



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

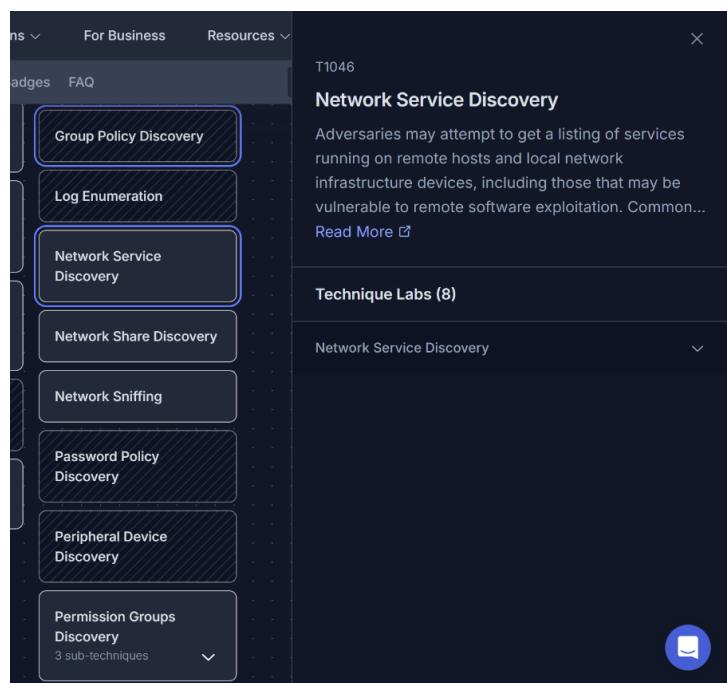
La gran mayoría de paquetes que recibió la dirección IP 10.0.2.15 en esta conversación fueron paquetes de capa 4 SYN por el puerto 113. Con todos estos patrones de tráfico se dedujo que la dirección IP 10.0.2.15 pertenece al servidor IIS y la dirección IP 10.0.2.4 pertenece al dispositivo del atacante.

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=1 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=0
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 Win
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=3 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=0
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 Win
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=0
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 Win
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\$.

Source	Src Port	Destination	Dst. Port	Protocol	Length	Info
10.0.2.15	445	10.0.2.4	37338	SMB2	228	Negotiate Protocol Response
10.0.2.4	37338	10.0.2.15	445	SMB2	284	Negotiate Protocol Request
10.0.2.15	445	10.0.2.4	37338	SMB2	294	Negotiate Protocol Response
10.0.2.4	37338	10.0.2.15	445	SMB2	228	Session Setup Request, NTLMSSP_NEGOTIATE
10.0.2.15	445	10.0.2.4	37338	SMB2	309	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_AUTH, User: WORKGROUP\root
10.0.2.4	37338	10.0.2.15	445	SMB2	588	Session Setup Request, NTLMSSP_AUTH, User: WORKGROUP\root
10.0.2.15	445	10.0.2.4	37338	SMB2	139	Session Setup Response
10.0.2.4	37338	10.0.2.15	445	SMB2	162	Tree Connect Request, Tree: '\\10.0.2.15\IPC\$'
10.0.2.15	445	10.0.2.4	37338	SMB2	138	Tree Connect Response, Tree: '\\10.0.2.15\IPC\$'
10.0.2.4	37338	10.0.2.15	445	SMB2	222	Ioctl Request FSCTL_GET_REFERRALS, Path: \\10.0.2.15\Documents
10.0.2.15	445	10.0.2.4	37338	SMB2	130	Ioctl Response, Error: STATUS_FS_DRIVER_REQUIRED
10.0.2.4	37338	10.0.2.15	445	SMB2	126	Tree Disconnect Request, Tree: '\\10.0.2.15\IPC\$'
10.0.2.15	445	10.0.2.4	37338	SMB2	126	Tree Disconnect Response, Tree: '\\10.0.2.15\IPC\$'
10.0.2.4	37338	10.0.2.15	445	SMB2	172	Tree Connect Request, Tree: '\\10.0.2.15\Documents'
10.0.2.15	445	10.0.2.4	37338	SMB2	138	Tree Connect Response, Tree: '\\10.0.2.15\Documents'
10.0.2.4	37338	10.0.2.15	445	SMB2	126	KeepAlive Request
10.0.2.15	445	10.0.2.4	37338	SMB2	126	KeepAlive Response
10.0.2.4	37338	10.0.2.15	445	SMB2	179	Create Request, File: <share>
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.

