
ANÁLISIS MALWARE

Laura Quijorna Velázquez

Junio 2023

**En la memoria que se presenta a continuación se detalla el análisis de un malware.
Tras dicho análisis, se determinó que se trataba de un ransomware llamado
MedusaLocker.**

MEMORIA

DATOS GENERALES

Se ha analizado el siguiente fichero:

- MD5 f6f120d1262b88f79debb5d848ac7db9
- SHA1 1339282f9b2d2a41326daf3cf284ec2ae8f0f93c
- SHA256
1bc0575b3fc6486cb2510dac1ac6ae4889b94a955d3eade53d3ba3a92d133281
- Ssdeep:
b'6144:c5vMUmRTTgwnfeP+Jx1cLNAlyBcc9WrEWUC4wQh/6BeX:/U8Tgufnx1cLNn
cgQWUUQh/+e'
- Nombre: 1bc0575b3fc6486cb2510dac
- Tipo: PE32 executable (GUI) Intel 80386, for MS Windows
- Tamaño: 241152 bytes
- TimeStamp del PE: 2019-10-31 06:08:40
- Lenguaje: Inglés US

ANÁLISIS ESTÁTICO

Durante el análisis estático llevado a cabo con Cape se ha podido extraer la siguiente información:

- **Reglas YARA:**
 - vmdetect - Possibly employs anti-virtualization techniques - Author: nex
 - INDICATOR_SUSPICIOUS_GENRansomware - detects command variations typically used by ransomware - Author: ditekSHen
 - INDICATOR_SUSPICIOUS_EXE_UACBypass_CMSTPCOM - Detects Windows exceutables bypassing UAC using CMSTP COM interfaces. MITRE (T1218.003) - Author: ditekSHen
 - UPX - Author: Kevin Breen <kevin@techanarchy.net>
 - MedusaLocker - MedusaLocker Payload - Author: ditekshen

Estas detecciones proporcionan información sobre las técnicas que se utilizan durante la ejecución del malware. Éstas son:

- Emplea técnicas de antivirtualización.
- Detecta variaciones de comandos típicos de un ransomware
- Con cmstp.exe omite el control de cuentas de usuario y ejecuta comandos arbitrarios desde un INF malicioso a través de una interfaz COM elevada automáticamente. Es de esta manera como elude el UAC y consigue elevar privilegios.
- Utiliza empaquetado UPX, es decir, tiene packer.

- **Estructura del PE :**

- UPX0
- UPX1 → Con entropía que sobrepasa el 7,5 (7,93), esto quiere decir que tiene un payload o un packer.
- .rsrc

Con la estructura del PE queda claro que tiene un packer.

- **Strings:**

En los strings se puede observar que importan librerías dinámicas:

```
ADVAPI32.dll  
CRYPT32.dll  
IPHLPAPI.DLL  
KERNEL32.DLL  
MPR.dll  
NETAPI32.dll  
ole32.dll  
OLEAUT32.dll  
Rstrtmgr.DLL  
SHELL32.dll  
WS2_32.dll
```

Descripción de librerías:

- Kernel32.dll → esta librería es característica por tener acceso y manipulación de memoria, archivos, creación de procesos y hardware. Observando más en profundidad he podido constatar que se ejecutan funciones dentro de la librería de Kernel32 que posiblemente estén relacionadas con métodos anti debugging.

```
kernel32.dll.GetTickCount
```

```
kernel32.dll.GetVolumePathNamesForVolumeNameW  
kernel32.dll.FindVolumeClose  
kernel32.dll.SetVolumeMountPointW  
kernel32.dll.FindFirstVolumeW  
kernel32.dll.QueryDosDeviceW  
kernel32.dll.GetEnvironmentVariableW  
kernel32.dll.GetLogicalDrives  
kernel32.dll.GetProcessHeap
```

```
kernel32.dll.GetConsoleMode  
kernel32.dll.GetConsoleCP
```

```
kernel32.dll.GetTimeFormatW  
kernel32.dll.GetDateFormatW
```

```
kernel32.dll.Sleep
```

- advapi.dll → parece tener una posible relación con la encriptación y registro de claves. Esta librería, a modo general, es la encargada de algunas funciones un poco más avanzadas como registro y administración de servicios.

```
advapi32.dll.CryptExportKey  
advapi32.dll.RegCreateKeyW  
advapi32.dll.RegOpenKeyExW  
advapi32.dll.RegSetValueExW  
advapi32.dll.RegCloseKey  
advapi32.dll.CryptReleaseContext  
advapi32.dll.CryptGenKey  
advapi32.dll.CryptImportKey  
advapi32.dll.OpenProcessToken  
advapi32.dll.GetTokenInformation
```

- Crypt32 → contiene funciones de mensajería criptográfica y de certificado en CryptoAPI.

```
crypt32.dll.CryptStringToBinaryA
```

