

# Practica Análisis de Malware

De

Daniel Shved



## OBJETIVOS:

- Analizar un malware, sacándole toda la información posible, en la cual se encuentran datos generales, análisis estatico, análisis dinamico, herramientas online, comportamiento, mitigación y recomendaciones.

Ademas se añadira información a la plataforma Viper

## HERRAMIENTAS USADAS PARA EL ANALISIS DE MALWARE

- CAPE
- TRIA.GE
- ANY.RUN
- ANALYZE.INTEZER.COM
- JOESANDBOX.COM
- VIRUSTOTAL.COM

## DATOS GNERALES:

### Se ha analizado el siguiente fichero:

- Nombre: 8cc84c910910535990b7ec98
- Tipo: PE32 executable (GUI) Intel 80386, for MS Windows
- Tamaño: 212480 bytes
- MD5: a57745a30d63f511d28aa43e4b710e1c
- SHA1: 5985e7d1831784fd15de2cc62451deb16b65b046
- SHA256: 8cc84c910910535990b7ec98b521f7bb84774a78fa488a27dacff 5590a7322e3
- SHA3-384: a4d474c03a27132484c5ebda6e12715cef86624e72c9a8ff44ec98ed828f9039e15988a6af16efdb311223d77125829f
- CRC32: FDD14294
- TLSH: T14324BF02F2D0C473D5DA20F252155FF6EEFAE83204769D87C3581AA54E686D2E71A2CF
- Ssdeep: 6144:634cRT8CJLtVXW+BPGaDEoi/Siazel15:s4OT8CJpVm+BuaDm/Sps

## Analisis Estatico:

### Reglas Yara:

- Cape ha detectado 3 reglas yara:

Hit: PID 0 triggered the Yara rule 'INDICATOR\_SUSPICIOUS\_GENRansomware'

Hit: PID 0 triggered the Yara rule 'EXE\_in\_LNK'

Hit: PID 0 triggered the Yara rule 'Long\_RelativePath\_LNK'

De ello sabemos:

- Indicativo de ser un ransomware, es un .exe Buscando informacion con los hashes llegamos a la conclusión de que es un ransomware de la familia cerber
- 

Detection(s): **Cerber**

### Estructura de PE

Sections					
Name	RAW Address	Virtual Address	Virtual Size	Size of Raw Data	Characteristics
.text	0x0000400	0x00001000	0x00015593	0x00015600	IMAGE_SCN_CNT_CODE IMAGE_SCN_MEM_EXECUTE IMAGE_SCN_MEM_READ
.rdata	0x00015a00	0x00017000	0x00003d50	0x00003e00	IMAGE_SCN_CNT_INITIALIZED_DATA IMAGE_SCN_MEM_READ
.data	0x00019800	0x0001b000	0x00003878	0x00001200	IMAGE_SCN_CNT_INITIALIZED_DATA IMAGE_SCN_MEM_READ IMAGE_SCN_MEM_WRITE
.cdata	0x0001aa00	0x0001f000	0x00019004	0x00019200	IMAGE_SCN_CNT_INITIALIZED_DATA IMAGE_SCN_MEM_READ IMAGE_SCN_MEM_WRITE
.CRT	0x00033c00	0x00039000	0x00000004	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA IMAGE_SCN_MEM_READ

La entropía no supera el 6,9 (en r.data) y la siguiente mas alta es 6,66 en .txt por lo que deducimos que **no usa ningun Packer**

## Strings

Observamos mas indicios que confirmas que es un ransomwere con llamadas a funciones de encriptación.

```
CryptQueryObject
CertGetNameStringW
CertFreeCertificateContext
CertFindCertificateInStore
CryptMsgGetParam
CryptDecodeObjectEx
CRYPT32.dll
InternetConnectA
InternetCrackUrlA
InternetReadFile
HttpOpenRequestA
HttpSendRequestA
InternetOpenA
InternetCloseHandle
WININET.dll
StrStrIW
StrChrW
PathUnquoteSpacesW
PathFindFileNameW
StrChrIW
StrCmpNIW
StrCpyNW
StrChrIA
StrStrIA
StrSpnA
StrCmpNIA
PathRemoveExtensionW
StrCmpIW
StrToIntA
StrChrA
StrCmpNW
PathMatchSpecW
SHLWAPI.dll
```

Seguidamente vemos multiples comprobaciones e intentos de conexión a internet.

```
InternetConnectA
InternetCrackUrlA
InternetReadFile
HttpOpenRequestA
HttpSendRequestA
InternetOpenA
InternetCloseHandle
WININET.dll
```

