



DICIEMBRE 2022

ANÁLISIS DE MALWARE

Práctica final

Informe redactado por:
Angie Aristizabal



RECURSOS UTILIZADOS

Para hacer el siguiente análisis se ha hecho uso de :

*La máquina facilitada en clase de Cape y su página web

*La página web polyswarm.network

*La página web analyze.intezer

Desgraciadamente la pagina viper no me ha dejado cargar el malware habiendolo intentado en varias ocasiones.

El malware usado fue subido en la siguiente fecha a la plataforma de GitHub 10-12-2022

DATOS GENERALES

Nombre del archivo: 87658a3c5cd72eddc1f3c52b

Tipo: PE32 executable

Tipo de Malware: LockBit (Ransomware)

Tamaño: 982528 bytes

TimeStamp del PE: 2021-07-26 07:34:01

MD5: 4d41b282814b01eb1cc3198951f6e6c1

SHA1: d9b039e7517b7577b2adbb0f3d840bf788371ace

SHA256: 87658a3c5cd72eddc1f3c52b489ed43e59a0d044c849f300e0f7537568e0502f

SHA3-384: b63ec2fdfa915a980bffef4f94314a258bf0e8bcc7b5dee171d92d1d59e25ff5424e6ae3800de84613edb8b1f56f1f76

ANÁLISIS ESTÁTICO

En el análisis hecho con CAPE, se ha podido extraer la siguiente información:

-Dos reglas YARA detectaron el ejecutable analizado:

- INDICATOR_SUSPICIOUS_EXE_UACBypass_CMSTPCOM - Detects Windows executables bypassing UAC using CMSTP COM interfaces. MITRE (T1218.003) - Author: ditekSHen
- shellcode_stack_strings - Match x86 that appears to be stack string creation. - Author: William Ballenthin

Con esto vemos que intenta evadir el sistema

ESTRUCTURA DEL PE

Contamos con estas cabeceras:

- .text
- .data
- .idata

Ninguno con entropía alta. La más alta es ".data" con 6.79

STRINGS

Método anti-sandbox revisando la hora del equipo :

```
GetSystemTime
```

Busca ver que privilegios tiene y escalarlos:

```
Elevation:Administrator!new:
```

```
CheckTokenMembership  
CreateWellKnownSid
```

Importa datos con .idata

Inhabilita antivirus:

```
displayname=789  
[Software\Policies\Microsoft\Windows Defender  
;DisableAntiSpyware  
][Software\Policies\Microsoft\Windows Defender\Real-Time Protection  
;DisableRealtimeMonitoring  
][Software\Policies\Microsoft\Windows Defender\Spynet  
;SubmitSamplesConsent  
][Software\Policies\Microsoft\Windows Defender\Threats  
;Threats_ThreatSeverityDefaultAction  
][Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction  
][Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction  
][Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction  
][Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction  
][Software\Policies\Microsoft\Windows Defender\UX Configuration  
;Notification_Suppress
```

Posible ruta del ransomware:

```
\Registry\Machine\Software\Classes\.lockbit  
LockBit  
\Registry\Machine\Software\Classes\Lockbit  
\Registry\Machine\Software\Classes\Lockbit\DefaultIcon  
\Registry\Machine\Software\Classes\Lockbit\shell  
LockBit Class  
\Registry\Machine\Software\Classes\Lockbit\shell\Open  
\Registry\Machine\Software\Classes\Lockbit\shell\Open\Command  
"C:\Windows\system32\mshta.exe" "%s"  
\Registry\Machine\Software\Classes\  
\DefaultIcon  
\??\C:\windows\system32\%02X%02X%02X.ico  
\Registry\Machine\Software\Classes\.lockbit\DefaultIcon
```

Ejecutable encontrado y tareas programadas :

```
ScheduledTasks  
\ScheduledTasks.xml  
C:\Windows\System32\taskkill.exe
```

Se encuentra esto sabiendo que Network Share brinda la capacidad de acceder a una ubicación de red usando las credenciales del usuario administrador actual o diferentes credenciales:

```
NetworkShares  
\NetworkShares.xml
```

```
%s\%02X%02X%02X%02X.lock
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
{2C5F9FCC-F266-43F6-BFD7-838DAE269E11}
\lockBit_Ransomware.hta
```


