



INFORME DE ANÁLISIS FORENSE DIGITAL

Investigación forense de actividad sospechosa en el equipo del Director

Ejecutivo

Daniel Stix Soto

Madrid, 16 de junio de 2025

Índice

Antecedentes

1. Resumen Ejecutivo y Conclusiones

<i>1.1 ¿Hay algún software instalado en el equipo que pueda haber robado esta foto?</i>	<i>5</i>
<i>1.2 ¿Cuándo se instaló dicho software o desde cuándo se ejecuta?</i>	<i>6</i>
<i>1.3 ¿Cómo llegó al equipo dicho software?</i>	<i>7</i>
<i>1.4 ¿Hay algún mecanismo de persistencia?</i>	<i>8</i>
<i>1.5 ¿Cómo se ha exfiltrado la fotografía?</i>	<i>9</i>
<i>1.6 ¿Estaban activos los servicios de protección? Firewall, UAC, Defender</i>	<i>10</i>

2. Análisis detallado

<i>2.1 Detección y localización del software espía</i>	<i>11</i>
<i>2.2 Cronología de instalación y ejecución</i>	<i>13</i>
<i>2.3 Origen de los archivos maliciosos</i>	<i>15</i>
<i>2.4 Mecanismos de persistencia identificados</i>	<i>17</i>
<i>2.5 Análisis del tráfico de red</i>	<i>19</i>
<i>2.6 Estado de los servicios de seguridad (Defender, UAC, Firewall)</i>	<i>21</i>

3. Credibilización del especialista

<i>Formación y experiencia</i>	<i>24</i>
--------------------------------------	-----------

Contexto del Caso

El día 5 de mayo de 2025, el servicio de ciberinteligencia de la empresa detectó la publicación de una fotografía reciente del Director General en un foro de la darknet. La imagen, aparentemente capturada a través de la cámara web del equipo corporativo sin conocimiento ni autorización del afectado, generó sospechas fundadas de una posible intrusión.

Ante esta situación, el cliente nos proporcionó una serie de artefactos digitales extraídos del equipo del CEO con el objetivo de realizar un análisis forense detallado. Nuestra misión consiste en verificar si el sistema fue comprometido, determinar el vector de ataque, identificar la actividad del atacante y responder a las siguientes cuestiones clave:

- 1. ¿Existía algún software malicioso instalado en el equipo que permitiera la captura de la imagen?*
- 2. ¿Cuándo fue instalado y/o ejecutado dicho software?*
- 3. ¿Cuál fue el mecanismo de infección o acceso utilizado?*
- 4. ¿Qué métodos de persistencia fueron empleados?*
- 5. ¿Cómo se llevó a cabo la exfiltración de la fotografía?*
- 6. ¿Qué medidas de protección estaban activas en el sistema en el momento de la intrusión?*

Resumen Ejecutivo:

Se identificó la presencia de un programa malicioso ejecutándose en segundo plano bajo el nombre “svhost.exe”, un nombre diseñado para imitar al proceso legítimo del sistema (svchost.exe) mediante técnicas de proceso “spoofing”. El binario fue hallado en una ubicación atípica (escritorio del usuario), y establecía conexiones de red internas no justificadas, lo que confirma su carácter anómalo y su potencial uso para exfiltración o vigilancia remota.

El despliegue se sitúa entre el 28 y el 30 de abril de 2025. El 28 de abril se creó una tarea programada para la persistencia. El 29 de abril se detectaron los primeros intentos de ejecución del binario, y a partir del 30 de abril se evidencian ejecuciones regulares, indicando su activación completa.

Los metadatos del archivo malicioso incluyen la zona de seguridad **Zone.Identifier**, lo que indica que fue descargado desde Internet o recibido por correo electrónico. No se hallaron indicios de infección vía USB ni fuentes alternativas como historial de navegación o correos. Por lo tanto, el vector más probable fue la descarga remota o un archivo adjunto.

