

ERIC SERRANO MARÍN



PRÁCTICA 4.2 – PLATAFORMA LET'S DEFEND
INCIDENTES DE CIBERSEGURIDAD

ERIC SERRANO MARÍN
CETI

Contenido

Lets defend - Windows Forensics	3
Initial Access was made through a Malicious Document delivered through email. What was the full path where the document was downloaded?	3
Herramientas: FTK Imager y Shellbags.	3
Respuesta 1	6
What's the document name? (The document which was delivered via phishing)	7
Herramienta: RBCmd.....	7
Respuesta 2	7
What's the stager name which connected to the attacker C2 server(Fullpath\name) .	8
Herramientas: Amcache Parser y PECmd.	8
Respuesta 3	10
The attacker manipulated MACB Timestamps of the stager executable to confuse Analysts. Analyze the timestamps of the stager and verify the original timestamp and tampered one. (ORIGINAL TIMESTAMP : TAMPERED TIMESTAMP)	10
Herramienta: MFT Explorer.....	10
Respuesta 4	11
The attacker set up persistence by manipulating registry keys. All we know is that GlobalFlags image file technique was used to set up persistence. When exiting a certain process, the attacker persistence executable is executed. What's the name of that process?.....	13
Herramienta: RegistryExplorer.....	13
Respuesta 5	14
Whats the full path alongside name of the executable which is setup for persistence?(FULLPATH\Filename).....	15
Respuesta 6	15
The attacker logged in via RDP and then performed lateral Movement. Attacker accessed an Internal network-connected Device via RDP. What command was run on cmd after successful RDP into Other Windows machine?	15
Herramienta: BMC-tools	15
Respuesta 7	17
The attacker tried to download a tool from the user's browser in that second machine. What's the tool name? (name.ext).....	17
Respuesta 8	18
What command was executed which resulted in privilege escalation?	19
Herramienta: DeepBlueCLI	19
Respuesta 9	20
What framework was used by the attacker?	20

Respuesta 10	20
Ransomware Attack.....	21
Please you find the dropped dll, include the whole path including the dll file	22
Respuesta 1	22
What is the MD5 hash for the dll?.....	23
Respuesta 2	23
What is the name of ransomware note that got dropped?.....	23
Respuesta 3	23
What is the URL that the initial payload was downloaded from? (Include the whole URL with the payload)	24
Respuesta 4	24
The ransomware drops the copy of the legitimate application into the Temp folder. Please provide the filename including the extension	25
Respuesta 5	25
What is the name of the ransomware?	26
Respuesta 6	26
Finalización.....	26
Incluye un apartado en el documento en el que indiques la forma correcta de obtener las evidencias con las que has trabajado en las investigaciones.	27
Registra en una de las herramientas de seguimiento de incidentes que vimos en la unidad anterior (Catalyst o FIR) los incidentes que has investigado. Entrega capturas de cada uno de los incidentes registrados en el que se aprecien todos los datos que has registrado.	27
Windows Forensics.....	27
Ransomware Attack.....	29

Lets defend - Windows Forensics

La gran mayoría de las herramientas empleadas se pueden encontrar en el siguiente enlace: <https://ericzimmerman.github.io/#!index.md>

Vamos a dar por hecho que nuestra organización ha sido blanco de una campaña de phishing dirigida. Se ha detectado que el correo de phishing fue abierto por 3 sistemas en nuestra red. Para abordar esta situación, se ha recopilado una imagen de triaje rápido de uno de los sistemas infectados, y se ha proporcionado para su análisis con el objetivo de identificar las Técnicas, Tácticas y Procedimientos utilizadas por los atacantes.

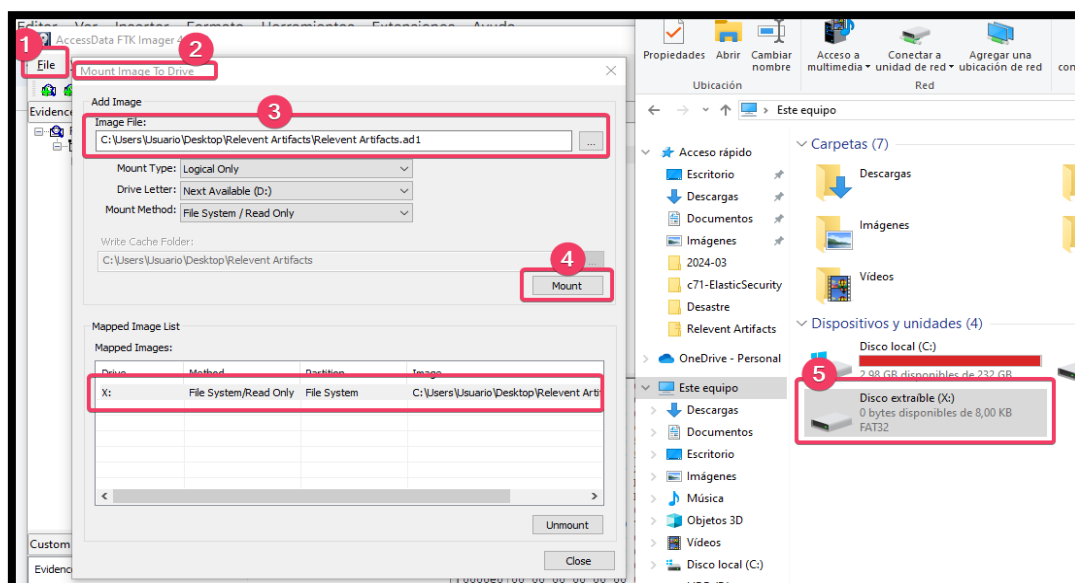
Nuestro objetivo es identificar las técnicas y tácticas empleadas por el atacante, de manera que nuestro equipo de respuesta a incidentes pueda responder efectivamente y mitigar cualquier compromiso adicional en toda la red.

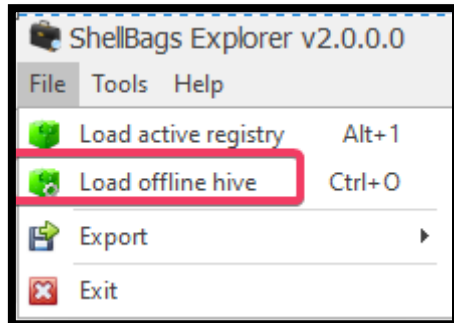
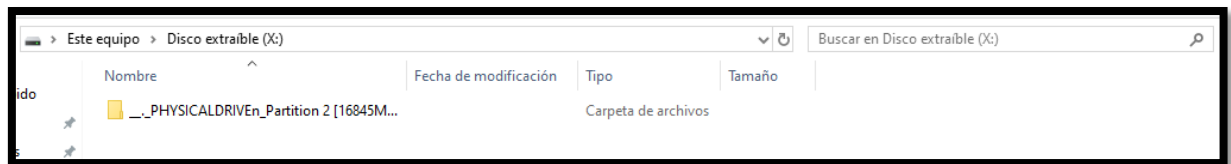
Para ver el contenido del archivo descargable del escenario vamos a usar FTK Imager.

Initial Access was made through a Malicious Document delivered through email. What was the full path where the document was downloaded?

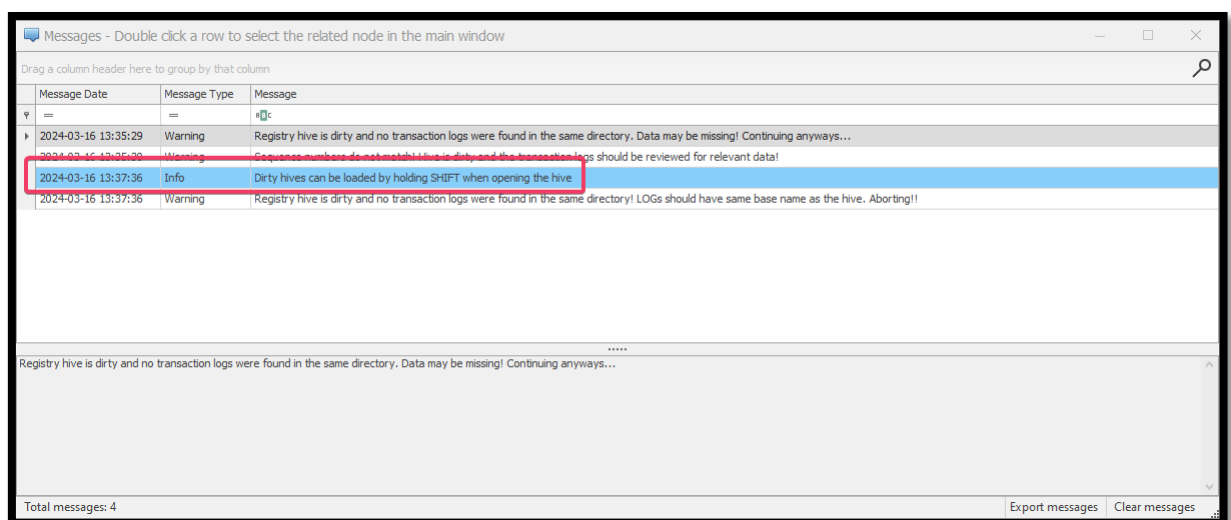
Herramientas: [FTK Imager](#) y [Shellbags](#).

Lo primero que tenemos que hacer es montarlo.

