

CyberDenders Write-up: Lockdown Lab

Practice > Lockdown

Lockdown Lab

Reconstruct a multi-stage intrusion by analyzing network traffic, memory, and malware artifacts using Wireshark, Volatility, and VirusTotal, mapping findings to MITRE ATT&CK.

Category: Network Forensics

Tactics: Execution Persistence Privilege Escalation Defense Evasion Discovery Lateral Movement Command and Control

Tools: Wireshark MemProcFS Volatility 3 FLOSS/Strings Threat Intel tools

Easy 1hr ★★★★★ 4.6

[Bookmark](#) [Join the Lab Squad](#) [Report an Issue](#)

Scenario

TechNova Systems' SOC has detected suspicious outbound traffic from a public-facing IIS server in its cloud platform—activity suggestive of a web-shell drop and covert connections to an unknown host.

As the forensic examiner, you have three critical artefacts in hand: a PCAP capturing the initial traffic, a full memory image of the server, and a malware sample recovered from disk.

Reconstruct the intrusion and all of the attacker's activities so TechNova can contain the breach and strengthen its defenses.

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:

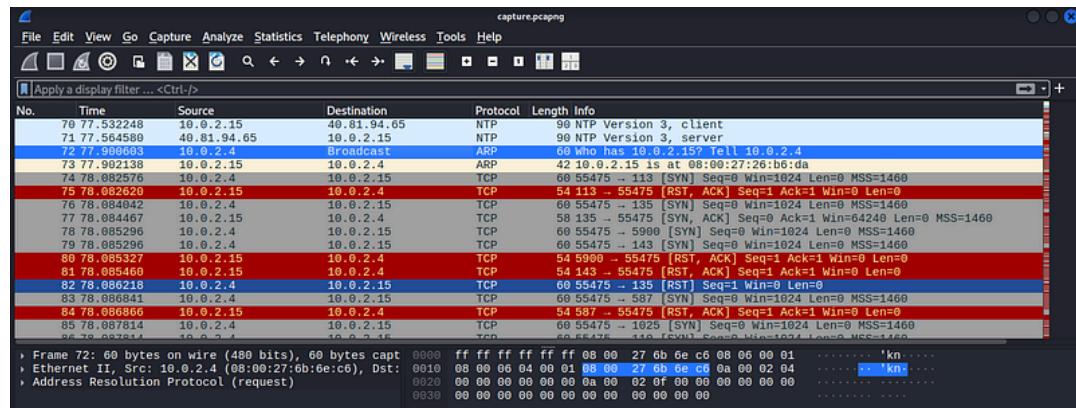
Source consulted: <https://www.clrn.org/what-does-red-mean-in-wireshark/>

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

The screenshot shows the MITRE ATT&CK website. The navigation bar includes links for Metrics, Tactics, Techniques, Defenses, CTI, Resources, Benefactors, and Blog. A search bar is also present. The main content area displays the 'Boot or Logon Autostart Execution' technique, which is categorized under 'BITS Jobs' and 'Boot or Logon Autostart Execution'. The sub-techniques section lists 14 items. The description notes that adversaries may configure system settings to automatically execute programs during boot or logon. The sub-technique T1547 (ID: T1547) is detailed, listing its sub-techniques (T1547.001 through T1547.015), tactics (Persistence, Privilege Escalation), platforms (Linux, Network Devices, Windows, macOS), version (1.3), and creation date (23 January 2020).