No.	Time	Source	Src Port	Destination	Dst. Port	Protocol	Length	Info	
3585	2024-09-10 00:49:51.952...	10.0.2.15	49688	10.0.2.4	4443	TCP	66	49688 → 4443 [SYN, ECE, CWR] Seq=0 Win=64240	

Memory Dump Analysis:

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
g585BB01919536-1.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 TimeStamp    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?

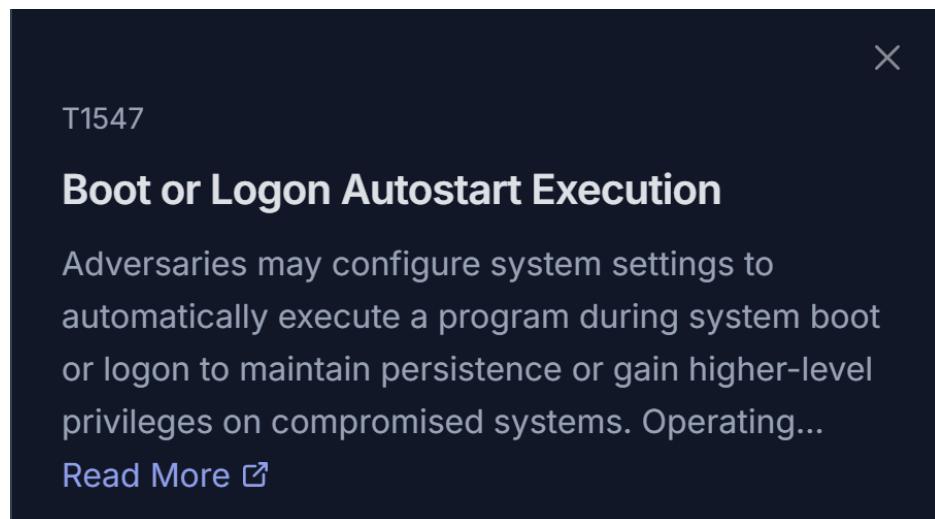
R: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\updatenow.exe, T1547

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”.

```
*** 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\HddiskVolume1\Windows\System32\inetrvr  
*** 980       4332    updatenow.exe  0xce06574db1c0 3      -      0      True    2024-09-10 06:08:23.000000 UTC  N/A    \Device\HddiskVolume1\ProgramData\Microsoft\Windows\Start Menu\Programs  
\StartUp\updatenow.exe  "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\updatenow.exe"  C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\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.

```
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
```

Malware Sample Analysis:

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

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.

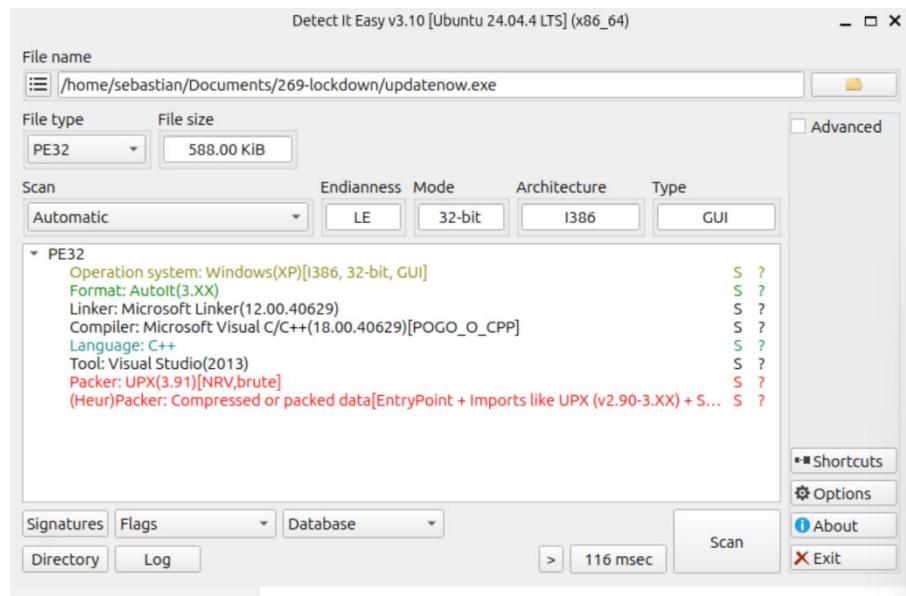
```
FLARE FLOSS RESULTS (version 3.1.1)