All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.
Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc. Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
<https://tox.chat/download.html>
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID: 3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7
If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser
<http://lockbitat6vx573eeqofwgoglmutr3a35nygvokja5uucop4kykyd.onion>
<https://binblog.at>

<https://bigblog.at>

Profundizando en las páginas dejadas en la nota por parte de los autores del ransomware. Podemos encontrar lo siguiente gracias a la página virustotal :

Esta relacionado con el ransomware LockBit como efectivamente nos informó previamente el análisis con CAPE

New with VT Collections? [Learn more](#) or [Create one](#)



Lockbit Black 3.0

Created
5 months ago

Updated
5 months ago

First submission
-

Last submission
-

Owner [dm_adms](#)

[cve-2014-3931](#) [cve-2005-0068](#) [cve-2004-0790](#) [base64-embedded](#) [contains-embedded-js](#) [contains-elf](#) [contains-pe](#)

Collection created from Graph <https://www.virustotal.com/graph/g04a5daa8de0e4ffa8d38d98220523aea9149b5804c214e3fb6ff3036903d8cf3>





IOCS

GRAPH


COMMUNITY

☐ Related file hashes 10 / 518

Export Tools

	Detections	Size	First seen	Last seen
<input type="checkbox"/>  LockBit.exe peexe cve-2005-0068 cve-2004-0790 runtime-modules ...	64 / 71	862.50 KB	2021-07-14 15:56:50	2022-12-08 11:11:20
<input type="checkbox"/>  _bsite_url_{7C5A40EF-A0FB-4BFC-874A-C0F2E089FA8E}.com	0 / 58	4.50 KB	2022-01-21 09:29:08	2022-01-21 09:29:08
<input type="checkbox"/>  _e884dc7c37a1a24ef3472674574d3367079bf0a2a.sample peexe runtime-modules checks-network-adapters long-sleeps ...	55 / 67	959.50 KB	2021-11-22 23:52:18	2021-11-22 23:52:18
<input type="checkbox"/>  This file has not been submitted to VirusTotal yet	-			

New with VT Collections? [Learn more](#) or [Create one](#)



LockBit 3.0 Ransomware Case Study: A Huge Cybersecurity Risk

Created
2 months ago

Updated
2 months ago

First submission
-

Last submission
-

Owner [patricksvgrapi](#)

No tags

(2022-10-05) <https://blog.criminalip.io/2022/09/23/lockbit-3-0-ransomware/>

IOCS

GRAPH

COMMUNITY

☐ Related IP addresses 1 / 1

Export Tools

	Detections	Autonomous System	Country Code
<input type="checkbox"/> 13.107.4.52 13.107.4.0/22	2 / 97	8068 (MICROSOFT-CORP-MSN-AS-BLOCK)	US

☐ Related URLs 10 / 22

Export Tools

	Detections	Status	First Seen	Last seen	Submissions
<input type="checkbox"/> https://www.criminalip.io/domain/rep... www.criminalip.io 104.22.2.20	0 / 88	200	2022-09-23 17:17:22	2022-09-23 17:17:22	1
<input type="checkbox"/> http://lockbitapt5x4zkjbcqmz6frdhec... lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukks	7 / 91	-	2021-12-11 -----	2022-12-02 -----	115

Se puede notar que esta página es relativamente reciente observando la fecha del primer registro de esta

The screenshot shows a security alert interface. At the top, a red circle with the number '9' indicates the number of vendors that flagged the URL. Below this, a message states: '9 security vendors flagged this URL as malicious'. The URL in question is <http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4kykd.onion/>. The alert was received on 2022-12-12 at 13:07:39 UTC, 10 hours ago. The interface includes tabs for 'DETECTION', 'DETAILS' (selected), and 'COMMUNITY' (with 5 items). Under 'Categories', it lists: Forcepoint ThreatSeeker (proxy avoidance), Comodo Valkyrie Verdict (unknown), and alphaMountain.ai (Malicious). The 'History' section shows: First Submission (2021-07-03 20:33:15 UTC), Last Submission (2022-12-12 13:07:39 UTC), and Last Analysis (2022-12-12 13:07:39 UTC). The 'HTTP Response' section is empty. The 'Final URL' is the same as the one in the alert.

