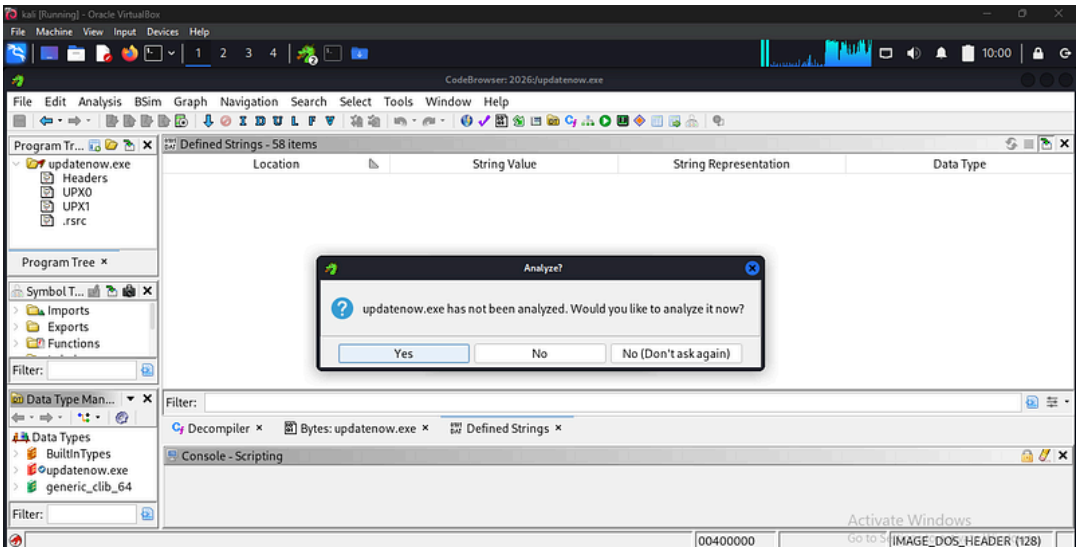
Process:

Ghidra was launched during the analysis.

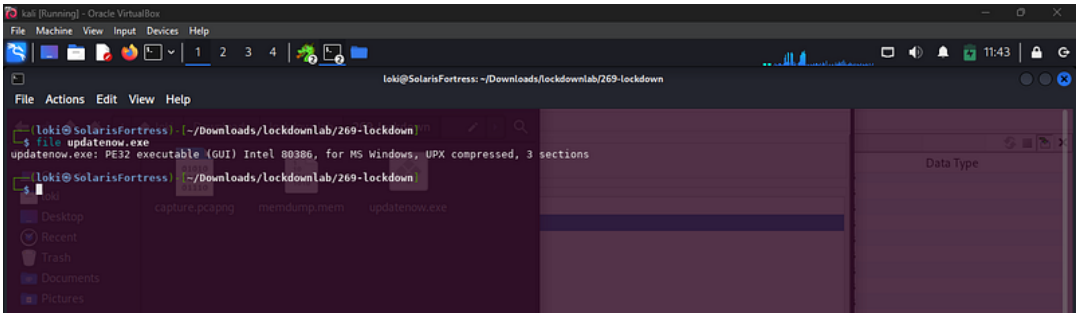
The file **updatenow.exe** was added to a new project.





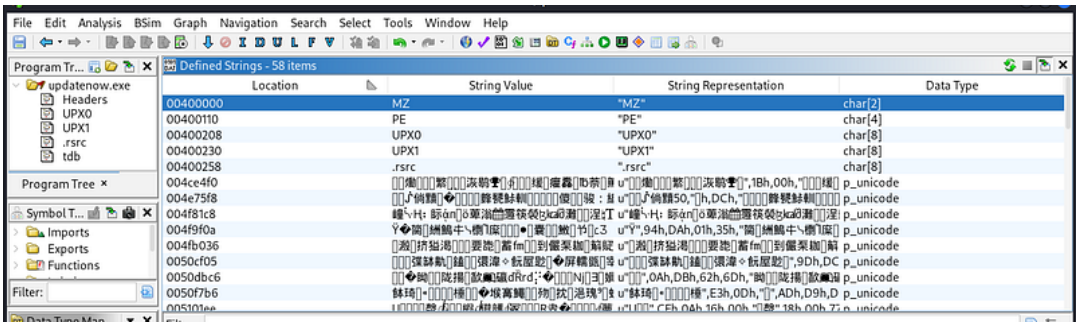


The file command was used to inspect the executable, which revealed the following information:



updatenow.exe: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed, 3 sections

This indicates that **UPX** was used as the packer.



