

Challege REvil Corp

- *Andres Valdivieso Pinilla - Líder de Ciberseguridad (Consultor)*
- *www.linkedin.com/in/andres-valdivieso-pinilla*

Como parte del apoyo en el uso de la herramienta Redline realice el desafío de REvil Corp en esta maquina podemos encontrar un ejercicio de respuesta a incidentes donde necesitamos analizar un host infectado mediante Redline.

Investigación del punto final comprometido



El Escenario Que Nos Presentan en el Desafío

Nos indica que Uno de los empleados de Lockman Group llamó al departamento de TI; el usuario estaba frustrado y mencionó que todos sus archivos habían cambiado de nombre a una extensión de archivo extraña que nunca había visto antes.

Después de observar la estación de trabajo del usuario, el técnico de TI ya sabía lo que estaba sucediendo y transfirió el caso al equipo de respuesta a incidentes para que investigaran más a fondo.

y que nosotros somos los encargados de responder a los incidentes.

Contextualización

******Antes de entrar a la resolución de este desafío me gustaría contextualizar un poco sobre la herramienta:

- Donde tenemos que Redline®, es una de las principales herramientas gratuita de seguridad de endpoints de FireEye, ofrece a los usuarios capacidades de investigación de host para encontrar señales de actividad maliciosa mediante el análisis de archivos y memoria y el desarrollo de un perfil de evaluación de amenazas. Utilice Redline para recopilar, analizar y filtrar datos de endpoints y realizar análisis de IOC y revisión de aciertos. Además, los usuarios de Endpoint Security (HX) de FireEye pueden abrir recopilaciones de triaje directamente en Redline para realizar un análisis en profundidad, lo que permite al usuario establecer la cronología y el alcance de un incidente.
 - Esto es lo que podemos hacer usando Redline:
 - Recopilar datos de registro (solo hosts de Windows)
 - Recopilar procesos en ejecución
 - Recopilar imágenes de memoria (antes de Windows 10)
 - Recopilar el historial del navegador
 - Busque cadenas sospechosas
 - Y Mucho mas.
- También podemos apoyarnos en otra de las herramientas de FireEye como el IOC Editor. El editor de indicadores de compromiso (IOC) de FireEye es una herramienta gratuita que proporciona una interfaz para gestionar datos y manipular las estructuras lógicas de los IOC. Los IOC son documentos XML que ayudan a los responsables de responder a incidentes a capturar información diversa sobre amenazas, incluidos los atributos de archivos maliciosos, las características de los cambios de registro y los artefactos en la memoria. El editor de IOC incluye:
 - Manipulación de las estructuras lógicas que definen el IOC
 - Aplicación de metainformación a los IOC, incluidas descripciones detalladas o

etiquetas arbitrarias

- Conversión de IOC en filtros XPath
- Gestión de listas de “términos” utilizados en los IOC

Ya con esta contextualización comenzamos a realizar la Cacería!.

Responda las preguntas a continuación

¿Cuál es el nombre completo del empleado comprometido?

De acuerdo con lo indicado en el escenario el archivo que contiene la información del evento esta en el escritorio, al abrirlo tenemos dos menús uno que nos muestra los datos analizados y un panel mas grande del costado derecho como estamos buscando el nombre del usuario, se debe buscar en el **System Information** acá tenemos información del equipo en general:

The screenshot shows the Redline application interface. The left sidebar contains a tree view with 'System Information' highlighted. The main panel displays system details in three sections: System Information, BIOS Information, and Operating System Information. The 'User Information' section at the bottom shows the logged-in user as John Coleman.

System Information	
System Date:	2021-08-02 23:05:05Z
Time Zone DST:	Eastern Daylight Time
Time Zone Standard:	Eastern Standard Time
Processor Identity:	Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz
Processor Type:	Multiprocessor Free
Primary Network Adapter MAC:	00-0c-29-66-77-da
Total Physical Memory:	3 Gigabytes
Available Physical Memory:	2.148 Gigabytes
Drives:	c:, d:
Uptime:	02:41:18
Containment State:	normal
Clock Skew:	00:00:00
State Agent Status:	monitoring_disabled

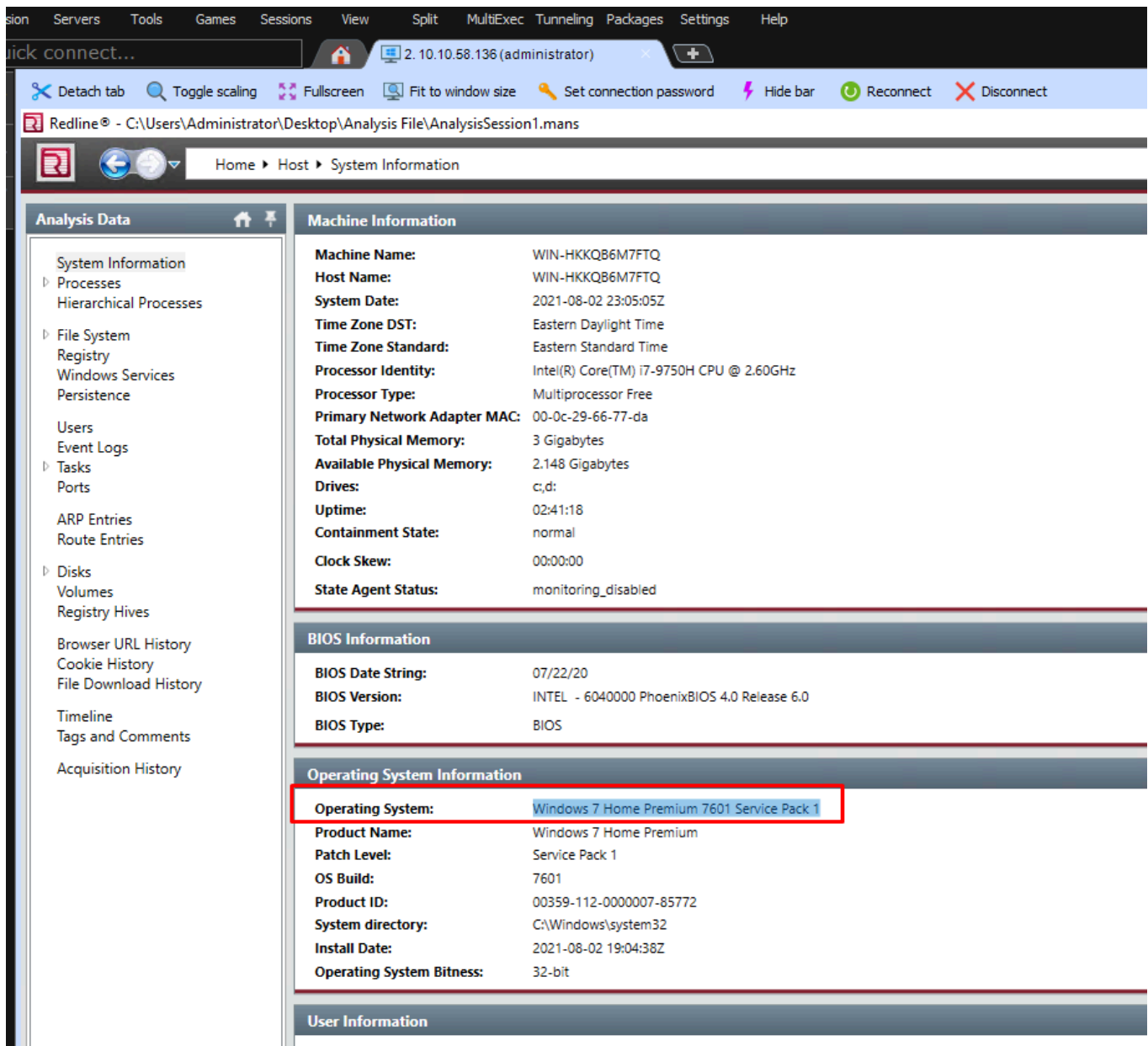
BIOS Information	
BIOS Date String:	07/22/20
BIOS Version:	INTEL - 6040000 PhoenixBIOS 4.0 Release 6.0
BIOS Type:	BIOS

