REPORT LockdownLab

Analyst: Ruslan
Date: 2026-01-19

1. Incident Summary

During the investigation, it was determined that the Windows IIS server with IP address 10.0.2.15 was compromised by host 10.0.2.4. The attack enabled network reconnaissance, unauthorized file writing via SMB, web shell download, and installation of parent software with a persistence mechanism. This compromise allows the attacker to secure code execution and maintain a stable command and control channel.

2. Detection Details

Anomalous activity was detected during network traffic analysis and forensic data analysis. Signs of a port scan of the target host were detected, followed by SMB connections and file writing to directories accessible by the IIS web server. Additionally, atypical outgoing connections to the non-standard TCP port 4443 were detected.

3. Analysis

Network logs confirm that host 10.0.2.4 was actively scanning ports of server 10.0.2.15. After the reconnaissance phase, the attacker gained access to the SMB shares and placed a shell.aspx file in a web-accessible IIS directory. The file's size and structure indicate a web shell designed for remote command execution.

After placing the web shell, a reverse communication channel was established, initiated from the victim server to an external host on TCP port 4443. This connection was persistent and was used for remote system management.

As part of their next steps, the attacker placed the executable file updatenow.exe in the Windows startup directory. Memory analysis revealed that this binary was launched by the w3wp.exe process, which is anomalous behavior for IIS and confirms the service was compromised. The file was packed using UPX and was identified as malware from the AgentTesla family.

Network interaction with the domain cp8nl.hyperhost.ua, used as a control infrastructure, was also recorded.

4. Impact Assessment

The server compromise is considered complete. The attacker has achieved remote code execution and established a persistence mechanism. The presence of AgentTesla indicates a risk of credential theft and possible information leakage. There is a possibility of further escalation of the attack, including lateral movement within the network.

5. Indicators of Compromise

The following indicators were confirmed during the investigation:

- Attacker's IP address: 10.0.2.4.

- Compromised host: 10.0.2.15.
- Web shell: shell.aspx.
- Malicious file: updatenow.exe.
- C2 domain: cp8nl.hyperhost.ua.
- Port used: TCP/4443.

Conclusion

The investigation confirms a targeted attack on an IIS server using a web shell and subsequent installation of a persistent RAT. The incident poses a high risk to the infrastructure and requires host isolation, removal of malicious components, and further in-depth analysis of the environment.

Analysis

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

Statistics → Conversations → IPv4:

Ethernet · 12 | IPv4 · 16 | IPv6 · 4 | TCP · 1085 | UDP · 39

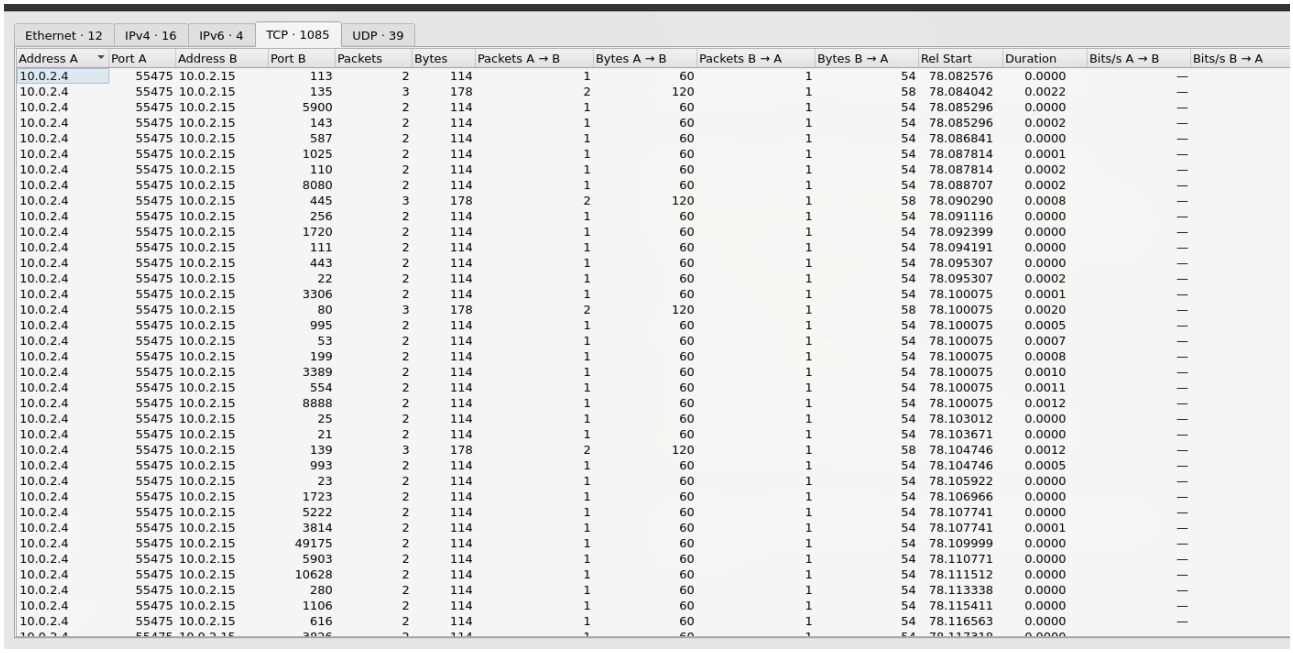
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.0.2.4	10.0.2.15	6,007	3,652 k	4,166	3,468 k	1,841	184 k	78.082576	1434.6036	19 k	
10.0.2.15	52.252.198.177	4	228	2	108	2	120	0.000000	0.2820	3,063	
10.0.2.15	192.168.1.1	52	4,656	46	3,624	6	1,032	0.948048	1029.9916	28	
10.0.2.15	20.242.39.171	35	19 k	16	12 k	19	6,743	0.957982	3.4821	29 k	
10.0.2.15	216.58.200.163	12	1,526	7	792	5	734	53.663407	63.3154	100	
10.0.2.15	23.58.93.34	24	3,450	14	1,805	10	1,645	53.750251	63.2284	228	
10.0.2.15	40.81.94.65	14	1,260	7	630	7	630	77.532248	1280.2031	3	
10.0.2.15	10.0.2.3	10	4,660	5	1,710	5	2,950	84.517280	1199.3760	11	
10.0.2.15	224.0.0.22	25	1,350	25	1,350	0	0	84.546591	1199.7954	9	
10.0.2.15	224.0.0.251	14	1,274	14	1,274	0	0	84.560786	1199.3855	8	
10.0.2.15	224.0.0.252	7	462	7	462	0	0	84.567243	1199.3847	3	
10.0.2.15	104.26.10.240	4	228	2	108	2	120	102.344396	0.0098	87 k	
10.0.2.15	10.0.2.255	2	486	2	486	0	0	145.653875	720.2510	5	
10.0.2.15	20.42.73.29	24	11 k	11	5,459	13	5,670	573.288138	1.2100	36 k	
10.0.2.15	20.198.118.190	5	550	2	207	3	343	608.774473	343.0272	4	
10.0.2.15	20.198.119.143	21	8,222	11	2,870	10	5,352	1030.943915	0.3470	66 k	

We see a large number of packets sent from host 10.0.2.4 to host 10.0.2.15. One host sends many requests/packets, but the responses are significantly smaller and "lighter" in size.

Answer: 10.0.2.4

2. 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?

