CyberDefenders

RESOLUCIÓN DE LABORATORIO

Caso: Lockdown (CyberDefenders)

Investigación forense (DFIR) de un servidor IIS, abarcando el análisis de red (PCAP), extracción de procesos ocultos en memoria RAM y perfilamiento del malware Agent Tesla.

Sebastian David
Torres Reyes

Escenario:

El SOC de TechNova Systems ha detectado tráfico saliente sospechoso desde un servidor IIS público en su plataforma en la nube. Esta actividad sugiere una caída de la web-shell y conexiones encubiertas a un host desconocido.

Como examinador forense, usted cuenta con tres elementos críticos: un PCAP que captura el tráfico inicial, una imagen de memoria completa del servidor y una muestra de malware recuperada del disco. Reconstruya la intrusión y todas las actividades del atacante para que TechNova pueda contener la brecha y reforzar sus defensas.

Herramientas utilizadas:

- Wireshark
- Volatility 3
- flare-floss
- Detect It Easy (DIE)
- VirusTotal
- Tria.ge

PCAP Analysis:

P1: Tras inundar el host IIS con sondeos rápidos, el atacante revela su origen. ¿Qué dirección IP generó este tráfico de reconocimiento?

R: 10.0.2.4

A través del análisis de Estadísticas > Conversaciones (IPv4) en Wireshark, se identificó un volumen anómalo de tráfico originado desde la IP 10.0.2.4 hacia la 10.0.2.15, sumando un total de 6007 paquetes, lo que indica un escaneo de red agresivo.

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

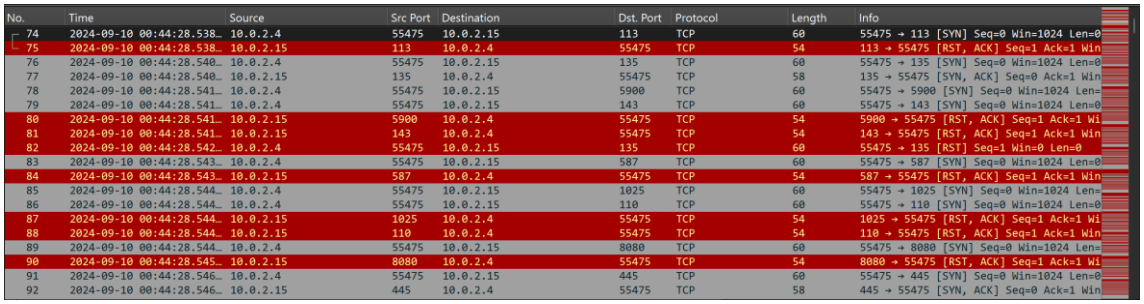
Dirección A	Dirección B	Paquetes	Bytes
10.0.2.4	10.0.2.15	6,007	4 MB
10.0.2.15	10.0.2.3	10	5 kB
10.0.2.15	10.0.2.255	2	486 bytes
10.0.2.15	20.42.73.29	24	11 kB
10.0.2.15	20.198.118.190	5	550 bytes
10.0.2.15	20.198.119.143	21	8 kB
10.0.2.15	20.242.39.171	35	20 kB
10.0.2.15	23.58.93.34	24	3 kB
10.0.2.15	40.81.94.65	14	1 kB
10.0.2.15	52.252.198.177	4	228 bytes
10.0.2.15	104.26.10.240	4	228 bytes
10.0.2.15	192.168.1.1	52	5 kB
10.0.2.15	216.58.200.163	12	2 kB
10.0.2.15	224.0.0.22	25	1 kB
10.0.2.15	224.0.0.251	14	1 kB
10.0.2.15	224.0.0.252	7	462 bytes

En la ventana de Endpoints también se notó que la dirección IP 10.0.2.15 transmitió 2012 paquetes y recibió 4248 paquetes, mientras que la dirección IP 10.0.2.4 transmitió 4166 paquetes y recibió 1841 paquetes.