Operating System Information	
Operating System:	Windows 7 Home Premium 7601 Service Pack 1
Product Name:	Windows 7 Home Premium
Patch Level:	Service Pack 1
OS Build:	7601
Product ID:	00359-112-0000007-85772
System directory:	C:\Windows\system32
Install Date:	2021-08-02 19:04:38Z
Operating System Bitness:	32-bit

User Information	
Registered Owner:	Windows User
Registered Organization:	Not Available
Domain:	WORKGROUP
Logged in User:	John Coleman
Logged on User:	WIN-HKKQB6M7FTQ\John Coleman\WORKGROUP\WIN-HKKQB6M7FTQ\$

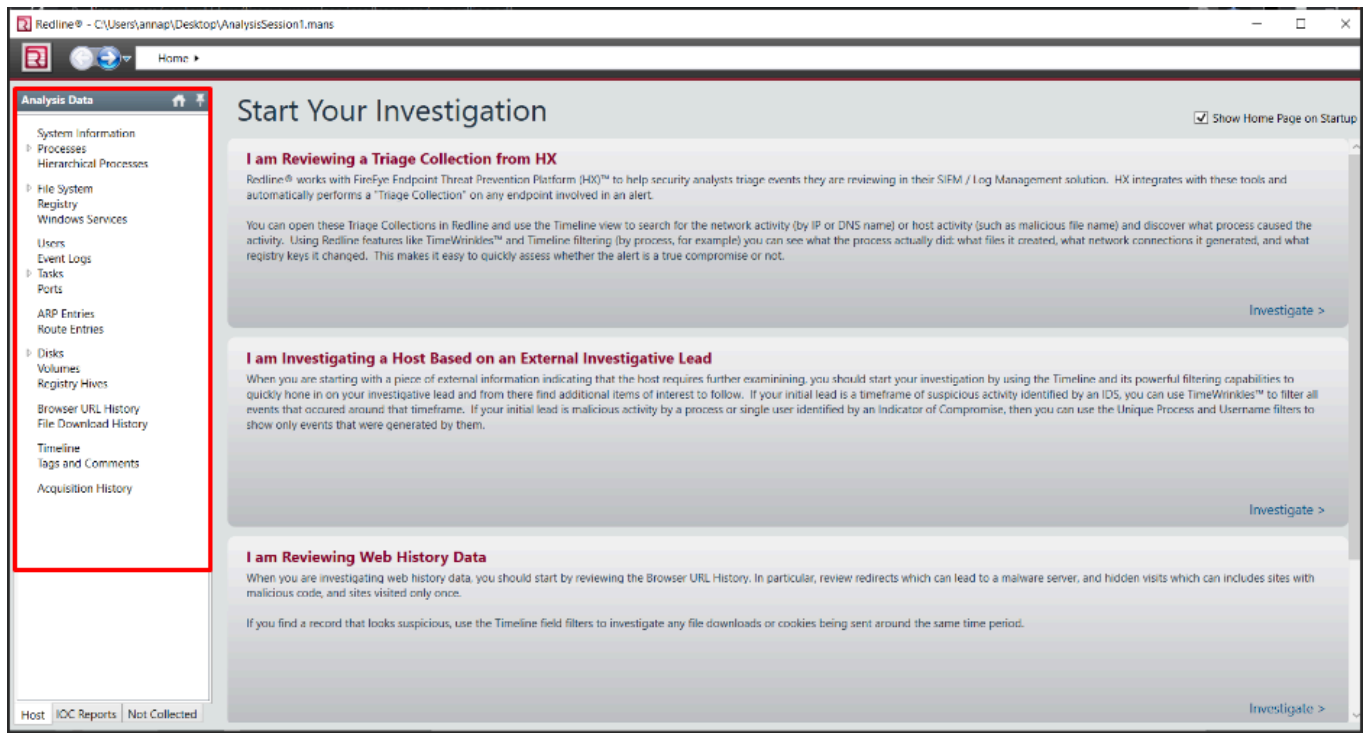
¿Cuál es el sistema operativo del host comprometido?

Ahora solicitan que proporcionemos el S.O. este esta en el mismo lugar:

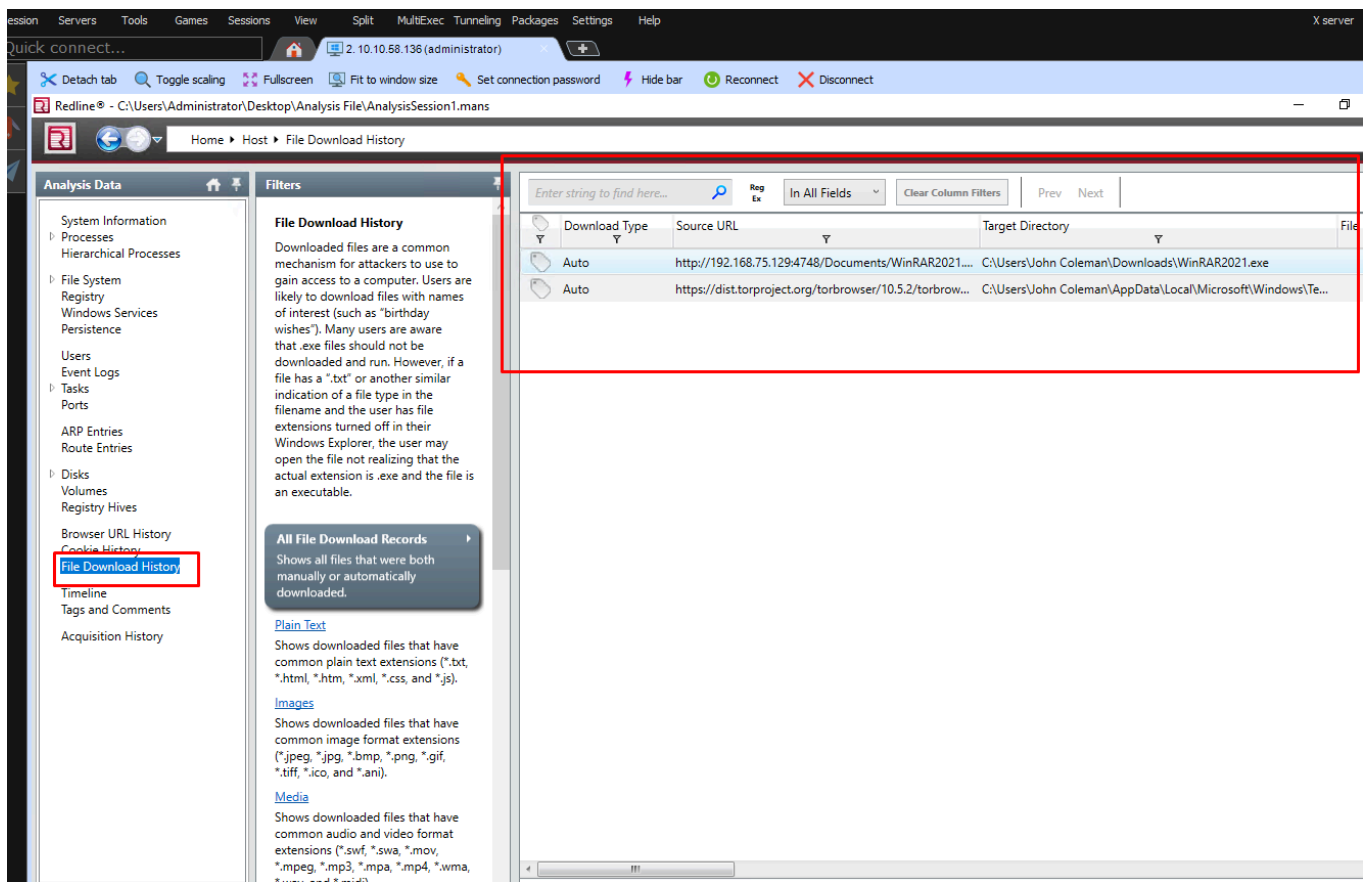


¿Cuál es el nombre del ejecutable malicioso que abrió el usuario?