Statistics → Conversations: → TCP:



Ethernet · 12 | IPv4 · 16 | IPv6 · 4 | TCP · 1085 | UDP · 39

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.0.2.4	55475	10.0.2.15	113	2	114	1	60	1	54	78.082576	0.0000	—	
10.0.2.4	55475	10.0.2.15	135	3	178	2	120	1	58	78.084042	0.0022	—	
10.0.2.4	55475	10.0.2.15	5900	2	114	1	60	1	54	78.085296	0.0000	—	
10.0.2.4	55475	10.0.2.15	143	2	114	1	60	1	54	78.085296	0.0002	—	
10.0.2.4	55475	10.0.2.15	587	2	114	1	60	1	54	78.086841	0.0000	—	
10.0.2.4	55475	10.0.2.15	1025	2	114	1	60	1	54	78.087814	0.0001	—	
10.0.2.4	55475	10.0.2.15	110	2	114	1	60	1	54	78.087814	0.0002	—	
10.0.2.4	55475	10.0.2.15	8080	2	114	1	60	1	54	78.088707	0.0002	—	
10.0.2.4	55475	10.0.2.15	445	3	178	2	120	1	58	78.090290	0.0008	—	
10.0.2.4	55475	10.0.2.15	256	2	114	1	60	1	54	78.091116	0.0000	—	
10.0.2.4	55475	10.0.2.15	1720	2	114	1	60	1	54	78.092399	0.0000	—	
10.0.2.4	55475	10.0.2.15	111	2	114	1	60	1	54	78.094191	0.0000	—	
10.0.2.4	55475	10.0.2.15	443	2	114	1	60	1	54	78.095307	0.0000	—	
10.0.2.4	55475	10.0.2.15	22	2	114	1	60	1	54	78.095307	0.0002	—	
10.0.2.4	55475	10.0.2.15	3306	2	114	1	60	1	54	78.100075	0.0001	—	
10.0.2.4	55475	10.0.2.15	80	3	178	2	120	1	58	78.100075	0.0020	—	
10.0.2.4	55475	10.0.2.15	995	2	114	1	60	1	54	78.100075	0.0005	—	
10.0.2.4	55475	10.0.2.15	53	2	114	1	60	1	54	78.100075	0.0007	—	
10.0.2.4	55475	10.0.2.15	199	2	114	1	60	1	54	78.100075	0.0008	—	
10.0.2.4	55475	10.0.2.15	3389	2	114	1	60	1	54	78.100075	0.0010	—	
10.0.2.4	55475	10.0.2.15	554	2	114	1	60	1	54	78.100075	0.0011	—	
10.0.2.4	55475	10.0.2.15	8888	2	114	1	60	1	54	78.100075	0.0012	—	
10.0.2.4	55475	10.0.2.15	25	2	114	1	60	1	54	78.103012	0.0000	—	
10.0.2.4	55475	10.0.2.15	21	2	114	1	60	1	54	78.103671	0.0000	—	
10.0.2.4	55475	10.0.2.15	139	3	178	2	120	1	58	78.104746	0.0012	—	
10.0.2.4	55475	10.0.2.15	993	2	114	1	60	1	54	78.104746	0.0005	—	
10.0.2.4	55475	10.0.2.15	23	2	114	1	60	1	54	78.105922	0.0000	—	
10.0.2.4	55475	10.0.2.15	1723	2	114	1	60	1	54	78.106966	0.0000	—	
10.0.2.4	55475	10.0.2.15	5222	2	114	1	60	1	54	78.107741	0.0000	—	
10.0.2.4	55475	10.0.2.15	3814	2	114	1	60	1	54	78.107741	0.0001	—	
10.0.2.4	55475	10.0.2.15	49175	2	114	1	60	1	54	78.109999	0.0000	—	
10.0.2.4	55475	10.0.2.15	5903	2	114	1	60	1	54	78.110771	0.0000	—	
10.0.2.4	55475	10.0.2.15	10628	2	114	1	60	1	54	78.111512	0.0000	—	
10.0.2.4	55475	10.0.2.15	280	2	114	1	60	1	54	78.113338	0.0000	—	
10.0.2.4	55475	10.0.2.15	1106	2	114	1	60	1	54	78.115411	0.0000	—	
10.0.2.4	55475	10.0.2.15	616	2	114	1	60	1	54	78.116563	0.0000	—	