Busca archivos, copia borra. shlwapi.dll es una Shell. ws2\_32.dll controla conexiones de red. mpr.dll también tiene funciones de red.

```
PathFindFileNameW
StrChrIW
StrCmpNIW
StrCpyNW
StrChrIA
StrStrIA
StrSpnA
StrCmpNIA
PathRemoveExtensionW
StrCmplW
StrToIntA
StrChrA
StrCmpNW
PathMatchSpecW
SHLWAPI.dll
GetFileVersionInfoSizeW
VERSION.dll
WNetCloseEnum
WNetOpenEnumW
WNetEnumResourceW
MPR.dll
CheckSumMappedFile
imagehlp.dll
WS2_32.dll
GetFileSize
SetFilePointer
SetEndOfFile
GetUserNameW
MoveFileExW
HeapFree
NetUserSetInfo
GetProcessHeap
WriteFile
GetSystemDirectoryW
Sleep
GetSystemWow64DirectoryW
FormatMessageW
ReadFile
CreateFileW
```

Múltiples referencias a encriptación (keys), Sacar información del sistema, ejecución de código por Shell.

```
RegEnumKeyExW
RegCloseKey
CommandLineToArgvW
SetErrorMode
GetSystemWindowsDirectoryW
GetModuleHandleW
OpenMutexW
GetVolumeInformationW
RegEnumKeyW
wsprintfW
IstrcatW
GetProcAddress
GetDateFormatW
SetFilePointerEx
WaitForSingleObject
SetEvent
OutputDebugStringW
SetFileTime
InitializeCriticalSection
LeaveCriticalSection
GetTimeFormatW
GetFileAttributesW
FileTimeToSystemTime
GetFileSizeEx
EnterCriticalSection
CreateEventW
CryptDestroyKey
GetFileTime
DeleteCriticalSection
CloseHandle
FileTimeToLocalFileTime
IstropcyW
CryptAcquireContextW
CryptGetKeyParam
ExitProcess
CoUninitialize
ShellExecuteExW
GetForegroundWindow
GetLastError
```

## Motores AV:

Ha sido detectado por 60/72 de los motores AV de virustotal:

60 / 72

60 security vendors and 2 sandboxes flagged this file as malicious

8cc84c910910535990b7ec98b521f7bb84774a78fa488a27dacf5590a7322e3  
poqexec.exe

207.50 KB  
Size

2022-12-13 16:41:16 UTC  
11 hours ago

EXE

peexe malware runtime-modules detect-debug-environment checks-network-adapters long-sleeps direct-cpu-clock-access calls-wmi persistence suspicious-udp

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Security Vendors' Analysis

Acronis (Static ML)	ⓘ Suspicious	Ad-Aware	ⓘ Gen.Variant.Razy.807639
AhnLab-V3	ⓘ Trojan/Win32.Zerber.C2324441	Alibaba	ⓘ Ransom.Win32/Cerber.682e57c
ALYac	ⓘ Gen.Variant.Razy.807639	Antiy-AVL	ⓘ Trojan/Win32.BTSGeneric
Arcabit	ⓘ Trojan.Razy.DC52D7	Avast	ⓘ Win32:Evo-gen [Trj]
AVG	ⓘ Win32:Evo-gen [Trj]	Avira (no cloud)	ⓘ TR/Hijacker.Gen
BitDefender	ⓘ Gen.Variant.Razy.807639	BitDefenderTheta	ⓘ Gen.NN.ZexaF.36106.muW@am3mlkQ
Bkav Pro	ⓘ W32.AI.Detect.malware1	ClamAV	ⓘ Win.Ransomware.Cerber-10
CrowdStrike Falcon	ⓘ Win/malicious_confidence_100% (W)	Cybereason	ⓘ Malicious.30d63f
Cylance	ⓘ Unsafe	Cynet	ⓘ Malicious (score: 100)
Cyren	ⓘ W32/ABRisk.YTXZ-9113	DrWeb	ⓘ Trojan.Encoder.4691

Varios mencionan que es un ransomware de la familia cerber.