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 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\$

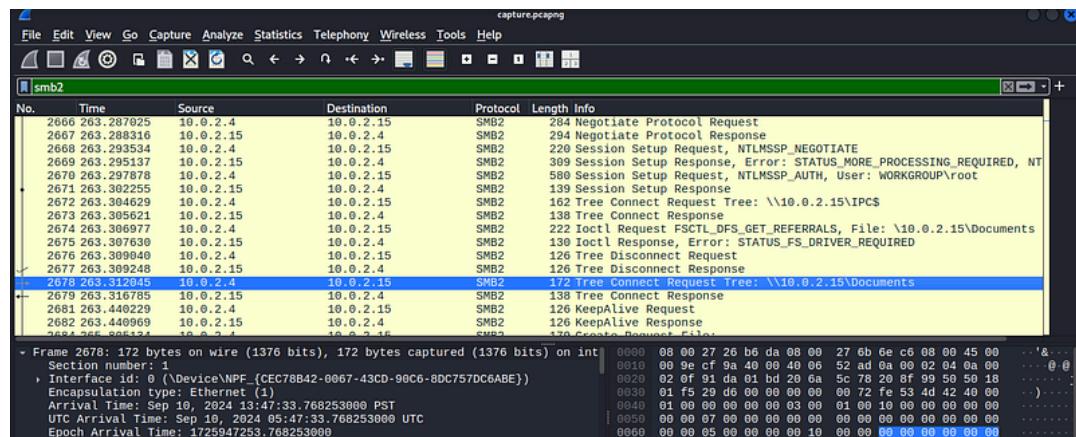
process:

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?

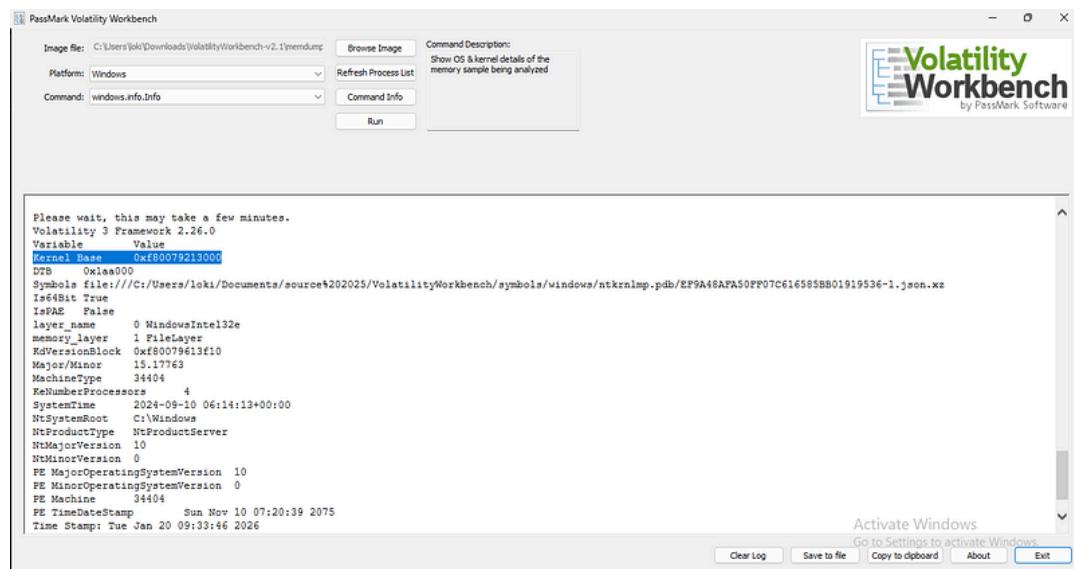
flag: oxf80079213000

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

```

PS C:\Users\loki\Downloads\VolatilityWorkbench-v2.1> ./volatility.exe -f ./memdump.mem imageinfo
Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win10x64_17134, Win10x64_14393, Win10x64_10586, Win10x64_16299, Win2016x64_14393, Win10x64_17763, Win10x64_15063 (Instantiated with Win10x64_15063)
AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (C:\Users\loki\Downloads\VolatilityWorkbench-v2.1\memdump.mem)
PAE type : No PAE
DTB : 0xlaaa000L
KDBG : 0xf80079610a80L
Number of Processors : 4
Image Type (Service Pack) : 0
KPCR for CPU 0 : 0xfffffff800781db900L
KPCR for CPU 1 : 0xfffffaa81f3c20000L
KPCR for CPU 2 : 0xfffffaa81f3cc0000L
KPCR for CPU 3 : 0xfffffaa81f3dc1c00L
HUSER_SHARED_DATA : 0xfffff78000000000L
Image date and time : 2024-09-10 06:14:13 UTC+0000
Image local date and time : 2024-09-10 11:44:13 +0530