Additionally, within Ghidra, navigating to the **Defined Strings** or the **Program Trees** section shows **UPX0** and **UPX1**, which are well-known indicators of UPX-packed binaries.

Q10
Weight : 2 | Solved : 888

Threat-intel analysis shows the malware beaconing to its command-and-control host. Which fully qualified domain name (FQDN) does it contact?

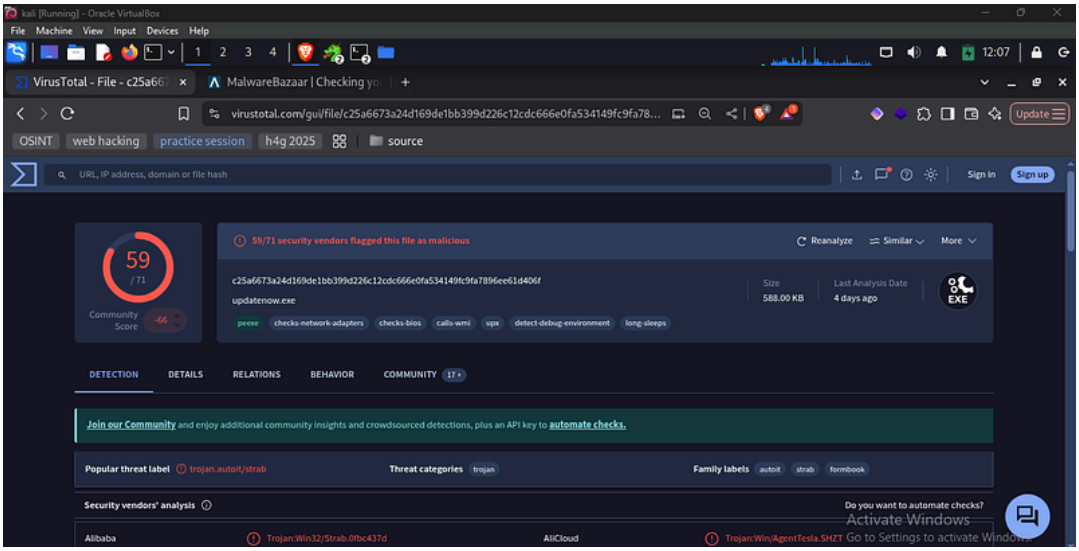
flag : cp8nl.hyperhost.ua

Process:

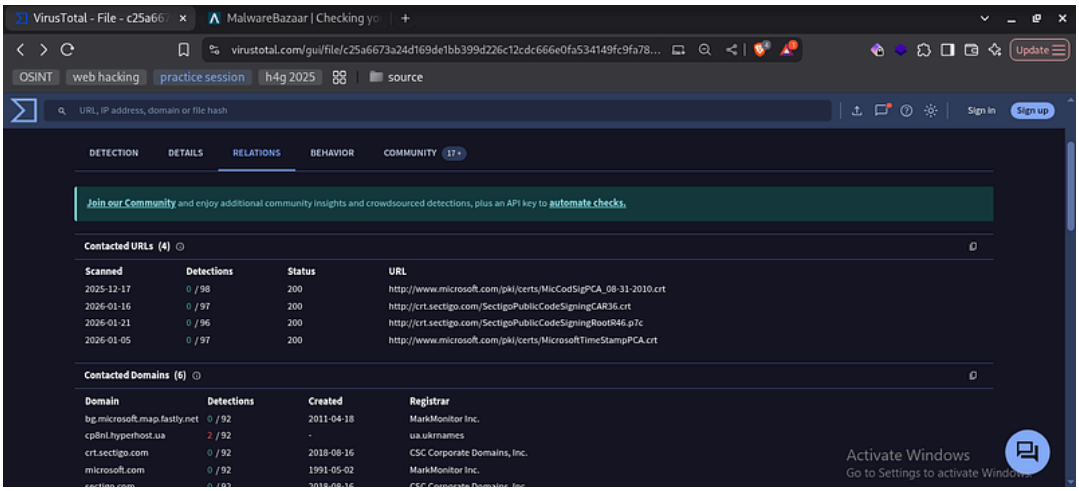
As mentioned during the threat intelligence phase, it was assumed that this file had already been reported. The analysis therefore proceeded by checking the file on **VirusTotal** or **MalwareBazaar**.