Ethernet · 12 | IPv4 · 17 | IPv6 · 6 | TCP · 1097 | UDP · 51

Dirección	Paquetes	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
10.0.2.15	6,260	4 MB	2,012	218 kB	4,248	3 MB
10.0.2.4	6,007	4 MB	4,166	3 MB	1,841	184 kB
192.168.1.1	52	5 kB	6	1 kB	46	4 kB
224.0.0.22	25	1 kB	0	0 bytes	25	1 kB
20.242.39.171	35	20 kB	19	7 kB	16	13 kB
23.58.93.34	24	3 kB	10	2 kB	14	2 kB
224.0.0.251	14	1 kB	0	0 bytes	14	1 kB
20.42.73.29	24	11 kB	13	6 kB	11	5 kB
20.198.119.143	21	8 kB	10	5 kB	11	3 kB
40.81.94.65	14	1 kB	7	630 bytes	7	630 bytes
216.58.200.163	12	2 kB	5	734 bytes	7	792 bytes
224.0.0.252	7	462 bytes	0	0 bytes	7	462 bytes
10.0.2.3	10	5 kB	5	3 kB	5	2 kB
10.0.2.255	2	486 bytes	0	0 bytes	2	486 bytes
20.198.118.190	5	550 bytes	3	343 bytes	2	207 bytes
52.252.198.177	4	228 bytes	2	120 bytes	2	108 bytes
104.26.10.240	4	228 bytes	2	120 bytes	2	108 bytes

La gran mayoría de paquetes que recibió la dirección IP 10.0.2.15 en esta conversación fueron paquetes de capa 4 SYN por el puerto 113. Con todos estos patrones de tráfico se dedujo que la dirección IP 10.0.2.15 pertenece al servidor IIS y la dirección IP 10.0.2.4 pertenece al dispositivo del atacante.