- Iphlpapi.dll → es un módulo que contiene las funciones usadas por el Windows IP Helper API permitiendo recuperar y modificar los ajustes de configuración de red para el equipo local.

```
iphlpapi.dll.IcmpSendEcho  
iphlpapi.dll.IcmpCloseHandle  
iphlpapi.dll.GetAdaptersInfo  
iphlpapi.dll.IcmpCreateFile
```

- shell32.dll → contiene las funciones del API del shell de Windows, se utilizan para abrir páginas webs y ficheros.

shell32.dll.SHCreateLocalServerRunDll

- Ws2_32.dll → son las encargadas de la parte de redes. Su uso significa que se está accediendo a una red o que la aplicación realiza tareas relacionadas con la red.
- oleaut32.dll → facilita la comunicación de datos significativos entre las aplicaciones de software.

ole32.dll.CoTaskMemFree
ole32.dll.StringFromGUID2

- Rstrtmgr.dll se considera un tipo de archivo Restart Manager. Este tipo de archivo permite que todas las aplicaciones y servicios críticos se apaguen y reinicien . Esto libera los archivos que están en uso y permite que se completen las operaciones de instalación

rstrtmgr.dll.RmShutdown
rstrtmgr.dll.RmRegisterResources
rstrtmgr.dll.RmStartSession
rstrtmgr.dll.RmGetList
rstrtmgr.dll.RmEndSession

En los strings aparecen una serie de funcionalidades de windows que parecen ser que se pueden estar ejecutando:

```
RegCloseKey  
CryptStringToBinaryA  
IcmpSendEcho  
ExitProcess  
GetProcAddress  
LoadLibraryA  
VirtualProtect  
WNetGetConnectionW  
NetShareEnum  
CoGetObject  
RmGetList  
SHEmptyRecycleBinW
```

Algunas de estas funciones se describen de la siguiente manera:

- CryptStringToBinary convierte una cadena formateada en una matriz de bytes.
- IcmpSendEcho envía una solicitud de eco ICMP IPv4 y devuelve las respuestas en forma de eco. La llamada se devuelve cuando el tiempo de espera ha expirado.
- LoadLibraryA carga el módulo especificado en el espacio de direcciones del proceso de llamada y devuelve un identificador que se puede usar en GetProcAddress para obtener la dirección de una función DLL.
- GetProcAddress recupera la dirección de una función exportada (también conocida como procedimiento) o variable de la librería dinámica (DLL) especificada.
- VirtualProtect cambia la protección en una región de páginas confirmadas en el espacio de direcciones virtuales del proceso de llamada.
- WNetGetConnectionW recupera el nombre del recurso de red asociado con un dispositivo local.
- NetShareEnum recupera información sobre cada recurso compartido en un servidor.

- RmGetList obtiene una lista de todas las aplicaciones y servicios que actualmente usan recursos que se han registrado con la sesión de Restart Manager.
- SHEmptyRecycleBinW vacía la papelera de reciclaje en la unidad especificada.

Viendo la descripción de las librerías junto con las funciones, es posible que se esté instalando un software que probablemente será el malware y esté realizando una conexión con la botnet a través del protocolo de Icmp. Además podría ser que esté intentando obtener datos del sistema, bien para modificarlos, eliminarlos o encriptarlos.

- Motores AV (Extraído de VT)

- El fichero .exe ha sido detectado por un total de 62/71 motores AV en VirusTotal mediante Cape:

<https://www.virustotal.com/gui/file/1bc0575b3fc6486cb2510dac1ac6ae4889b94a955d3eade53d3ba3a92d133281>

2023-06-15	62 / 71	Win32 EXE	1bc0575b3fc6486cb2510dac1ac6ae4889b94a955d3eade53d3ba3a92d133281.exe
------------	---------	-----------	--

- El fichero comprimido ha sido detectado por un total de 3/62 motores AV.

2023-04-10	3 / 62	ZIP	9682372408.zip
------------	--------	-----	----------------

- También aparece una detección de un archivo .html que ha sido detectado por un total de 6/59 motores AV.

✓ 2023-04-06	6 / 59	HTML	HOW_TO_RECOVER_DATA.html
--------------	--------	------	--------------------------

ANÁLISIS DINÁMICO

Para el análisis dinámico se ha utilizado Cape y MitreAttack, donde después de la realización del análisis se han podido extraer los siguientes datos:

Collects and encrypts information about the computer likely to send to C2 server
SetUnhandledExceptionFilter detected (possible anti-debug)
Uses Windows APIs to generate a cryptographic key
A file with an unusual extension was attempted to be loaded as a DLL.
Possible date expiration check, exits too soon after checking local time
Anomalous file deletion behavior detected (10+)
Dynamic (imported) function loading detected
Enumerates running processes
Expresses interest in specific running processes
Repeatedly searches for a not-found process, may want to run with startbrowser=1 option
Reads data out of its own binary image
Manipulates data from or to the Recycle Bin
A process created a hidden window
Creates RWX memory
Creates an autorun.inf file
Uses Windows utilities for basic functionality