## Analisis Dinamico:

Para el análisis dinámico hemos usado cape y tria.ge. Además más abajo hay un hipervínculo de un informe de joesandbox con el mismo hash (a la espera de tener cuenta). Hemos sacado los siguientes datos:

- Busca cuantas cuentas de usuarios tiene el sistema
- Crea un filtro de excepciones (antisanbox?)
- Comprueba hora del sistema (antisandbox?)
- Borra archivos temporales
- Llama a una función que permite cargar script
- Llama a ip-api.com:80/json

- Ejecuta muchos procesos ocultos en segundo plano. Funciones de almacenamiento, instalación de programas

```
A process created a hidden window
process: explorer.exe -> C:\Windows\SysWOW64\ZNY3koa9OqPg1TnjU\AdapterTroubleshooter.exe
type: call
pid: 1120
cid: 1863
call: ('timestamp': '2022-12-13 00:06:22.558', 'thread_id': '992', 'caller': '0x0003d519e', 'parentcaller': '0x00170f07', 'category': 'process', 'api': 'ShellExecuteExW', 'status': True, 'return_value': '433a5c57696e646f77735c537973574f5736345c5a4e59336b6f1394f71506731546e6a6c4a5c4164617074657254726f75626c65736866f7465722e657865'), {'name': 'process: explorer.exe -> C:\Windows\SysWOW64\bRK1H7EuZ_hyHPLmu\bthudtask.exe
type: call
pid: 1600
cid: 1865
call: ('timestamp': '2022-12-13 00:06:32.604', 'thread_id': '1904', 'caller': '0x0008519e', 'parentcaller': '0x00170f07', 'category': 'process', 'api': 'ShellExecuteExW', 'status': True, 'return_value': '433a5c57696e646f77735c537973574f5736345c5c2524b3148377445755a20687948504c6d755c62746875647461736b2e657865'), {'name': 'Parameters', 'value': '', 'raw_value': ''}, {'name': 'process: explorer.exe -> C:\Windows\SysWOW64\nv1EamdMkbR9Mdz_kl ddcw.exe
type: call
pid: 268
cid: 1884
call: ('timestamp': '2022-12-13 00:06:37.901', 'thread_id': '2640', 'caller': '0x0008519e', 'parentcaller': '0x00170f07', 'category': 'process', 'api': 'ShellExecuteExW', 'status': True, 'return_value': '433a5c57696e646f77735c537973574f5736345c5c6e39763145616d644d6b6252394d647a5f6b5c646363772e657865'), {'name': 'Parameters', 'value': '', 'raw_value': ''}, {'name': 'Show: process: explorer.exe -> C:\Windows\SysWOW64\if_ovnUp1GO6G7yi_eq\edudedit.exe
type: call
pid: 2024
cid: 1880
call: ('timestamp': '2022-12-13 00:06:49.198', 'thread_id': '2536', 'caller': '0x0008519e', 'parentcaller': '0x00170f07', 'category': 'process', 'api': 'ShellExecuteExW', 'status': True, 'return_value': '433a5c57696e646f77735c537973574f5736345c5c6206f766e557031474f36473779695f65715c65756463656469742e657865'), {'name': 'Parameters', 'value': '', 'raw_value': ''}, {'name': 'process: explorer.exe -> C:\Windows\SysWOW64\isPRc_K_5beU-colHbr\iscsidi.exe
type: call
pid: 1728
cid: 1874
call: ('timestamp': '2022-12-13 00:06:53.354', 'thread_id': '3032', 'caller': '0x0008519e', 'parentcaller': '0x00170f07', 'category': 'process', 'api': 'ShellExecuteExW', 'status': True, 'return_value': '433a5c57696e646f77735c537973574f5736345c73505263204b20356265552d636f6c4862725c6973637369636c692e657865'), {'name': 'Parameters', 'value': '', 'raw_value': ''}, {'name': 'process: explorer.exe -> C:\Windows\SysWOW64\w3JFXMsqxbW-LtzBBY\iscsidi.exe
type: call
pid: 2696
cid: 1877
call: ('timestamp': '2022-12-13 00:07:03.901', 'thread_id': '3044', 'caller': '0x0008519e', 'parentcaller': '0x00170f07', 'category': 'process', 'api': 'ShellExecuteExW', 'status': True, 'return_value': '433a5c57696e646f77735c537973574f5736345c76334a46784d73717862572d4c747a4242595c6973637369636c692e657865'), {'name': 'Parameters', 'value': '', 'raw_value': ''}, {'name': 'process: explorer.exe -> C:\Windows\SysWOW64\w3JFXMsqxbW-LtzBBY\iscsidi.exe
```

- **Carga .exe y los ejecuta:**

```
Drops a binary and executes it
binary: C:\Users\ama\AppData\Roaming\91A3A19B-3C0B-2720-83B9-996EBBC78C29\HOSTNAME.EXE
```

- **Intenta conectarse a 512 ips diferentes**
- Genera trafico http que apunta a ip-api.com:80/json sin cabecera, que se asocia a malware.
- Muchas conexiones UDP
- **Mira tu ip publica**
- Hace un ping -n posible antisandbox
- Mata procesos
- **Injection en el explorador de archivos.**
- **Textualmente, “Excibe características de un ransomware cerber”**
- Intenta retrasar el análisis durante un periodo muy largo (Antisandbox)
- Se instala entre los programas que se lanzan automáticamente al iniciar Windows.
- **Intenta reconocer el antivirus instalado**
- **Crea copias de si mismo**

- Borra archivos
- Mecanicas asociadas a persistencia
- Usa líneas de comando sospechosas
- Tria.ge lo asocia al troyano bancario gozi
- Borra backup files.