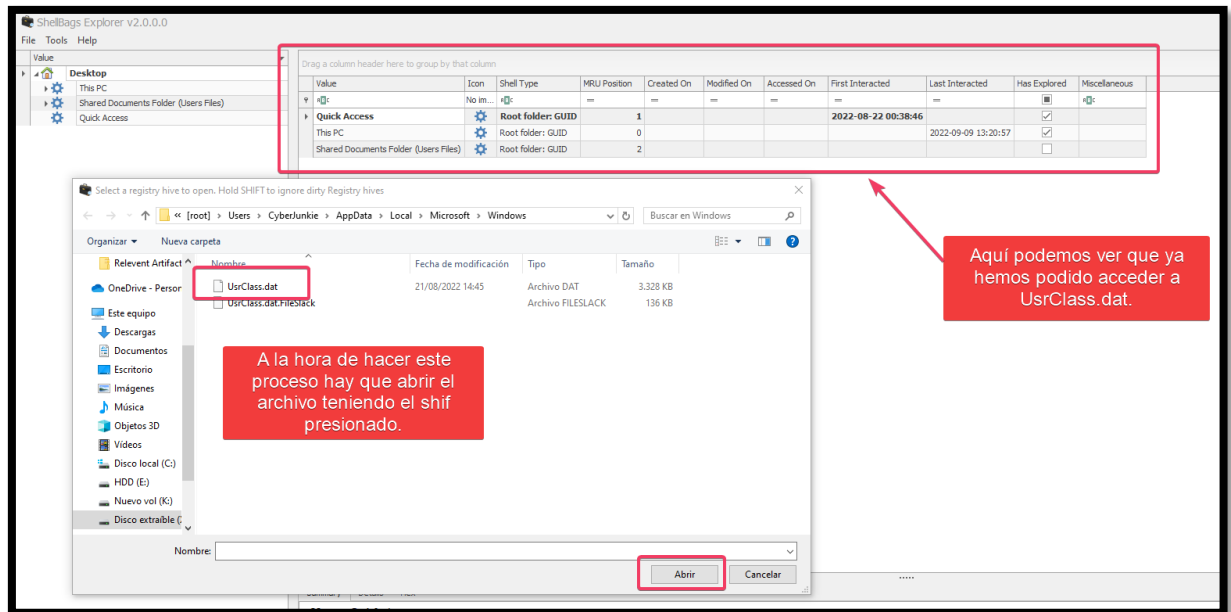




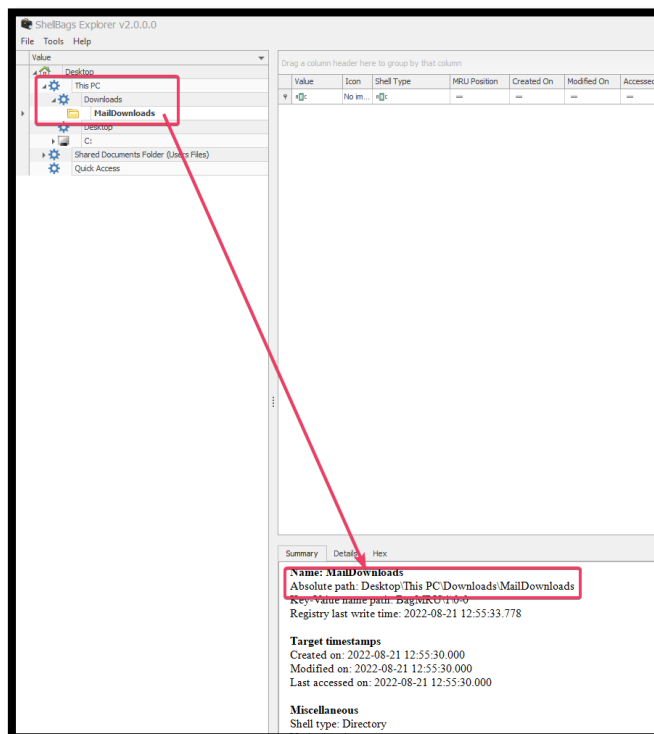
Si observamos lo que nos sale a la hora de intentar abrir el archivo con ShellBags, es que está 'Dirty', por lo que nos dice que lo abramos manteniendo el shift.



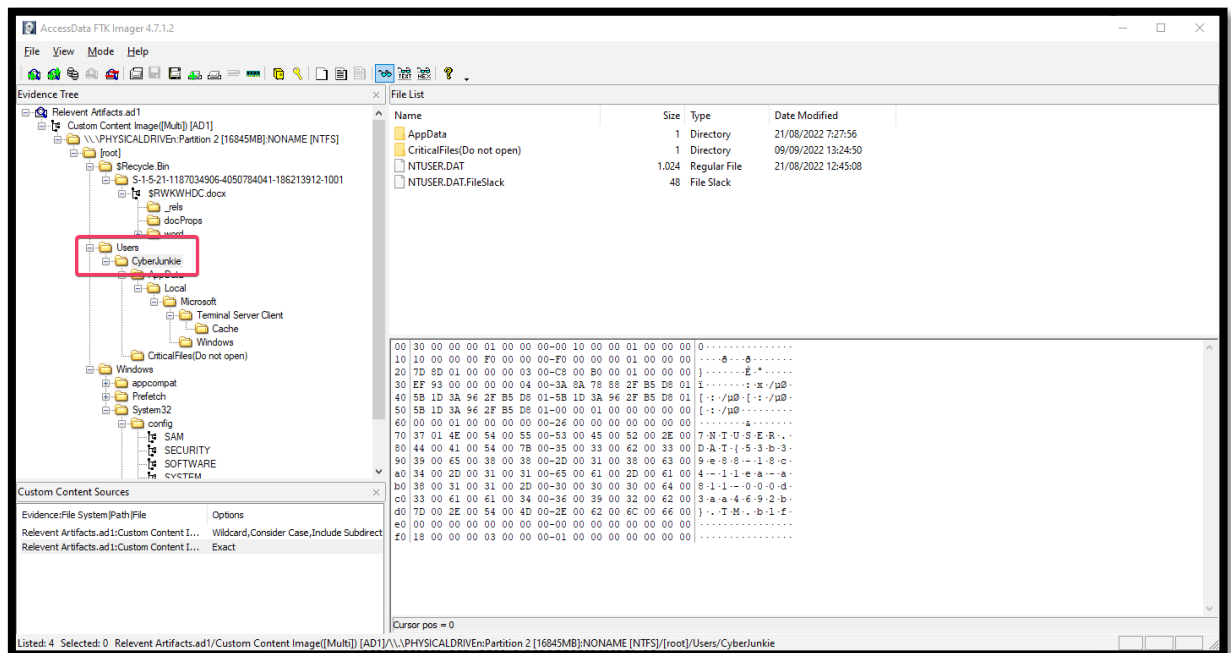
Abrimos el archivo `UsrClass.dat`, (root/Users/CyberJunkie/AppData/Local/Microsoft/Windows), queremos este archivo porque es el que almacena información relacionada con las preferencias y configuraciones de usuario específicas.



Como nos dice el ejercicio que el phishing se realizó descargando un archivo por mail, vamos a dar por hecho que es la ruta que nos pone abajo.

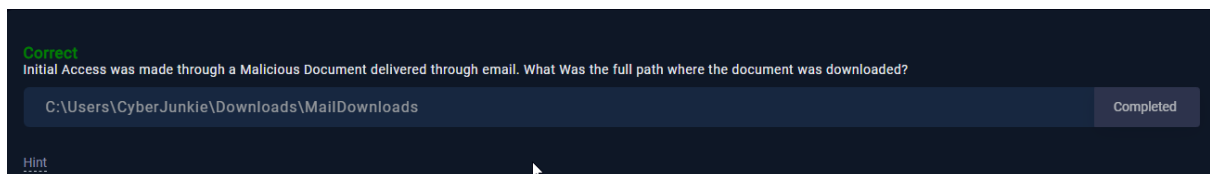


Aunque esta ruta habrá que cambiarla para que sea más precisa: C:\Users\CyberJunkie\Downloads\MailDownloads, sabemos que es ese usuario entre otras cosas por esto:



Respuesta 1

C:\Users\CyberJunkie\Downloads\MailDownloads



What's the document name? (The document which was delivered via phishing)

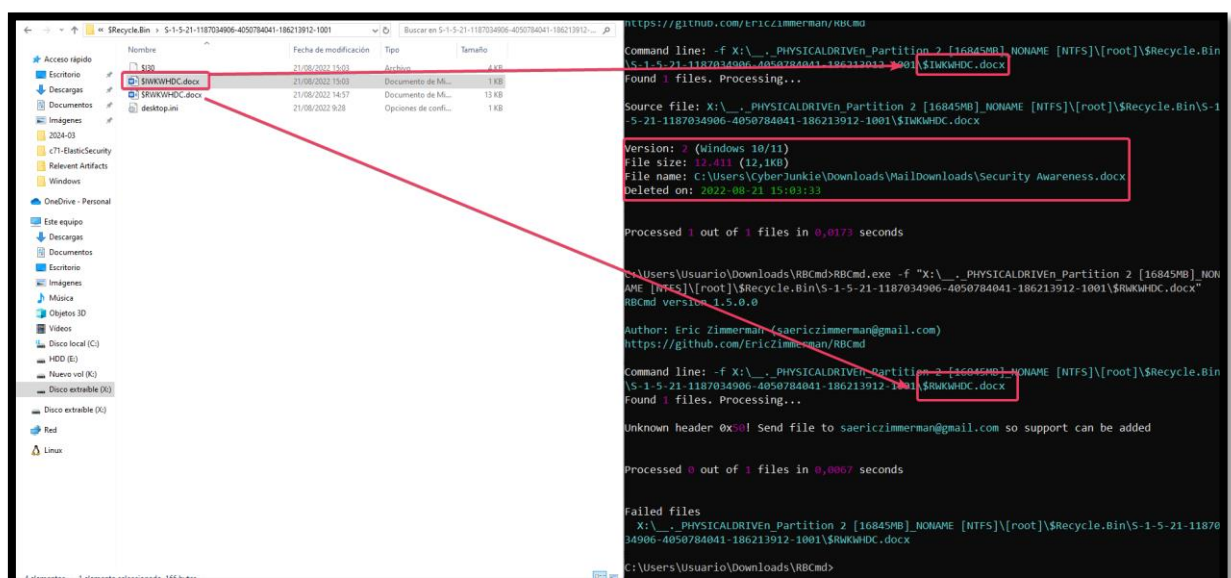
Herramienta: [RBCmd](#).

La carpeta MailDownloads no nos aparece en lo que tenemos montado, pero sí que nos aparece una papelera de reciclaje.

Nombre	Fecha de modificación	Tipo	Tamaño
\$I30	21/08/2022 15:03	Archivo	4 KB
\$IWKWHDC.docx	21/08/2022 15:03	Documento de Mi...	1 KB
\$RWKWHDC.docx	21/08/2022 14:57	Documento de Mi...	13 KB
desktop.ini	21/08/2022 9:28	Opciones de confi...	1 KB

RBCmd es una herramienta que examina, interpreta y extrae información de un recurso específico, en este caso, los artefactos de la Papelera de Reciclaje.

RBCmd	1.5.0.0 1.5.0.0	Recycle Bin artifact (INFO2/\$I) parser
-------	---	---



Se borró un archivo llamado Security Awareness.docx en fecha 2022-08-21.

Respuesta 2

Security Awareness.docx

What's the stager name which connected to the attacker C2 server(Fullpath\name)

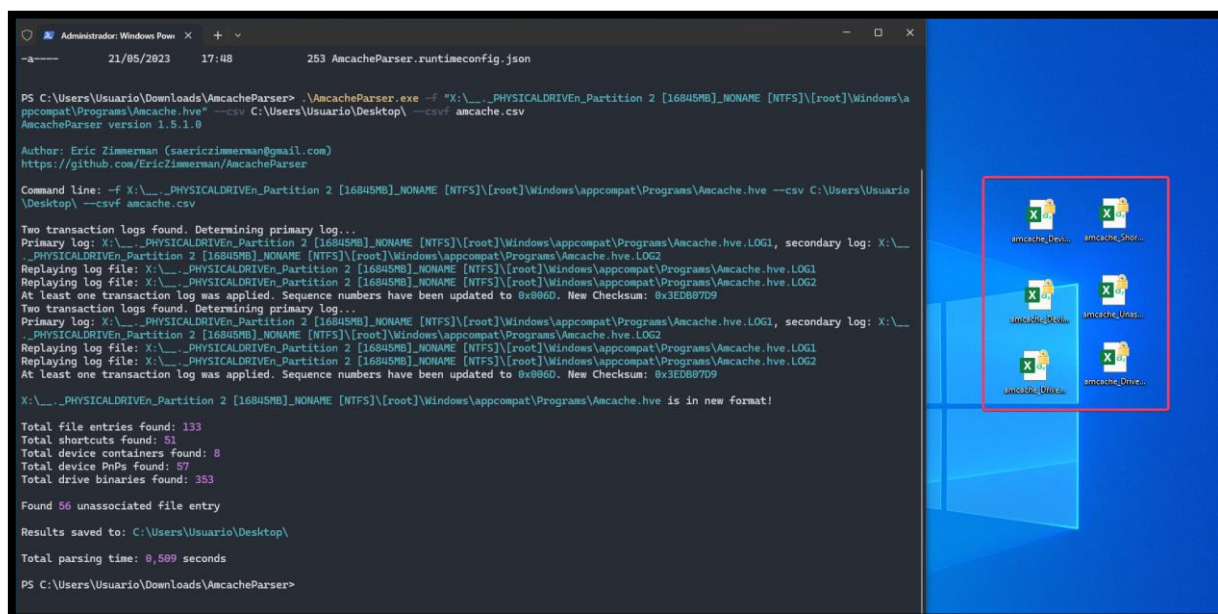
Herramientas: [Amcache Parser](#) y [PECmd](#).