- Utiliza las APIs de Windows para generar una clave criptográfica y para ejecutar comportamientos para llamar a los servicios del sistema operativo de bajo nivel dentro del kernel, como los que involucran hardware/dispositivos, memoria y procesos

API	Arguments
CryptGenKey	AlgId: AES_256

- Carga un archivo con una extensión DLL:

LdrLoadDll	Flags: 0x00000000 FileName: C:\Windows\sysnative\slui.exe BaseAddress: 0x00000000
-------------------	---

- Encuentra anomalías en diferentes ficheros:

```

file: C:$Recycle.Bin\S-1-5-21-2225935160-554833140-588599421-1000\R44QTP5.py
file: C:$Recycle.Bin\S-1-5-21-2225935160-554833140-588599421-1000$I44QTP5.py
file: C:$Recycle.Bin\S-1-5-21-2225935160-554833140-588599421-1000$RNB7KZ3.pub
file: C:$Recycle.Bin\S-1-5-21-2225935160-554833140-588599421-1000$INB7KZ3.pub
file: C:\Windows\Tasks\svhost.job
file: C:\Windows\sysnative\Tasks\svhost
file: C:\Windows\Tasks\svhost.job
file: C:\Windows\sysnative\wbem\Performance\WmiApRpl.h
file: C:\Windows\sysnative\wbem\Performance\WmiApRpl.ini
file: C:\Windows\inf\WmiApRpl\0009\WmiApRpl.ini
file: C:\Windows\inf\WmiApRpl\000A\WmiApRpl.ini
file: C:\Windows\inf\WmiApRpl\WmiApRpl.h
file: C:\Windows\sysnative\PerfStringBackup.TMP

```

- Hace importación dinámica de librerías cuando se carga en memoria (esto ya se ha mencionado también al principio del informe).

```
DynamicLoader: kernel32.dll/Process32NextW
DynamicLoader: kernel32.dll/Process32FirstW
DynamicLoader: kernel32.dll/CreateProcessW
DynamicLoader: kernel32.dll/GetTickCount
DynamicLoader: kernel32.dll/CopyFileW
DynamicLoader: kernel32.dll/GetCurrentProcess
DynamicLoader: kernel32.dll/WriteConsoleW
DynamicLoader: kernel32.dll/CreateToolhelp32Snapshot
DynamicLoader: kernel32.dll/OpenProcess
DynamicLoader: kernel32.dll/WaitForSingleObject
DynamicLoader: kernel32.dll/TerminateProcess
DynamicLoader: kernel32.dll/FindClose
DynamicLoader: kernel32.dll/FindNextVolumeW
DynamicLoader: kernel32.dll/GetVolumePathNamesForVolumeNameW
DynamicLoader: kernel32.dll/FindVolumeClose
DynamicLoader: kernel32.dll/SetVolumeMountPointW
DynamicLoader: kernel32.dll/FindFirstVolumeW
```

- Enumera procesos en ejecución, seguramente esto lo haga para detectar si el sistema es virtualizado:

```
process: System with pid 4
process: smss.exe with pid 260
process: csrss.exe with pid 336
process: wininit.exe with pid 364
process: csrss.exe with pid 388
process: winlogon.exe with pid 424
process: services.exe with pid 468
process: lsass.exe with pid 484
process: lsm.exe with pid 492
process: svchost.exe with pid 588
process: svchost.exe with pid 652
process: svchost.exe with pid 736
process: svchost.exe with pid 804
process: svchost.exe with pid 860
```

- Además, expresa interés en determinados procesos en ejecución:

ProcessName: system ProcessId: 4
ProcessName: smss.exe ProcessId: 260
ProcessName: csrss.exe ProcessId: 336
ProcessName: wininit.exe ProcessId: 364
ProcessName: csrss.exe ProcessId: 388

- Busca un proceso con un nombre concreto que no encuentra pero aún así sigue buscando (no sé cuál es).
- Lee datos y los saca fuera de su propia imagen binaria. Esto es indicativo de que tiene un payload. Indagando más he podido ver que el nombre del payload es: **svhost**
- Manipula datos desde o hacia la papelera de reciclaje, probablemente para eliminarlos o encriptarlos. Los ciberdelincuentes pueden destruir los datos y archivos para no hacer posible la recuperación de éstos.