Posteriormente ya entramos a buscar la información que esta asociada con el ejecutable malicioso para esto podemos ver el panel izquierdo en este encontramos los datos que se recolectaron, dentro de ellos podemos ver que tenemos una gran cantidad de opciones que se analizaron demos determinar que opción escoger (Es bueno antes de analizar darse un paseo por todos los ítems analizados para ver que datos nos muestran):



Después de validar los menús vemos que lo que buscamos esta en la ruta de los archivos descargados, acá podemos ver que fue lo que descargo el usuario y encontramos dos recursos :



Ingresamos a los recursos dando doble clic y validamos que información contienen y determinamos que la descarga maliciosa se ve después de descargar el siguiente archivo Desde esta parte no mostrare la respuesta con e fin de que lo repliquen en la plataforma debido a que es la mejor forma de aprender a usar la herramienta quedaran algunas indicaciones de cual puede ser la respuesta si ingresan y validan los eventos verán las mismas horas tamaños de archivo y podrán deducir cual es este:

The screenshot shows the Redline application window. The title bar reads "Redline® - C:\Users\Administrator\Desktop\Analysis File\AnalysisSession1.mans". The breadcrumb navigation shows "Home > Host > File Download History > Full Detailed Information".

Analysis Data (Left Sidebar):

- System Information
- Processes
 - Hierarchical Processes
- File System
 - Registry
 - Windows Services
 - Persistence
- Users
 - Event Logs
- Tasks
 - Ports
- ARP Entries
- Route Entries
- Disks
 - Volumes
 - Registry Hives
- Browser URL History
- Cookie History
- File Download History** (highlighted with a red box)
- Timeline
- Tags and Comments
- Acquisition History

File Download Information (Main Panel):

Type:	Auto
Source URL:	[REDACTED] Documents [REDACTED]
Target Directory:	C:\Users\John Coleman\Downloads\ [REDACTED]
Filename:	Not Available
Temporary Path:	Not Available
File Size:	164 Kilobytes
Bytes Downloaded:	164 Kilobytes
State:	Not Available
MIME Type:	Not Available
Referrer:	Not Available
Can Auto Resume:	Not Available
Cache Flags:	Not Available
Cache Hits:	0
Full HTTP Header:	Not Available

Download Timestamps (Main Panel):

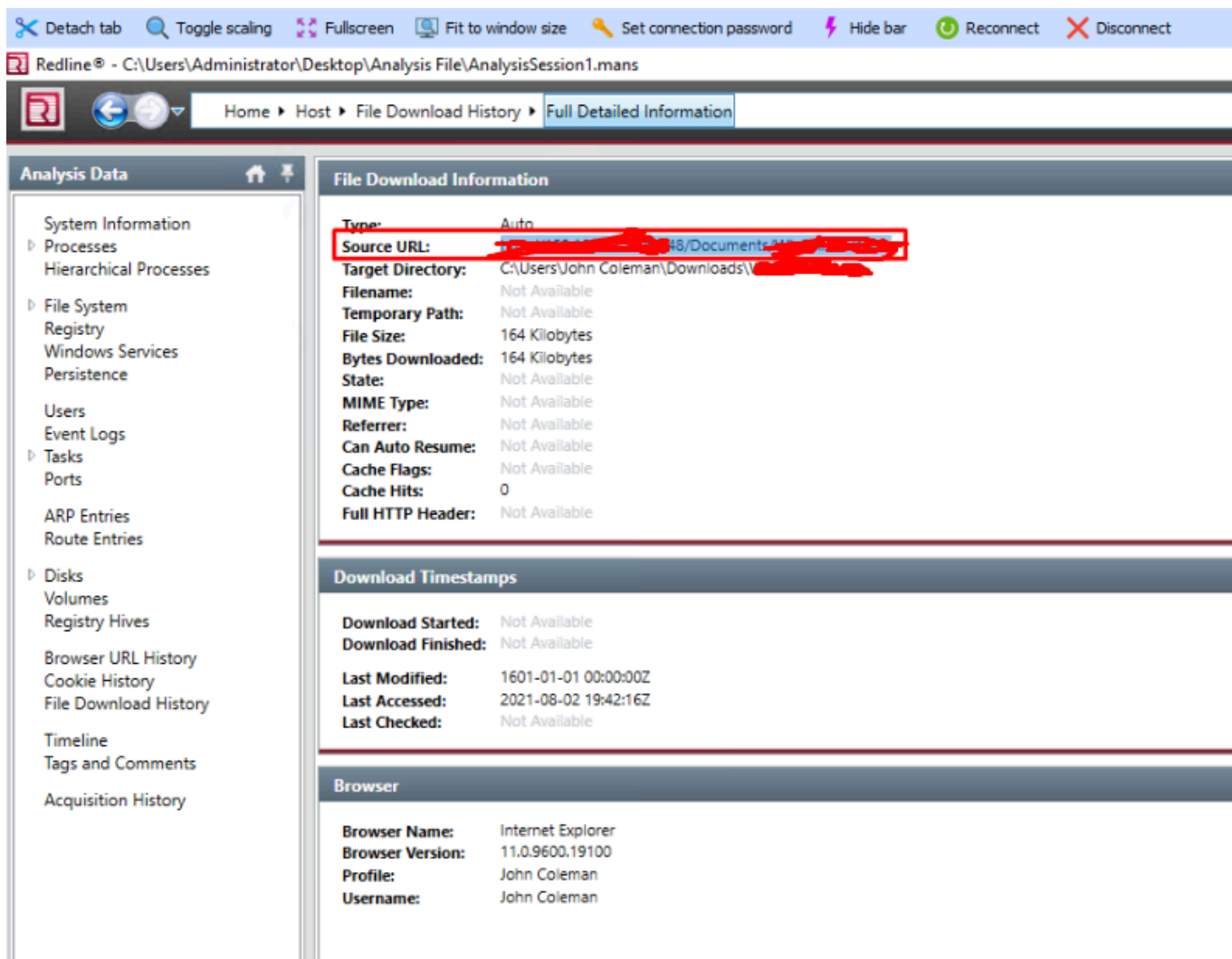
Download Started:	Not Available
Download Finished:	Not Available
Last Modified:	1601-01-01 00:00:00Z
Last Accessed:	2021-08-02 19:42:16Z
Last Checked:	Not Available

Browser (Main Panel):

Browser Name:	Internet Explorer
Browser Version:	11.0.9600.19100
Profile:	John Coleman
Username:	John Coleman

¿Cuál es la URL completa que visitó el usuario para descargar el binario malicioso? (incluya también el binario)

Ya que logramos determinar el archivo también podemos responder cual era la URL completa de la descarga que la encontramos en el mismo menú:



¿Cuál es el hash MD5 del binario?

Ahora nos piden validar el MD5 esto o podremos encontrar en el File System en la carpeta de descargas del usuario:

The screenshot shows the Redline application window. On the left, the 'Analysis Data' sidebar has 'File System' selected. The 'Filters' pane shows 'Users' and 'John Coleman' checked. The main pane displays a list of files with columns 'Full Path', 'File Name', and 'Size'. The file 'C:\Users\John Coleman\Downloads\t48s39la-readme.txt' is highlighted. The right pane shows 'Selected Item Details' for this file, including the MD5 hash: 890a58f200c0m231650f9e1b088e58f.

Full Path	File Name	Size
C:\Users		4 Kilobyte
C:\Users\desktop.ini	desktop.ini	174 Bytes
C:\Users\John Coleman		8 Kilobyte
C:\Users\John Coleman\d60dff40.lock	d60dff40.lock	0 Bytes
C:\Users\John Coleman\Downloads		4 Kilobyte
C:\Users\John Coleman\Downloads\d60dff40.lock	d60dff40.lock	0 Bytes
C:\Users\John Coleman\Downloads\desktop.ini	desktop.ini	282 Bytes
C:\Users\John Coleman\Downloads\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilobyte
C:\Users\John Coleman\Downloads\t48s39la-readme.txt	t48s39la-readme.txt	164 Kilobyte
C:\Users\John Coleman\NTUSER.DAT(6cced2f1-6e01-11de-8be...	NTUSER.DAT(6cced2f1-6...	64 Kilobyte
C:\Users\John Coleman\NTUSER.DAT(6cced2f1-6e01-11de-8be...	NTUSER.DAT(6cced2f1-6...	512 Kilobyte
C:\Users\John Coleman\NTUSER.DAT(6cced2f1-6e01-11de-8be...	NTUSER.DAT(6cced2f1-6...	512 Kilobyte
C:\Users\John Coleman\ntuser.ini	ntuser.ini	20 Bytes
C:\Users\John Coleman\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilobyte

File Metadata

Full Path: C:\Users\John Coleman\Downloads

Size: 164 Kilobytes

Attributes: Archive

inode: Not Available

File Hashes

MD5: 890a58f200c0m231650f9e1b088e58f

SHA1: Not Available

SHA256: Not Available

Timestamps

Created: 2021-08-02 19:21:50Z

Modified: 2021-08-02 23:21:34Z

Accessed: 2021-08-02 19:42:16Z

Changed: 2021-08-02 19:45:24Z

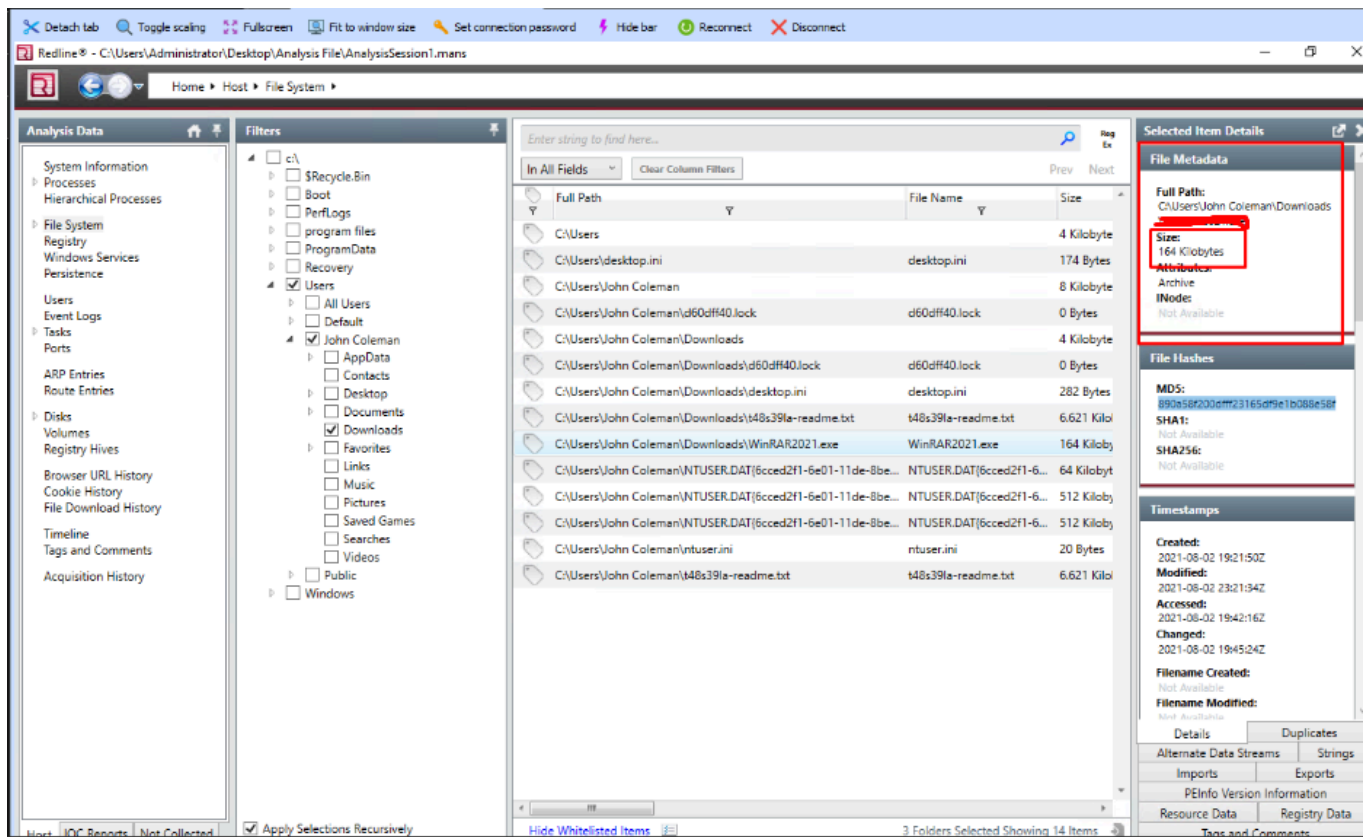
Filename Created: Not Available

Filename Modified: Not Available

Como apoyo deje a la vista el MD5 del artefacto.

¿Cuál es el tamaño del binario en kilobytes?

Validando el mismo evento podemos ver que el tamaño se encuentra en el menú de detalles en el File Path:



Ya hemos logrado identificar hasta este punto cual fue el archivo que se uso para el ataque de manera inicial pero nos indican que este archivo genero una modificacion en las extensiones de los archivos del usuario y que debemos determinar ¿Cuál es la extensión a la que se renombraron los archivos del usuario?

Para ello tenemos que pensar donde podríamos encontrar esta información y lo primero que se me ocurrió fue validar los archivos desde el escritorio y desde las descargas para ver si podía ver algo, por lo que volvi a usar la informacion del File System:

Encontré dos opciones una de ella esta a simple vista que es la .lock pero habían otros archivos que tenían una extensión diferente por lo que validando determine que la extensión era:

The screenshot displays the Redline application window. The top menu bar includes options like Session, Servers, Tools, Games, Sessions, View, Split, MultiExec, Tunneling, Packages, Settings, and Help. Below the menu, there's a toolbar with icons for Detach tab, Toggle scaling, Fullscreen, Fit to window size, Set connection password, Hide bar, Reconnect, and Disconnect. The main window shows a file system view for the user John Coleman. The left sidebar has a tree view with categories like System Information, Processes, Handles, Memory Sections, Strings, Ports, Hierarchical Processes, File System (highlighted with a red box), Registry, Windows Services, Persistence, Users, Event Logs, Tasks, Ports, ARP Entries, Route Entries, Disks, Volumes, Registry Hives, Browser URL History, Cookie History, File Download History, Timeline, Tags and Comments, and Acquisition History. The central pane shows a list of files and folders for the user John Coleman. The 'Filters' pane on the right shows a tree view of the file system with checkboxes for various locations. The 'Desktop' and 'Downloads' folders are highlighted with red boxes. The main list shows files like 'C:\Users\John Coleman\Desktop\d60dff40.lock', 'C:\Users\John Coleman\Desktop\DBG_LOG.TXT', 'C:\Users\John Coleman\Desktop\desktop.ini', 'C:\Users\John Coleman\Desktop\Finance', 'C:\Users\John Coleman\Desktop\Finance\CreditCardInfo.txt.t4s39la', 'C:\Users\John Coleman\Desktop\Finance\d60dff40.lock', 'C:\Users\John Coleman\Desktop\passwords.txt.t4s39la', 'C:\Users\John Coleman\Desktop\sdl-redline.zip.t4s39la', 'C:\Users\John Coleman\Desktop\t4s39la-readme.txt', 'C:\Users\John Coleman\Downloads', 'C:\Users\John Coleman\Downloads\d60dff40.lock', 'C:\Users\John Coleman\Downloads\desktop.ini', 'C:\Users\John Coleman\Downloads\t4s39la-readme.txt', and 'C:\Users\John Coleman\Downloads\WinRAR2021.exe'. The 'Downloads' folder is highlighted with a red box. The bottom status bar shows '3 Folders Selected Showing 17 Items'.

Ya que se logro determinar cual es el tipo de extension ahora nos piden detrmnar cuantos archivos fueron renombrados. ¿Cuál es el número de archivos que fueron renombrados y cambiados a esa extensión?