El registro de Amcache es una base de datos utilizada por Windows para almacenar información sobre aplicaciones y archivos ejecutables en el sistema. Al analizar este registro, puedes obtener información sobre los programas instalados, archivos ejecutables, accesos directos y dispositivos asociados en el sistema.

Comando: .\AmcacheParser.exe -f "X:___.PHYSICALDRIVE_n_Partition 2 [16845MB] NONAME

```
[NTFS][root]\Windows\appcompat\Programs\Amcache.hve" --csv
C:\Users\Usuario\Desktop\ --csvf amcache.csv
```

Este comando ejecuta Amcache Parser con la opción -f para especificar el registro de Amcache a analizar, también usé -csv para especificar dónde guardar los archivos en formato CSV y csvf para especificar el nombre del archivo CSV. La salida nos muestra que ha encontrado archivos no asociados y ha guardado los resultados en Desktop.



En este paso no hemos encontrado nada, así que vamos a probar con PECmd.

<https://i.imgur.com/NUmj2LS.gif>

En el archivo txt podemos encontrar lo siguiente:

```

Last accessed on: 2024-03-17 22:33:13

Executable name: SECURITYPATCH.EXE
Hash: 3B79B19E
File size (bytes): 24.412
Version: Windows 10 or Windows 11

Run count: 1
Last run: 2022-08-21 13:03:02

Volume information:

#0: Name: \VOLUME{01d8a61b008e7f85-8800da49} Serial: 8800DA49 Created: 2022-08-02 02:53:11 Directories: 15 File references: 65

Directories referenced: 15

00: \VOLUME{01d8a61b008e7f85-8800da49}\$EXTEND
01: \VOLUME{01d8a61b008e7f85-8800da49}\USERS
02: \VOLUME{01d8a61b008e7f85-8800da49}\USERS\CYBERJUNKIE
03: \VOLUME{01d8a61b008e7f85-8800da49}\USERS\CYBERJUNKIE\APPDATA
04: \VOLUME{01d8a61b008e7f85-8800da49}\USERS\CYBERJUNKIE\APPDATA\ROAMING
05: \VOLUME{01d8a61b008e7f85-8800da49}\USERS\CYBERJUNKIE\APPDATA\ROAMING\MICROSOFT
06: \VOLUME{01d8a61b008e7f85-8800da49}\USERS\CYBERJUNKIE\APPDATA\ROAMING\MICROSOFT\CRYPTO
07: \VOLUME{01d8a61b008e7f85-8800da49}\USERS\CYBERJUNKIE\APPDATA\ROAMING\MICROSOFT\CRYPTO\RSA
08: \VOLUME{01d8a61b008e7f85-8800da49}\USERS\CYBERJUNKIE\APPDATA\ROAMING\MICROSOFT\CRYPTO\RSA\S-1-5-21-1187034906-4050784041-186213912-1001
09: \VOLUME{01d8a61b008e7f85-8800da49}\USERS\CYBERJUNKIE\DESKTOP
10: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS
11: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\APPPATCH
12: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\GLOBALIZATION
13: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\GLOBALIZATION\SORTING
14: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\SYSTEM32

Files referenced: 50

00: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\SYSTEM32\NTDLL.DLL
01: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\SYSTEM32\KERNEL32.DLL
02: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\SYSTEM32\KERNELBASE.DLL
03: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\SYSTEM32\LOCALE.NLS
04: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\SYSTEM32\APPHelp.DLL
05: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\SYSTEM32\APPATCH\CVCMATH.CPP
06: \VOLUME{01d8a61b008e7f85-8800da49}\USERS\CYBERJUNKIE\DESKTOP\SECURITYPATCH.EXE (Executable: True)
07: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\SYSTEM32\WS2_32.DLL
08: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\SYSTEM32\RPCRT4.DLL

```

```

Last accessed on: 2024-03-17 22:33:13

Executable name: SECURITYPATCH.EXE
Hash: 3B79B19E
File size (bytes): 24.412
Version: Windows 10 or Windows 11

Run count: 1
Last run: 2022-08-21 13:03:02

Volume information:

#0: Name: \VOLUME{01d8a61b008e7f85-8800da49} Serial: 8800DA49 Created: 2022-08-02 02:53:11 Directories: 15 File references: 65

Directories referenced: 15

00: \VOLUME{01d8a61b008e7f85-8800da49}\$EXTEND
01: \VOLUME{01d8a61b008e7f85-8800da49}\USERS
02: \VOLUME{01d8a61b008e7f85-8800da49}\USERS\CYBERJUNKIE
03: \VOLUME{01d8a61b008e7f85-8800da49}\USERS\CYBERJUNKIE\APPDATA
04: \VOLUME{01d8a61b008e7f85-8800da49}\USERS\CYBERJUNKIE\APPDATA\ROAMING
05: \VOLUME{01d8a61b008e7f85-8800da49}\USERS\CYBERJUNKIE\APPDATA\ROAMING\MICROSOFT
06: \VOLUME{01d8a61b008e7f85-8800da49}\USERS\CYBERJUNKIE\APPDATA\ROAMING\MICROSOFT\CRYPTO
07: \VOLUME{01d8a61b008e7f85-8800da49}\USERS\CYBERJUNKIE\APPDATA\ROAMING\MICROSOFT\CRYPTO\RSA
08: \VOLUME{01d8a61b008e7f85-8800da49}\USERS\CYBERJUNKIE\APPDATA\ROAMING\MICROSOFT\CRYPTO\RSA\S-1-5-21-1187034906-4050784041-186213912-1001
09: \VOLUME{01d8a61b008e7f85-8800da49}\USERS\CYBERJUNKIE\DESKTOP
10: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS
11: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\APPPATCH
12: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\GLOBALIZATION
13: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\GLOBALIZATION\SORTING
14: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\SYSTEM32

Files referenced: 50

00: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\SYSTEM32\NTDLL.DLL
01: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\SYSTEM32\KERNEL32.DLL
02: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\SYSTEM32\KERNELBASE.DLL
03: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\SYSTEM32\LOCALE.NLS
04: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\SYSTEM32\APPHelp.DLL
05: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\SYSTEM32\APPATCH\CVCMATH.CPP
06: \VOLUME{01d8a61b008e7f85-8800da49}\USERS\CYBERJUNKIE\DESKTOP\SECURITYPATCH.EXE (Executable: True)
07: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\SYSTEM32\WS2_32.DLL
08: \VOLUME{01d8a61b008e7f85-8800da49}\WINDOWS\SYSTEM32\RPCRT4.DLL

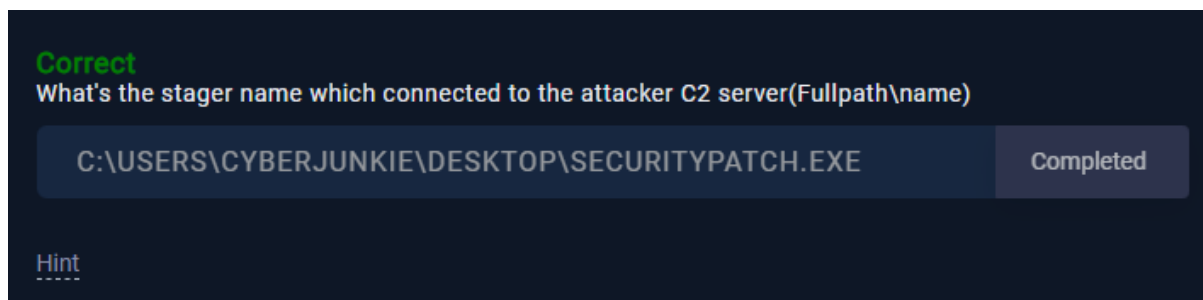
```

Esto confirma la ejecución de Security Patch que ha hecho el usuario Cyberjunkie.

Basada en la evidencia este archivo podría ser el stager utilizado para conectarse al servidor C2 del atacante.