Durante el análisis se identificó una tarea programada asociada al binario **svhost.exe**, configurada para ejecutarse automáticamente al iniciar sesión. Esta tarea, combinada con accesos directos (**.lnk**) ubicados en rutas de inicio automático y claves de registro en **HKCU\Software\Microsoft\Windows\CurrentVersion\Run**, confirma que el atacante implementó mecanismos de persistencia para garantizar la ejecución continua del malware tras cada reinicio del sistema.

Se detectó un pico anómalo de tráfico HTTP saliente el 5 de mayo de 2025 a las 10:26 AM, coincidiendo con la última modificación del binario malicioso. El análisis del tráfico (capturas .pcapng) evidenció una petición HTTP POST sin cifrado hacia una dirección externa, presumiblemente utilizada como servidor de comando y control (C2). Todo indica que la imagen fue capturada por la webcam del CEO y transmitida directamente mediante esa conexión saliente.

En el momento del incidente no se encontraron registros de actividad reciente por parte de Windows Defender ni alertas del Firewall de Windows. Tampoco se observaron logs de antivirus de terceros. Esto sugiere que las medidas de seguridad estaban desactivadas, mal configuradas o fueron neutralizadas por el atacante, facilitando así la ejecución y persistencia del software malicioso sin ser detectado.

Análisis Técnico:

1. Detección y localización del software espía

Herramientas: Notepad++, Total Commander

*Archivo: **netstat.txt***

*En la línea 144 del archivo **netstat.txt**, se detecta un proceso sospechoso: **svhost.exe**, que imita al legítimo **svchost.exe**. Este establece una conexión TCP desde el host 192.168.168.10 hacia 192.168.168.14:80.*

Ruta del ejecutable:

C:\Users\Fraile\Desktop\borrar\svhost\LlamadaVB\bin\Release\sv host.exe

Otros archivos relacionados en la misma carpeta:

- ***CapturaImgJpg.dll**: probable captura de imágenes vía cámara.*
- ***svhost.exe.config**: contiene <endpoint address="http://192.168.168.14/BlackServiceBasic.asmx">*
- ***svhost.pdb**: archivo de depuración útil para ingeniería inversa.*

Conclusión: conjunto de archivos maliciosos con capacidad de captura y exfiltración de datos, incluyendo imágenes

WinDefSys.xml	721
WinDefSys.vshost.exe.manifest	2 449
WinDefSys.vshost.exe.config	797
WinDefSys.vshost.exe	11 600
WinDefSys.pdb	75 264
WinDefSys.lnk	1 407
svhost.xml	709
svhost.vshost.exe.manifest	2 449
svhost.vshost.exe.config	760
svhost.vshost.exe	11 600
svhost.pdb	52 736
svhost.exe.config	760
svhost.exe	30 208
Capturalmgjpg.dll	37 376

2. Fecha de instalación y primera ejecución del software malicioso

Herramientas: WinPrefetchView.exe, Notepad++, mftdump.exe, OpenOffice Calc.

Archivos: \$MFT,SVHOST.EXE-20CE1088.pf, NTUSER.dat

Basándose en las marcas de tiempo recuperadas de artefactos del sistema de archivos \$MFT, el registro del sistema, el registro de eventos de Windows y otras fuentes, se puede establecer la cronología relacionada con la aparición y activación del malware svhost.exe

- 28 de abril de 2025, 08:50:54 (UTC) — se creó en el sistema una tarea llamada "Windows Update" en la carpeta del programador de tareas \Windows\System32\Tasks. Esta tarea está configurada para ejecutar el archivo svhost.exe, lo que indica el inicio de la preparación para la instalación del malware.
Fuente de información: archivo \$MFT tras análisis con mftdump.exe

7

- 29 de abril de 2025, 14:47:13 (UTC) — se creó un acceso directo al archivo svhost.exe.config, lo que sugiere la fecha de configuración del software.