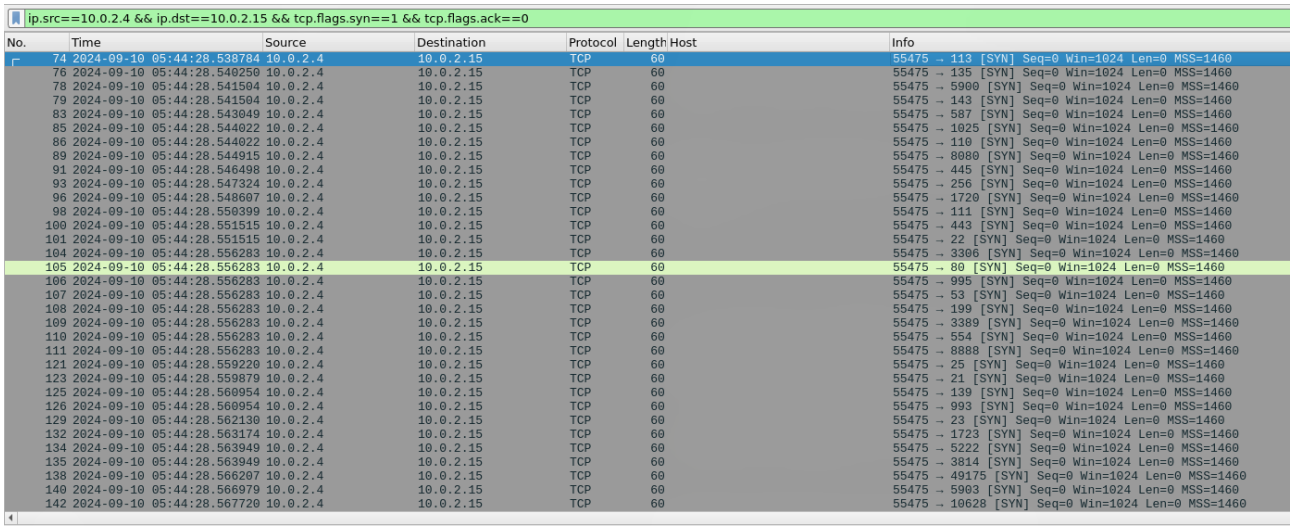
It can be seen that one source 10.0.2.4 from one source port 55475 goes to 10.0.2.15 via many different destination ports.

Using the filter: ip.src==10.0.2.4 && ip.dst==10.0.2.15 && tcp.flags.syn==1 && tcp.flags.ack==0, you can see a series of SYNs to different ports.

This is most likely Network Service Discovery (T1046): "which services/ports are available on the host."

Answer: T1046

3. 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?