+-----+
| file path | \Windows\system32\cmd.exe
| Identified language | unknown
| extracted strings | 
| static strings | 8408 (42891 characters)
| language strings | 0 ( 0 characters)
| stack strings | 0
| tight strings | 0
| decoded strings | 0
| S |
+-----+


FLOSS STATIC STRINGS (8408)

+-----+
| FLOSS STATIC STRINGS: ASCII (8402) |
+-----+
!This program cannot be run in DOS mode.
B1GhB
UPX0
UPX1
UPX2
UPX3
UPX4
UPX5
UPX6
UPX7
UPX8
UPX9
UPX10
UPX11
UPX12
UPX13
UPX14
UPX15
UPX16
UPX17
UPX18
UPX19
UPX20
UPX21
UPX22
UPX23
UPX24
UPX25
UPX26
UPX27
UPX28
UPX29
UPX30
UPX31
UPX32
UPX33
UPX34
UPX35
UPX36
UPX37
UPX38
UPX39
UPX40
UPX41
UPX42
UPX43
UPX44
UPX45
UPX46
UPX47
UPX48
UPX49
UPX50
UPX51
UPX52
UPX53
UPX54
UPX55
UPX56
UPX57
UPX58
UPX59
UPX60
UPX61
UPX62
UPX63
UPX64
UPX65
UPX66
UPX67
UPX68
UPX69
UPX70
UPX71
UPX72
UPX73
UPX74
UPX75
UPX76
UPX77
UPX78
UPX79
UPX80
UPX81
UPX82
UPX83
UPX84
UPX85
UPX86
UPX87
UPX88
UPX89
UPX90
UPX91
UPX92
UPX93
UPX94
UPX95
UPX96
UPX97
UPX98
UPX99
UPX100
UPX101
UPX102
UPX103
UPX104
UPX105
UPX106
UPX107
UPX108
UPX109
UPX110
UPX111
UPX112
UPX113
UPX114
UPX115
UPX116
UPX117
UPX118
UPX119
UPX120
UPX121
UPX122
UPX123
UPX124
UPX125
UPX126
UPX127
UPX128
UPX129
UPX130
UPX131
UPX132
UPX133
UPX134
UPX135
UPX136
UPX137
UPX138
UPX139
UPX140
UPX141
UPX142
UPX143
UPX144
UPX145
UPX146
UPX147
UPX148
UPX149
UPX150
UPX151
UPX152
UPX153
UPX154
UPX155
UPX156
UPX157
UPX158
UPX159
UPX160
UPX161
UPX162
UPX163
UPX164
UPX165
UPX166
UPX167
UPX168
UPX169
UPX170
UPX171
UPX172
UPX173
UPX174
UPX175
UPX176
UPX177
UPX178
UPX179
UPX180
UPX181
UPX182
UPX183
UPX184
UPX185
UPX186
UPX187
UPX188
UPX189
UPX190
UPX191
UPX192
UPX193
UPX194
UPX195
UPX196
UPX197
UPX198
UPX199
UPX200
UPX201
UPX202
UPX203
UPX204
UPX205
UPX206
UPX207
UPX208
UPX209
UPX210
UPX211
UPX212
UPX213
UPX214
UPX215
UPX216
UPX217
UPX218
UPX219
UPX220
UPX221
UPX222
UPX223
UPX224
UPX225
UPX226
UPX227
UPX228
UPX229
UPX230
UPX231
UPX232
UPX233
UPX234
UPX235
UPX236
UPX237
UPX238
UPX239
UPX240
UPX241
UPX242
UPX243
UPX244
UPX245
UPX246
UPX247
UPX248
UPX249
UPX250
UPX251
UPX252
UPX253
UPX254
UPX255
UPX256
UPX257
UPX258
UPX259
UPX260
UPX261
UPX262
UPX263
UPX264
UPX265
UPX266
UPX267
UPX268
UPX269
UPX270
UPX271
UPX272
UPX273
UPX274
UPX275
UPX276
UPX277
UPX278
UPX279
UPX280
UPX281
UPX282
UPX283
UPX284
UPX285
UPX286
UPX287
UPX288
UPX289
UPX290
UPX291
UPX292
UPX293
UPX294
UPX295
UPX296
UPX297
UPX298
UPX299
UPX300
UPX301
UPX302
UPX303
UPX304
UPX305
UPX306
UPX307
UPX308
UPX309
UPX310
UPX311
UPX312
UPX313
UPX314
UPX315
UPX316
UPX317
UPX318
UPX319
UPX320
UPX321
UPX322
UPX323
UPX324
UPX325