- Un proceso creó una ventana oculta seguramente para ocultar actividades maliciosas que puedan ser vistas por los usuarios.

```
process: 1bc0575b3fc6486cb2510dac.exe -> vssadmin.exe Delete Shadows /All /Quiet
process: 1bc0575b3fc6486cb2510dac.exe -> bcdedit.exe /set {default} recoveryenabled No
process: 1bc0575b3fc6486cb2510dac.exe -> bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
process: 1bc0575b3fc6486cb2510dac.exe -> wbadmin DELETE SYSTEMSTATEBACKUP
process: 1bc0575b3fc6486cb2510dac.exe -> wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
process: 1bc0575b3fc6486cb2510dac.exe -> wmic.exe SHADOWCOPY /nointeractive
process: 1bc0575b3fc6486cb2510dac.exe -> vssadmin.exe Delete Shadows /All /Quiet
process: 1bc0575b3fc6486cb2510dac.exe -> bcdedit.exe /set {default} recoveryenabled No
process: 1bc0575b3fc6486cb2510dac.exe -> bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
process: 1bc0575b3fc6486cb2510dac.exe -> wbadmin DELETE SYSTEMSTATEBACKUP
process: 1bc0575b3fc6486cb2510dac.exe -> wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
process: 1bc0575b3fc6486cb2510dac.exe -> wmic.exe SHADOWCOPY /nointeractive
process: 1bc0575b3fc6486cb2510dac.exe -> vssadmin.exe Delete Shadows /All /Quiet
process: 1bc0575b3fc6486cb2510dac.exe -> bcdedit.exe /set {default} recoveryenabled No
process: 1bc0575b3fc6486cb2510dac.exe -> bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
process: 1bc0575b3fc6486cb2510dac.exe -> wbadmin DELETE SYSTEMSTATEBACKUP
process: 1bc0575b3fc6486cb2510dac.exe -> wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
process: 1bc0575b3fc6486cb2510dac.exe -> wmic.exe SHADOWCOPY /nointeractive
process: svchost.exe -> \\?\C:\Windows\system32\wbem\WMIADAP.EXE
```

- Crea una memoria con permisos de lectura y escritura, seguramente para la manipulación de los datos.
- Crea un fichero que suele ser utilizado para ejecutar el malware en dispositivos extraíbles, este fichero es “**autorun.inf**”.
- Usa las utilidades de windows para funcionalidades básicas y lanza comandos de ejecución sospechosos:

```
command: bcdedit.exe /set {default} recoveryenabled No
command: bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
command: wmic.exe SHADOWCOPY /nointeractive
command: wmic.exe SHADOWCOPY /nointeractive
```

- Crea un proceso (**svhost.exe**) desde una localización sospechosa.

C:\Users\ama\AppData\Roaming\svhost.exe

Este proceso realmente se ubica en "%SystemRoot%\System32\svchost.exe y no desde donde se está ejecutando. Puede ser un indicio de que está utilizando el nombre de un archivo legítimo de windows para ocultarse mientras está siendo ejecutado. Es por lo que podríamos decir que el malware se está enmascarando.

Este archivo posiblemente sea el que se ejecute cada vez que se inicie el sistema, siendo lo que va a crear persistencia. Se ejecuta a través del mecanismo de persistencia **taskend.exe**

```
taskeng.exe 2248 taskeng.exe {494CB41B-DEF8-46F4-8C8C-B26100635D2C}  
S-1-5-21-2225935160-554833140-588599421-1000:ama-PC\ama:Interactive:LUA[1]
```

- Realiza una gran cantidad de llamadas de encriptación usando la misma clave, posiblemente indicativo del comportamiento de encriptación de archivos de ransomware. Seguramente el objetivo sea hacer los datos inaccesibles y reclamar una compensación económica a la víctima para la obtención de la clave de descifrado.
- Modifica el comportamiento de los archivos de limpieza haciendo una eliminación masiva de ellos. Primero lo que hace es modificar los datos de sus directorios y después los elimina, almacenándose en la papelera de reciclaje, de ahí que tengan que ser eliminados de nuevo. Probablemente esto lo haga para que los datos no puedan ser recuperados.
- Intenta eliminar o modificar las shadow copies.

```
ImagePathName: C:\Windows\system32\vssadmin.exe  
CommandLine: vssadmin.exe Delete Shadows /All /Quiet
```

- Modifica los ajustes de configuración de arranque deshabilitando el sistema de recuperación.
- Intentos de eliminar la copia de seguridad del estado del sistema:

CommandLine: wbadmin DELETE SYSTEMSTATEBACKUP

- Organización de datos recopilados en una ubicación o directorio central antes de la exfiltración. El motivo de organizar los datos en una ubicación centralizada es para minimizar al máximo posible las conexiones con la botnet.
- Los ciberdelincuentes dejan un mensaje de rescate de datos dirigido a el/los usuario/s. Deja en varias carpetas el archivo: HOW_TO_RECOVER_DATA.html.

```
<html> <style type="text/css"> body { background-color: #5f5f5f; } h1, h3 { text-align: center; text-transform: uppercase; font-weight: normal; } /*...*/ .tabs1 { display: block; margin: auto; } .tabs1 .head { text-align: center; float: top; padding: 0px; text-transform: uppercase; font-weight: normal; display: block; background: #81beff; color: #DF0101; font-size: 30px; } .tabs1 .identi { font-size: 10px; text-align: center; float: top; padding: 15px; display: block; background: #81beff; color: #DFDFDF; } .tabs .content { background: #5f5f5f; text-align: center; color: #000000; padding: 25px 15px; font-size: 15px; font-weight: 400; line-height: 20px; } .tabs .content a { color: #df0130; font-size: 23px; font-style: italic; text-decoration: none; line-height: 35px; } .tabs .content .text { padding: 25px; line-height: 1.2; } </style> <body> <div class="tabs1"> <div class="head"> <b>Your personal ID:</b></div> <div class="identi"> <span style="width:1000px; color: #ffffff; font-size: 10px;">5470810C19E4473412B6D3FF64D827012B8E98DFAF83F3353E88CC11F35DA99D4B3F6626FADEC12470F53D72A7D132160CC5104DC478BBFF4D9235A89F681A7A<br>96874AF810434E7441F9A728E5<br><br> <!-- !!! dont changing this !!! --> </div> </div> <!-- --> <div class="tabs"> <!--tab--> <div class="tab"> <div id="tab-content1" class="content"> <div class="text"> <!--text data --> <b>/\ YOUR COMPANY NETWORK HAS BEEN PENETRATED /\</b><br> <b>All your important files have been encrypted</b><br> <br> <br> Your files are safe! Only modified. (RSA+AES)<br><br> ANY ATTEMPT TO RESTORE YOUR FILES WITH THIRD-PARTY SOFTWARE<br> WILL PERMANENTLY CORRUPT IT.<br> DO NOT MODIFY ENCRYPTED FILES.<br> DO NOT RENAME ENCRYPTED FILES.<br><br> No software available on internet can help you. We are the only ones able to<br> solve your problem.<br><br> We gathered highly confidential/personal data. These data are currently stored on<br> a private server. This server will be immediately destroyed after your payment.<br> If you decide to not pay, we will release your data to public or re-seller.<br> So you can expect your data to be publicly available in the near future.<br><br> We only seek money and our goal is not to damage your reputation or prevent<br> your business from running.<br><br> You will can send us 2-3 non-important files and we will decrypt it for free<br> to prove we are able to give your files back.<br><br> <!--text data --> <hr> <b>Contact us for price and get decryption software.</b><br><br> <a>qd7pcafncosqlqu3ha8fcx4h6sr7zlwagzpcdcnytiw3b6varaevq5yd.onion</a><br> <br> * Note that this server is available via Tor browser only<br><br> Follow the instructions to open the link:<br> 1. Type the address "https://www.torproject.org" in your Internet browser. It opens the Tor site.<br> 2. Press "Download Tor", then press "Download Tor Browser Bundle", install and run it.<br> 3. Now you have Tor browser. In the Tor Browser open <a>qd7pcafncosqlqu3ha8fcx4h6sr7zlwagzpcdcnytiw3b6varaevq5yd.onion</a><br> </a> 4. Start a chat and follow the further instructions. <br> <br> <b>If you can not use the above link, use the email:</b><br> <a href="mailto:ihelp01@decorous.cyou">ihelp01@decorous.cyou</a> <br> <a href="mailto:ihelp01@wholeness.business">ihelp01@wholeness.business</a> <br> <p>* To contact us, create a new free email account on the site: <a href="https://protonmail.com">protonmail.com</a> <br> <b> IF YOU DONT CONTACT US WITHIN 72 HOURS, PRICE WILL BE HIGHER.</b><br> </div> </div> <!--tab--> <!--text data --> </div> </div> <!--tab--> </div> </div> </body> </html>
```

- Edita los ficheros añadiendo el formato de extensión “.marlock07”




```
C:\Users\ama\Downloads\office 2010 standard\x64\Outlook.es-es\OutlookMUI.xml.marlock07
C:\Users\ama\Downloads\office 2010 standard\x64\Outlook.es-es\setup.xml
C:\Users\ama\Downloads\office 2010 standard\x64\Outlook.es-es\setup.xml.marlock07
C:\Users\ama\Downloads\office 2010 standard\x64\PowerPoint.es-es\*
C:\Users\ama\Downloads\office 2010 standard\x64\PowerPoint.es-es\PowerPointMUI.msi
D:\sources\replacementmanifests\srui-repl.man
C:\Users\ama\Downloads\office 2010 standard\x64\PowerPoint.es-es\PowerPointMUI.msi.marlock07
D:\sources\replacementmanifests\stickynotes-replacement.man
C:\Users\ama\Downloads\office 2010 standard\x64\PowerPoint.es-es\PowerPointMUI.xml
D:\sources\replacementmanifests\suacore-wow64-rm.man
C:\Users\ama\Downloads\office 2010 standard\x64\PowerPoint.es-es\PowerPointMUI.xml.marlock07
```