Signatures
Enumerates user accounts on the system
SetUnhandledExceptionFilter detected (possible anti-debug)
Yara rule detections observed from a process memory dump/dropped files/CAPE
Possible date expiration check, exits too soon after checking local time
Anomalous file deletion behavior detected (10+)
Dynamic (Imported) function loading detected
Performs HTTP requests potentially not found in PCAP.
A process created a hidden window
Drops a binary and executes it
Creates RWX memory
Multiple direct IP connections
HTTP traffic contains suspicious features which may be indicative of malware related traffic
Creates an excessive number of UDP connection attempts to external IP addresses
Performs some HTTP requests
Looks up the external IP address.
A ping command was executed with the -n argument possibly to delay analysis
Uses Windows utilities for basic functionality

Behavioural detection: Injection (Inter-process)
A process attempted to delay the analysis task by a long amount of time.
Exhibits behavior characteristic of Cerber ransomware
Created a process from a suspicious location
Installs itself for autorun at Windows startup
Behavioural detection: Injection (Process Hollowing)
Attempts to identify installed AV products by installation directory
Creates a copy of itself
Deletes executed files from disk
Deletes its original binary from disk
Executed a process and injected code into it, probably while unpacking
Registers an application compatibility shim database for persistence
Attempts to modify Explorer settings to prevent hidden files from being displayed
Uses suspicious command line tools or Windows utilities
command: id /c taskkill /f /im "8cc84c910910535990b7ec98.exe" > NUL & ping -n 1 127.0.0.1 > NUL & del "C:\Users\ama\AppData\Local\Temp\8cc84c910910535990b7ec98.exe" > NUL
command: id /c taskkill /f /im "8cc84c910910535990b7ec98.exe" > NUL & ping -n 1 127.0.0.1 > NUL & del "C:\Users\ama\AppData\Local\Temp\8cc84c910910535990b7ec98.exe" > NUL
command: C:\Windows\system32\cmd.exe /d /c taskkill /f /im "8cc84c910910535990b7ec98.exe" > NUL & ping -n 1 127.0.0.1 > NUL & del "C:\Users\ama\AppData\Local\Temp\8cc84c910910535990b7ec98.exe" > NUL
command: taskkill /f /im "8cc84c910910535990b7ec98.exe" > NUL & ping -n 1 127.0.0.1 > NUL & del "C:\Users\ama\AppData\Local\Temp\8cc84c910910535990b7ec98.exe" > NUL
Screenshots



#### Cerber

Cerber is a widely used ransomware-as-a-service (RaaS), first seen in 2017.

cerber

ransomware

#### Gozi

Gozi is a well-known and widely distributed banking trojan.

gozi

banker

trojan

#### Modifies visibility of hidden/system files in Explorer

evasion

#### Deletes shadow copies

Ransomware often targets backup files to inhibit system recovery.

ransomware

#### Modifies boot configuration data using bcdedit

ransomware

evasion

#### Adds policy Run key to start application

persistence

#### Downloads MZ/PE file

#### Executes dropped EXE

#### Modifies extensions of user files

Ransomware generally changes the extension on encrypted files.