9 / 91

9 security vendors flagged this URL as malicious

<http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4kykd.onion/>

2022-12-12 13:07:39 UTC
10 hours ago

Community Score

DETECTION DETAILS COMMUNITY 5

Categories

Forcepoint ThreatSeeker proxy avoidance
Comodo Valkyrie Verdict unknown
alphaMountain.ai Malicious

History

First Submission 2021-07-03 20:33:15 UTC
Last Submission 2022-12-12 13:07:39 UTC
Last Analysis 2022-12-12 13:07:39 UTC

HTTP Response

Final URL
<http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4kykd.onion/>

Formando parte de una enorme red de conexiones dejandonos sin ningún hilo del que tirar ya que no se puede concretar alguna conexión concreta que nos sea útil

The screenshot shows a network diagram with a central node labeled 'Embedded urls' and a pop-up window displaying details for a specific URL. The central node is connected to many other nodes, represented by icons of documents and folders. The pop-up window shows the following information:

9 / 91 <http://lockbitapt6vx57t3eeqjofwgcglmutr...>

First Seen	2021-07-03 20:33:15
Last Seen	2022-12-12 13:07:39
Submissions	260

Detections

Bkav	Undetected
CMC Threat Intelligence	Undetected
Snort IP sample list	Undetected
VX Vault	Undetected
ViriBack	Undetected

... and 86 items more

Click to select Double click to expand

Y por parte del segundo URL facilitado por medio de la nota no se pudo encontrar gran información más allá de que es malicioso :

The screenshot shows the VirusTotal interface for the URL `https://bigblog.at/`. At the top, a search bar contains the URL. Below it, a circular progress indicator shows a score of 7 out of 90. A red banner states "7 security vendors flagged this URL as malicious". The URL is listed as `https://bigblog.at/bigblog.at` with a timestamp of "2022-11-12 04:13:38 UTC" and "1 month ago". Below this, the "DETECTION" tab is active, showing a table of security vendors' analysis.

Security Vendors' Analysis			
alphaMountain.ai	Malicious	Antiy-AVL	Malicious
Fortinet	Malware	Kaspersky	Malware
Seclookup	Malicious	Sophos	Malware
Viettel Threat Intelligence	Malicious	Abusix	Clean

LIBRERIAS

Por medio de estas, podemos rescatar lo siguiente que nos confirman datos recolectados previamente con las strings:

- `0x4fa02c PathAppendW` : Método para agregar temporalmente una ruta
- `0x4fa018 CreateProcessW` : Crea procesos
- `0x4fa01c GetSystemTime` : Método anti sandbox revisando la hora
- `0x4fa00c CheckTokenMembership`: Revisa los privilegios del usuario
- `0x4fa010 CreateWellKnownSid` : Crea identificadores de seguridad conocidos
- `0x4fa038 CoSetProxyBlanket` : seguramente busca configurar la manta de seguridad que se aplica a los servidores proxy

MITRE ATT&CK

En esta sección nos encontramos procedimientos. Muchos de ellos vuelven a confirmar datos que ya habíamos recogido:

- T1057 - Aquí vemos que descubre procedimientos, en este caso que enumera e insiste en procesos
- T1059- En este vemos que ejecuta comandos y scripts de persistencia con "bcdedit_command"
- T1070- Borra logs
- T1112- Modifica registros en esta ocasión crean persistencia con un "autorun"
- T1202- Ejecución de comandos indirectos, que seguramente sean para eludir restricciones de seguridad al momento de ejecutar comandos y usa utilidades de Windows
- T1564- Esconde artefactos, y lo más probable es que se trate de ejecutar archivos de forma oculta.
- T1071- Echa mano en las conexiones de red
- T1074- Manipula la papelera en el tema de datos.
- T1485- Borra logs nuevamente
- T1486- Encripta los datos del ransomware
- T1490- Crea persistencia inhabilitando la recuperación del sistema
- T1547- Más persistencia asegurándose de un inicio automático del ransomware