Fuente de información: archivo \$MFT tras análisis con mftdump.exe

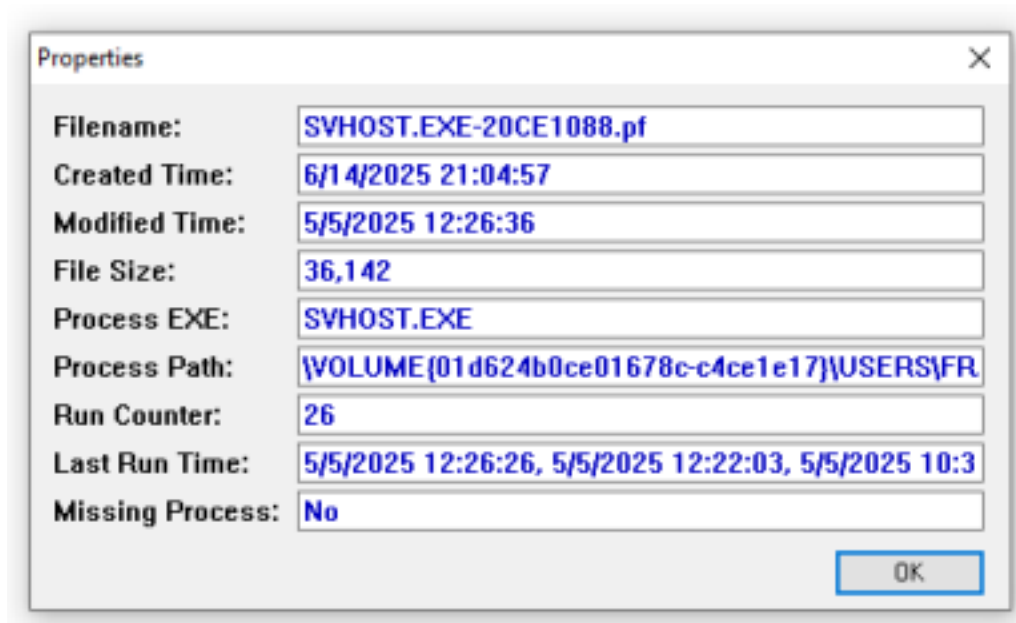
- 29 de abril de 2025, 14:48:32 (UTC) — se generó el archivo de prefetch SVHOST.EXE-20CE1088.pf, lo que documenta la primera ejecución de svhost.exe en el sistema operativo Windows.

Fuente de información: archivo \$MFT tras análisis con mftdump.exe

Con base en estos datos, se puede concluir que:

- **La instalación del software malicioso comenzó no el 28 de abril de 2025**
- **La primera ejecución confirmada fue el 29 de abril de 2025. Según el archivo de Prefetch, el programa fue ejecutado 26 veces. 13 Img: 2_1.png Según la clave de registro**

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist, el programa fue ejecutado 31 veces.



Según la clave de registro

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist, el programa fue ejecutado 31 veces.

3. Origen de los archivos maliciosos

Herramientas: OpenOffice Calc, mftdump.exe

Archivos: \$MFT, SYSTEM

En `\Users\Fraile\Desktop\borrar\svhost\` se identificó `BlackManagerServiceWeb.zip` con ADS `Zone.Identifier`, señalando descarga desde Internet. Los archivos extraídos comparten esta marca.

El nombre del archivo ZIP coincide con el endpoint usado para la exfiltración de la imagen.