ransomware

#### Registers COM server for autorun

persistence

#### Sets file execution options in registry

persistence

## Informe Mitre:

Mitre ATTACK						
Discovery	Defense Evasion	Privilege Escalation	Command and Control	Execution	Impact	Persistence
<ul style="list-style-type: none"><li>• T1033 - System Owner/User Discovery<ul style="list-style-type: none"><li>◦ user_enum</li></ul></li><li>• T1083 - File and Directory Discovery<ul style="list-style-type: none"><li>◦ anttav_detectfile</li></ul></li><li>• T1518 - Software Discovery<ul style="list-style-type: none"><li>◦ anttav_detectfile</li></ul></li></ul>	<ul style="list-style-type: none"><li>• T1055 - Process Injection<ul style="list-style-type: none"><li>◦ injection_inter_process</li></ul></li><li>• T1070 - Indicator Removal on Host<ul style="list-style-type: none"><li>◦ deletes_executed_files</li></ul></li><li>• T1112 - Modify Registry<ul style="list-style-type: none"><li>◦ stealth_hiddenreg</li><li>◦ persistence_autorun</li></ul></li><li>• T1202 - Indirect Command Execution<ul style="list-style-type: none"><li>◦ suspicious_command_tools</li><li>◦ uses_windows_utilities</li></ul></li><li>• T1562 - Impair Defenses<ul style="list-style-type: none"><li>◦ stealth_hiddenreg</li></ul></li><li>• T1564 - Hide Artifacts<ul style="list-style-type: none"><li>◦ stealth_window</li><li>◦ stealth_hiddenreg</li></ul></li></ul>	<ul style="list-style-type: none"><li>• T1055 - Process Injection<ul style="list-style-type: none"><li>◦ injection_inter_process</li></ul></li><li>• T1546 - Event Triggered Execution<ul style="list-style-type: none"><li>◦ persistence_shim_database</li></ul></li><li>• T1547 - Boot or Logon Autostart Execution<ul style="list-style-type: none"><li>◦ persistence_autorun</li></ul></li></ul>	<ul style="list-style-type: none"><li>• T1071 - Application Layer Protocol<ul style="list-style-type: none"><li>◦ http_request</li><li>◦ recon_checkip</li><li>◦ network_multiple_direct_ip_connections</li><li>◦ network_http</li><li>◦ procmem_yara</li><li>◦ network_cnc_http</li><li>◦ suspicious_ping_use</li></ul></li><li>• T1095 - Non-Application Layer Protocol<ul style="list-style-type: none"><li>◦ network_excessive_udp</li></ul></li></ul>	<ul style="list-style-type: none"><li>• T1106 - Native API<ul style="list-style-type: none"><li>◦ process_creation_suspicious_location</li></ul></li><li>• T1129 - Shared Modules<ul style="list-style-type: none"><li>◦ dropper</li></ul></li></ul>	<ul style="list-style-type: none"><li>• T1485 - Data Destruction<ul style="list-style-type: none"><li>◦ anomalous_deletefile</li></ul></li></ul>	<ul style="list-style-type: none"><li>• T1546 - Event Triggered Execution<ul style="list-style-type: none"><li>◦ persistence_shim_database</li></ul></li><li>• T1547 - Boot or Logon Autostart Execution<ul style="list-style-type: none"><li>◦ persistence_autorun</li></ul></li></ul>

## Analisis de Red:

El ransomware ha intentado hacer 512 conexiones a hosts de Rusia, Montenegro y EEUU Se ha conectado a un dns: ip-api.com y a las siguientes ips por protocolo tcp:

Hosts (513)	DNS (1)	TCP (12)	UDP (2612)	HTTP (1)	SMTP (0)	IRC (0)	ICMP (0)	Suricata Alerts (0)	Suricata TLS (0)	Suricata HTTP (0)	Suricata Files (0)
Source	Source Port	Destination	Destination Port								
192.168.122.6	49168	208.95.112.1	80								
192.168.122.6	49172	208.95.112.1	80								
192.168.122.6	49275	93.184.220.29	80								
192.168.122.6	49280	93.184.220.29	80								
192.168.122.6	49286	93.184.220.29	80								
192.168.122.6	49294	93.184.220.29	80								
192.168.122.6	49296	93.184.220.29	80								
192.168.122.6	49302	2.21.181.38	443								
192.168.122.6	49307	2.22.245.40	443								
192.168.122.6	49309	2.22.245.40	443								
192.168.122.6	49311	2.22.245.40	443								
192.168.122.6	49322	93.184.220.29	80								

## Muestra de ips Rusas:

Hosts (513)	DNS (1)	TCP (12)	UDP (2612)	HTTP (1)	SMTP (0)	IRC (0)	ICMP (0)	Suricata Alerts (0)	Suricata TLS (0)	Suricata HTTP (0)	Suricata Files (0)
Direct	IP	Country Name									
Y	31.184.235.255 [VT]	Russian Federation									
Y	31.184.235.254 [VT]	Russian Federation									
Y	31.184.235.253 [VT]	Russian Federation									
Y	31.184.235.252 [VT]	Russian Federation									
Y	31.184.235.251 [VT]	Russian Federation									
Y	31.184.235.250 [VT]	Russian Federation									
Y	31.184.235.249 [VT]	Russian Federation									

Mencion a que aunque Cape y los sandbox online identifican estas ips como rusas, virus total y <https://ip-api.com/#31.184.235.243> las asocia a reino unido. Posible servidor intermedio/redireccion hacia la botnet.