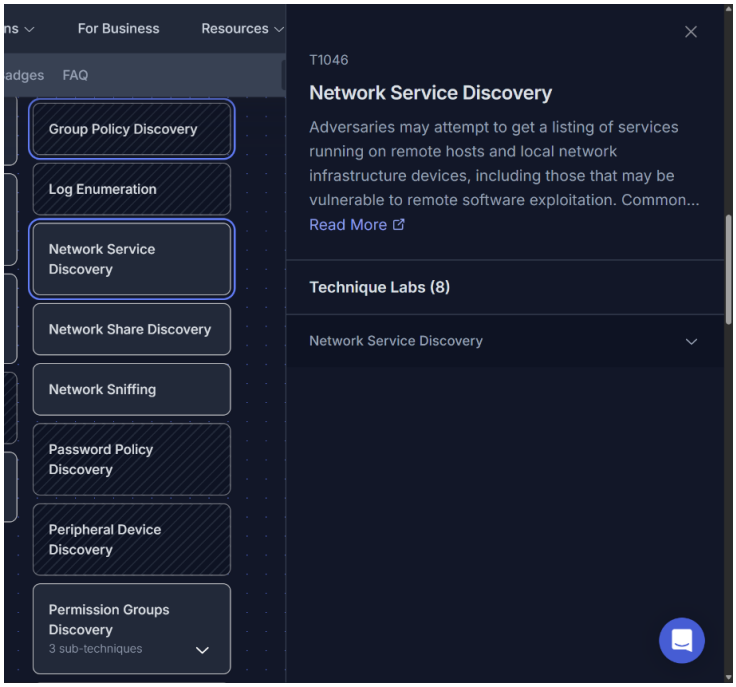


No.	Time	Source	Src Port	Destination	Dst. Port	Protocol	Length	Info
74	2024-09-10 00:44:28.538…	10.0.2.4	55475	10.0.2.15	113	TCP	60	55475 → 113 [SYN] Seq=0 Win=1024 Len=0
75	2024-09-10 00:44:28.538…	10.0.2.15	113	10.0.2.4	55475	TCP	54	113 → 55475 [RST, ACK] Seq=1 Ack=1 Win
76	2024-09-10 00:44:28.540…	10.0.2.4	55475	10.0.2.15	135	TCP	60	55475 → 135 [SYN] Seq=0 Win=1024 Len=0
77	2024-09-10 00:44:28.540…	10.0.2.15	135	10.0.2.4	55475	TCP	58	135 → 55475 [SYN, ACK] Seq=0 Ack=1 Win
78	2024-09-10 00:44:28.541…	10.0.2.4	55475	10.0.2.15	5900	TCP	60	55475 → 5900 [SYN] Seq=0 Win=1024 Len=
79	2024-09-10 00:44:28.541…	10.0.2.4	55475	10.0.2.15	143	TCP	60	55475 → 143 [SYN] Seq=0 Win=1024 Len=0
80	2024-09-10 00:44:28.541…	10.0.2.15	5900	10.0.2.4	55475	TCP	54	5900 → 55475 [RST, ACK] Seq=1 Ack=1 Wi
81	2024-09-10 00:44:28.541…	10.0.2.15	143	10.0.2.4	55475	TCP	54	143 → 55475 [RST, ACK] Seq=1 Ack=1 Win
82	2024-09-10 00:44:28.542…	10.0.2.4	55475	10.0.2.15	135	TCP	60	55475 → 135 [RST] Seq=1 Win=0 Len=0
83	2024-09-10 00:44:28.543…	10.0.2.4	55475	10.0.2.15	587	TCP	60	55475 → 587 [SYN] Seq=0 Win=1024 Len=0
84	2024-09-10 00:44:28.543…	10.0.2.15	587	10.0.2.4	55475	TCP	54	587 → 55475 [RST, ACK] Seq=1 Ack=1 Win
85	2024-09-10 00:44:28.544…	10.0.2.4	55475	10.0.2.15	1025	TCP	60	55475 → 1025 [SYN] Seq=0 Win=1024 Len=
86	2024-09-10 00:44:28.544…	10.0.2.4	55475	10.0.2.15	110	TCP	60	55475 → 110 [SYN] Seq=0 Win=1024 Len=0
87	2024-09-10 00:44:28.544…	10.0.2.15	1025	10.0.2.4	55475	TCP	54	1025 → 55475 [RST, ACK] Seq=1 Ack=1 Wi
88	2024-09-10 00:44:28.544…	10.0.2.15	110	10.0.2.4	55475	TCP	54	110 → 55475 [RST, ACK] Seq=1 Ack=1 Win
89	2024-09-10 00:44:28.544…	10.0.2.4	55475	10.0.2.15	8080	TCP	60	55475 → 8080 [SYN] Seq=0 Win=1024 Len=
90	2024-09-10 00:44:28.545…	10.0.2.15	8080	10.0.2.4	55475	TCP	54	8080 → 55475 [RST, ACK] Seq=1 Ack=1 Wi
91	2024-09-10 00:44:28.546…	10.0.2.4	55475	10.0.2.15	445	TCP	60	55475 → 445 [SYN] Seq=0 Win=1024 Len=0
92	2024-09-10 00:44:28.546…	10.0.2.15	445	10.0.2.4	55475	TCP	58	445 → 55475 [SYN, ACK] Seq=0 Ack=1 Win

P2: El atacante, concentrándose en un solo servicio abierto para establecerse, realiza una enumeración dirigida. ¿Qué ID de técnica de MITRE ATT&CK cubre esta actividad?