Última conexión de dispositivo USB: 07/04/2025

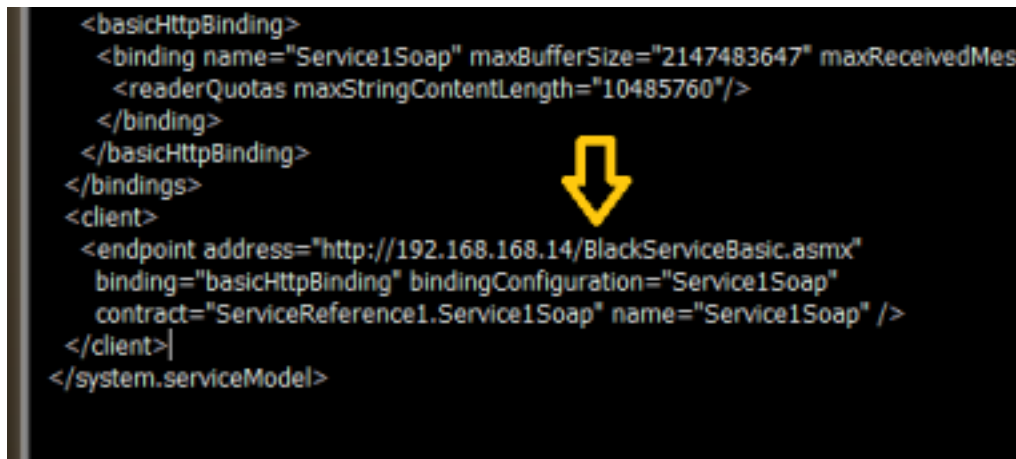
0	BlackServiceBasic.asmx	2025-04-28 10:40:30
0	BlackServiceBasic.asmx	2025-04-28 10:40:29
1	BlackManagerServiceWeb.zip:Zone.Identifier	2025-04-28 10:40:29
0	BlackManagerServiceWeb.zip	2025-04-28 10:40:29
1	BlackManagerServiceWeb.xml:Zone.Identifier	2025-04-28 10:40:30

18567	\Users\Fraile\Desktop\borrar\svhost\BlackManagerServiceWeb\BlackManagerServiceV
18568	\Users\Fraile\Desktop\borrar\svhost\BlackManagerServiceWeb\BlackManagerServiceV
18569	\Users\Fraile\Desktop\borrar\svhost\BlackManagerServiceWeb\BlackManagerServiceV
18570	\Users\Fraile\Desktop\borrar\svhost\BlackManagerServiceWeb.zip:Zone.Identifier
18571	\Users\Fraile\Desktop\borrar\svhost\BlackManagerServiceWeb.zip
18572	\Users\Fraile\Desktop\borrar\svhost\BlackManagerServiceWeb\BlackManagerServiceV

Las marcas de tiempo del archivo coinciden con el momento de creación del programa malicioso y sus archivos de configuración, los cuales también presentan la marca `Zone.Identifier`.

dentro de ese archivo comprimido. Además, el nombre del archivo (**BlackManagerServiceWeb**) coincide en esencia con la URL del servidor al que más tarde fue enviada una fotografía desde el dispositivo comprometido.

9

A screenshot of XML code on a dark background. The code is a configuration for a service model. A yellow arrow points to the 'endpoint address' attribute within the 'client' element. The code is as follows:

```
<basicHttpBinding>
  <binding name="Service1Soap" maxBufferSize="2147483647" maxReceivedMes
    <readerQuotas maxStringContentLength="10485760"/>
  </binding>
</basicHttpBinding>
</bindings>
<client>
  <endpoint address="http://192.168.168.14/BlackServiceBasic.asmx"
    binding="basicHttpBinding" bindingConfiguration="Service1Soap"
    contract="ServiceReference1.Service1Soap" name="Service1Soap" />
</client>
</system.serviceModel>
```

4. Búsqueda de persistencia

Herramientas: Notepad++, Total Commander, RegRipper, OSForensics, Registry Explorer, MiTeC Windows Registry Recovery