The file **updatenow.exe** was uploaded to VirusTotal.

Results showed that **59 out of 71** security vendors flagged the file as malicious.



To further investigate, the **Relations** section was examined.
Under this category, the contacted domains were listed.



One of the domains identified was **cp8nl.hyperhost.ua**, which had a detection rate of **2/92**.
This confirms the domain that was previously identified during the investigation.

Q11
Weight : 2 | Solved : 889

Open-source intel associates that hash with a well-known commodity RAT. To which malware family does the sample belong?

flag : AgentTesla

Process:

The analysis continued by reviewing additional categories in the **Community** section, where the malware family was identified.

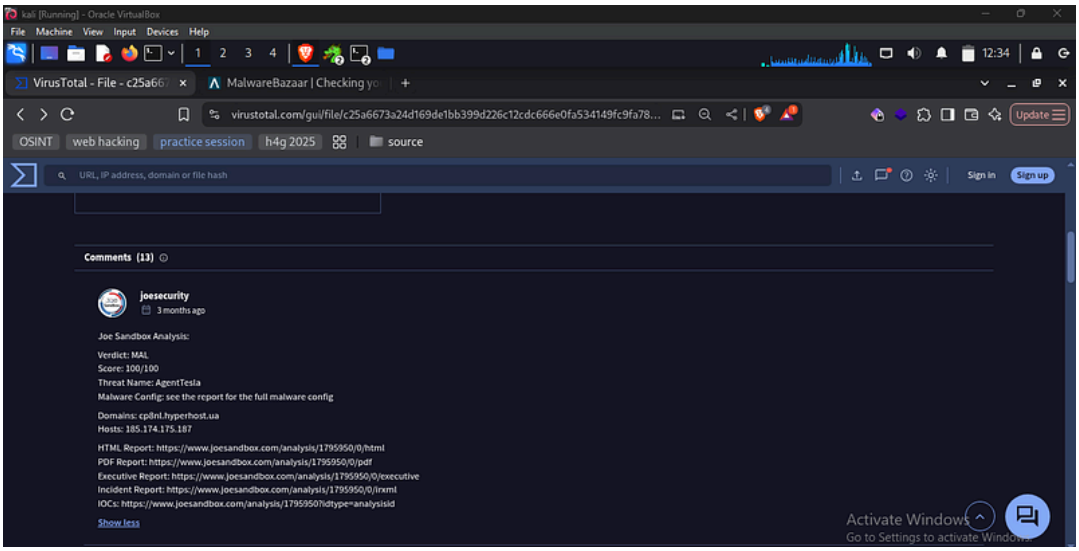
Based on the sandbox analysis from **Joe Sandbox**, the following results were reported:

Joe Sandbox Analysis:

- **Verdict:** MAL
- **Score:** 100/100
- **Threat Name:** AgentTesla
- **Malware Configuration:** Refer to the report for the complete malware configuration
- **Domains:** cp8nl.hyperhost.ua
- **Hosts:** 185.174.175.187

Reports:

- HTML Report: https://www.joesandbox.com/analysis/1795950/0/html
- PDF Report: https://www.joesandbox.com/analysis/1795950/0/pdf
- Executive Report: https://www.joesandbox.com/analysis/1795950/0/executive
- Incident Report: https://www.joesandbox.com/analysis/1795950/0/irxml
- Indicators of Compromise (IOCs): https://www.joesandbox.com/analysis/1795950?idtype=analysisid



This confirms that **updatenow.exe** belongs to the **AgentTesla** malware family and is associated with the previously identified domain and host.

By Alexander Sapo on January 24, 2026.

Canonical link

Exported from Medium on February 7, 2026.