- Creación de mutexes (mecanismo de bloqueo para secuenciar el acceso a un recurso del sistema) serían los siguientes:

```
{8761ABBD-7F85-42EE-B272-A76179687C63}  
Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0000  
Local\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511  
Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0001  
Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0002  
Global\ADAP_WMI_ENTRY  
Global\RefreshRA_Mutex  
Global\RefreshRA_Mutex_Lib  
Global\RefreshRA_Mutex_Flag  
Installing  
Global\LOADPERF_MUTEX
```

Análisis de memoria

Se han detectado las reglas Yara que se mencionaron al principio dentro de los Dumps
Process:

Type	MedusaLocker Payload: 32-bit executable
File Name	ba6e9aa9870aae21ba6a123dad47fb01f7c450ca0989b21e16c4071a8c04de5c
File Type	PE32 executable (GUI) Intel 80386, for MS Windows
File Size	719872 bytes
Process	1bc0575b3fc6486cb2510dac.exe
PID	1588
Path	C:\Users\lama\AppData\Local\Temp\1bc0575b3fc6486cb2510dac.exe
MD5	9bd8806d540b085ea2706cb0507932bc
SHA1	63b7e5e6ed9d147ef04eba4b4c4139579a0eda1b
SHA256	ba6e9aa9870aae21ba6a123dad47fb01f7c450ca0989b21e16c4071a8c04de5c [VT] [MWDB] [Bazaar]
SHA3-384	c30647f8d33e02b82e138806500c85c1dc9dc9295bc308ecbdb30fbc170a0db180728cdd04f3ef5302ba66d6f8c3080a
CRC32	D5673469
TLSH	T129E49D103482C532E9B301738E7ED56EA16DFDB10B3854D7A3CC652E5FB99E23A32256
Ssdeep	b'12288:KXjK0wk7lxWRMon2i3KmQLeOZ6iwgDQ8biVVLGhh30puZkudE:oll7UWRMonRKHLLeQJwgaVVyH7E'
Yara	<ul style="list-style-type: none"> • vmdetect - Possibly employs anti-virtualization techniques - Author: nex • INDICATOR_SUSPICIOUS_GENRansomware - detects command variations typically used by ransomware - Author: ditekShen • INDICATOR_SUSPICIOUS_EXE_UACBypass_CMSTPCOM - Detects Windows executables bypassing UAC using CMSTP COM interfaces. MITRE (T1218.003) - Author: ditekShen
CAPE Yara	<ul style="list-style-type: none"> • UPX - Author: Kevin Breen <kevin@technarchy.net> • MedusaLocker - MedusaLocker Payload - Author: ditekshen
PE	  File  Strings

Análisis de red

- TCP

Source	Source Port	Destination	Destination Port
192.168.122.6	49226	192.168.122.1	445
192.168.122.6	49233	192.168.122.1	445

El puerto de destino es el 445 perteneciente a SMB el cual permite a una aplicación o al usuario de una aplicación compartir archivos, discos, directorios, impresoras, puertos seriales y mail slots, a través de una red que usa el sistema operativo

Microsoft Windows. Por lo tanto, este puerto podría ser utilizado para adquirir información del sistema origen.

- UDP

Source	Source Port	Destination	Destination Port
192.168.122.6	61215	239.255.255.250	3702
192.168.122.6	55167	239.255.255.250	3702
192.168.122.6	63187	239.255.255.250	1900

- ICMP (Protocolo de mensajes de control de Internet): es un protocolo que no está tan supervisado como el TCP/UDP y sirve a los ciberdelincuentes para ocultar comunicaciones. Este protocolo está enmarcado como protocolo de capa de no aplicación OSI.










Source	Destination	ICMP Type
192.168.122.6	192.168.122.1	8
192.168.122.6	192.168.122.1	8

Herramientas Online:

Virustotal:

- <https://www.virustotal.com/gui/file/1bc0575b3fc6486cb2510dac1ac6ae4889b94a955d3eade53d3ba3a92d133281/>
- Detecciones: 62
- Conexiones: a través del puerto 80 y 443 para hacer conexiones a páginas webs. A continuación se especifica el nombre corporativo de a quién pertenece cada ip.