ip.src==10.0.2.4 && ip.dst==10.0.2.15 && tcp.flags.syn==1 && tcp.flags.ack==0

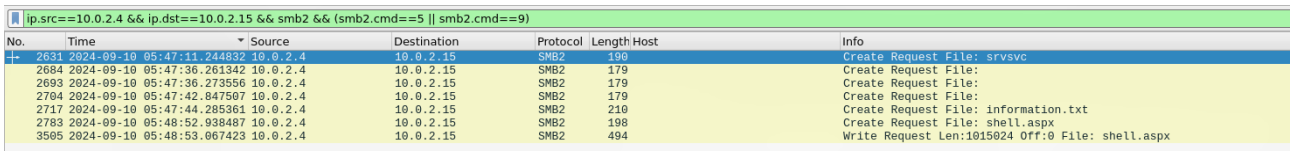
No.	Time	Source	Destination	Protocol	Length	Host	Info
74	2024-09-10 05:44:28.538784	10.0.2.4	10.0.2.15	TCP	60		55475 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
76	2024-09-10 05:44:28.540250	10.0.2.4	10.0.2.15	TCP	60		55475 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78	2024-09-10 05:44:28.541504	10.0.2.4	10.0.2.15	TCP	60		55475 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
79	2024-09-10 05:44:28.541504	10.0.2.4	10.0.2.15	TCP	60		55475 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
83	2024-09-10 05:44:28.543049	10.0.2.4	10.0.2.15	TCP	60		55475 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
85	2024-09-10 05:44:28.544022	10.0.2.4	10.0.2.15	TCP	60		55475 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
86	2024-09-10 05:44:28.544022	10.0.2.4	10.0.2.15	TCP	60		55475 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
89	2024-09-10 05:44:28.544915	10.0.2.4	10.0.2.15	TCP	60		55475 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
91	2024-09-10 05:44:28.546498	10.0.2.4	10.0.2.15	TCP	60		55475 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
93	2024-09-10 05:44:28.547324	10.0.2.4	10.0.2.15	TCP	60		55475 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
96	2024-09-10 05:44:28.548607	10.0.2.4	10.0.2.15	TCP	60		55475 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
98	2024-09-10 05:44:28.550399	10.0.2.4	10.0.2.15	TCP	60		55475 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
100	2024-09-10 05:44:28.551515	10.0.2.4	10.0.2.15	TCP	60		55475 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
101	2024-09-10 05:44:28.551515	10.0.2.4	10.0.2.15	TCP	60		55475 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
104	2024-09-10 05:44:28.556283	10.0.2.4	10.0.2.15	TCP	60		55475 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
105	2024-09-10 05:44:28.556283	10.0.2.4	10.0.2.15	TCP	60		55475 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
106	2024-09-10 05:44:28.556283	10.0.2.4	10.0.2.15	TCP	60		55475 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
107	2024-09-10 05:44:28.556283	10.0.2.4	10.0.2.15	TCP	60		55475 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
108	2024-09-10 05:44:28.556283	10.0.2.4	10.0.2.15	TCP	60		55475 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
109	2024-09-10 05:44:28.556283	10.0.2.4	10.0.2.15	TCP	60		55475 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
110	2024-09-10 05:44:28.556283	10.0.2.4	10.0.2.15	TCP	60		55475 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
111	2024-09-10 05:44:28.556283	10.0.2.4	10.0.2.15	TCP	60		55475 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
121	2024-09-10 05:44:28.559220	10.0.2.4	10.0.2.15	TCP	60		55475 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
123	2024-09-10 05:44:28.559879	10.0.2.4	10.0.2.15	TCP	60		55475 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
125	2024-09-10 05:44:28.560954	10.0.2.4	10.0.2.15	TCP	60		55475 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
126	2024-09-10 05:44:28.560954	10.0.2.4	10.0.2.15	TCP	60		55475 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
129	2024-09-10 05:44:28.562130	10.0.2.4	10.0.2.15	TCP	60		55475 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
132	2024-09-10 05:44:28.563174	10.0.2.4	10.0.2.15	TCP	60		55475 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
134	2024-09-10 05:44:28.563949	10.0.2.4	10.0.2.15	TCP	60		55475 → 5222 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135	2024-09-10 05:44:28.563949	10.0.2.4	10.0.2.15	TCP	60		55475 → 3814 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
138	2024-09-10 05:44:28.566207	10.0.2.4	10.0.2.15	TCP	60		55475 → 49175 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
140	2024-09-10 05:44:28.566979	10.0.2.4	10.0.2.15	TCP	60		55475 → 5903 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
142	2024-09-10 05:44:28.567720	10.0.2.4	10.0.2.15	TCP	60		55475 → 10628 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Answer:
1. \\10.0.2.15\IPC$

2. \\10.0.2.15\Documents

4. 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?

ip.src==10.0.2.4 && ip.dst==10.0.2.15 && smb2 && (smb2.cmd==5 || smb2.cmd==9)



ip.src==10.0.2.4 && ip.dst==10.0.2.15 && smb2 && (smb2.cmd==5 || smb2.cmd==9)