R: T1046

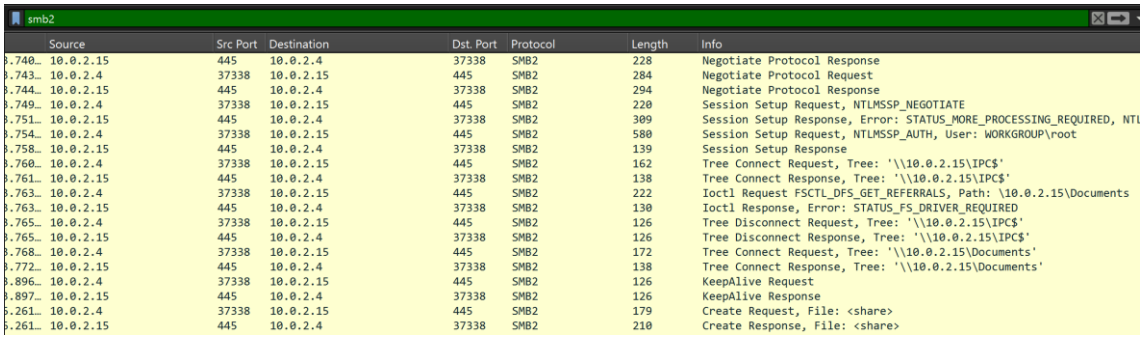
Como el atacante ya realizó un reconocimiento y encontró el puerto 80 abierto entonces, al realizar la enumeración dirigida se pudo inferir que el atacante se encuentra en la táctica DISCOVERY. Luego el atacante que ya tiene acceso inicial intenta descubrir cualquier información útil dentro del servicio HTTP mediante una enumeración dirigida. Este proceso se puede relacionar con la técnica Network Service Discovery con ID T1046.



P3: Al revisar el tráfico SMB, observa dos solicitudes consecutivas de Tree Connect que exponen las primeras acciones de las sondas de intrusión en el host IIS. ¿A qué dos rutas UNC completas se accede?

R: \\10.0.2.15\Documents, \\10.0.2.15\IPC$

Se aplicó el filtro “smb2” para visualizar solamente los paquetes SMB en su versión estándar. Luego de una inspección se notó dos solicitudes consecutivas de Tree Connect. El atacante había ingresado las siguientes dos rutas UNC: \\10.0.2.15\Documents, \\10.0.2.15\IPC$.