## Muestra de ips de Montenegro:

Y	31.184.234.255 [VT]	Montenegro									
Y	31.184.234.254 [VT]	Montenegro									
Y	31.184.234.253 [VT]	Montenegro									
Y	31.184.234.252 [VT]	Montenegro									
Y	31.184.234.251 [VT]	Montenegro									
Y	31.184.234.250 [VT]	Montenegro									

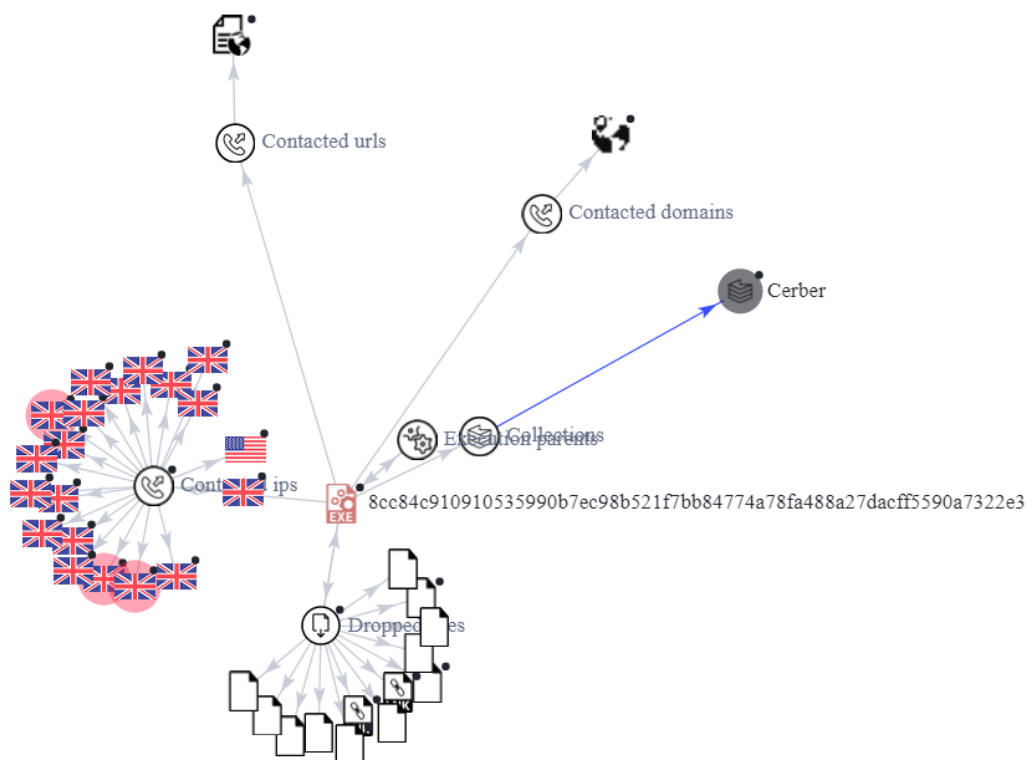
Muestra ip única de EEUU, esta ultima es correspondiente a <https://ip-api.com/> que utiliza para sacar nuestra ip publica:

N	208.95.112.1 [VT]	United States
Looks up the external IP address		
domain: ip-api.com		

Tria.ge además identifico las siguientes URLs asociadas:

<http://bqyjebfh25oellur.onion.to/AA79-9F05-B08B-0046-168C>  
<http://bqyjebfh25oellur.onion.cab/AA79-9F05-B08B-0046-168C>  
<http://bqyjebfh25oellur.onion.nu/AA79-9F05-B08B-0046-168C>  
<http://bqyjebfh25oellur.onion.link/AA79-9F05-B08B-0046-168C>  
<http://bqyjebfh25oellur.tor2web.org/AA79-9F05-B08B-0046-168C>  
<http://bqyjebfh25oellur.onion/AA79-9F05-B08B-0046-168C>

## Resumen de la red:



## Arbol de Procesos:

- 8cc84c910910535990b7ec98.exe 2772
  - HOSTNAME.EXE 3004
    - explorer.exe 1120
    - explorer.exe 1600
    - explorer.exe 268
    - explorer.exe 2024
    - explorer.exe 1728
    - explorer.exe 2696
    - explorer.exe 1904
    - explorer.exe 2832
    - explorer.exe 2448
    - explorer.exe 2780
    - explorer.exe 2424
    - explorer.exe 3200
    - explorer.exe 4024
    - explorer.exe 1588
    - explorer.exe 3948
    - explorer.exe 1364
    - explorer.exe 3448
    - explorer.exe 2804
    - explorer.exe 3112
  - cmd.exe 1632 /d /c taskkill /f /im  
"8cc84c910910535990b7ec98.exe" > NUL & ping -n 1 127.0.0.1  
> NUL & del  
"C:\Users\ama\AppData\Local\Temp\8cc84c910910535990b7ec  
98.exe" > NUL
    - taskkill.exe 2152 taskkill /f /im  
"8cc84c910910535990b7ec98.exe"
    - PING.EXE 2372 ping -n 1 127.0.0.1
- explorer.exe 2228