UPX326
UPX327
UPX328
UPX329
UPX330
UPX331
UPX332
UPX333
UPX334
UPX335
UPX336
UPX337
UPX338
UPX339
UPX340
UPX341
UPX342
UPX343
UPX344
UPX345
UPX346
UPX347
UPX348
UPX349
UPX350
UPX351
UPX352
UPX353
UPX354
UPX355
UPX356
UPX357
UPX358
UPX359
UPX360
UPX361
UPX362
UPX363
UPX364
UPX365
UPX366
UPX367
UPX368
UPX369
UPX370
UPX371
UPX372
UPX373
UPX374
UPX375
UPX376
UPX377
UPX378
UPX379
UPX380
UPX381
UPX382
UPX383
UPX384
UPX385
UPX386
UPX387
UPX388
UPX389
UPX390
UPX391
UPX392
UPX393
UPX394
UPX395
UPX396
UPX397
UPX398
UPX399
UPX400
UPX401
UPX402
UPX403
UPX404
UPX405
UPX406
UPX407
UPX408
UPX409
UPX410
UPX411
UPX412
UPX413
UPX414
UPX415
UPX416
UPX417
UPX418
UPX419
UPX420
UPX421
UPX422
UPX423
UPX424
UPX425
UPX426
UPX427
UPX428
UPX429
UPX430
UPX431
UPX432
UPX433
UPX434
UPX435
UPX436
UPX437
UPX438
UPX439
UPX440
UPX441
UPX442
UPX443
UPX444
UPX445
UPX446
UPX447
UPX448
UPX449
UPX450
UPX451
UPX452
UPX453
UPX454
UPX455
UPX456
UPX457
UPX458
UPX459
UPX460
UPX461
UPX462
UPX463
UPX464
UPX465
UPX466
UPX467
UPX468
UPX469
UPX470
UPX471
UPX472
UPX473
UPX474
UPX475
UPX476
UPX477
UPX478
UPX479
UPX480
UPX481
UPX482
UPX483
UPX484
UPX485
UPX486
UPX487
UPX488
UPX489
UPX490
UPX491
UPX492
UPX493
UPX494
UPX495
UPX496
UPX497
UPX498
UPX499
UPX500
UPX501
UPX502
UPX503
UPX504
UPX505
UPX506
UPX507
UPX508
UPX509
UPX510
UPX511
UPX512
UPX513
UPX514
UPX515
UPX516
UPX517
UPX518
UPX519
UPX520
UPX521
UPX522
UPX523
UPX524
UPX525
UPX526
UPX527
UPX528
UPX529
UPX530
UPX531
UPX532
UPX533
UPX534
UPX535
UPX536
UPX537
UPX538
UPX539
UPX540
UPX541
UPX542
UPX543
UPX544
UPX545
UPX546
UPX547
UPX548
UPX549
UPX550
UPX551
UPX552
UPX553
UPX554
UPX555
UPX556
UPX557
UPX558
UPX559
UPX560
UPX561
UPX562
UPX563
UPX564
UPX565
UPX566
UPX567
UPX568
UPX569
UPX570
UPX571
UPX572
UPX573
UPX574
UPX575
UPX576
UPX577
UPX578
UPX579
UPX580
UPX581
UPX582
UPX583
UPX584
UPX585
UPX586
UPX587
UPX588
UPX589
UPX590
UPX591
UPX592
UPX593
UPX594
UPX595
UPX596
UPX597
UPX598
UPX599
UPX600
UPX601
UPX602
UPX603
UPX604
UPX605
UPX606
UPX607
UPX608
UPX609
UPX610
UPX611
UPX612
UPX613
UPX614
UPX615
UPX616
UPX617
UPX618
UPX619
UPX620
UPX621
UPX622
UPX623
UPX624
UPX625
UPX626
UPX627
UPX628
UPX629
UPX630
UPX631
UPX632
UPX633
UPX634
UPX635
UPX636
UPX637
UPX638
UPX639
UPX640
UPX641
UPX642
UPX643
UPX644
UPX645
UPX646
UPX647
UPX648
UPX649
UPX650
UPX651
UPX652
UPX653
UPX654
UPX655
UPX656
UPX657
UPX658
UPX659
UPX660
UPX661
UPX662
UPX663
UPX664
UPX665
UPX666
UPX667
UPX668
UPX669
UPX670
UPX671
UPX672
UPX673
UPX674
UPX675
UPX676
UPX677
UPX678
UPX679
UPX680
UPX681
UPX682
UPX683
UPX684
UPX685
UPX686
UPX687
UPX688
UPX689
UPX690
UPX691