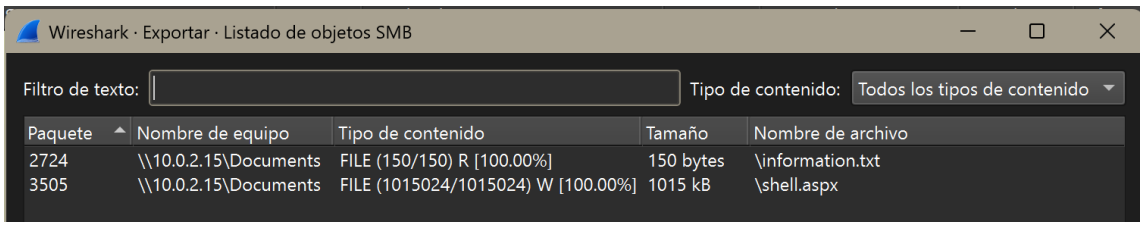

smb2

Source	Src Port	Destination	Dst. Port	Protocol	Length	Info
3.740… 10.0.2.15	445	10.0.2.4	37338	SMB2	228	Negotiate Protocol Response
3.743… 10.0.2.4	37338	10.0.2.15	445	SMB2	284	Negotiate Protocol Request
3.744… 10.0.2.15	445	10.0.2.4	37338	SMB2	294	Negotiate Protocol Response
3.749… 10.0.2.4	37338	10.0.2.15	445	SMB2	220	Session Setup Request, NTLMSSP_NEGOTIATE
3.751… 10.0.2.15	445	10.0.2.4	37338	SMB2	309	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTL
3.754… 10.0.2.4	37338	10.0.2.15	445	SMB2	580	Session Setup Request, NTLMSSP_AUTH, User: WORKGROUP\root
3.758… 10.0.2.15	445	10.0.2.4	37338	SMB2	139	Session Setup Response
3.760… 10.0.2.4	37338	10.0.2.15	445	SMB2	162	Tree Connect Request, Tree: '\\10.0.2.15\IPC$'
3.761… 10.0.2.15	445	10.0.2.4	37338	SMB2	138	Tree Connect Response, Tree: '\\10.0.2.15\IPC$'
3.763… 10.0.2.4	37338	10.0.2.15	445	SMB2	222	Ioctl Request FSCTL_DFS_GET_REFERRALS, Path: \10.0.2.15\Documents
3.763… 10.0.2.15	445	10.0.2.4	37338	SMB2	130	Ioctl Response, Error: STATUS_FS_DRIVER_REQUIRED
3.765… 10.0.2.4	37338	10.0.2.15	445	SMB2	126	Tree Disconnect Request, Tree: '\\10.0.2.15\IPC$'
3.765… 10.0.2.15	445	10.0.2.4	37338	SMB2	126	Tree Disconnect Response, Tree: '\\10.0.2.15\IPC$'
3.768… 10.0.2.4	37338	10.0.2.15	445	SMB2	172	Tree Connect Request, Tree: '\\10.0.2.15\Documents'
3.772… 10.0.2.15	445	10.0.2.4	37338	SMB2	138	Tree Connect Response, Tree: '\\10.0.2.15\Documents'
3.896… 10.0.2.4	37338	10.0.2.15	445	SMB2	126	KeepAlive Request
3.897… 10.0.2.15	445	10.0.2.4	37338	SMB2	126	KeepAlive Response
5.261… 10.0.2.4	37338	10.0.2.15	445	SMB2	179	Create Request, File: <share>
5.261… 10.0.2.15	445	10.0.2.4	37338	SMB2	210	Create Response, File: <share>

P4: Dentro del recurso compartido, el atacante instala una carga útil accesible desde la web que permitirá la ejecución remota de código. ¿Cuál es el nombre del archivo malicioso que subieron y qué longitud de bytes se especifica en la solicitud de escritura SMB2 correspondiente?

R: shell.aspx,1015024

Empleando la función 'Export Objects > SMB' de Wireshark, se logró extraer el payload transferido por la red. Se identificó el archivo shell.aspx (típicamente usado para ejecutar código del lado del servidor en entornos IIS), el cual fue subido al recurso compartido por el atacante, confirmando una inyección exitosa con un tamaño de 1015024 bytes.


Wireshark · Exportar · Listado de objetos SMB

Filtro de texto: Tipo de contenido: Todos los tipos de contenido

Paquete	Nombre de equipo	Tipo de contenido	Tamaño	Nombre de archivo
2724	\\10.0.2.15\Documents	FILE (150/150) R [100.00%]	150 bytes	\information.txt
3505	\\10.0.2.15\Documents	FILE (1015024/1015024) W [100.00%]	1015 kB	\shell.aspx

P5: El shell recién instalado devuelve la llamada al atacante a través de un puerto poco común, pero compatible con el firewall. ¿Qué puerto de escucha usó el atacante para la shell inversa?

R: 4443

Un indicador clave de una *reverse shell* es cuando el servidor comprometido inicia una nueva conexión hacia el atacante. Para aislar este evento, se aplicó el filtro "tcp.flags.syn == 1 && tcp.flags.ack == 0 && ip.src == 10.0.2.15 && ip.dst == 10.0.2.4". Esto reveló que el servidor intentó establecer un túnel TCP hacia la máquina atacante a través del puerto no estándar 4443.

Memory Dump Aanlysis:

P6: Su instantánea de memoria captura el núcleo del sistema in situ, lo que proporciona un contexto vital para la brecha. ¿Cuál es la dirección base del núcleo en el volcado?

R: 0xf80079213000

Se hizo uso de Volatility 3 para tener la información de la captura instantánea de la memoria RAM. El plugin windows.info determinó que la dirección base del kernel es 0xf80079213000.