Para esto podemos usar el timeline en este podemos ver a nivel de archivo procesos eventos de log y demás, por lo que usaremos las opciones de file y veremos los que fueron modificados y cambiados, esto nos dará una respuesta de los maches que se encontraron bajo este parámetro:

Redline - C:\Users\Administrator\Desktop\Analysis File\AnalysisSession1.mans

Home Host Timeline

Analysis Data

- System Information
- Processes
 - Handles
 - Memory Sections
 - Strings
 - Ports
 - Hierarchical Processes
- File System
 - Imports
 - Exports
 - Strings
 - Alternate Data Streams
 - PEInfo Version Information
 - Resource Data
 - Registry
 - Windows Services
 - Persistence
- Users
 - Event Logs
- Tasks
 - Triggers
 - Actions
- Ports
- ARP Entries
- Route Entries
- Disks
 - Partitions
 - Volumes
 - Registry Hives
- Browser URL History
- Cookie History
- File Download History
- Timeline**
- Tags and Comments
- Acquisition History

Timeline Configuration

Show All Deselect All

Files:

- ☐ Created
- ☐ Accessed
- ☒ Modified
- ☒ Changed
- ☐ FilenameCreated
- ☐ FilenameAccessed
- ☐ FilenameModified
- ☐ FilenameChanged

Processes:

- ☐ StartTime

Registry:

- ☐ Modified

Event Logs:

- ☐ GenTime
- ☐ WriteTime

Tasks:

- ☐ NextRunTime
- ☐ MostRecentRunTime
- ☐ CreationDate
- ☐ Trigger/Begin
- ☐ Trigger/End

User Accounts:

- ☐ LastLogin

System Information:

- ☐ SystemDate
- ☐ InstallDate
- ☐ NetworkInfo/DHCPLeaseExpires
- ☐ NetworkInfo/DHCPLeaseObtained

Ports:

- ☐ CreationTime

Fields TimeWrinkles™ 0

TimeCrunches™ 0 Users Processes

.48s391e

In All Fields Clear Column Filters Prev Next matches found

Timestamp	Field	Summary
2021-08-02 19:44:56Z	File/Modified	Path: C:\Users\All Users\Microsoft\Windows\WER\ReportArchive\Kerne... MD5: 9b502b85d9k
2021-08-02 19:44:56Z	File/Changed	Path: C:\Users\All Users\Microsoft\Windows\WER\ReportArchive\Kerne... MD5: 9b502b85d9k
2021-08-02 19:45:02Z	File/Modified	Path: C:\Users\John Coleman\AppData\Roaming\Microsoft MD5:
2021-08-02 19:45:02Z	File/Changed	Path: C:\Users\John Coleman\AppData\Roaming\Microsoft MD5:
2021-08-02 19:45:02Z	File/Modified	Path: C:\Users\John Coleman\AppData\Roaming\Microsoft\MMC MD5:
2021-08-02 19:45:02Z	File/Changed	Path: C:\Users\John Coleman\AppData\Roaming\Microsoft\MMC MD5:
2021-08-02 19:45:02Z	File/Modified	Path: C:\Users\John Coleman\AppData\Roaming\Microsoft\Windows\R... MD5: bce6c764040
2021-08-02 19:45:02Z	File/Changed	Path: C:\Users\John Coleman\AppData\Roaming\Microsoft\Windows\R... MD5: bce6c764040
2021-08-02 19:45:09Z	File/Modified	Path: C:\Windows\infsetupapi.dev.log MD5: 210633a477f5
2021-08-02 19:45:09Z	File/Changed	Path: C:\Windows\infsetupapi.dev.log MD5: 210633a477f5
2021-08-02 19:45:19Z	File/Modified	Path: C:\Users\John Coleman\AppData\Roaming\Microsoft\Windows\R... MD5: 505a1ba62b2
2021-08-02 19:45:19Z	File/Changed	Path: C:\Users\John Coleman\AppData\Roaming\Microsoft\Windows\R... MD5: 505a1ba62b2
2021-08-02 19:45:24Z	File/Changed	Path: C:\Users\John Coleman\Downloads\WinRAR2021.exe MD5: 890a58020d8
2021-08-02 19:45:44Z	File/Modified	Path: C:\Users\John Coleman\AppData\Local\Microsoft\Windows Mail\... MD5:
2021-08-02 19:45:44Z	File/Changed	Path: C:\Users\John Coleman\AppData\Local\Microsoft\Windows Mail\... MD5:
2021-08-02 19:45:45Z	File/Modified	Path: C:\Windows\Prefetch\ReadyBoot\Trace5.flr MD5: 3f06b236ca2
2021-08-02 19:46:00Z	File/Modified	Path: C:\Users\John Coleman MD5:
2021-08-02 19:46:00Z	File/Changed	Path: C:\Users\John Coleman MD5:
2021-08-02 19:46:00Z	File/Modified	Path: C:\Users\John Coleman\Contacts MD5:
2021-08-02 19:46:00Z	File/Changed	Path: C:\Users\John Coleman\Contacts MD5:
2021-08-02 19:46:00Z	File/Modified	Path: C:\Users\John Coleman\Contacts\cd60df40.lock MD5: d41d8cd98f0
2021-08-02 19:46:00Z	File/Changed	Path: C:\Users\John Coleman\Contacts\cd60df40.lock MD5: d41d8cd98f0
2021-08-02 19:46:00Z	File/Modified	Path: C:\Users\John Coleman\Contacts\John Coleman.contacts.48s391e MD5: 230239ee3d

Show Details 174/41

Ya sabemos donde encontrar cambios y modificaciones y creaciones en la maquina por lo que ahora solicitan saber ¿Cuál es la ruta completa al fondo de pantalla que fue cambiado por un atacante, incluido el nombre de la imagen?

Usamos la misma opción pero esta vez vamos a buscar por creación, en esta opción sabemos que se cambia la imagen de fondo de pantalla y que esta es de extensión .BMP por lo que al filtrar nos encontraremos con la siguiente vista:

Redline® - C:\Users\Administrator\Desktop\Analysis File\AnalysisSession1.mans

Home ▶ Host ▶ Timeline Full Detailed Information

Analysis Data

- System Information
- Processes
 - Handles
 - Memory Sections
 - Strings
 - Ports
- Hierarchical Processes
- File System
 - Imports
 - Exports
 - Strings
 - Alternate Data Streams
 - PEInfo Version Information
 - Resource Data
- Registry
- Windows Services
- Persistence
- Users
- Event Logs
- Tasks
 - Triggers
 - Actions
- Ports
- ARP Entries
- Route Entries
- Disks
 - Partitions
 - Volumes
 - Registry Hives
- Browser URL History
- Cookie History
- File Download History
- Timeline
- Tags and Comments
- Acquisition History

File Metadata

Full Path: C:\Users\John Coleman\AppData\Local\Temp\██████████

Size: 5.82 Megabytes

Attributes: Archive, NotContentIndexed

Inode: Not Available

File Hashes

MD5: 6ee4ec854707a6b51d5f4c9894234df2

SHA1: Not Available

SHA256: Not Available

Timestamps

Created: 2021-08-02 19:46:21Z

Modified: 2021-08-02 19:46:21Z

Accessed: 2021-08-02 19:46:21Z

Changed: 2021-08-02 19:46:21Z

Filename Created: Not Available

Filename Modified: Not Available

Filename Accessed: Not Available

Filename Changed: Not Available

User Information

Username: WIN-HKKQB6M7FTQ\John Coleman

Security ID: S-1-5-21-1353384816-572941898-2751933276-1000

Security Type: SidTypeUser

File Path Parts

Device Path: \Device\HarddiskVolume1

Drive Letter: C

File Directory Path: Users\John Coleman\AppData\Local\Temp

File Name: hk8.bmp

File Extension: bmp

PEInfo

Details Duplicates Alternate Data Streams Strings Imports Exports PEInfo Version Information Resource

Después me di cuenta que podía haber usado os filtros solo para la fecha en la que se vio el incidente con el fin de segmentar mejor los datos esto también ayudaría a encontrar la respuesta.

Ya que tenemos mas información sobre el artefacto nos solicitan validar la nota que dejó el atacante para el usuario en el escritorio; y que proporcionemos el nombre de la nota con la extensión.

Acá volvemos a tener que buscar la información en el File System en la misma pregunta nos piden validar en el Escritorio así que vamos a la ruta y vemos que existen 12 elementos de los cuales podemos ver una que se llama:

Quick connect...