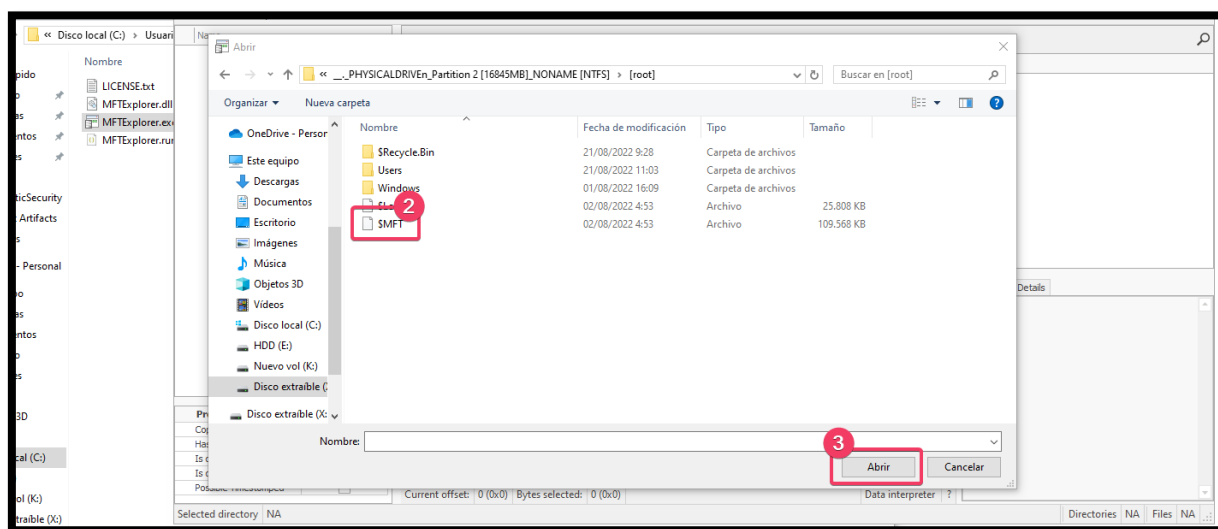
Respuesta 3

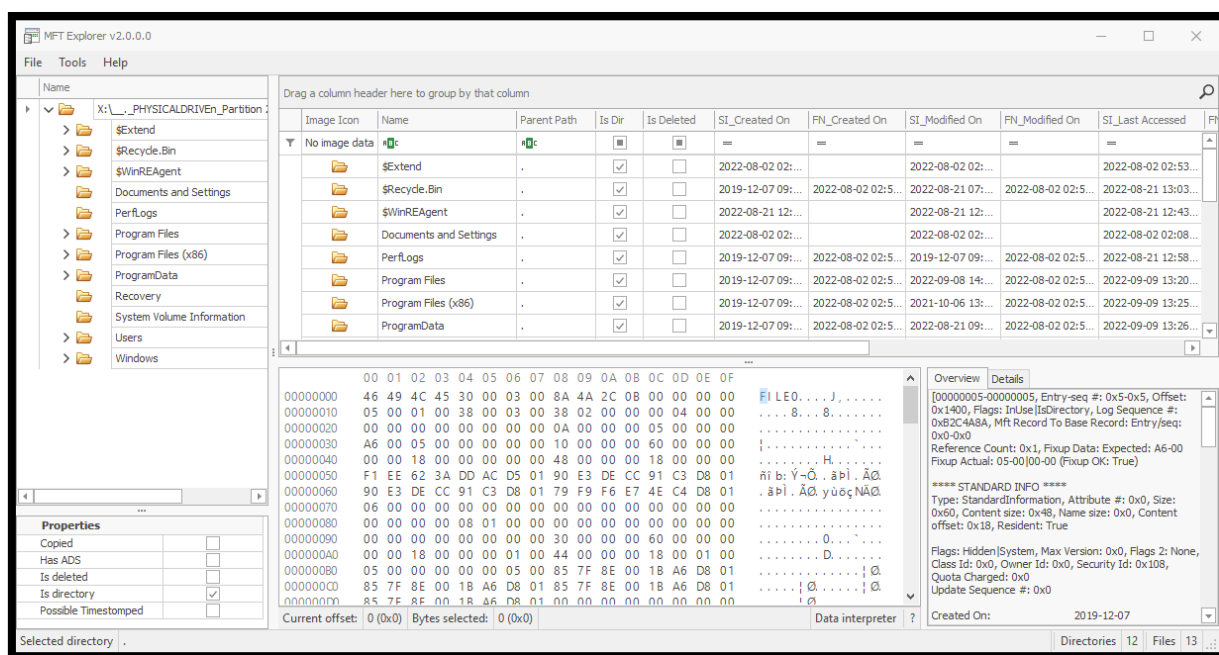
C:\USERS\CYBERJUNKIE\DESKTOP\SECURITYPATCH.EXE



The attacker manipulated MACB Timestamps of the stager executable to confuse Analysts. Analyze the timestamps of the stager and verify the original timestamp and tampered one. (ORIGINAL TIMESTAMP : TAMPERED TIMESTAMP)

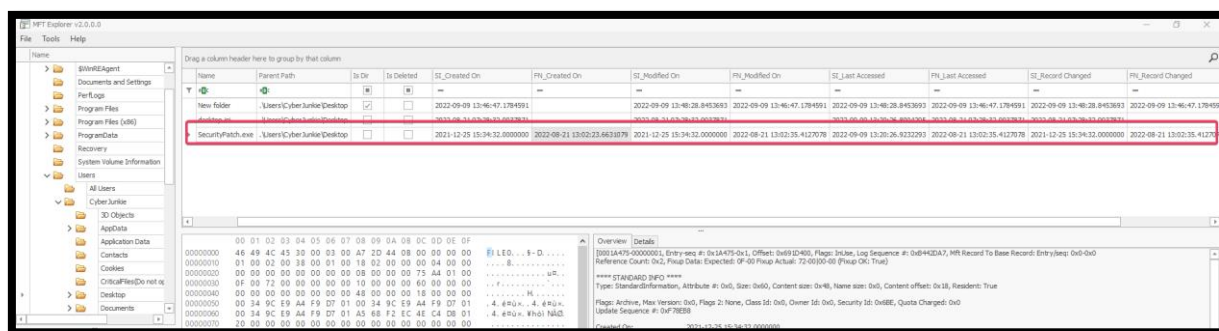
Herramienta: [MFT Explorer](#)





En los datos podemos observar que han hecho que el archivo parezca que lleva 8 meses más de lo que debería en el sistema, ya que hay dos momentos de creación, el 25 de diciembre de 2021 a las 15:34:32 y el 21 de agosto de 2022 a las 13:02:23.

La marca de tiempo original es el del 21 de agosto de 2022, pero el atacante modificó la marca de tiempo a 25 de diciembre de 2021. También nos damos cuenta que el formato de respuesta incluye milisegundos y aquí no aparecen.



Respuesta 4

2022-08-21 13:02:23:2021-12-25 15:34:32

Sale que está mal, pero después de un rato intentando formas distintas de ponerlo me ha dado por buscar información y por lo que se ve es un problema de la web.

You have already sent this answer.

The attacker manipulated MACB Timestamps of the stager executable to confuse Analysts. Analyze the timestamps of the stager and verify the original timestamp and tampered one. (ORIGINAL TIMESTAMP : TAMPERED TIMESTAMP)

2022-08-21 13:02:23:2021-12-25 15:34:32

Hint
.....

Páginas como <https://medium.com/@clumpstar/windows-forensics-dfir-029098add076> dicen que es un problema con la página web.

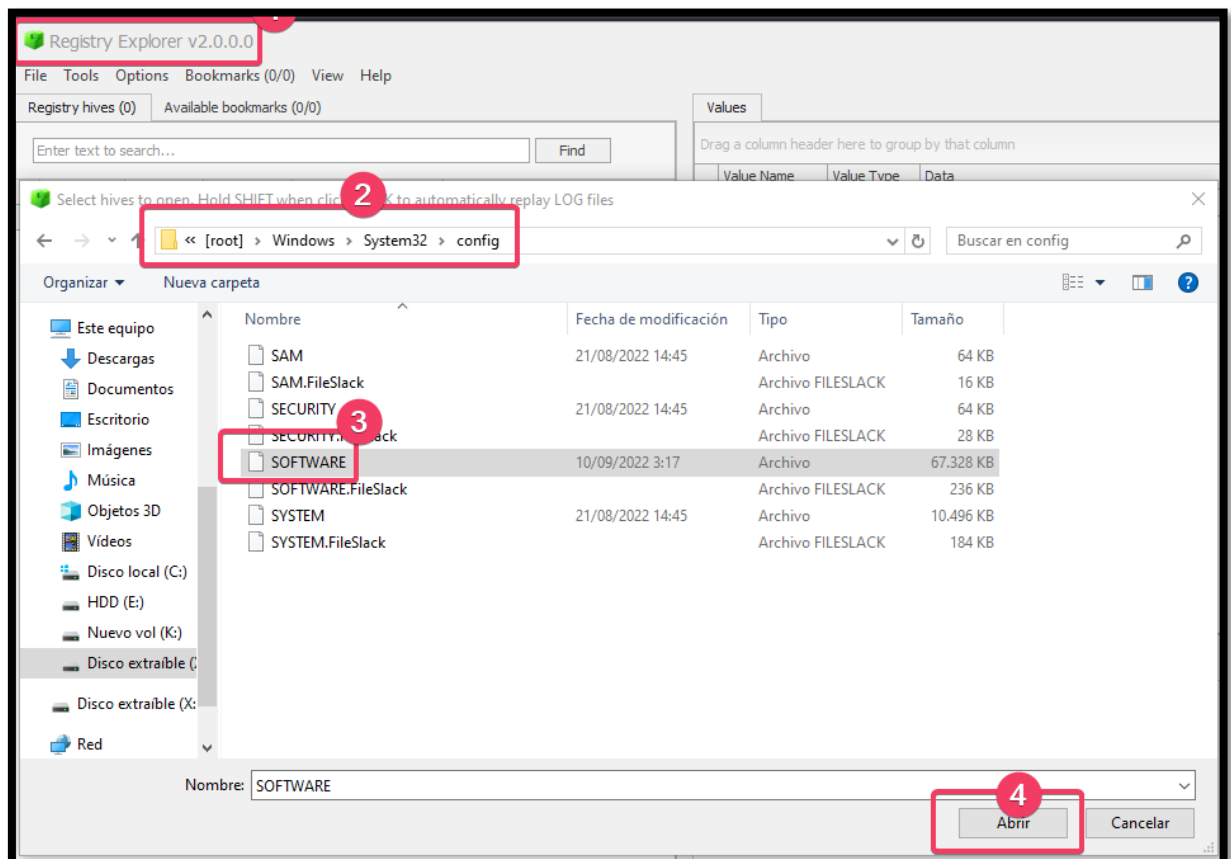
Therefore the Solution is 2022-08-21 13:02:23:2021-12-25 15:34:32

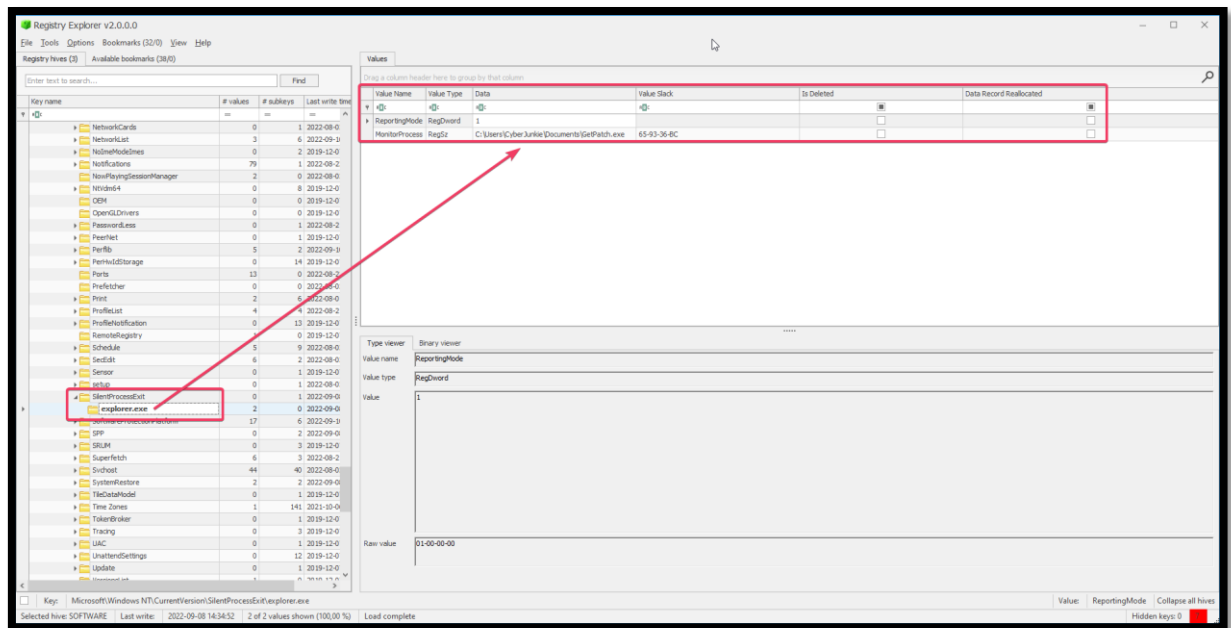
NOTE : since there is some problem from letsdefend.io's side the solution is not getting submitted.

The attacker set up persistence by manipulating registry keys. All we know is that GlobalFlags image file technique was used to set up persistence. When exiting a certain process, the attacker persistence executable is executed. What's the name of that process?

Herramienta: [RegistryExplorer.](#)

Decidí mirar directamente en el archivo "SOFTWARE" del registro porque sabía que allí se almacenan configuraciones cruciales del sistema.