IP Traffic

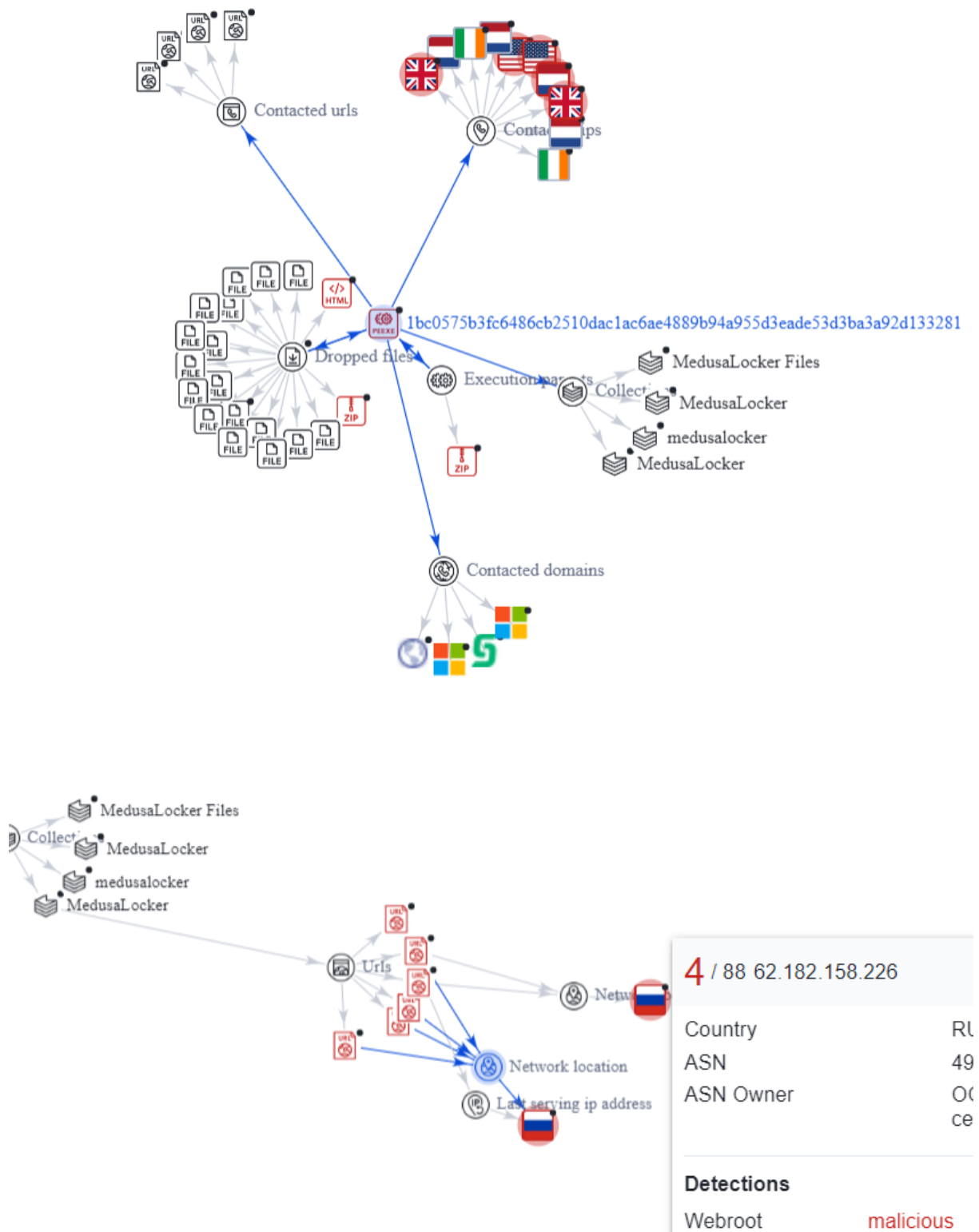
 192.229.221.95:80 (TCP)
 20.190.159.71:443 (TCP)
 20.31.108.18:443 (TCP)
 209.197.3.8:80 (TCP)
 23.202.229.57:443 (TCP)
 40.126.32.74:443 (TCP)
 40.127.240.158:443 (TCP)
 87.248.202.1:80 (TCP)
 93.184.221.240:80 (TCP)

- 192.229.221.95:80 → Edgecast Inc (red de entrega de contenido)
- 20.190.159.71:443 → Microsoft
- 20.31.108.18:443 → Microsoft
- 209.197.3.8:80 → Highwinds Network Group (nube)
- 23.202.229.57:443 → Akamai Technologies, Inc. (nube)
- 40.126.32.74:443 → Microsoft
- 40.127.240.158:443 → Microsoft
- 87.248.202.1:80 → Ripe Ncc Whois (Base de datos)
- 93.184.221.240:80 → <http://www.ripe.net/whois> (Probablemente esté usando esta base de datos para obtener información acerca de la Ip de la víctima).