## Importacion de bibliotecas:

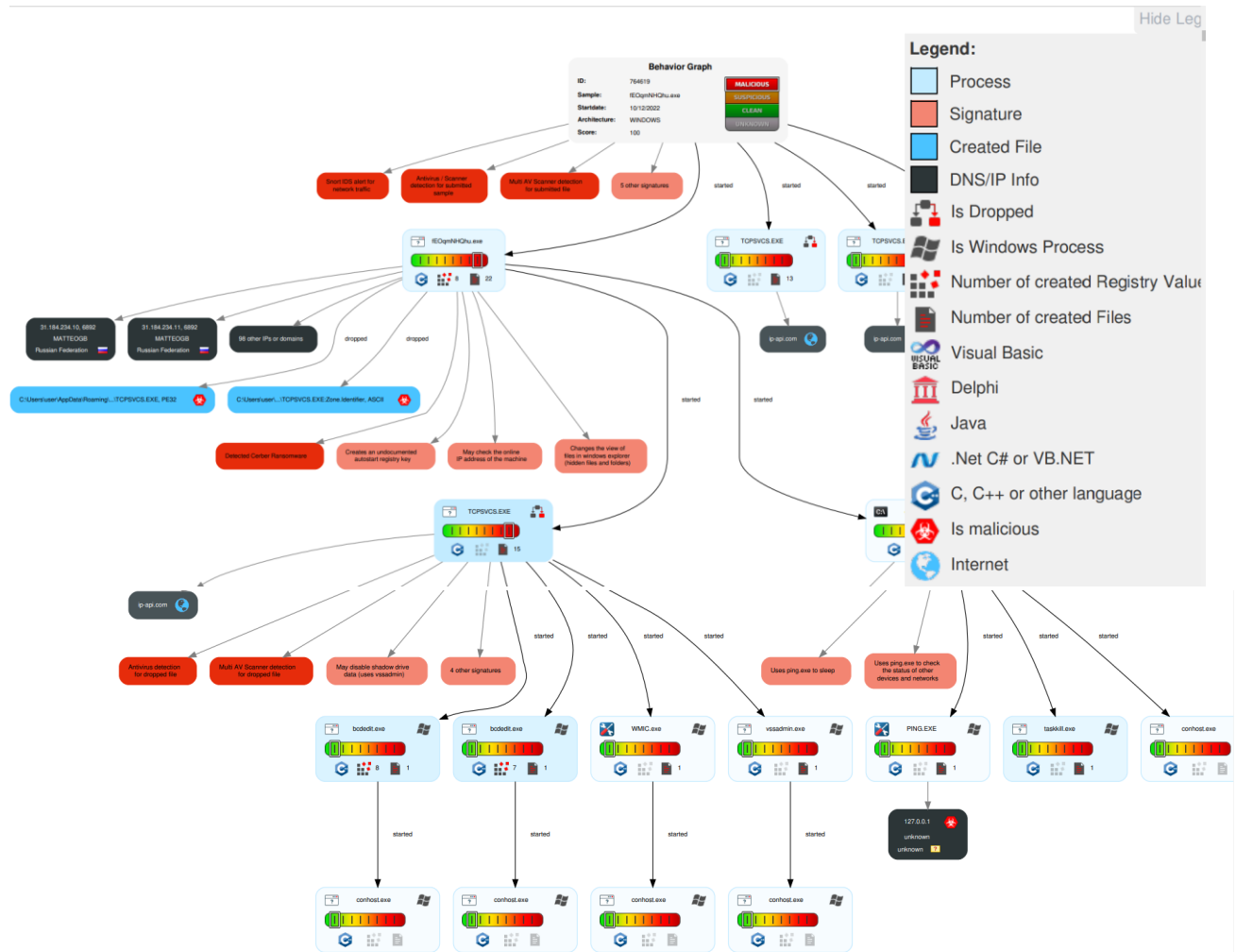
- MPR.dll
- imagehlp.dll
- CRYPT32.dll
- KERNEL32.dll
- OLEAUT32.dll
- NETAPI32.dll
- SHELL32.dll
- ntdll.dll
- VERSION.dll
- WININET.dll
- GDI32.dll