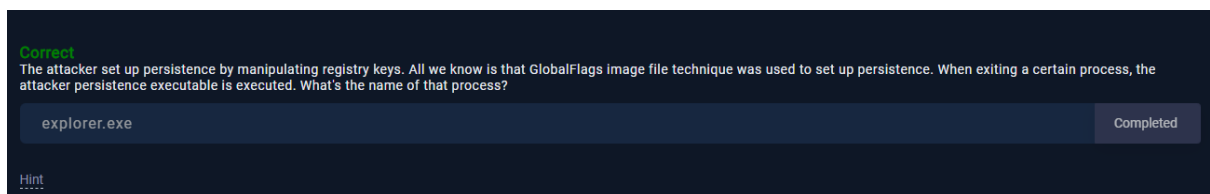




El atacante ha establecido persistencia al añadir una entrada de depurador en el registro para el proceso explorer.exe. Cuando explorer.exe se cierra, se ejecuta el archivo GetPatch.exe, que es el ejecutable de persistencia del atacante. Este descubrimiento se realizó utilizando Registry Explorer para inspeccionar la rama del registro SOFTWARE, específicamente la clave Image File Execution Options.

Respuesta 5

explorer.exe



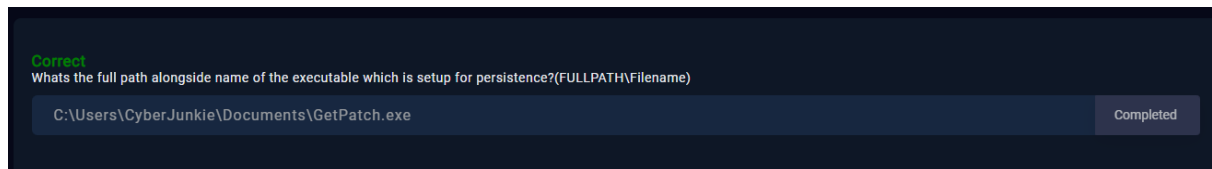
Whats the full path alongside name of the executable which is setup for persistence?(FULLPATH\Filename)

La respuesta la teníamos en la captura de la pregunta 5.

Values					
Drag a column header here to group by that column					
	Value Name	Value Type	Data	Value Slack	Is D
▼	RegC	RegDword	RegC	RegC	
▶	ReportingMode	RegDword			
▶	MonitorProcess	RegSz	C:\Users\CyberJunkie\Documents\GetPatch.exe	65-93-36-BC	

Respuesta 6

C:\Users\CyberJunkie\Documents\GetPatch.exe



The attacker logged in via RDP and then performed lateral Movement. Attacker accessed an Internal network-connected Device via RDP. What command was run on cmd after successful RDP into Other Windows machine?

Herramienta: **BMC-tools**

Tenemos que encontrar el archivo de caché de RDP.

```
X:\_\_PHYSICALDRIVE\Partition          2          [16845MB]_NONAME
[NTFS][root]\Users\CyberJunkie\AppData\Local\Microsoft\Terminal      Server
Client
```

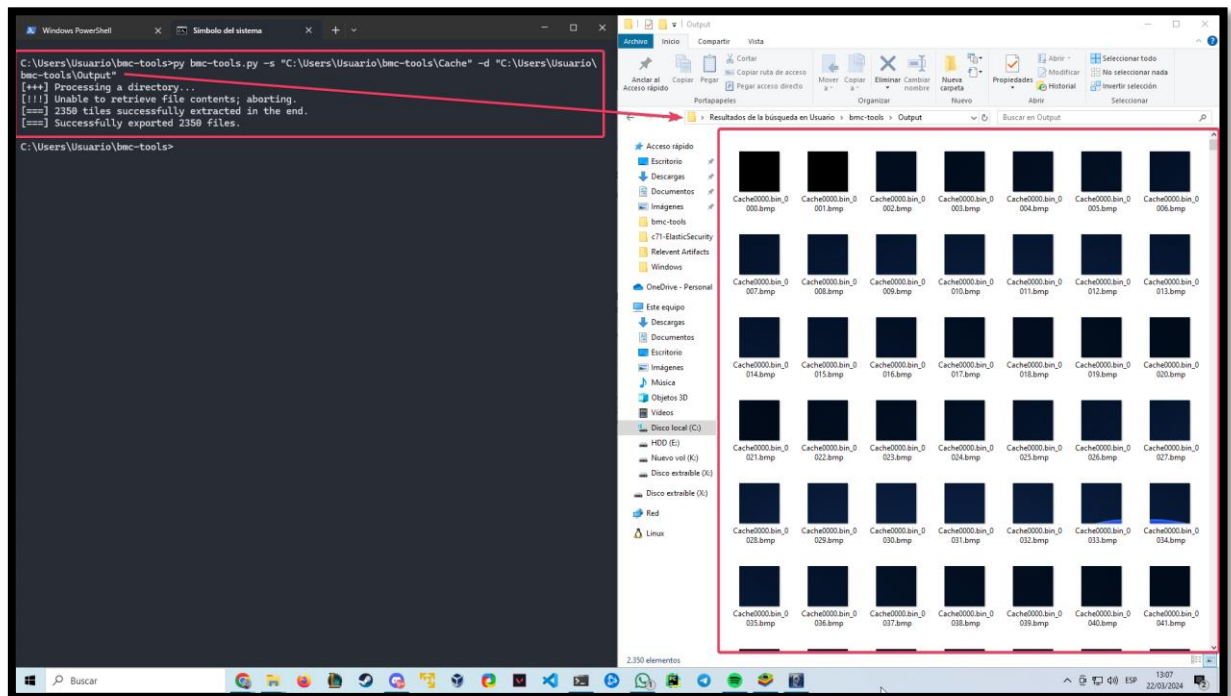
<< Users > CyberJunkie > AppData > Local > Microsoft > Terminal Server Client > Cache				
Buscar en Cache				
	Nombre	Fecha de modificación	Tipo	Tamaño
	bcache24.bmc	08/09/2022 16:37	Archivo BMC	0 KB
	Cache0000.bin	08/09/2022 16:40	Archivo BIN	37.628 KB

El caché de Bitmap en RDP al conectar a un escritorio remoto mediante RDP, almacena imágenes frecuentemente accedidas, reduciendo así la cantidad de datos transmitidos por la red y mejorando el rendimiento general de la conexión.

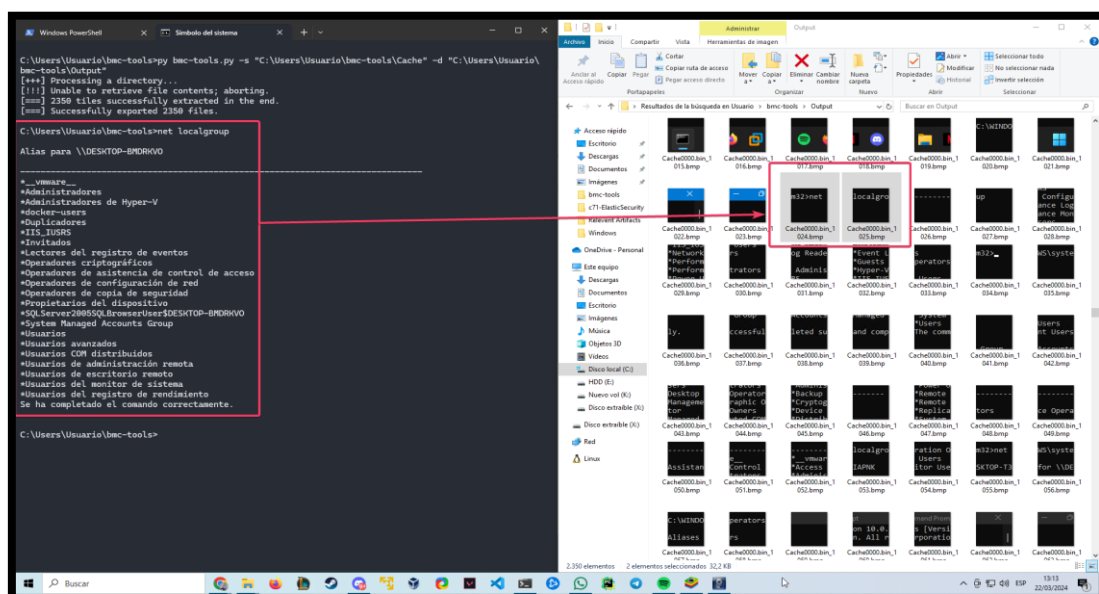
Se divide en caché de bitmap persistente, para imágenes reutilizables, y no persistente, para imágenes de uso único.

```
py      bmc-tools.py      -s      "C:\Users\Usuario\bmc-tools\Cache"      -d
"C:\Users\Usuario\bmc-tools\Output"
```

Iniciamos la herramienta diciéndole dónde está la carpeta de la que queremos sacar los datos y usamos el -d para elegir dónde sacarlo todo.



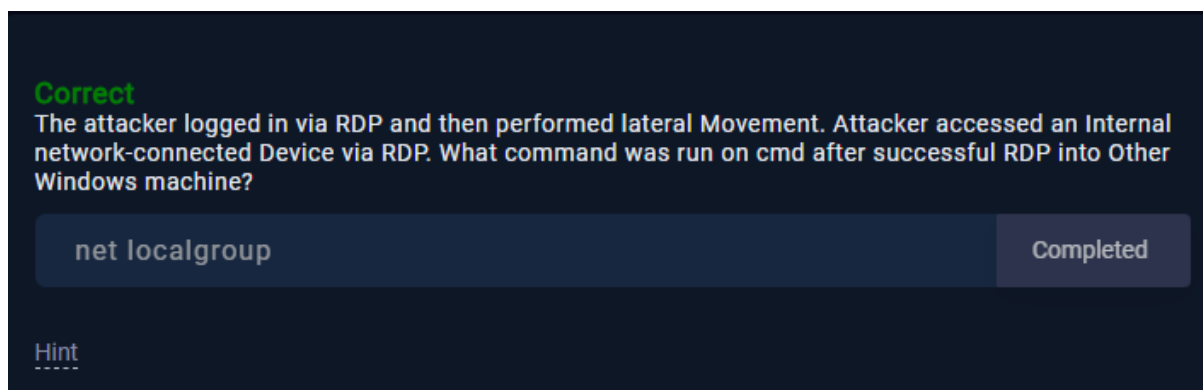
2350 archivos han sido exportados, hay que ir mirando entre todos ellos.



Por lo tanto, el comando `net localgroup` se utilizó para obtener información sobre los grupos locales en el dispositivo comprometido como parte de la fase de reconocimiento y movimientos laterales por parte del atacante.