No.	Time	Source	Destination	Protocol	Length	Host	Info
2631	2024-09-10 05:47:11.244832	10.0.2.4	10.0.2.15	SMB2	190		Create Request File: srvsvc
2684	2024-09-10 05:47:36.261342	10.0.2.4	10.0.2.15	SMB2	179		Create Request File:
2693	2024-09-10 05:47:36.273556	10.0.2.4	10.0.2.15	SMB2	179		Create Request File:
2704	2024-09-10 05:47:42.847507	10.0.2.4	10.0.2.15	SMB2	179		Create Request File:
2717	2024-09-10 05:47:44.285361	10.0.2.4	10.0.2.15	SMB2	210		Create Request File: information.txt
2783	2024-09-10 05:48:52.938487	10.0.2.4	10.0.2.15	SMB2	198		Create Request File: shell.aspx
3505	2024-09-10 05:48:53.067423	10.0.2.4	10.0.2.15	SMB2	494		Write Request Len:1015024 Off:0 File: shell.aspx

Downloaded malicious file name: shell.aspx

Byte length in SMB2 Write Request: 1015024 bytes

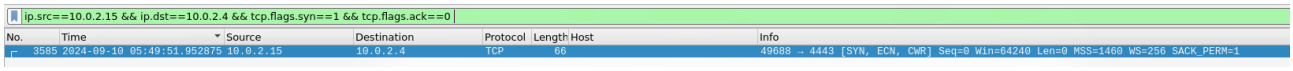
Answer: shell.aspx, 1015024

5. 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?

ip.src==10.0.2.15 && ip.dst==10.0.2.4 && tcp.flags.syn==1 && tcp.flags.ack==0

49688 is the client's source (ephemeral) port, which is chosen randomly/temporarily by the OS.

4443 is the destination port on 10.0.2.4, i.e., the port the client is attempting to connect to.



Answer: 4443

6. 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?

vol -f memdump.mem windows.info

```
Kernel Base     0xf80079213000
DTB     0x1aa000
Symbols file:///home/ruslan/.local/lib/python3.10/site-packages/volatility3/symbols/windows/ntkrnlmp.pdb/EF9A48AFA50FF07C616585BB01919536-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf80079613f10
Major/Minor     15.17763
MachineType     34404
KeNumberProcessors      4
SystemTime      2024-09-10 06:14:13+00:00
NtSystemRoot    C:\Windows
NtProductType   NtProductServer
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Sun Nov 10 07:20:39 2075
```

Answer: 0xf80079213000

7.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?

python3 vol.py -f memdump.mem windows.pslist

```
4332    2452    w3wp.exe        0xce06574ca080  0       -       0       False   2024-09-10 05:44:45.000000 UTC  2024-09-10 06:10:48.000000 UTC  Disabled
1676    1628    taskhostw.exe   0xce0656e46080  6       -       1       False   2024-09-10 05:52:43.000000 UTC  N/A     Disabled
900     4332    updatenow.exe   0xce0657ddb1c0  3       -       0       True    2024-09-10 06:08:23.000000 UTC  N/A     Disabled
```

There's w3wp.exe (PID 4332)—an IIS Worker Process. It started at 05:44:45 and exited at 06:10:48.

Suspicious: updatenow.exe (PID 900). Parent (PPID) = 4332 = w3wp.exe (IIS). This means the IIS process launched updatenow.exe.

vol -f memdump.mem windows.cmdline --pid 900

```
ruslan@pop-os:~/Downloads/269-lockdown$ vol -f memdump.mem windows.cmdline --pid 900
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
PID     Process Args

900     updatenow.exe   "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\updatenow.exe"
```

MITRE ATT&CK T1547 (Boot or Logon Autostart Execution) is a persistence technique where an attacker configures a system so that their malicious code automatically runs when Windows boots or when a user logs on.