UPX692
UPX693
UPX694
UPX695
UPX696
UPX697
UPX698
UPX699
UPX700
UPX701
UPX702
UPX703
UPX704
UPX705
UPX706
UPX707
UPX708
UPX709
UPX710
UPX711
UPX712
UPX713
UPX714
UPX715
UPX716
UPX717
UPX718
UPX719
UPX720
UPX721
UPX722
UPX723
UPX724
UPX725
UPX726
UPX727
UPX728
UPX729
UPX730
UPX731
UPX732
UPX733
UPX734
UPX735
UPX736
UPX737
UPX738
UPX739
UPX740
UPX741
UPX742
UPX743
UPX744
UPX745
UPX746
UPX747
UPX748
UPX749
UPX750
UPX751
UPX752
UPX753
UPX754
UPX755
UPX756
UPX757
UPX758
UPX759
UPX760
UPX761
UPX762
UPX763
UPX764
UPX765
UPX766
UPX767
UPX768
UPX769
UPX770
UPX771
UPX772
UPX773
UPX774
UPX775
UPX776
UPX777
UPX778
UPX779
UPX780
UPX781
UPX782
UPX783
UPX784
UPX785
UPX786
UPX787
UPX788
UPX789
UPX790
UPX791
UPX792
UPX793
UPX794
UPX795
UPX796
UPX797
UPX798
UPX799
UPX800
UPX801
UPX802
UPX803
UPX804
UPX805
UPX806
UPX807
UPX808
UPX809
UPX810
UPX811
UPX812
UPX813
UPX814
UPX815
UPX816
UPX817
UPX818
UPX819
UPX820
UPX821
UPX822
UPX823
UPX824
UPX825
UPX826
UPX827
UPX828
UPX829
UPX830
UPX831
UPX832
UPX833
UPX834
UPX835
UPX836
UPX837
UPX838
UPX839
UPX840
UPX841
UPX842
UPX843
UPX844
UPX845
UPX846
UPX847
UPX848
UPX849
UPX850
UPX851
UPX852
UPX853
UPX854
UPX855
UPX856
UPX857
UPX858
UPX859
UPX860
UPX861
UPX862
UPX863
UPX864
UPX865
UPX866
UPX867
UPX868
UPX869
UPX870
UPX871
UPX872
UPX873
UPX874
UPX875
UPX876
UPX877
UPX878
UPX879
UPX880
UPX881
UPX882
UPX883
UPX884
UPX885
UPX886
UPX887
UPX888
UPX889
UPX890
UPX891
UPX892
UPX893
UPX894
UPX895
UPX896
UPX897
UPX898
UPX899
UPX900
UPX901
UPX902
UPX903
UPX904
UPX905
UPX906
UPX907
UPX908
UPX909
UPX910
UPX911
UPX912
UPX913
UPX914
UPX915
UPX916
UPX917
UPX918
UPX919
UPX920
UPX921
UPX922
UPX923
UPX924
UPX925
UPX926
UPX927
UPX928
UPX929
UPX930
UPX931
UPX932
UPX933
UPX934
UPX935
UPX936
UPX937
UPX938
UPX939
UPX940
UPX941
UPX942
UPX943
UPX944
UPX945
UPX946
UPX947
UPX948
UPX949
UPX950
UPX951
UPX952
UPX953
UPX954
UPX955
UPX956
UPX957
UPX958
UPX959
UPX960
UPX961
UPX962
UPX963
UPX964
UPX965
UPX966
UPX967
UPX968
UPX969
UPX970
UPX971
UPX972
UPX973
UPX974
UPX975
UPX976
UPX977
UPX978
UPX979
UPX980
UPX981
UPX982
UPX983
UPX984
UPX985
UPX986
UPX987
UPX988
UPX989
UPX990
UPX991
UPX992
UPX993
UPX994
UPX995
UPX996
UPX997
UPX998
UPX999
UPX1000
UPX1001
UPX1002
UPX1003
UPX1004
UPX1005
UPX1006
UPX1007
UPX1008
UPX1009
UPX10010
UPX10011
UPX10012
UPX10013
UPX10014
UPX10015
UPX10016
UPX10017
UPX10018
UPX10019
UPX10020
UPX10021
UPX10022
UPX10023
UPX10024
UPX10025
UPX10026
UPX10027
UPX10028
UPX10029
UPX10030
UPX10031
UPX10032
UPX10033
UPX10034
UPX10035
UPX10036
UPX10037
UPX10038
UPX10039
UPX10040
UPX10041
UPX10042
UPX10043
UPX10044
UPX10045
UPX10046