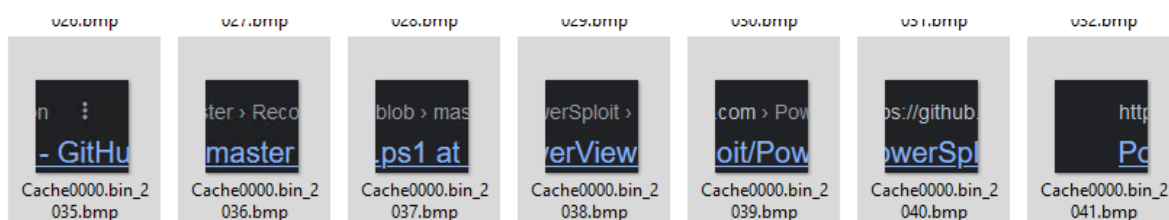
Respuesta 7

`net localgroup`

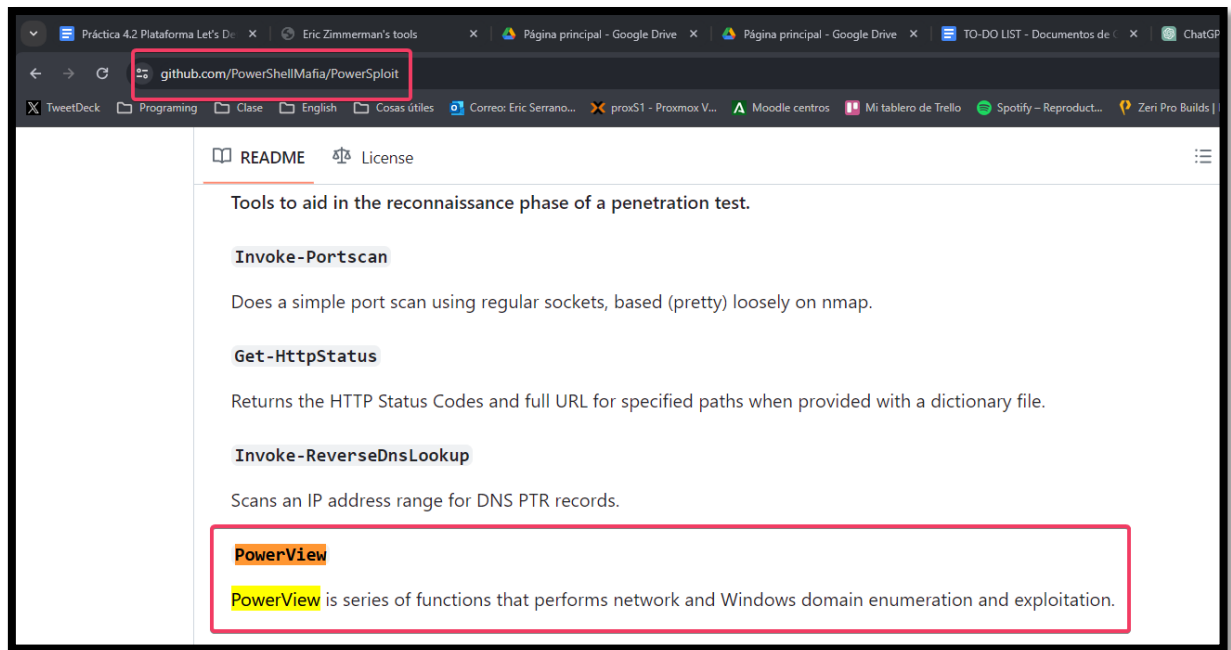


The attacker tried to download a tool from the user's browser in that second machine. What's the tool name? (name.ext)

Para esta parte vamos a seguir investigando el Output que hemos obtenido anteriormente.



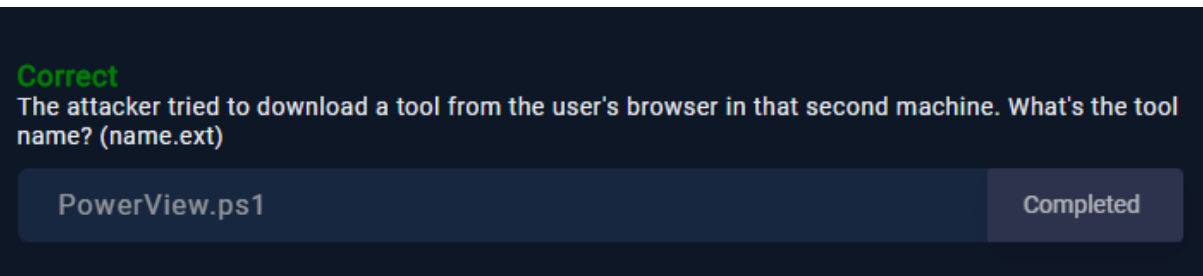
Encontramos lo siguiente buscando por PowerView.



Sospechamos que esto es lo que ha intentado descargar. PowerView es una serie de funciones que realiza enumeración y explotación de redes y dominios de Windows.

Respuesta 8

PowerView.ps1



What command was executed which resulted in privilege escalation?

Herramienta: [DeepBlueCLI](#)

Para esta pregunta, vamos a empezar por buscar el archivo System.evtx porque contiene registros detallados de eventos relacionados con el sistema operativo Windows. Este archivo nos va a ayudar a encontrar pistas importantes sobre las actividades y eventos que han ocurrido en el sistema, incluyendo cualquier comando ejecutado, servicios instalados o modificados, y eventos de interacción del usuario. Al examinar este archivo de registro, podemos identificar cualquier actividad sospechosa o indicadores de compromiso que nos permitan entender cómo ocurrió la escalada de privilegios en el sistema.

```
PS C:\Users\Usuario\DeepBlueCLI> ./DeepBlue.ps1 System.evtx

Date      : 21/08/2022 15:14:42
Log        : System
EventID    : 7045
Message    : Suspicious Service Command
Results    : Service name: kyvckn
             Metasploit-style cmd with pipe (possible use of
             meterpreter 'getsystem')

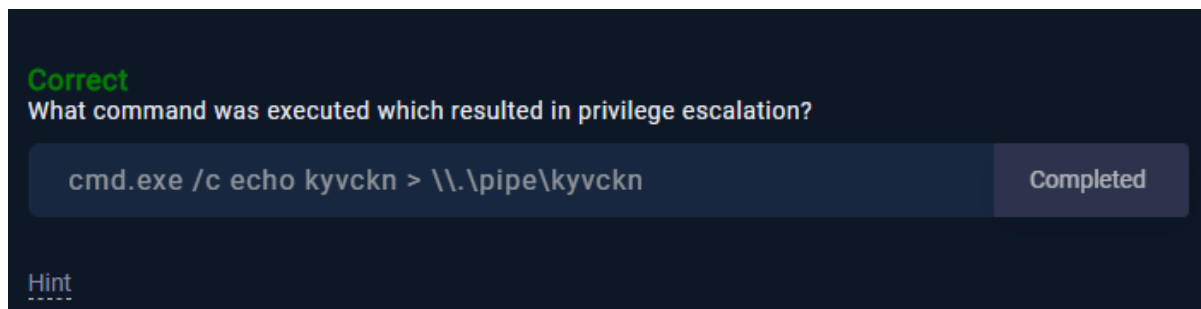
Command    : cmd.exe /c echo kyvckn > \\.\pipe\kyvckn
Decoded    :

Date      : 02/08/2022 4:06:23
Log        : System
EventID    : 7030
Message    : Interactive service warning
Results    : Service name: Printer Extensions and Notifications
             Malware (and some third party software) trigger this
             warning
Command    :
Decoded    :
```

El resultado revela que la escalada de privilegios se realizó mediante el comando **cmd.exe /c echo kyvckn > \\.\pipe\kyvckn**. Este comando es característico de las actividades de explotación, ya que sigue un patrón típico de Metasploit-style cmd con pipe, lo que sugiere el posible uso de Meterpreter.

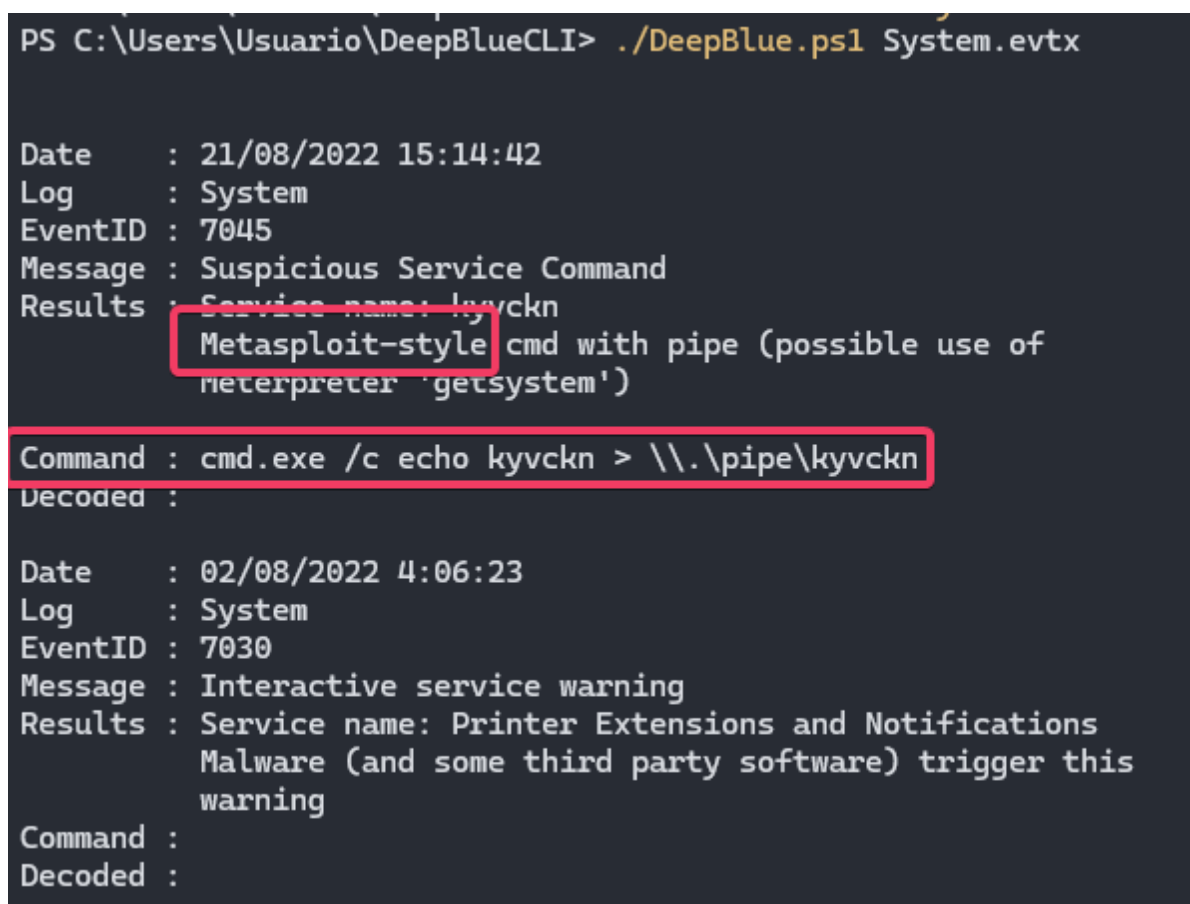
Respuesta 9

cmd.exe /c echo kyvckn > \\.\pipe\kyvckn



What framework was used by the attacker?