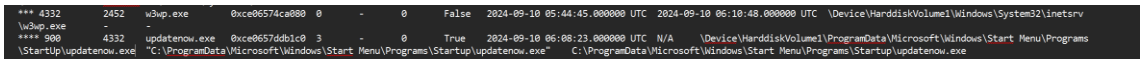
```
Variable        Value

Kernel Base     0xf80079213000
DTB     0x1aa000
Symbols file:///C:/Users/sebas/AppData/Local/Temp/_MEI328882/volatility3/symbols/windows/ntkrnlmp.pdb/EF9A48AFA50FF07C61
6585BB01919536-1.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
```

P7: Un servicio de confianza lanza un ejecutable desconocido que reside fuera de la pila habitual de IIS, lo que indica una implantación de persistencia. ¿Cuál es la ruta completa final en disco de dicho ejecutable y qué ID de la técnica de persistencia de MITRE ATT&CK corresponde a este comportamiento?

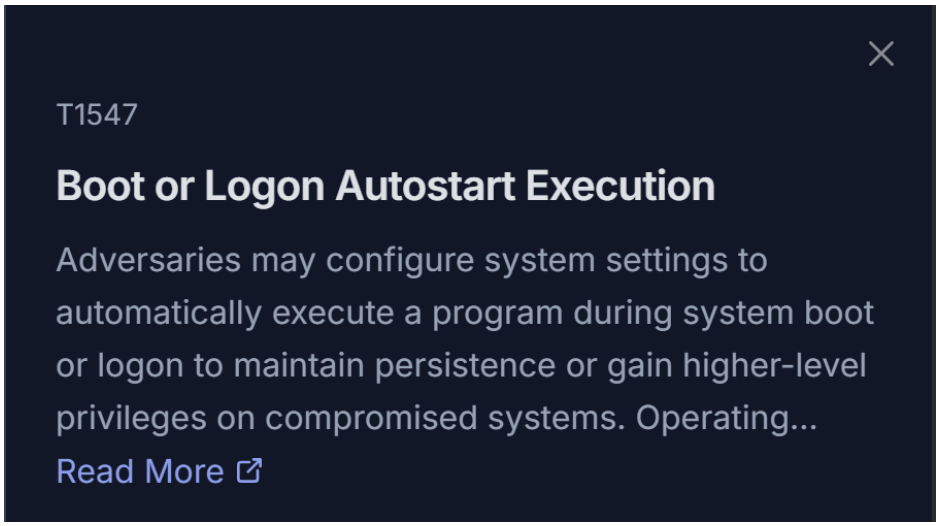
R: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\updatenow.exe, T1547

Cuando se trata de IIS uno de los servicios más importantes de confianza es w3wp.exe ya que actúa como el motor de ejecución de aplicaciones web en IIS. Para visualizar el árbol de procesos y verificar si este o algún otro servicio lanza un ejecutable se usó la herramienta Volatility 3 con el comando 'vol.exe -f "RUTA DEL ARCHIVO .mem" windows.pstree > pstree.txt' y se descubrió que el servicio w3wp.exe lanzó un ejecutable con el nombre de "updatenow.exe".



El servicio w3wp.exe no esta diseñado para lanzar aplicaciones externas sino para procesar solicitudes web. Sabiendo esto, se dedujo que el ejecutable desconocido tiene como ruta "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\updatenow.exe"

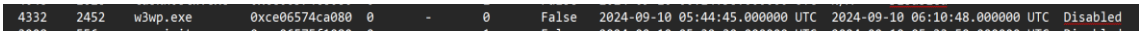
El ejecutable se encuentra en el directorio Startup, un directorio usado para ejecuciones automáticas, esta técnica esta relacionada a la técnica de resistencia "Boot or Logon Autostart Execution" con el ID T1547.



P8: El tráfico saliente del shell inverso lo gestiona un proceso integrado de Windows que también genera el ejecutable implantado. ¿Cómo se llama este proceso y bajo qué PID se ejecuta?