UPX10047
UPX10048
UPX10049
UPX10050
UPX10051
UPX10052
UPX10053
UPX10054
UPX10055
UPX10056
UPX10057
UPX10058
UPX10059
UPX10060
UPX10061
UPX10062
UPX10063
UPX10064
UPX10065
UPX10066
UPX10067
UPX10068
UPX10069
UPX10070
UPX10071
UPX10072
UPX10073
UPX10074
UPX10075
UPX10076
UPX10077
UPX10078
UPX10079
UPX10080
UPX10081
UPX10082
UPX10083
UPX10084
UPX10085
UPX10086
UPX10087
UPX10088
UPX10089
UPX10090
UPX10091
UPX10092
UPX10093
UPX10094
UPX10095
UPX10096
UPX10097
UPX10098
UPX10099
UPX100100
UPX100101
UPX100102
UPX100103
UPX100104
UPX100105
UPX100106
UPX100107
UPX100108
UPX100109
UPX100110
UPX100111
UPX100112
UPX100113
UPX100114
UPX100115
UPX100116
UPX100117
UPX100118
UPX100119
UPX100120
UPX100121
UPX100122
UPX100123
UPX100124
UPX100125
UPX100126
UPX100127
UPX100128
UPX100129
UPX100130
UPX100131
UPX100132
UPX100133
UPX100134
UPX100135
UPX100136
UPX100137
UPX100138
UPX100139
UPX100140
UPX100141
UPX100142
UPX100143
UPX100144
UPX100145
UPX100146
UPX100147
UPX100148
UPX100149
UPX100150
UPX100151
UPX100152
UPX100153
UPX100154
UPX100155
UPX100156
UPX100157
UPX100158
UPX100159
UPX100160
UPX100161
UPX100162
UPX100163
UPX100164
UPX100165
UPX100166
UPX100167
UPX100168
UPX100169
UPX100170
UPX100171
UPX100172
UPX100173
UPX100174
UPX100175
UPX100176
UPX100177
UPX100178
UPX100179
UPX100180
UPX100181
UPX100182
UPX100183
UPX100184
UPX100185
UPX100186
UPX100187
UPX100188
UPX100189
UPX100190
UPX100191
UPX100192
UPX100193
UPX100194
UPX100195
UPX100196
UPX100197
UPX100198
UPX100199
UPX100200
UPX100201
UPX100202
UPX100203
UPX100204
UPX100205
UPX100206
UPX100207
UPX100208
UPX100209
UPX100210
UPX100211
UPX100212
UPX100213
UPX100214
UPX100215
UPX100216
UPX100217
UPX100218
UPX100219
UPX100220
UPX100221
UPX100222
UPX100223
UPX100224
UPX100225
UPX100226
UPX100227
UPX100228
UPX100229
UPX100230
UPX100231
UPX100232
UPX100233
UPX100234
UPX100235
UPX100236
UPX100237
UPX100238
UPX100239
UPX100240
UPX100241
UPX100242
UPX100243
UPX100244
UPX100245
UPX100246
UPX100247
UPX100248
UPX100249
UPX100250
UPX100251
UPX100252
UPX100253
UPX100254
UPX100255
UPX100256
UPX100257
UPX100258
UPX100259
UPX100260
UPX100261
UPX100262
UPX100263
UPX100264
UPX100265
UPX100266
UPX100267
UPX100268
UPX100269
UPX100270
UPX100271
UPX100272
UPX100273
UPX100274
UPX100275
UPX100276
UPX100277
UPX100278
UPX100279
UPX100280
UPX100281
UPX100282
UPX100283
UPX100284
UPX100285
UPX100286
UPX100287
UPX100288
UPX100289
UPX100290
UPX100291
UPX100292
UPX100293
UPX100294
UPX100295
UPX100296
UPX100297
UPX100298
UPX100299
UPX100300
UPX100301
UPX100302
UPX100303
UPX100304
UPX100305
UPX100306
UPX100307
UPX100308