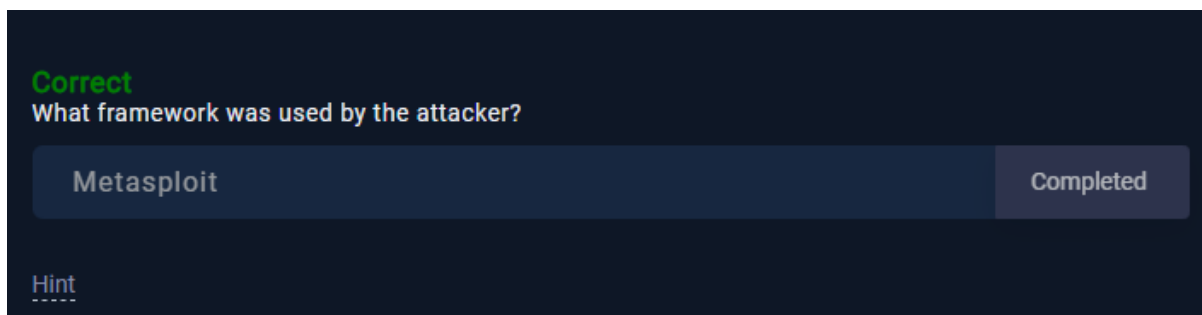
Esta pregunta se puede responder con la anterior, porque como se puede observar también nos lo dice la captura.



Se usó Metasploit.

Respuesta 10

Metasploit



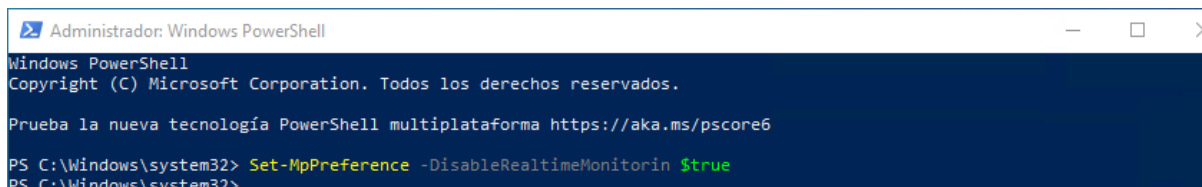
Ransomware Attack

En este laboratorio, voy a analizar un volcado de memoria de una máquina comprometida en busca de evidencia de un ataque de ransomware. Utilizando herramientas como "Redline", examinaré patrones característicos, cambios en el sistema y actividad sospechosa para identificar la presencia y naturaleza del ransomware, así como los posibles daños causados al sistema comprometido.

Para este laboratorio vamos a utilizar una máquina virtual ya que vamos a trabajar con un Ransomware.

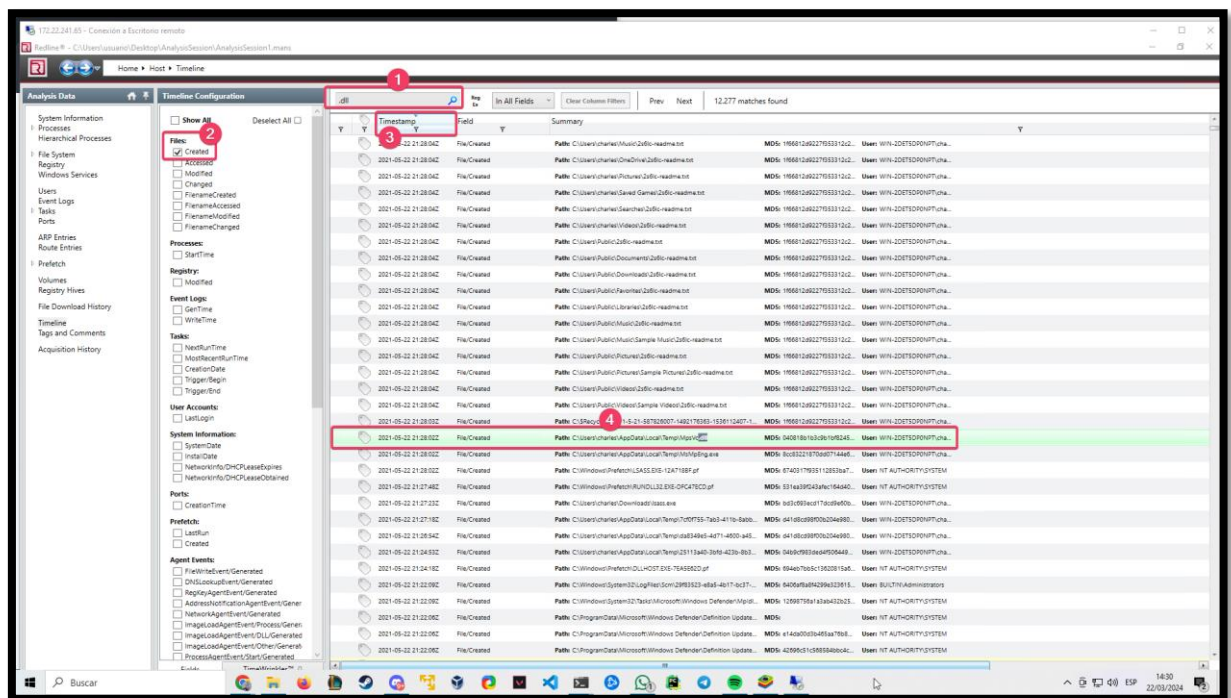
Preparación del laboratorio.

Desactivamos el firewall de windows (realtime monitor), así nuestro archivo malicioso no se borrará.



Enlace de instalación de Redline: [Redline | FireEye Market](#)

Please you find the dropped dll, include the whole path including the dll file



Respuesta 1

Correct

Please you find the dropped dll, include the whole path including the dll file

C:\Users\charles\AppData\Local\Temp\MpsVc.dll

Completed

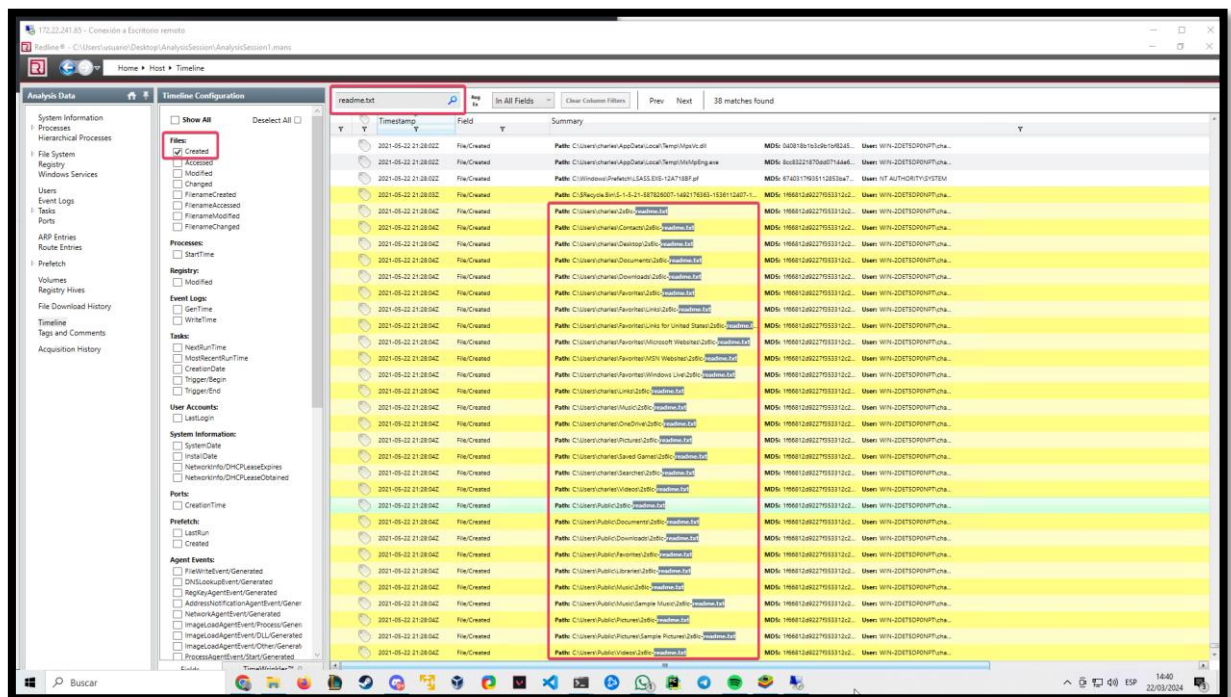
What is the MD5 hash for the dll?

Lo tenemos en lo encontrado anteriormente.

Respuesta 2

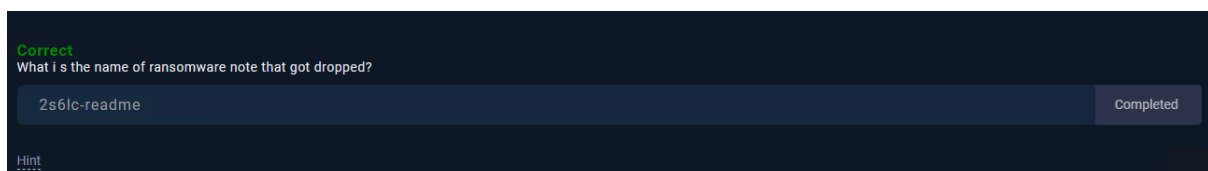


What is the name of ransomware note that got dropped?

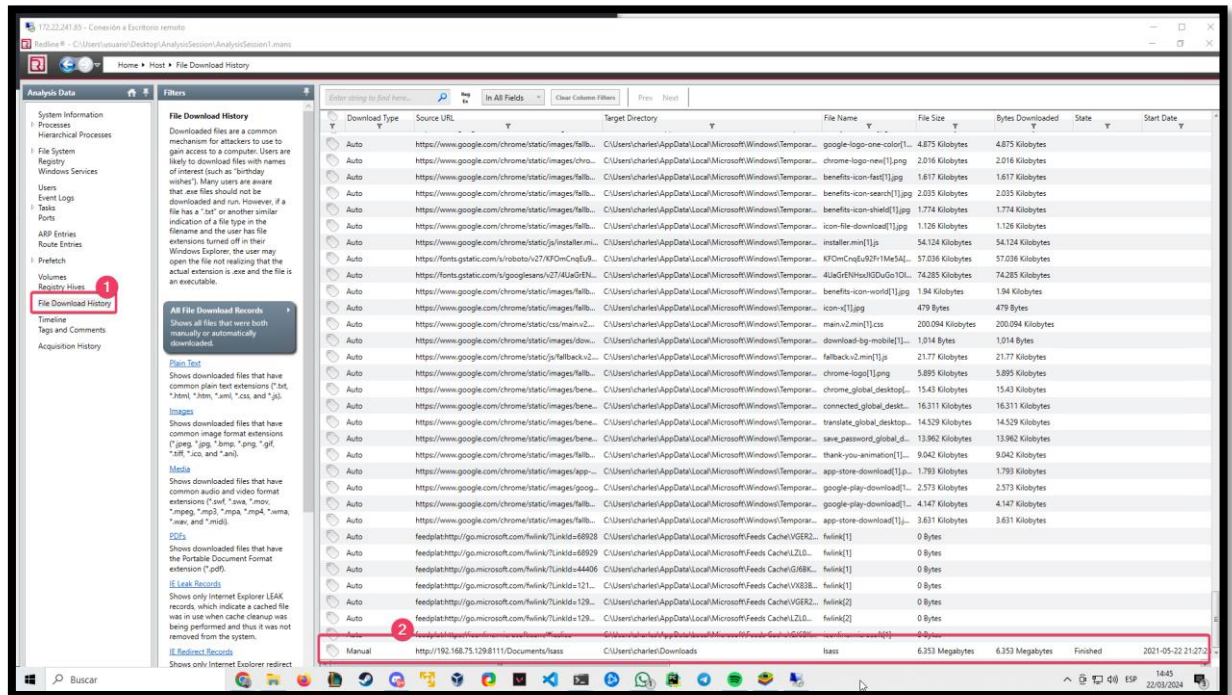


Todos los archivos fueron encriptados y el ransomware estaba soltando los archivos preguntando por el ransomware.