R: w3wp.exe, 4332

El análisis de memoria confirma que el proceso responsable de ejecutar la *web shell* (shell.aspx) y establecer la conexión reversa es w3wp.exe, operando bajo el PID4332.

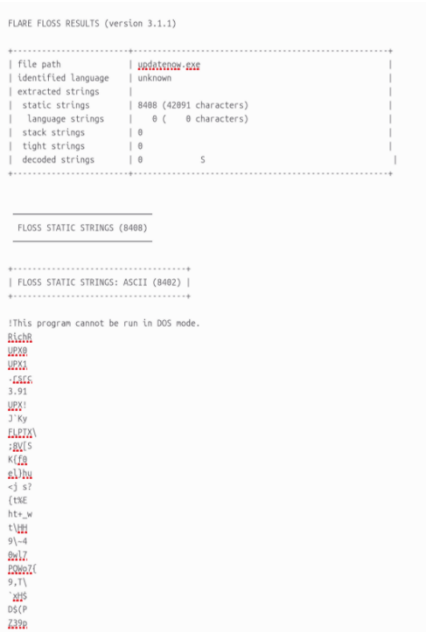


Malware Sample Analysis:

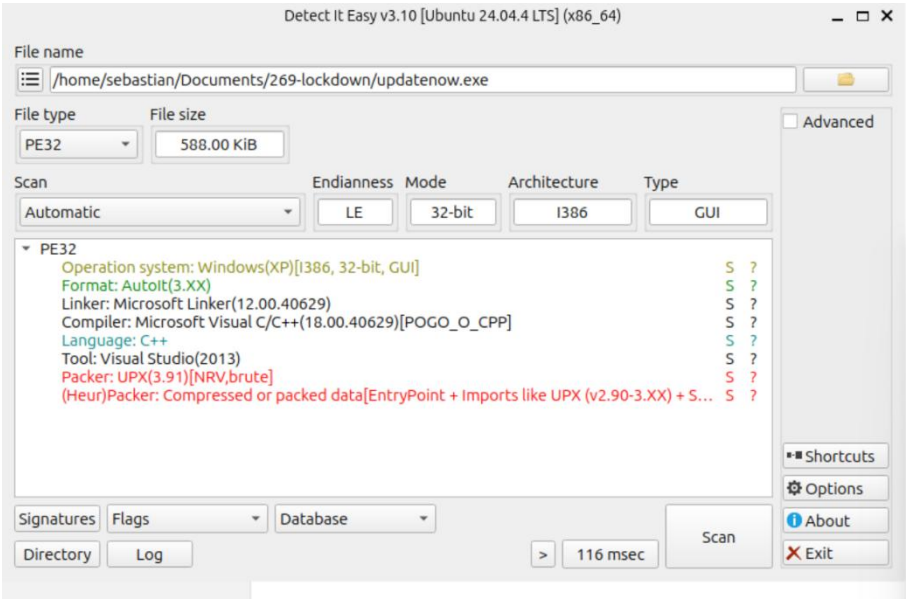
P9: La inspección estática revela que el binario se comprimió para dificultar el análisis. ¿Qué empaquetador se utilizó para ofuscarlo?

R: UPX

Mediante una herramienta llamada flare-floss usada para realizar análisis estático se verificó la ofuscación del ejecutable. Aquí se encontró una gran cantidad de datos inentendibles u ocultos.



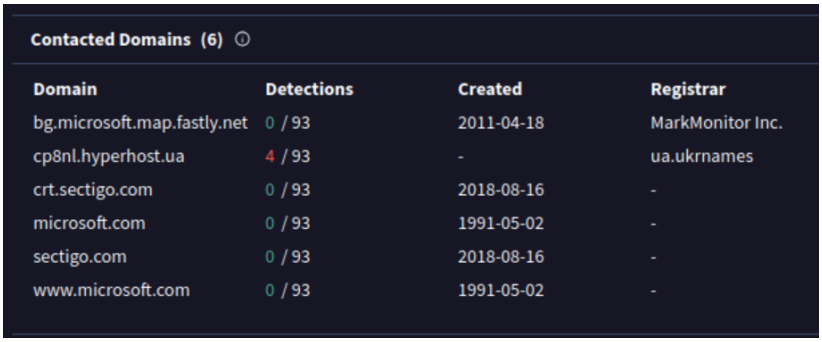
Para extraer la información de lo que se usó para crear este ejecutable malicioso se hizo uso de otra herramienta, Detect It Easy (DIE), que cuenta con una base de datos extensa y que también realiza análisis estático de ejecutables, pero se centra en la comparación de firmas digitales. Finalmente se halló información y el nombre del empaquetador llamado UPX.