ANÁLISIS DINÁMICO

Para este se ha usado la sandbox de CAPE, donde hemos podido recoger los siguientes datos:

FIRMAS

Para este se ha usado la sandbox de CAPE, donde hemos podido recoger los siguientes datos:

- Un método antisandbox intentando detectar si esta siendo ejecutado bajo la supervisión de un depurador
- Método antisandbox por medio de los adaptadores de red
- Ha sido detectado por una regla YARA de CAPE :
PID 2108 triggered the Yara rule 'INDICATOR_SUSPICIOUS_GENRansomware'
- Método antisandbox viendo la hora local
- Podemos ver que intenta conectase 510 veces a IP's muertas aunque ninguna de ellas nos da información por medio de VirusTotal
- Importación de librerías al momento de la ejecución
- Enumera procesos entre los cuales podemos encontrar lo siguiente :

La ejecución de ciertos ejecutables bastantes sospechosos:

- **conhost.exe** → el proceso de un programa (criptominero) que está diseñado para minar la criptomoneda Monero.
- **msiexec.exe** → Proporciona los medios para instalar, modificar y realizar operaciones en Windows Installer desde la línea de comandos.
- **dllhost.exe** → está diseñado para forzar la apertura de páginas web no confiables, engañosos y maliciosos
- **Rundll32.exe** → objetivo de hackers que buscan esconder varias infecciones de ordenador como spywares, keyloggers, troyanos y otras dentro del sistema

- Expresa interés en ciertos procesos

- Manipula datos de la papelería como ya habíamos visto anteriormente, aquí parece ser que se da los permisos y pasa por las siguientes rutas. Dando a entender que de esta forma se deshace de pruebas:

- file:C:\\$Recycle.Bin\S-1-5-21-2225935160-554833140-588599421-1000\I44QTP5.py
 - file:C:\\$Recycle.Bin\S-1-5-21-2225935160-554833140-588599421-1000\INB7KZ3.pub
 - file:C:\\$Recycle.Bin\S-1-5-21-2225935160-554833140-588599421-1000\desktop.ini

- Proceso en ventana oculta donde encontramos la ejecución del ransomware:

- 87658a3c5cd72eddc1f3c52b.exe -> cmd.exe

Podemos ver que borra los backups y crea persistencia:

```
/c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no'  
'/c wevtutil cl system
```

- Intenta esconderse del depurador con :

- ThreadHideFromDebugger→ hace que cualquier excepción omitirá el depurador y presionará SEH o explotará y bloqueará la aplicación

- Crea una memoria RWX : estas automatizan la gestión entre los dos niveles principales de la jerarquía de memoria: memoria principal y disco.

• Como habíamos visto anteriormente hace uso de las utilidades de Windows:

■ Borrando backups → C:\Windows\System32\cmd.exe" /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no
cmd.exe /c vssadmin Delete Shadows /All /Quiet
cmd.exe /c wmic SHADOWCOPY /nointeractive

■ Creando la persistencia → bcdedit /set {default} bootstatuspolicy ignoreallfailures

• Modifica la configuración de boot (más persistencia)

• Se autoinstala para hacer autorun en el equipo (persistencia)

• La regla YARA que identifica el tipo de malware:

■ Lockbit:
[{'Yara': '87658a3c5cd72eddc1f3c52b489ed43e59a0d044c849f300e0f7537568e0502f'}]]

• Borra logs y eventos de Windows como ya sabíamos

• Intenta borrar las shadowcopies (también ya lo sabíamos)

• Crea instrucciones para desenscriptar el ransomware "LockBit"

• Usa comandos maliciosos y utilidades de Windows

SetUnhandledExceptionFilter detected (possible anti-debug)
Checks adapter addresses which can be used to detect virtual network interfaces
Yara rule detections observed from a process memory dump/dropped files/CAPE
Possible date expiration check, exits too soon after checking local time
Attempts to connect to a dead IP:Port (510 unique times)
Dynamic (imported) function loading detected
Enumerates running processes
Expresses interest in specific running processes
Manipulates data from or to the Recycle Bin
A process created a hidden window
NtSetInformationThread: attempt to hide thread from debugger
Creates RWX memory
Uses Windows utilities for basic functionality

Modifies boot configuration settings

Installs itself for autorun at Windows startup

CAPE detected the Lockbit malware

Clears Windows events or logs

Attempts to delete or modify volume shadow copies

Creates a known LockBit ransomware decryption instruction / key file.