Respuesta 3



What is the URL that the initial payload was downloaded from? (Include the whole URL with the payload)



Sospechamos que podría ser esa de ahí, ya que está hecha manualmente, también porque todas las demás urls son la mayoría de Windows o de Microsoft, total, que a la vista se ve sospechoso.

Respuesta 4

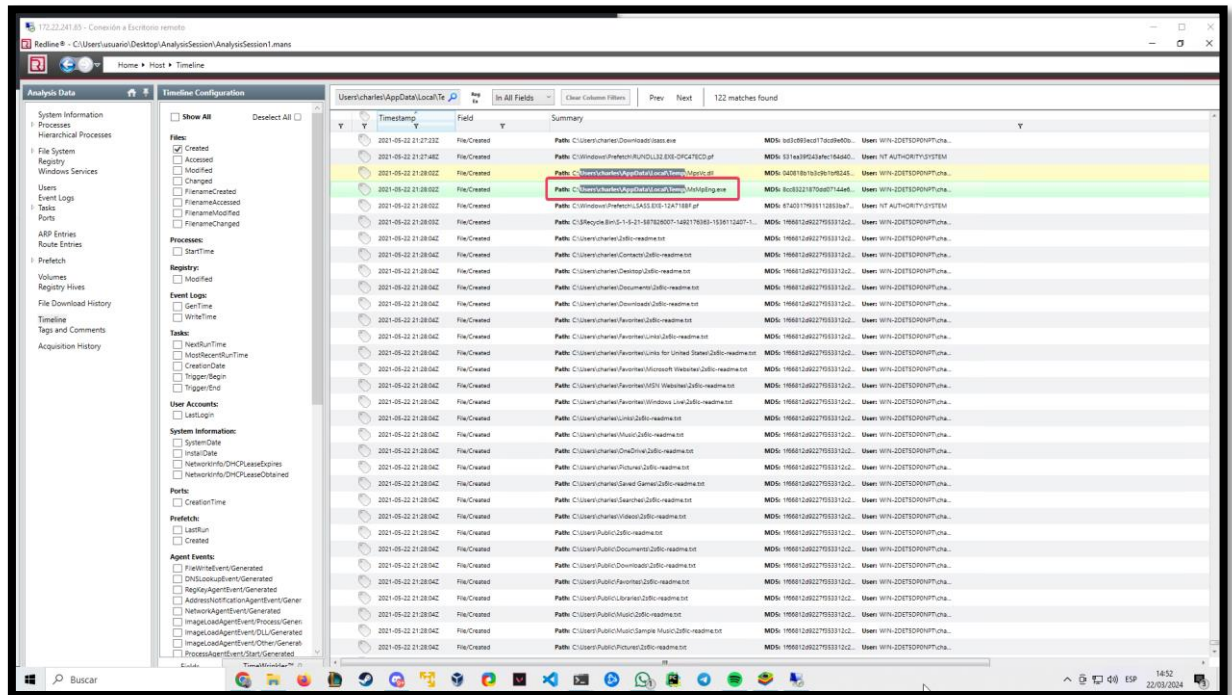
Correct

What is the URL that the initial payload was downloaded from? (Include the whole URL with the payload)

http://192.168.75.129:8111/Documents/lsass

Completed

The ransomware drops the copy of the legitimate application into the Temp folder. Please provide the filename including the extension



Respuesta 5

Correct

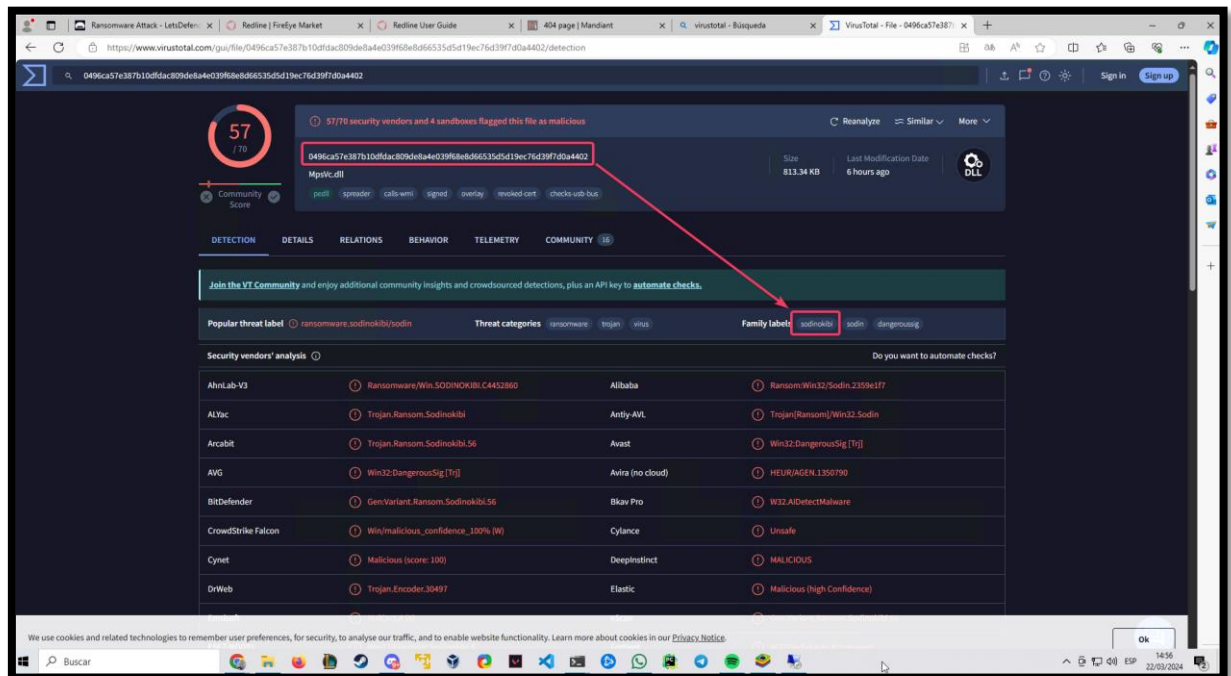
The ransomware drops the copy of the legitimate application into the Temp folder. Please provide the filename including the extension

MsmEng.exe

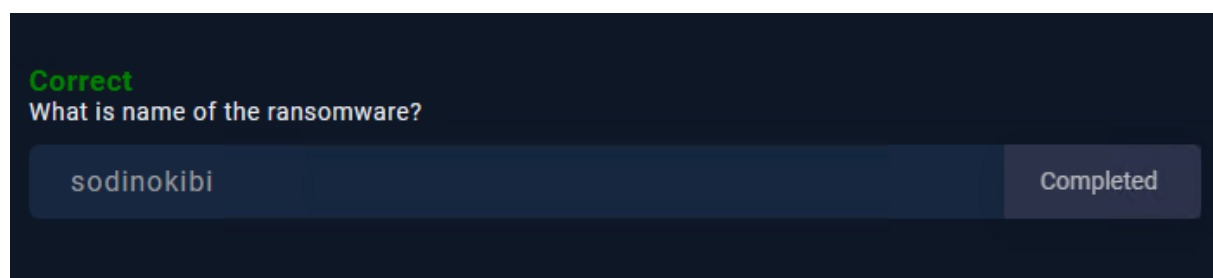
Completed

What is the name of the ransomware?

Vamos a buscar en virustotal el MD5 del archivo MpsVc.dll que es el Ransomware.



Respuesta 6



Finalización.



Incluye un apartado en el documento en el que indiques la forma correcta de obtener las evidencias con las que has trabajado en las investigaciones.

La forma correcta de obtener evidencias implica (en este caso) usar FTK Imager con acceso de solo lectura al disco, iniciar la adquisición y verificar la integridad de la imagen. Luego utilizaríamos el comando dd para copiar la imagen a otro medio de almacenamiento.

Este proceso garantizaría la validez y protección de las evidencias.

Registra en una de las herramientas de seguimiento de incidentes que vimos en la unidad anterior (Catalyst o FIR) los incidentes que has investigado. Entrega capturas de cada uno de los incidentes registrados en el que se aprecien todos los datos que has registrado.

Windows Forensics

Pondríamos el evento una vez descubierto el caso de phishing.

localhost/events/new/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

FIR New event Dashboard Incidents Events Stats search... Currently logged in as admin [logout] [Admin]

New event

Save

Summary

Subject
Incidente de Phishing detectado

Business Lines

Category
Phishing

Status
Open

Detection
CERT

Severity
3

Date / Time
2024-03-24 12:30:31

Confidentiality
C1

☒ Is an incident

Incident details

Actor
Entity

Plan
A

☐ Major incident

Description

B I H₁ H₂

Se ha identificado un incidente de phishing dirigido a nuestra organización, con la apertura del correo malicioso en tres sistemas de la red. Se ha realizado un análisis inicial en uno de los sistemas infectados para identificar las Técnicas, Tácticas y Procedimientos utilizados por los atacantes. El objetivo es permitir que nuestro equipo de respuesta a incidentes responda y mitigue cualquier compromiso adicional en la red.

Una vez resuelto lo cerraremos.

ADD COMMENT

Action

Closed

Date

2024-03-24 11:30



B I H_v H_Δ | 🔗 </> | ☰ ☷ 📅 - | 👁 ?

Incidente resuelto.

Cancel

Save changes

Comments (1) Threat Intel

		Comment	Action
2024-03-24 11:30	admin	Incidente resuelto.	Closed  

Ransomware Attack

← → ↻ 🏠

🔍 📄 localhost/events/new/ ☆ 🔔 📄 ☰

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

FIR New event Dashboard Incidents Events Stats 🔍 search... Currently logged in as admin [logout] [Admin]

New event Save

Summary

Incident details

Subject

Ataque ransomware

Business Lines

✖ CERT

Actor

Entity

Plan

B

Major incident

Category

Malware

Status

Open

Detection

CERT

Severity

2

Date / Time

2024-03-24 12:43:07

Confidentiality

C1

☒ Is an incident

Description

B I H_v H_s 🔗 </> ☰ ☷ 📄 - 👁 ?

Se ha extraído el volcado de memoria de la máquina comprometida como parte de la investigación de un posible ataque ransomware. El objetivo es encontrar evidencias del ataque de ransomware y determinar su alcance y efectos en el sistema comprometido.

ADD COMMENT ✕

Action

Closed

Date

2024-03-24 11:43

B I H_v H_s 🔗 </> ☰ ☷ 📄 - 👁 ?

Incidente resuelto.

Date ▼	Category	Subject	Lines	Severity	Status	Detection	Leader	Last Action	Plan	Lvl	IH	Edit
2024-03-24	★ Malware	Ataque ransomware	CERT	2	Closed	CERT	Entity	Closed an hour ago	B	C1	admin	✎
2024-03-24	★ Phishing	Incidente de Phishing detectado en tres sistemas de red		3	Closed	CERT	Entity	Closed an hour ago	A	C1	admin	✎