```

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

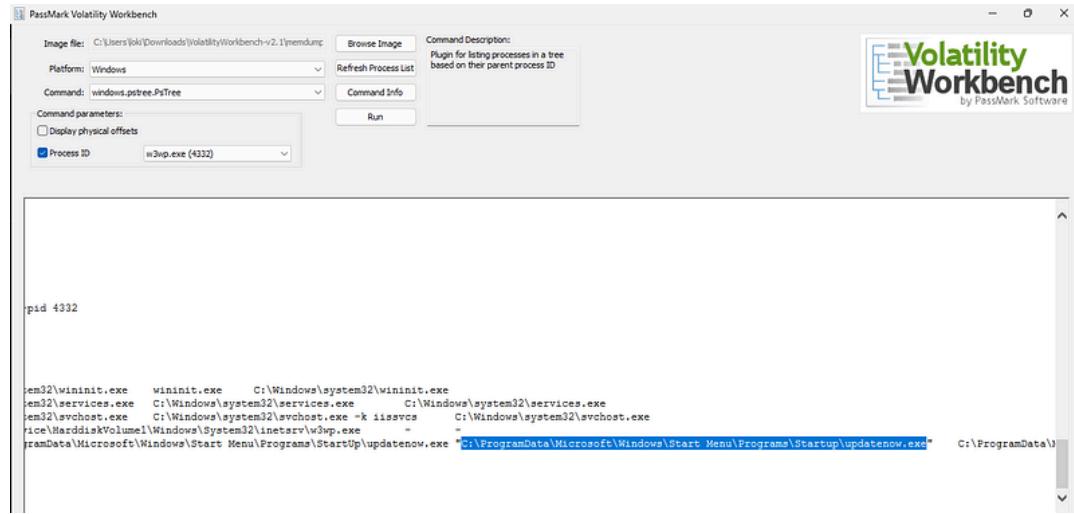
PID specified: **4332**

Findings:

```
***** 900 4332 updatenow.exe oxce0657ddb1c0 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"
```

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	Audit	Cmd	Path
508	396	wininit.exe	0xce0657e9a080	1	-	0	False	2024-09-10 05:29:04.000000 UTC	N/A			\Device\HarddiskVolume1\Windows\System32\wi
* 628	508	services.exe	0xce0657eba080	7	-	0	False	2024-09-10 05:29:06.000000 UTC	N/A			\Device\HarddiskVolume1\Windows\System32\se
** 2452	628	svchost.exe	0xce06571cb280	15	-	0	False	2024-09-10 05:30:04.000000 UTC	N/A			\Device\HarddiskVolume1\Windows\System32\sv
*** 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\ProgramData
**** 900	4332	updatenow.exe	0xce0657ddb1c0	3	-	0	True	2024-09-10 06:08:23.000000 UTC	N/A			\Device\HarddiskVolume1\ProgramData

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/>

MITRE | ATT&CK®

Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Resources ▾ Benefactors Blog ↗ Search ⚙

ATT&CK v18 has been released! Check out the blog post or changelog for more information.

Home > Techniques > Enterprise > Boot or Logon Autostart Execution

Boot or Logon Autostart Execution

Sub-techniques (14)

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon. [1][2][3][4] These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel.

Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

ID: T1547

Sub-techniques: T1547.001, T1547.002, T1547.003, T1547.004, T1547.005, T1547.006, T1547.007, T1547.008, T1547.009, T1547.010, T1547.012, T1547.013, T1547.014, T1547.015

① Tactics: Persistence, Privilege Escalation

① Platforms: Linux, Network Devices, Windows, macOS

Version: 1.3

Last updated: 2023-03-20

Created: 2019-03-20

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:

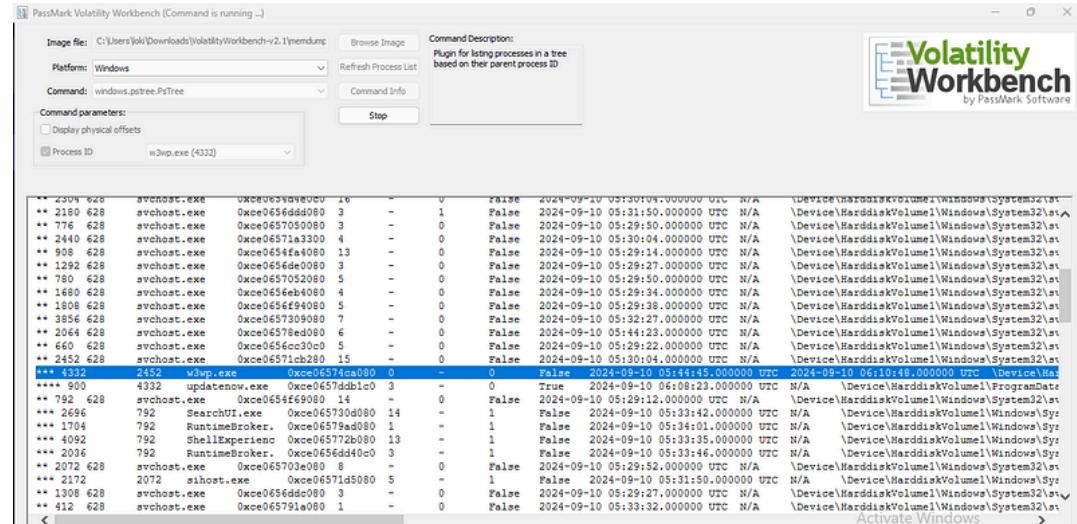
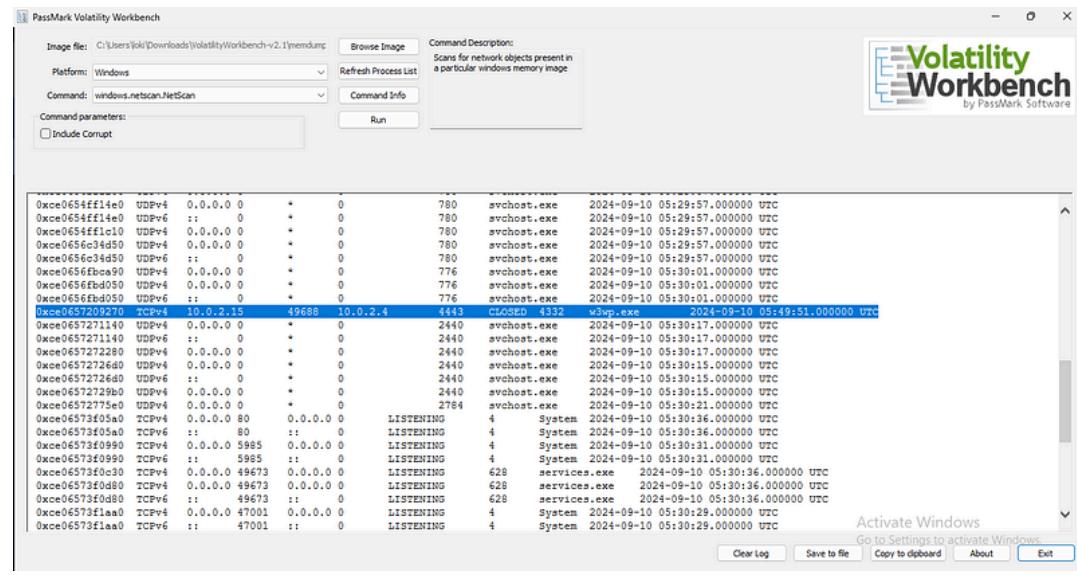
Revisiting the earlier network analysis, the threat actor's IP address **10.0.2.4** and the port **4443** were identified as being used within the internal network.