2. 10.10.58.136 (administrator)

Detach tab

Toggle scaling

Fullscreen

Fit to window size

Set connection password

Hide bar

Reconnect

Disconnect

Redline® - C:\Users\Administrator\Desktop\Analysis File\AnalysisSession1.mans

HomeHostFile System

Analysis Data

System Information

Processes

Handles

Memory Sections

Strings

Ports

Hierarchical Processes

File System

Imports

Exports

Strings

Alternate Data Streams

PEInfo Version Information

Resource Data

Registry

Windows Services

Persistence

Users

Event Logs

Tasks

Triggers

Actions

Ports

ARP Entries

Route Entries

Disks

Partitions

Volumes

Registry Hives

Browser URL History

Cookie History

File Download History

Timeline

Tags and Comments

Acquisition History

Filters

☐ C:\

☐ \$Recycle.Bin

☐ Boot

☐ PerfLogs

☐ program files

☐ ProgramData

☐ Recovery

☐ Users

☐ All Users

☐ Default

☐ John Coleman

☐ AppData

☐ Contacts

☒ Desktop

☐ Documents

☐ Downloads

☐ Favorites

☐ Links

☐ Music

☐ Pictures

☐ Saved Games

☐ Searches

☐ Videos

☐ Public

☐ Windows

.t48s39la

In All FieldsClear Column Filters

PrevNext

Full Path	File Name	Size
C:\Users\John Coleman\Desktop		4 Kilobyte
C:\Users\John Coleman\Desktop\d.e.c.r.y.p.t.o.r.exe	d.e.c.r.y.p.t.o.r.exe	66.5 Kilob
C:\Users\John Coleman\Desktop\d60dff40.lock	d60dff40.lock	0 Bytes
C:\Users\John Coleman\Desktop\DBG_LOG.TXT	DBG_LOG.TXT	117,813 K
C:\Users\John Coleman\Desktop\desktop.ini	desktop.ini	282 Bytes
C:\Users\John Coleman\Desktop\Finance		4 Kilobyte
C:\Users\John Coleman\Desktop\Finance\CreditCardInfo.txt.t48s39la	CreditCardInfo.txt.t48s39la	236 Bytes
C:\Users\John Coleman\Desktop\Finance\d60dff40.lock	d60dff40.lock	0 Bytes
C:\Users\John Coleman\Desktop\Finance\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilo
C:\Users\John Coleman\Desktop\passwords.txt.t48s39la	passwords.txt.t48s39la	251 Bytes
C:\Users\John Coleman\Desktop\sdl-redline.zip.t48s39la	sdl-redline.zip.t48s39la	76.385 Me
C:\Users\John Coleman\Desktop\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilo

Hide Whitelisted Items

2 Folders Selected Showing 12 Items

Selected Item Details

File Metadata

Full Path:

C:\Users\John Coleman\Desktop\t48s39la-readme.txt

Size:

6.621 Kilobytes

Attributes:

Archive

INode:

Not Available

File Hashes

MD5:

cb48d7c22e073fd8f36013dc8ac749fz

SHA1:

Not Available

SHA256:

Not Available

Timestamps

Created:

2021-08-02 19:46:00Z

Modified:

2021-08-02 19:46:00Z

Accessed:

2021-08-02 19:46:00Z

Changed:

2021-08-02 19:46:22Z

Filename Created:

Not Available

Filename Modified:

Not Available

Details

Duplicates

Alternate Data Streams

Strings

Imports

Exports

PEInfo Version Information

Resource Data

Registry Data

Tags and Comments

Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help

Quick connect... 2. 10.10.58.136 (administrator)

Detach tab Toggle scaling Fullscreen Fit to window size Set connection password Hide bar Reconnect Disconnect

Redline® - C:\Users\Administrator\Desktop\Analysis File\AnalysisSession1.mans

Home Host File System Full Detailed Information

Analysis Data

- System Information
 - Processes
 - Handles
 - Memory Sections
 - Strings
 - Ports
 - Hierarchical Processes
- File System
 - Imports
 - Exports
 - Strings
 - Alternate Data Streams
 - PEInfo Version Information
 - Resource Data
- Registry
 - Windows Services
 - Persistence
- Users
 - Event Logs
- Tasks
 - Triggers
 - Actions
- Ports
 - ARP Entries
 - Route Entries
- Disks
 - Partitions
 - Volumes
 - Registry Hives
- Browser URL History
- Cookie History
- File Download History
- Timeline
- Tags and Comments
- Acquisition History

File Metadata

Full Path: C:\Users\John Coleman\Desktop\t48s39ia-readme.txt

Size: 6.621 Kilobytes

Attributes: Archive

INode: Not Available

File Hashes

MD5: cb48d7c22e073fd8f36013dc8ac749fa

SHA1: Not Available

SHA256: Not Available

Timestamps

Created: 2021-08-02 19:46:00Z

Modified: 2021-08-02 19:46:00Z

Accessed: 2021-08-02 19:46:00Z

Changed: 2021-08-02 19:46:22Z

Filename Created: Not Available

Filename Modified: Not Available

Filename Accessed: Not Available

Filename Changed: Not Available

User Information

Username: WIN-HKKQB6M7FTQ\John Coleman

Security ID: S-1-5-21-1353384816-572941898-2751933278-1000

Security Type: SidTypeUser

File Path Parts

Device Path: \Device\HarddiskVolume1

Drive Letter: C

File Directory Path: Users\John Coleman\Desktop

File Name: t48s39ia-readme.txt

File Extension: txt

PEInfo

Host IOC Reports Not Collected

Details Duplicates Alternate Data Streams Strings Imports Exports PEInfo Version Information Resource Data Registry Data Tags and Comments

También nos indican que el atacante creó una carpeta llamada "Enlaces para Estados Unidos" en C:\Users\John Coleman\Favorites\ y dejó un archivo allí. Y que debemos proporcionar el nombre del archivo.

Usando la misma dinámica buscamos en la ruta de favoritos y en esta encontramos varios archivos, como pista nos indican que la respuesta esta asociada a un archivo que en el nombre contiene palabras en español:

Redline - C:\Users\Administrator\Desktop\Analysis File\AnalysisSession1.mans

Home ▶ Host ▶ File System ▶

Analysis Data

- System Information
- Processes
 - Handles
 - Memory Sections
 - Strings
 - Ports
- Hierarchical Processes
- File System**
- Imports
- Exports
- Strings
- Alternate Data Streams
- PEInfo Version Information
- Resource Data
- Registry
- Windows Services
- Persistence
- Users
- Event Logs
- Tasks
 - Triggers
 - Actions
- Ports
- ARP Entries
- Route Entries
- Disks
 - Partitions
 - Volumes
 - Registry Hives
- Browser URL History
- Cookie History
- File Download History
- Timeline
- Tags and Comments
- Acquisition History

Filters

- c:\
 - \$Recycle.Bin
 - Boot
 - PerfLogs
 - program files
 - ProgramData
 - Recovery
 - Users
 - All Users
 - Default
 - John Coleman
 - AppData
 - Contacts
 - Desktop
 - Documents
 - Downloads
 - Favorites**
 - Links
 - Music
 - Pictures
 - Saved Games
 - Searches
 - Videos
 - Public
 - Windows