Answer: C:\ProgramData\Microsoft\Windows\StartMenu\Programs\Startup\updatenow.exe, T1547

8. 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?

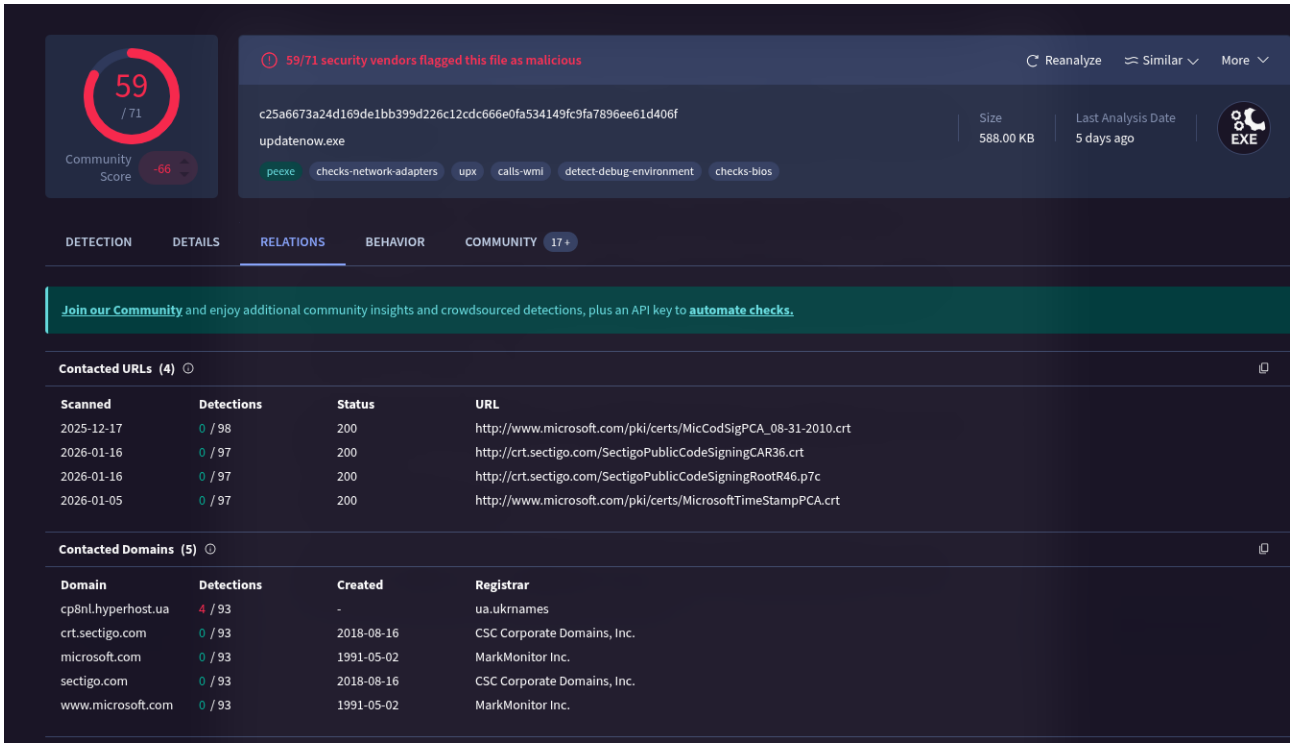
Answer: Answer: w3wp.exe, 4332

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

Using DIE we found answer: upx

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

Using VirusTotal:



By navigating to the 'Relations' section, we can find the domain we are looking for .

Answer: cp8nl.hyperhost.ua

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

You can see the verdicts in the Community section. AgentTesla is a common Windows Trojan spyware (RAT/infostealer) that typically steals user data: logins/passwords (browsers, email clients), keystrokes (keylogging), clipboard contents, sometimes taking screenshots and sending them to the attacker (often via SMTP/FTP/HTTP).

Answer: AgentTesla