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 05:49:51.000

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 oxce06574cao80 o-o 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

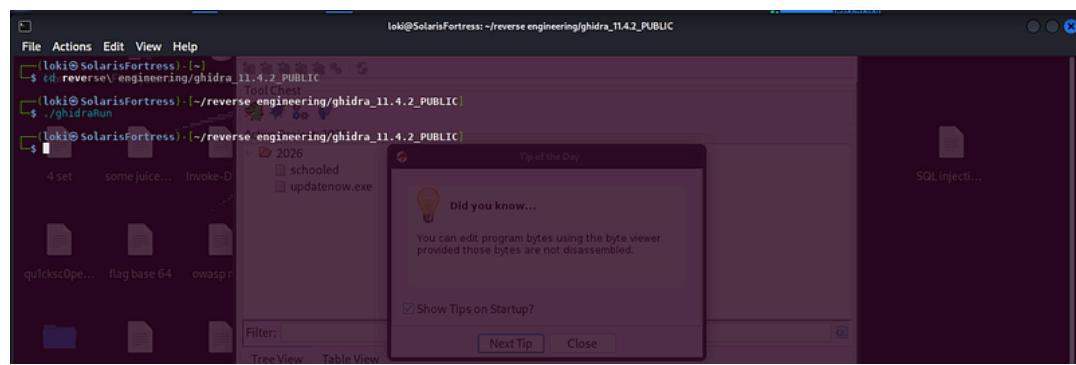
Static inspection reveals the binary has been packed to hinder analysis. Which packer was used to obfuscate it?

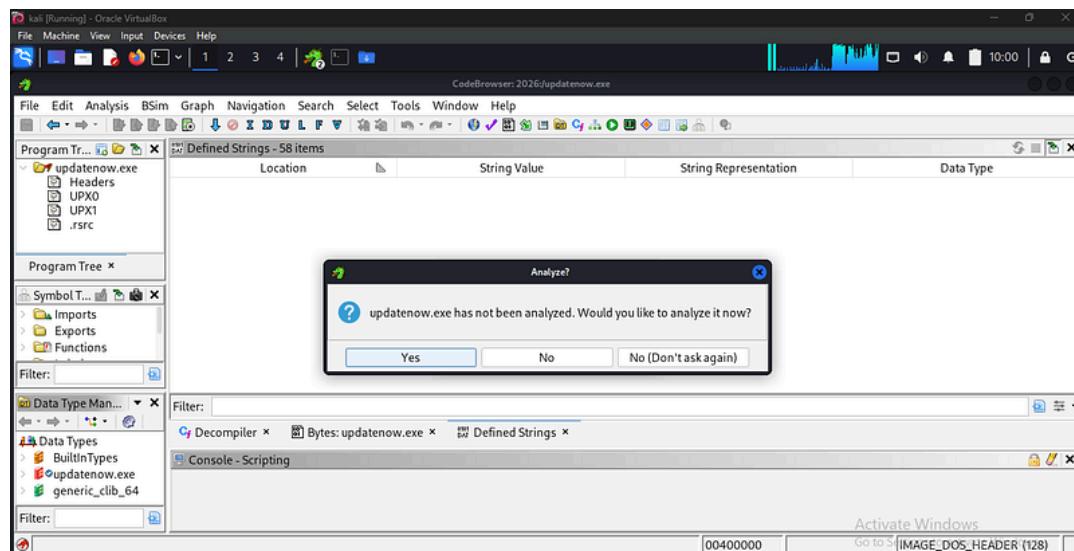
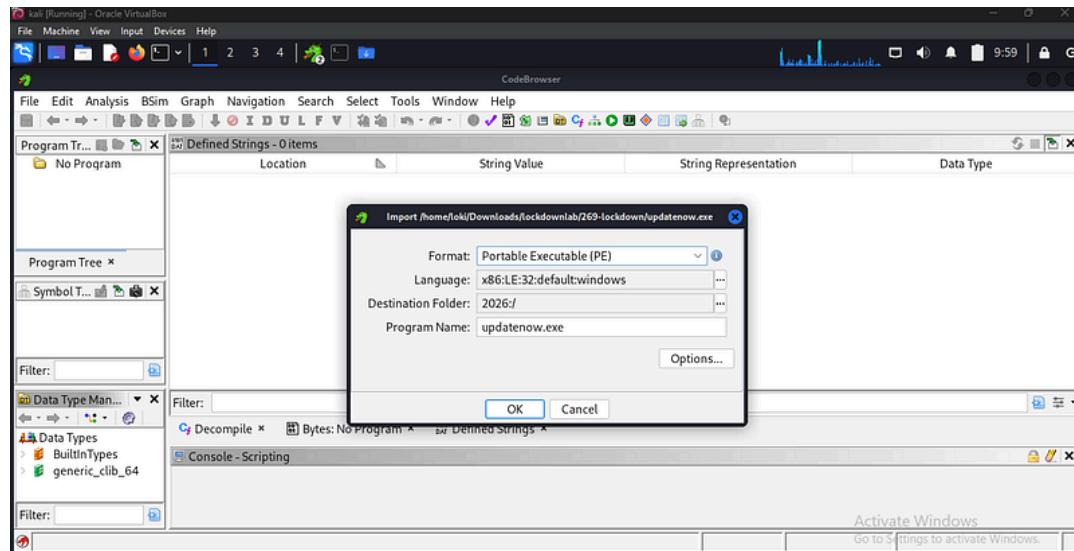
flag: UPX