- ADVAPI32.dll
- ole32.dll
- SHLWAPI.dll
- WS2\_32.dll
- USER32.dll

### Enlaces a informes de Herramientas Online:

- [analyze.intezer](#)
- [analyze.intezer informe](#)
- [virustotal](#)
- [Tria.ge](#)
- [Malwarebytes](#)
- [Filescan](#)

### Comportamiento:



- De forma resumida es un malware ransomware de la familia Cerber.
- Crea ordenes de autoejecutarse cuando el ordenador se inicie:  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\HOSTNAME  
HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\AutoRun  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run\HOSTNAME
- Crea ejecuta y copia payload:  
"C:\Windows\SysWOW64\explorer.exe"  
"C:\Users\ama\AppData\Roaming\{91A3A19B-3C0B-2720-83B9-996EBBC78C29}\HOSTNAME.EXE"  
  
"C:\Users\ama\AppData\Roaming\{91A3A19B-3C0B-2720-83B9-996EBBC78C29}\HOSTNAME.EXE"  
  
"C:\Users\ama\AppData\Roaming\{91A3A19B-3C0B-2720-83B9-996EBBC78C29}\HOSTNAME.EXE"  
  
"C:\Users\ama\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\HOSTNAME.lnk
- Entre los métodos antisandbox encontramos:
  - Saca información de los usuarios del sistema
  - Comprueba si estas haciendo debugging
  - Comprueba la fecha y hora
- Crea conexión para conocer la IP pública del PC al conectarse a [208.95.112.1](http://208.95.112.1)
- Descarga y ejecuta funciones de encriptación.
- Usa una gran red de conexiones UDP para intentar conectarse a la botnet.
- Te guía para que realices el pago a través de tor cambio del descifrado:

### How to get «Cerber Decryptor»?

1. Create a Bitcoin Wallet (we recommend [Blockchain.info](#))

2. Buy necessary amount of Bitcoins

Do not forget about the transaction commission in the Bitcoin network ( $\approx \text{B}0.0005$ ).

Here are our recommendations:

[LocalBitcoins.com](#) – the fastest and easiest way to buy and sell Bitcoins;  
[CoinCafe.com](#) – the simplest and fastest way to buy, sell and use Bitcoins;  
[BTCDirect.eu](#) – the best for Europe;  
[CEX.IO](#) – Visa / MasterCard;  
[CoinMama.com](#) – Visa / MasterCard;  
[HowToBuyBitcoins.info](#) – discover quickly how to buy and sell bitcoins in your local currency.

3. Send **B1.24** to the following Bitcoin address:

16LHfVGteAn61pdChrRewn7qo8gbpkcNr2

4. Control the amount transaction at the «Payments History» panel below

5. Get a link and download the software

## CERBER DECRYPTOR



### Your documents, photos, databases and other important files have been encrypted!

To decrypt your files you need to buy the special software – «Cerber Decryptor».

All transactions should be performed via **bitcoin** network only.

Within 7 days you can purchase this product at a special price: **B1.24** ( $\approx \$521$ ).

After 7 days the price of this product will increase up to: **B2.48** ( $\approx \$1043$ ).

The special price is available:

06 . 23:59:42

### Mitigacion:

## Borrar

### Claves de registro:

- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\HOSTNAME
- HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\AutoRun
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run\HOSTNAME

### Ficheros:

- C:\Users\ama\AppData\Roaming\{91A3A19B-3C0B-2720-83B9-996EBBC78C29}\HOSTNAME.EXE"
- data: "C:\Users\ama\AppData\Roaming\{91A3A19B-3C0B-2720-83B9-996EBBC78C29}\HOSTNAME.EXE"
- "C:\Users\ama\AppData\Roaming\{91A3A19B-3C0B-2720-83B9-996EBBC78C29}\HOSTNAME.EXE"
- C:\Users\ama\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\HOSTNAME.lnk
- En la última dirección posiblemente sean dos .lnk

## Acciones Adicionales:

- Aislar dispositivo infectado.
- Utilice restauración de sistema para volver a un estado limpio.
- Realizar copias de seguridad.
- Recordar que a día de hoy no hay ningún software que rompa o haga un bypass a la encriptación, por mucho que los antivirus lo anuncien.

## Recomendación:

- Usar un usuario sin permisos.
- Solo administrador debería de poder cambiar registros de Windows y los respaldos.
- Incluir las IPs y los hashes a las herramientas de detección.