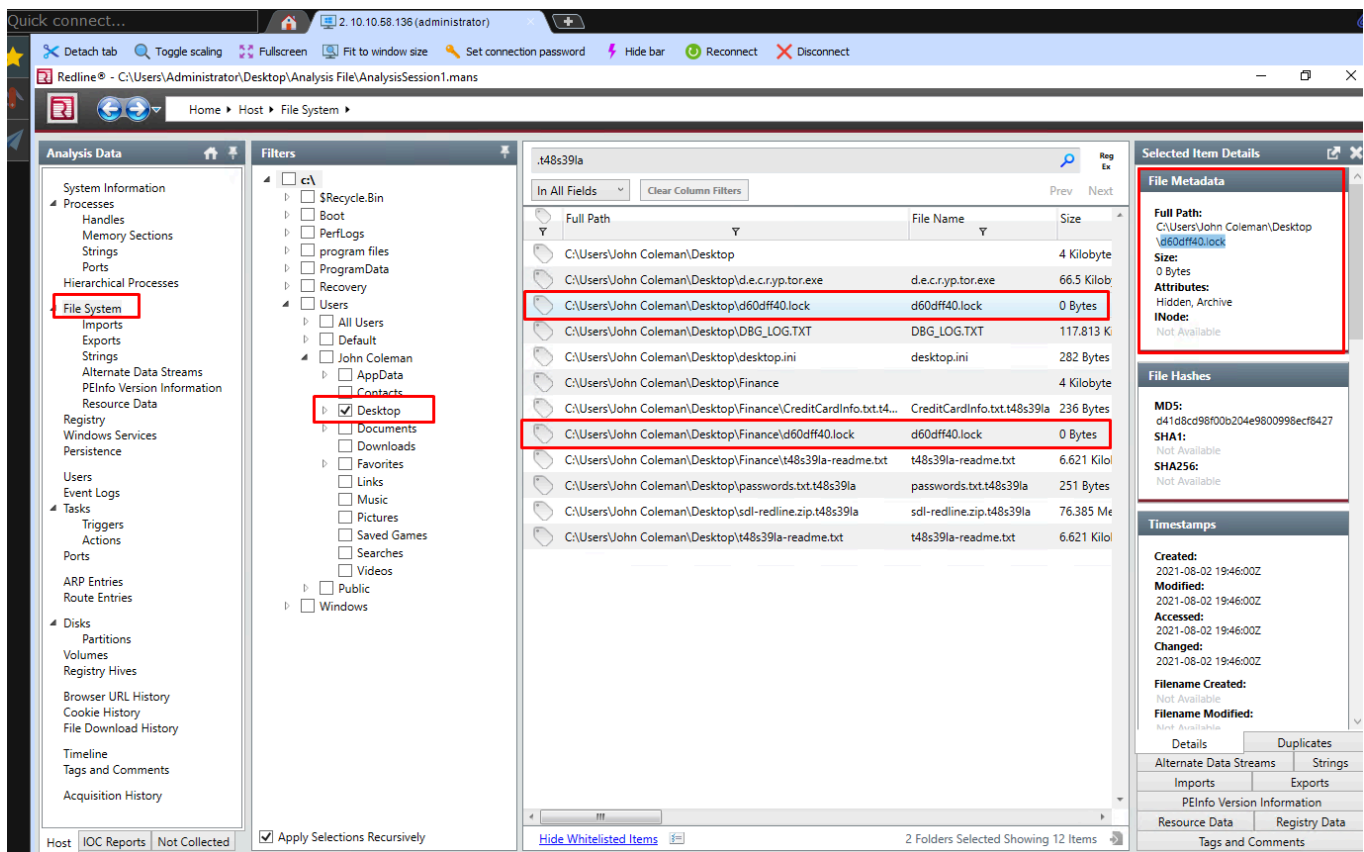
.t48s39la

In All Fields Clear Column Filters Prev Next

Full Path	File Name	Size
C:\Users\John Coleman\Favorites		4 Kilobyte
C:\Users\John Coleman\Favorites\d60dff40.lock	d60dff40.lock	0 Bytes
C:\Users\John Coleman\Favorites\desktop.ini	desktop.ini	402 Bytes
C:\Users\John Coleman\Favorites\Links		4 Kilobyte
C:\Users\John Coleman\Favorites\Links\d60dff40.lock	d60dff40.lock	0 Bytes
C:\Users\John Coleman\Favorites\Links\desktop.ini	desktop.ini	80 Bytes
C:\Users\John Coleman\Favorites\Links\Suggested Sites.url	Suggested Sites.url	302 Bytes
C:\Users\John Coleman\Favorites\Links\Suggested Sites.url.t48s39la-readme.txt	Suggested Sites.url.t48s39la-readme.txt	530 Bytes
C:\Users\John Coleman\Favorites\Links\Web Slice Gallery.url.t48s39la-readme.txt	Web Slice Gallery.url.t48s39la-readme.txt	454 Bytes
C:\Users\John Coleman\Favorites\Links for United States		4 Kilobyte
C:\Users\John Coleman\Favorites\Links for United States\d60dff40.lock	d60dff40.lock	0 Bytes
C:\Users\John Coleman\Favorites\Links for United States\desktop.ini	desktop.ini	224 Bytes
C:\Users\John Coleman\Favorites\Links for United States\Gobi... .gov.url.t48s39la-readme.txt	.gov.url.t48s39la-readme.txt	362 Bytes
C:\Users\John Coleman\Favorites\Links for United States\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilo
C:\Users\John Coleman\Favorites\Links for United States\USA... .gov.url.t48s39la-readme.txt	USA.gov.url.t48s39la-readme.txt	362 Bytes
C:\Users\John Coleman\Favorites\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilo

Host IOC Reports Not Collected Apply Selections Recursively Hide Whitelisted Items 3 Folders Selected Showing 17 Items

También nos piden buscar un archivo oculto que se creó en el escritorio del usuario y que tiene 0 bytes. proporcionando el nombre del archivo oculto.



Después de haber analizado esta información nos indican que el usuario descargó un descifrador con la esperanza de descifrar todos los archivos, pero no lo logró. Que proporcionemos el hash MD5 del archivo descifrador.

Ya que sabemos que lo que busco es un descifrador buscamos en los archivos analice en el Historial web debido lo que se indicaba en la pregunta y se puede ver que el usuario busco información asociada a los eventos ingreso a descargar el navegador de tor y también encontré el evento asociado a el descifrador:

Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help

Quick connect... 2.10.10.58.136 (administrator)

Detach tab Toggle scaling Fullscreen Fit to window size Set connection password Hide bar Reconnect Disconnect

Redline® - C:\Users\Administrator\Desktop\Analysis File\AnalysisSession1.mans

Home Host Browser URL History

Analysis Data

- System Information
- Processes
 - Handles
 - Memory Sections
 - Strings
 - Ports
- Hierarchical Processes
- File System
 - Imports
 - Exports
 - Strings
 - Alternate Data Streams
 - PEInfo Version Information
 - Resource Data
- Registry
 - Windows Services
 - Persistence
- Users
- Event Logs
- Tasks
 - Triggers
 - Actions
- Ports
- ARP Entries
- Route Entries
- Disks
 - Partitions
 - Volumes
- Registry Hives
- Browser URL History**
- Cookie History
- File Download History
- Timeline
- Tags and Comments
- Acquisition History

Filters

Review Browser URL History

When you are investigating web history data, you should start by reviewing the Browser URL History. In particular, review redirects which can lead to a malware server, and hidden visits which can include sites with malicious code, and sites visited only once.

If you find a record that looks suspicious, use the Timeline field filters to investigate any file downloads or cookies being sent around the same time period.

All URL Records
Shows all URL records.

Redirects
Shows all URL records for visit types that were a variation of a redirect, which is often used to bounce a user from site to site before finally reaching a malware staging server.

Visit From
Shows all records generated after the user first viewed another page, which can be valuable information in determining a sequence of events.

Visited Once
Shows only records that had exactly one visit; rarely visited sites are an indication of suspicious activity.

Visited Bookmarked URLs
Shows only records that were visited from a bookmark; bookmarked sites are indication of preferential

Enter string to find here...

In All Fields Clear Column Filters

Prev Next

Visit Type	URL	Page Title	Hostname
URL	https://acdn.adnxs.com/dmp/async_usersync.html?gd...		
URL	https://mwf-service.akamaized.net/mwf/js/bundle/1.5...		
URL	https://mwf-service.akamaized.net/mwf/css/bundle/1...		
URL	https://e1.emxdgt.com/put?d=d41&uid=2A56C1BE9...		
URL	https://cdn.taboola.com/TaboolaCookieSyncScript.js		
URL	https://static.adsafeprotected.com/main.gr.19.8.220.js		
URL	https://static.adsafeprotected.com/sca.17.5.10.js		
URL	https://static.adsafeprotected.com/skeleton.js		
URL	https://b1t-chidc2.zemanta.com/t/imp/impression/5...		
URL	https://cdn.js7k.com/rq/iv/inside.js		
URL	https://statics-marketingites-eus-ms-com.akamaize...		
URL	http://decryptor.top/644E7C8EFA02FB87		
URL	https://www.microsoft.com/en-us/edge/Assets/jquer...		
URL	https://www.microsoft.com/en-us/edge/Assets/css?v...		
URL	https://www.microsoft.com/en-us/edge/Assets/js?v1...		
URL	https://www.microsoft.com/mwfl_h/v3.54/mwfl-app/f...		
URL	https://www.microsoft.com/mwfl_h/v3.07/mwfl-app/f...		
URL	https://www.microsoft.com/onerfstatics/marketingit...		
URL	https://www.microsoft.com/onerfstatics/marketingit...		
URL	https://www.microsoft.com/en-us/edge		
URL	https://sb.scorecardresearch.com/beacon.js		
URL	https://service.idsync.analytics.yahoo.com/sp/v0/pixel...		