P10: El análisis de inteligencia de amenazas muestra que el malware se dirige a su host de comando y control. ¿A qué nombre de dominio completo (FQDN) se conecta?

R: cp8nl.hyperhost.ua

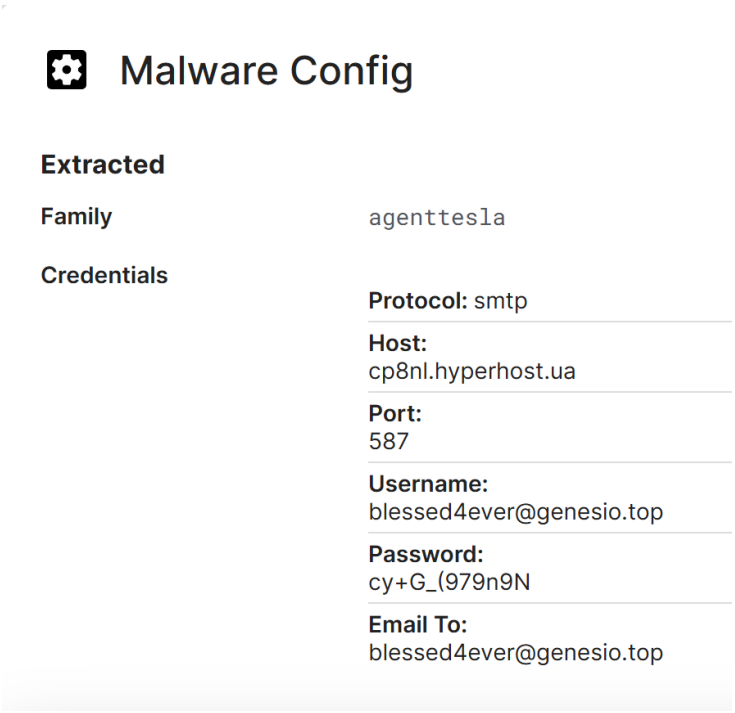
Al analizar el ejecutable malicioso en VirusTotal, en el apartado de Relations se pudo observar los dominios contactados. El único dominio detectado malicioso por los motores de antivirus fue cp8nl.hyperhost.ua.



Contacted Domains (6)

Domain	Detections	Created	Registrar
bg.microsoft.map.fastly.net	0 / 93	2011-04-18	MarkMonitor Inc.
cp8nl.hyperhost.ua	4 / 93	-	ua.ukrnames
crt.sectigo.com	0 / 93	2018-08-16	-
microsoft.com	0 / 93	1991-05-02	-
sectigo.com	0 / 93	2018-08-16	-
www.microsoft.com	0 / 93	1991-05-02	-

Adicionalmente, se utilizó Tria.ge para buscar la información del análisis dinámico del ejecutable malicioso. Aquí se comprueba que el host C&C al que se conecta el malware es cp8nl.hyperhost.ua.



P11: La inteligencia de código abierto asocia ese hash con un RAT común y conocido. ¿A qué familia de malware pertenece la muestra?

R: agenttesla

En la información encontrada del análisis dinámico también se pudo hallar la familia del malware. Esta familia llamada “agenttesla” es un RAT avanzado basado en el framwork .NET que se especializa en el robo de credenciales y datos confidenciales de sistemas Windows.