Uses suspicious command line tools or Windows utilities

HOST

No se ha detectado ninguno

DNS

No se ha detectado ninguno

ARCHIVOS A LOS QUE HA ACCEDIDO

Ruta del ejecutable →

C:\Users\ama\AppData\Local\Temp\87658a3c5cd72eddc1f3c52b.exe.Local\

Bloquea este archivo →

C:\1FB940CD.lock

Mira las zonas de seguridad del sistema →

C:\Windows\sysnative\cmd.exe:Zone.Identifier

Desinstala explorador →

C:\program files\mozilla firefox\uninstall*

C:\program files\mozilla firefox\uninstall\uninstall.log

Un archivo ejecutable del disco duro donde contiene código de la máquina →

C:\Program Files\Common Files\Microsoft Shared\OFFICE14\MSOXMLMF.DLL

Método antisandbox revisando la hora →

C:\Windows\sysnative\cmd.exe:Zone.Identifier

Ejecutables vistos →

C:\Windows\sysnative\wbem\WMIC.exe.Local\

C:\Windows\sysnative\bcdedit.exe

C:\Windows\sysnative\vssadmin.exe

ARCHIVOS MODIFICADOS

Ha entrado a todas las rutas de todas las aplicaciones del equipo, robando los datos y dejando un archivo .txt que ya es mencionado en la nota de rescate que pudimos ver en los strings.

C:\program files\microsoft games\FreeCell\es-ES\Restore-My-Files.txt
C:\program files\microsoft games\Hearts\es-ES\Restore-My-Files.txt
C:\program files\microsoft office\Office14\3082\Restore-My-Files.txt
C:\program files\mozilla firefox\browser\features\Restore-My-Files.txt
C:\program files\mozilla firefox\gmp-clearkey\0.1\Restore-My-Files.txt

KEY REGISTERS LEIDOS

Persistencia y manipulación →

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\LDAP\UseHostname
AsAlias
DisableUserModeCallbackFilter
HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Windows\CurrentVersion\P
olicies\Explorer\NoPropertiesMyComputer

Manipulación de software en su apartado de shellfolder →

KEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{9343812E-
1C37-4A49-A12E-4B2D810D956B}\ShellFolder\RestrictedAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\
{BD7A2E7B-21CB-41B2-A086-
B309680C6B7E}\ShellFolder\HideOnDesktopPerUser

Ejecutable en carpeta de control del explorador →

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet
Explorer\MAIN\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\87658
a3c5cd72eddc1f3c52b.exe

Permitiendo el paso a usuarios invitados no seguros→)

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\LanmanWorkstation\
NetworkProvider\name
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\LanmanWorkstation\
NetworkProvider\Class
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\LanmanWorkstation\
NetworkProvider\ProviderPath

Información total acerca del explorer y manipulación de este →

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{C870044B-F49E-4126-A9C3-B52A1FF411E8}\Security
HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Internet Explorer\MAIN\FeatureControl\FEATURE_MIME_HANDLING\WMIC.exe
HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Internet Explorer\MAIN\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE*

Persistencia →

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SystemStartOptions

KEY REGISTERS MODIFICADOS

Persistencia →

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\{18B9B5CD-5757-9DC4-05A1-05E5D2E7E1AC}

Conexiones →

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect

KEY REGISTERS ELIMINADOS

Posible eliminación de Proxys →

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass

Manipulación en la configuración de internet →

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName

Manipulación en la seguridad →

bcdedit /set {default} bootstatuspolicy ignoreallfailures

COMANDOS EJECUTADOS

Borra backups + persistencia →

```
C:\Windows\System32\cmd.exe" /c vssadmin delete shadows /all /quiet &
wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy
ignoreallfailures & bcdedit /set {default} recoveryenabled no
```

MUTEXES

```
\BaseNamedObjects\{E95740CD-E957-9DE8-05A1-B1E5E5E7B1AC}
Local\ZoneAttributeCacheCounterMutex
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex
```