Process:

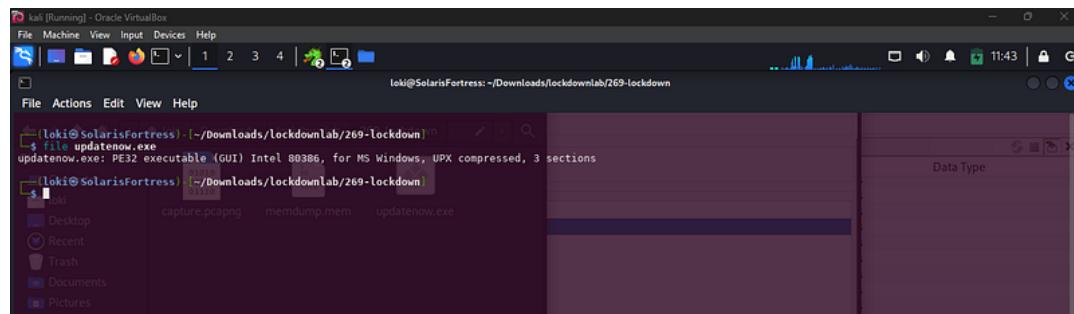
Ghidra was launched during the analysis.

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



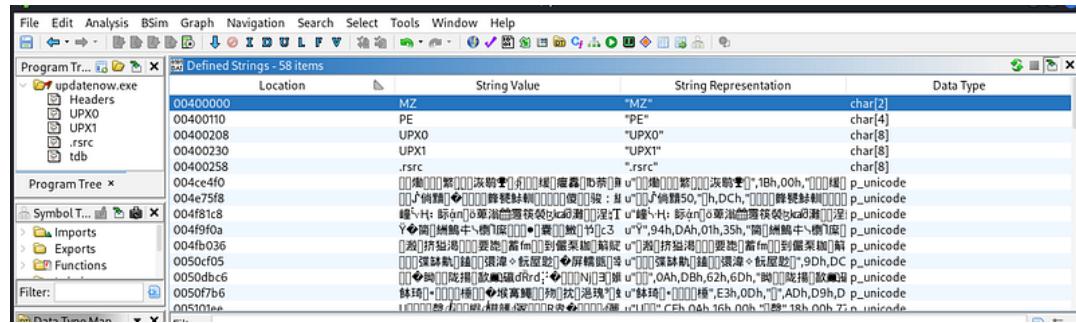


The file command was used to inspect the executable, which revealed the following information:



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.