UPX100309
UPX100310
UPX100311
UPX100312
UPX100313
UPX100314
UPX100315
UPX100316
UPX100317
UPX100318
UPX100319
UPX100320
UPX100321
UPX100322
UPX100323
UPX100324
UPX100325
UPX100326
UPX100327
UPX100328
UPX100329
UPX100330
UPX100331
UPX100332
UPX100333
UPX100334
UPX100335
UPX100336
UPX100337
UPX100338
UPX100339
UPX100340
UPX100341
UPX100342
UPX100343
UPX100344
UPX100345
UPX100346
UPX100347
UPX100348
UPX100349
UPX100350
UPX100351
UPX100352
UPX100353
UPX100354
UPX100355
UPX100356
UPX100357
UPX100358
UPX100359
UPX100360
UPX100361
UPX100362
UPX100363
UPX100364
UPX100365
UPX100366
UPX100367
UPX100368
UPX100369
UPX100370
UPX100371
UPX100372
UPX100373
UPX100374
UPX100375
UPX100376
UPX100377
UPX100378
UPX100379
UPX100380
UPX100381
UPX100382
UPX100383
UPX100384
UPX100385
UPX100386
UPX100387
UPX100388
UPX100389
UPX100390
UPX100391
UPX100392
UPX100393
UPX100394
UPX100395
UPX100396
UPX100397
UPX100398
UPX100399
UPX100400
UPX100401
UPX100402
UPX100403
UPX100404
UPX100405
UPX100406
UPX100407
UPX100408
UPX100409
UPX100410
UPX100411
UPX100412
UPX100413
UPX100414
UPX100415
UPX100416
UPX100417
UPX100418
UPX100419
UPX100420
UPX100421
UPX100422
UPX100423
UPX100424
UPX100425
UPX100426
UPX100427
UPX100428
UPX100429
UPX100430
UPX100431
UPX100432
UPX100433
UPX100434
UPX100435
UPX100436
UPX100437
UPX100438
UPX100439
UPX100440
UPX100441
UPX100442
UPX100443
UPX100444
UPX100445
UPX100446
UPX100447
UPX100448
UPX100449
UPX100450
UPX100451
UPX100452
UPX100453
UPX100454
UPX100455
UPX100456
UPX100457
UPX100458
UPX100459
UPX100460
UPX100461
UPX100462
UPX100463
UPX100464
UPX100465
UPX100466
UPX100467
UPX100468
UPX100469
UPX100470
UPX100471
UPX100472
UPX100473
UPX100474
UPX100475
UPX100476
UPX100477
UPX100478
UPX100479
UPX100480
UPX100481
UPX100482
UPX100483
UPX100484
UPX100485
UPX100486
UPX100487
UPX100488
UPX100489
UPX100490
UPX100491
UPX100492
UPX100493
UPX100494
UPX100495
UPX100496
UPX100497
UPX100498
UPX100499
UPX100500
UPX100501
UPX100502
UPX100503
UPX100504
UPX100505
UPX100506
UPX100507
UPX100508
UPX100509
UPX100510
UPX100511
UPX100512
UPX100513
UPX100514
UPX100515
UPX100516
UPX100517
```

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.

Malware Config

Extracted

Family agenttesla

Credentials

Protocol: smtp

Host:
cp8nl.hyperhost.ua

Port:
587

Username:
blessed4ever@genesio.top

Password:
cy+G_(979n9N

Email To:
blessed4ever@genesio.top

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 framework .NET que se especializa en el robo de credenciales y datos confidenciales de sistemas Windows.

Malware Config

Extracted

Family agenttesla