TCP DETECTADOS

192.168.122.1 → No fue detectada ninguna información en virus total

UDP DETECTADOS

51.137.137.111
239.255.255.250
192.168.122.255
224.0.0.252
192.168.122.6

De aquí podemos extraer por parte de esta → 224.0.0.252 . Por medio de la página web de virus total una relación con varias comunidades



1 security vendor flagged this IP address as malicious

224.0.0.252

multicast suspicious-udp



Community Score

DETECTION

DETAILS

RELATIONS

COMMUNITY 29 +

Security Vendors' Analysis

Comodo Valkyrie Verdict	Malware	Abusix
Acronis	Clean	ADMINUSLabs

224.0.0.252



Angie A



Hoplight IPs Collection

by anomali_dli
2022-08-05 15:46:20 UTC

IPs: 23

IP's that have detections against Hoplight file hashes



URSNIF 24-5-2022 Coll...

by FERVAR54
2022-08-20 10:32:41 UTC

Files: 26 | IPs: 30

Collection created from Graph <https://www.virustotal.com/graph/g460db4d742f0487cb5ea896ff548725...>



Why Twitter Is so fuck...

by dorkingbeauty1
2022-07-01 14:13:04 UTC

Domains: 40 | Files: 357 | IPs: 24 | URLs: 15

V2 - wow has "Flash" files and "Stagefrightlib.so" - trying to copy the links from VT link page for the git r...



Gozi RM3 01-09-2022 ...

by sirowa7979
2022-09-30 08:44:35 UTC

Domains: 1 | Files: 94 | IPs: 3 | URLs: 1

TIPO: TROYANOTROYANO: Gozi RM3SEGUIMIENTO A TRAFICO MALICIOSOS DE IOC.5ee51dfd1e...



SYNAPTICS Collection

by dmeethal1
2022-03-28 19:09:13 UTC

Domains: 8 | Files: 37 | IPs: 11 | URLs: 6

Collection created from Graph <https://www.virustotal.com/graph/g913f70ecf1d14711b191fb61525bb60...>



Autodesk keygen Coll...

by hackmallory
2022-08-12 09:32:13 UTC

Files: 96 | IPs: 30 | URLs: 4

Collection created from Graph <https://www.virustotal.com/graph/gb6c05a100eea43489b61d2e6b25043...>



RansomEXX 23-5-2022...

by FERVAR54
2022-05-23 18:28:36 UTC

Domains: 3 | Files: 355 | IPs: 23

Collection created from Graph <https://www.virustotal.com/graph/g327e6ab69d3e4e8a98d5fadaf50c76c...>



Copy of Destructive m...

by LauLau
2022-04-02 22:39:18 UTC

Domains: 23 | Files: 30 | IPs: 26 | URLs: 2

Collection created from Graph <https://www.virustotal.com/graph/ge04ba435815846bc9c8ea243507e26...>



QUASAR 20-5-2022 Co...

by sirowa7979
2022-05-20 14:22:01 UTC

Domains: 3 | Files: 406 | IPs: 25

Collection created from Graph <https://www.virustotal.com/graph/g1be08554200a4ae7a9d256f3630c9cc...>



Robtex.com Collection

by Axelo
2022-10-01 10:00:00 UTC

Domains: 597 | Files: 1011 | IPs: 204 | URLs: 57

type.id url, <https://www.robtx.com/dns-lookup/numervczny.pl> relationship.Last serving ip address ip ad...

DROPPED FILES

NOMBRE: \$INB7KZ3.pub

FILE TYPE: data

MD5: 45d45cc2c1a24df95f888d2a827e6915

SHA1: 3e0f08a56faa097ae9a0a59eb4ae0b3e63c54a94

SHA256:

37a911747236dfbcdfd1f8d61c00adfb98f17c283c72edfa59c40005de9e9047

NOMBRE: \$RNB7KZ3.pub

FILE TYPE: Composite Document File V2 Document

MD5: 0627b4727e2bfe1d1cb7f06b82bfcc5c

SHA1: 7399b9e033ded0ee565bd3de299b4d9d2f46d769

SHA256:

e050ea777d910137fff7c160992ec026ab4f76832b6c96701b114e379abf4ca3

NOMBRE: \$I44QTP5.py

FILE TYPE: data

MD5: cbf25f066a1ce16a26174081d9bf7b61

SHA1: 4101008f308b0c677acd263641c022e311912bec

SHA256:

d1cb6c1c4328c4dadb21b1f39623362cadb060929f0ea92d58fb1cce561c5f68

NOMBRE: Restore-My-Files.txt

FILE TYPE: ASCII text, with CRLF line terminators

MD5: 2d4b35c109f4c6a525d98a4b6de57a3b

SHA1: 96746354be008668c1ea83ea117a949a122cd952

SHA256:

7bb2a6c676c223da65588a79b893e3bf3a851d418f59c13b6786545eb91ff50b

NOMBRE: \$R44QTP5.py

FILE TYPE: Python script, ASCII text executable

MD5: 29197927e00d0dce84d0c357394123df

SHA1: 90f3cc0e5ed7393171a91fc86c0c00f1cea1f2d

SHA256:

d7b7bc36ec310f9d9e152e0452ffd8a742b56e25153ef7a978368f0d186fa3e5

PROCESOS

NOMBRE:

922573798226bb3edd57e1af161ab56f8dc51462f35e17faef4ac98142819b33

FILE TYPE: PE32+ executable (console) x86-64, for MS Windows

MD5: c9f6b2ac293d540d56158926bff75574

SHA256:

922573798226bb3edd57e1af161ab56f8dc51462f35e17faef4ac98142819b33

REGLA YARA : INDICATOR_SUSPICIOUS_GENRansomware - detects command variations typically used by ransomware - Author: ditekSHen

NOMBRE:

edec31f3d36bb4b2e96de3c363fc6b2b4479962aec843c76cc413a8310c4416

FILE TYPE: PE32+ executable (console) x86-64, for MS Windows

MD5: 0138aeea551a8bee52167387faa070eb

SHA256:

edec31f3d36bb4b2e96de3c363fc6b2b4479962aec843c76cc413a8310c4416

NOMBRE:

950781a0884345f16ced7342cb4b146f681c76fbf5919ed4cdc04403a8a6ced4

FILE TYPE: PE32+ executable (console) x86-64, for MS Windows

MD5: df479dd363cd59894514dfd12ac1aa65

SHA256:

950781a0884345f16ced7342cb4b146f681c76fbf5919ed4cdc04403a8a6ced4

NOMBRE:

748304b396b9536472297d1ad76f0d82d49752bdc2aad8dd3e779e7806baa3ed

FILE TYPE: PE32+ executable (console) x86-64, for MS Windows

MD5: 29c6ebbcc3b1b5413c05be9d8f7983e9

SHA256:

748304b396b9536472297d1ad76f0d82d49752bdc2aad8dd3e779e7806baa3ed

NOMBRE:

3841133b6c0481c4c1924112693266655b862e8a80db52b1a1f2859c82c6536a

FILE TYPE: PE32+ executable (console) x86-64, for MS Windows

MD5: 37af431ef94f7b5128c3b7fc086b71f5

SHA256:

3841133b6c0481c4c1924112693266655b862e8a80db52b1a1f2859c82c6536a

ANALYZE INTEZER

No arrojó ninguna información que ya supieramos gracias a CAPE a excepción de ciertas IP que tampoco daban información a traves de virustotal

POLYSWARM

No arrojó ninguna información que ya supieramos gracias a CAPE a excepción de ciertas IP que tampoco daban información a traves de virustotal

ARBOL

■ 87658a3c5cd72eddc1f3c52b.exe 2512

■ cmd.exe 2108 "C:\Windows\System32\cmd.exe" /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no

■ vssadmin.exe 2724 vssadmin delete shadows /all /quiet

• WMIC.exe 1740 wmic shadowcopy delete

• bcdedit.exe 1508 bcdedit /set {default} bootstatuspolicy ignoreallfailures

• bcdedit.exe 1532 bcdedit /set {default} recoveryenabled no

Con esto podemos concluir que este ransomware tiene programado ejecutarse en el sistema y borrar todos los datos posibles y eliminar su rastro. Dejando por último persistencia del malware