395 Items

Selected Item Details

URL Information

URL:
<http://decryptor.top/644E7C8EFA02FB87>

Page Title:
Not Available

Host Name:
Not Available

User Typed:
Not Available

Hidden:
Not Available

Visit Type:
URL

Visit Count:
0

Visit From:
Not Available

Thumbnail:
Not Available

Indexed Content:
Not Available

URL Timestamps

Last Visited:
2021-08-02 19:48:23Z

Last Visited Local:
Not Available

First Visited:
Not Available

First Bookmarked:
Not Available

Browser

Browser Name:
Internet Explorer

Browser Version:
Not Available

Details Duplicates

Tags and Comments

Con esto asumí que se vería el archivo en las descargas pero no lo encontré por lo que valide las demás rutas que ya había validado y en el escritorio logre encontrar un archivo con el nombre de:

The screenshot displays the Redline File System interface. On the left, the 'Analysis Data' sidebar shows a tree view with 'File System' and 'Desktop' highlighted. The main pane shows a list of files for the selected item 't48s391a'. The file 'C:\Users\John Coleman\Desktop\d.e.c.r.jp.tor.exe' is highlighted with a red box. The right sidebar shows 'Selected Item Details' for this file, including file metadata, hashes, and timestamps.

Full Path	File Name	Size
C:\Users\John Coleman\Desktop		4 Kilobyte
C:\Users\John Coleman\Desktop\d.e.c.r.jp.tor.exe	d.e.c.r.jp.tor.exe	66.5 Kilobyte
C:\Users\John Coleman\Desktop\d60dff40.lock	d60dff40.lock	0 Bytes
C:\Users\John Coleman\Desktop\DBG_LOG.TXT	DBG_LOG.TXT	117.813 KB
C:\Users\John Coleman\Desktop\desktop.ini	desktop.ini	282 Bytes
C:\Users\John Coleman\Desktop\Finance		4 Kilobyte
C:\Users\John Coleman\Desktop\Finance\CreditCardInfo.txt.t48s391a	CreditCardInfo.txt.t48s391a	236 Bytes
C:\Users\John Coleman\Desktop\Finance\d60dff40.lock	d60dff40.lock	0 Bytes
C:\Users\John Coleman\Desktop\Finance\t48s391a-readme.txt	t48s391a-readme.txt	6.621 Kilobyte
C:\Users\John Coleman\Desktop\passwords.txt.t48s391a	passwords.txt.t48s391a	251 Bytes
C:\Users\John Coleman\Desktop\sdl-redline.zip.t48s391a	sdl-redline.zip.t48s391a	76.385 MB
C:\Users\John Coleman\Desktop\t48s391a-readme.txt	t48s391a-readme.txt	6.621 Kilobyte

File Metadata

Full Path: C:\Users\John Coleman\Desktop\d.e.c.r.jp.tor.exe
Size: 66.5 Kilobytes
Attributes: Archive
INode: Not Available

File Hashes

MD5: f617a78c0d276682fdf528bb3e72560
SHA1: Not Available
SHA256: Not Available

Timestamps

Created: 2021-08-02 19:07:52Z
Modified: 2021-08-02 23:07:28Z
Accessed: 2021-08-02 19:50:07Z
Changed: 2021-08-02 19:50:07Z
Filename Created: Not Available
Filename Modified: Not Available

También nos solicitaron encontrar la ruta completa de la URL que proporcione el atacante en la nota del ransomware, desde la que se puede acceder a través del navegador normal para descifrar uno de los archivos cifrados de forma gratuita. El usuario intentó acceder a ella. Proporcione la ruta URL completa.

Debido a lo que había realizado en la pregunta anterior ya contaba con esta URL solo valide los detalles para sacar a ruta completa:

The screenshot shows the Redline software interface. The sidebar on the left contains various navigation options, with 'Browser URL History' highlighted. The main window displays a table of URL records. A red box highlights the 'URL' column, and another red box highlights the 'Selected Item Details' panel on the right, which shows information for the selected URL: <http://decryptor.top/644E7C8EFA02FB87>. The details include URL Information, URL Timestamps, and Browser information.

Con toda esta información ya podemos encontrar información asociada a el evento y al artefacto mediante fuentes de inteligencia por lo que podemos usar los siguientes links para ver mas información del evento:

- <https://www.virustotal.com/gui/file/5f56d5748940e4039053f85978074bde16d64bd5ba97f6f0026ba8172cb29e93/detection>
- <https://tria.ge/240203-xwllrsafcn>
- <https://www.hybrid-analysis.com/sample/5f56d5748940e4039053f85978074bde16d64bd5ba97f6f0026ba8172cb29e93>
- <https://malshare.com/sample.php?action=detail&hash=5f56d5748940e4039053f85978074bde16d64bd5ba97f6f0026ba8172cb29e93>
- <https://otx.alienvault.com/indicator/file/5f56d5748940e4039053f85978074bde16d64bd5ba97f6f0026ba8172cb29e93>

Apoyándose en estos links se puede realizar la ultima pregunta en la que se pueden encontrar mas datos del Ransomware com o ¿Cuáles son los tres nombres

asociados con el malware que infectó este host? (ingrese los nombres en orden alfabético)

5f56d5748940e4039053f85978074bde16d64bd5ba97f6f0026ba8172cb29e93

MDS

890a58f200dff23165df9e1b088e58f

SHA-174e3d82f7ee81109e150dc41112cf95b3a4b5307

SHA-2565f56d5748940e4039053f85978074bde16d64bd5ba97f6f0026ba8172cb29e93

Vhash015056656d7d5567

Authentihash23639031e41de37cf4f4093cd0e4856d28d7c81ae452ce5b85704ad2d872b28b

Rich PE header hashabb8c5410a224125a54651a3500ca0f0

SSDEEP3072:HpS5exkWi1bi4eTmIwDCnu/q2GB96Wjy-JvGWbntWUjyB9

TLSHT1D7F3C0126D9001F3C99742F1972B3FA7D6FEF939131525DF536188846F320D2BA2A22B

File typeWin32 EXEexecutable windows win32 pe peexe

MagicPE32 executable (GUI) Intel 80386, for MS Windows

TrIDWin32 Executable MS Visual C++ (generic) (47.3%) Win64 Executable (generic) (15.9%) Win32 Dynamic Link Library (generic) (9.9%) Win16 NE executable (generic) (7.9%)

DetectItEasyPE32 Compiler: Microsoft Visual C/C++ (19.00.24215) [C] Linker: Microsoft Linker (14.00.24215) Tool: Visual Studio (2015)

MagikaPEBIN

File size164.00 KB (167936 bytes)

History

Creation Time2019-06-10 15:29:32 UTC

First Submission2019-07-17 14:44:51 UTC

Last Submission2025-02-25 19:04:31 UTC

Last Analysis2025-02-22 16:53:41 UTC

Names

MicrosoftOfficeUpdate.bin

free-fm-2023.exe

malware_005D0000.bin

some_malicious_file.bin

MicrosoftOfficeWord.exe

890a58f200dff23165df9e1b088e58f.exe

REvil ransomware.exe

some_malicious_file

356.vir

bf7114f025fff7dbcb7aff8e4edeb0dd8a7b53c3766429a3c5f10142609968f9_005600000.bin

DashboardBrowseScan EndpointsCreate PulseSubmit SampleAPI Integration

FILEHASH - MDS

890a58f200dff23165df9e1b088e58f

Add to Pulse

Pulses5

AV Detections2

IDS Detections0

YARA Detections0

Alerts32

Analysis Overview

Analysis Date2 years ago

File Score21.6Malicious

Antivirus DetectionsWin32:Malware-gen, Win.Ransomware.Sodinokibi-6996917-1

Alerts32 Alerts

ransomware_file_moves

ransomware_appends_extensions

network_icmp

antisandbox_cuckoo_files

modifies_boot_config

modifies_certificates

process_interest

ransomware_extensions

ransomware_mass_file_delete

ransomware_shadowcopy

More

IP's Contacted15 IP's Contacted

101.99.77.144

104.18.47.246

134.119.253.108

160.153.189

174.142.126.20

More

Domains Contacted15 Domains Contacted

kompresory-opravy.com

apps.identrust.com

craftingalegacy.com

medicalsupportco.com

www.download.windowsupdate.com

More

Related PulsesOTX User-Created Pulses (5)

Related Tags9 Related Tags

Sodinokibi

Sodin

Ransomware

REvil

Ronjohnson.com

More

Gracias..!