- Detecta las conexiones maliciosas que podrían ser la botnet de las siguientes ips (algunas mencionadas en el punto anterior):

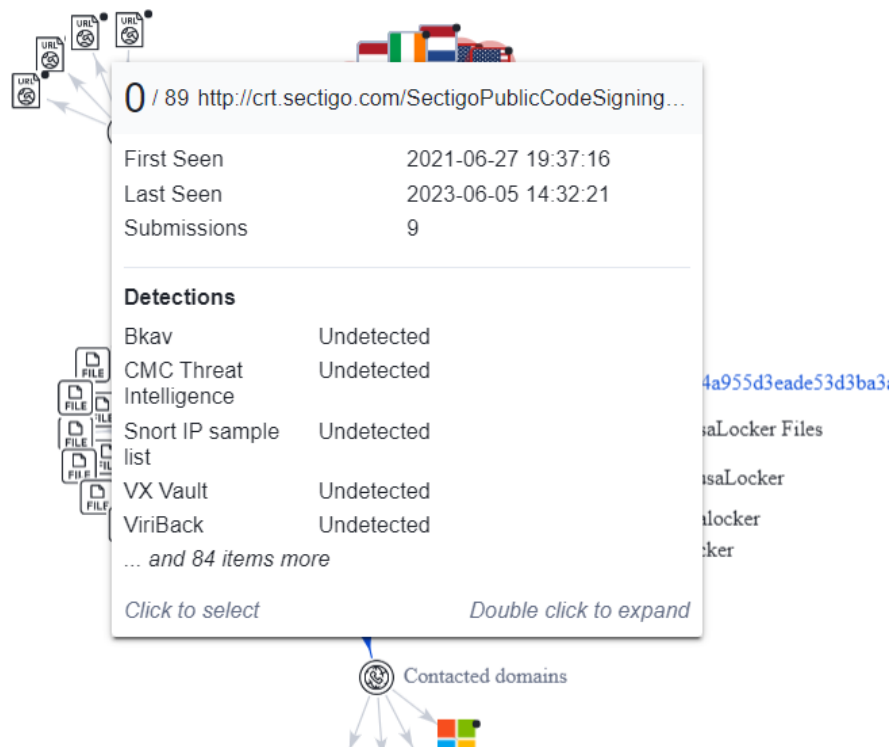
93.184.221.240 (ripe, base de datos)
192.229.221.95 (red de entrega contenido)
209.197.3.8 (nube)
87.248.202.1 (base de datos)
91.199.212.52 (Sectigo)

- Se contienen datos que parece que están en la botnet de otros MedusaLocker y ofrecen datos de urls e ips maliciosas





- Genera la clave pública desde la url crt.sectigo.com













- Conexión con una bases de datos propia:

System Property Lookups

IWbemServices::Connect

- Claves de registro:

- +  HKEY_CURRENT_USER\SOFTWARE\MDSLK
- +  HKEY_CURRENT_USER\SOFTWARE\MDSLK\Self
- +  HKEY_CURRENT_USER\Software\MDSLK\Self
- +  HKEY_CURRENT_USER\Software\Microsoft\RestartManager
- +  HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000
- +  HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Owner
- +  HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegFiles0000
- +  HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegFilesHash
- +  HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Sequence
- +  HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\SessionHash

MITIGACIONES:

- No abrir correos electrónicos de procedencia sospechosa. Si parece ser un correo electrónico de alguna procedencia conocida sugiriendo una descarga primero consultarlo con la organización a la que pertenezca para verificar la procedencia.
- Descargar programas y/o ficheros de lugares seguros, para ello hay que asegurarse de la veracidad de dicha página.
- Mantener el software y los sistemas operativos actualizados, ya que estas actualizaciones a menudo incluyen parches de seguridad que ayudan a protegerse.
- Realizar regularmente copias de seguridad de los archivos importantes, almacenándose en un lugar seguro y fuera de la red.
- Utilizar firewalls y herramientas de filtrado que ayuden a prevenir el acceso no autorizado a los sistemas y a bloquear el acceso a sitios web maliciosos o descargas de archivos peligrosos.
- Deshabilitar los puertos de acceso remoto (RDP) no utilizados y controlar los registros de acceso remoto para detectar cualquier actividad inusual.
- Nunca seguir la instrucción de deshabilitar las funciones de seguridad, si un correo electrónico o documento lo solicita.
- Establecer políticas de seguridad en el sistema para impedir la ejecución de ficheros desde directorios comúnmente utilizados por Ransomware (App Data, Local App Data, etc.)

CONCLUSIONES:

- El malware analizado es un ransomware llamado MedusaLocker perteneciente a la familia "STOP (Djvu)".
- Crea persistencia a través de un método que es taskend.exe para que sea ejecutado siempre que se inicie el equipo.
- Exporta librerías dinámicas y las ejecuta en memoria.
- Utiliza métodos anti-debugging.
- Hace conexiones a través de los protocolos tcp/udp e icmp, este último sirviéndole para ocultarse.
- Elimina la copia de seguridad del sistema y deshabilita el sistema de recuperación.
- Encripta ficheros del pc con una misma clave y hace eliminaciones masivas desde la papelera de reciclaje.
- Añade la extensión .marlock07 a los ficheros encriptados.
- Añade nota de rescate a las carpetas del pc.