59/71 security vendors flagged this file as malicious

c25a6673a24d169de1bb399d226c12cdc666e0fa534149fc9fa7896ee61d406f
updateNow.exe

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.autolostrab Threat categories: trojan Family labels: autolostrab, formbook

Security vendors' analysis: Alibaba (Trojan:Win32/Strab!rbc497d), AliCloud (Trojan:Win/AgentTesla.SHZ)

Activate Windows: Go to Settings to activate Windows

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

Scanned	Detections	Status	URL
2025-12-17	0 / 98	200	http://www.microsoft.com/pki/certs/MicCodSigPCA_08-31-2010.crt
2026-01-16	0 / 97	200	http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt
2026-01-21	0 / 96	200	http://crt.sectigo.com/SectigoPublicCodeSigningRootRA6.p7c
2026-01-05	0 / 97	200	http://www.microsoft.com/pki/certs/MicrosoftTimeStampPCA.crt

Domain	Detections	Created	Registrar
bg.microsoft.map.fastly.net	0 / 92	2011-04-18	MarkMonitor Inc., us.uknames
cp8nl.hyperhost.ua	2 / 92		
crt.sectigo.com	0 / 92	2018-08-16	CSC Corporate Domains, Inc.
microsoft.com	0 / 92	1991-05-02	MarkMonitor Inc.
sectigo.com	0 / 92	2018-08-16	CSC Corporate Domains, Inc.

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.

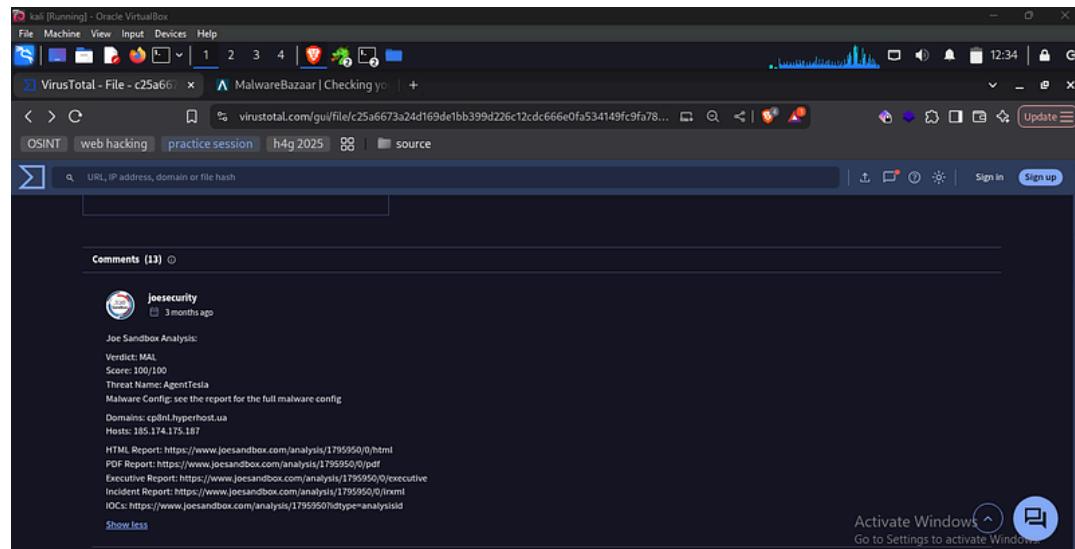
Based on the sandbox analysis from **Joe Sandbox**, the following results were reported:

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/o/html>
- PDF Report: <https://www.joesandbox.com/analysis/1795950/o/pdf>
- Executive Report: <https://www.joesandbox.com/analysis/1795950/o/executive>
- Incident Report: <https://www.joesandbox.com/analysis/1795950/o/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.