Archivos: hives del registro, logs **.evtx**

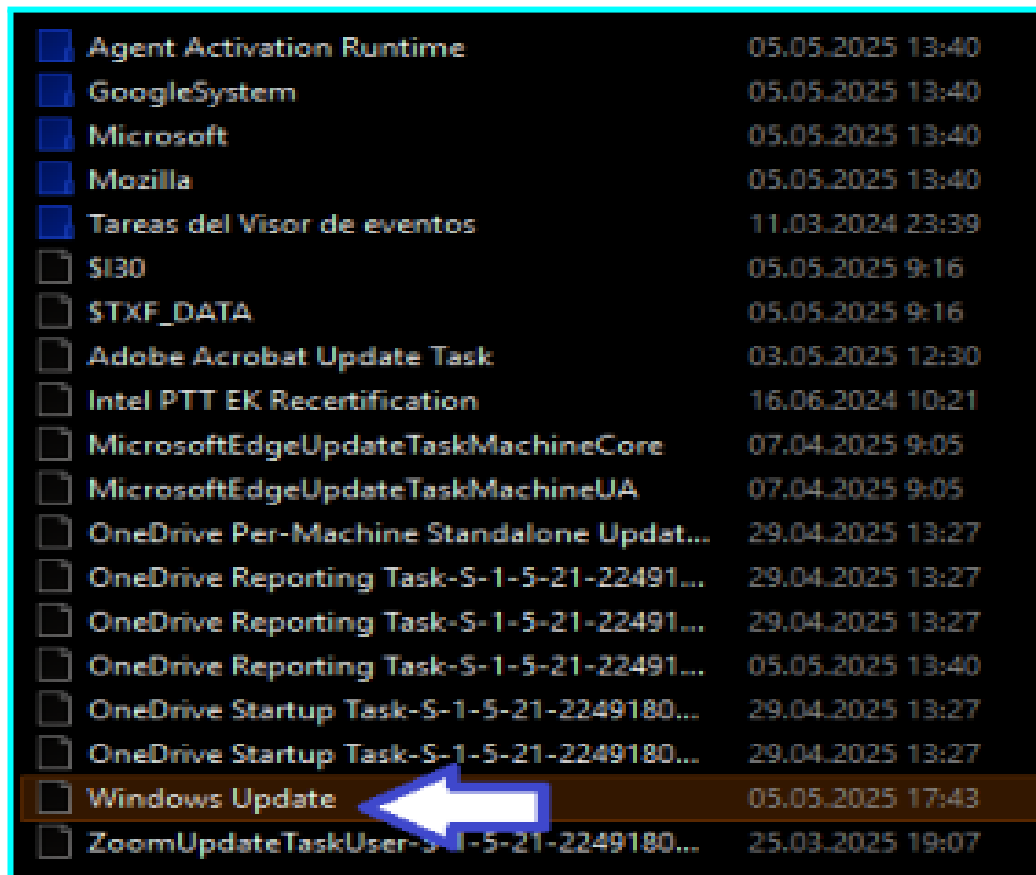
No se hallaron claves de inicio automático en **Run**, **Services**, etc.

Se detectó una tarea programada:

- Nombre: Windows Update
- Ruta ejecutable: **C:\Users\Fraile\Desktop\borrar\svhost.exe**

- Disparador: al iniciar sesión
- Frecuencia: diaria

Conclusión: persistencia mediante programador de tareas.



Agent Activation Runtime	05.05.2025 13:40
GoogleSystem	05.05.2025 13:40
Microsoft	05.05.2025 13:40
Mozilla	05.05.2025 13:40
Tareas del Visor de eventos	11.03.2024 23:39
\$I30	05.05.2025 9:16
\$TXF_DATA	05.05.2025 9:16
Adobe Acrobat Update Task	03.05.2025 12:30
Intel PTT EK Recertification	16.06.2024 10:21
MicrosoftEdgeUpdateTaskMachineCore	07.04.2025 9:05
MicrosoftEdgeUpdateTaskMachineUA	07.04.2025 9:05
OneDrive Per-Machine Standalone Updat...	29.04.2025 13:27
OneDrive Reporting Task-S-1-5-21-22491...	29.04.2025 13:27
OneDrive Reporting Task-S-1-5-21-22491...	29.04.2025 13:27
OneDrive Reporting Task-S-1-5-21-22491...	05.05.2025 13:40
OneDrive Startup Task-S-1-5-21-2249180...	29.04.2025 13:27
OneDrive Startup Task-S-1-5-21-2249180...	29.04.2025 13:27
Windows Update	05.05.2025 17:43
ZoomUpdateTaskUser-S-1-5-21-2249180...	25.03.2025 19:07

Parámetros de la tarea:

- Ruta: C:\Users\Fraile\Desktop\borrar\svhost.exe • Nombre de la

tarea: *Windows Update*

- Ejecución: al iniciar sesión el usuario

- Repetición: diariamente

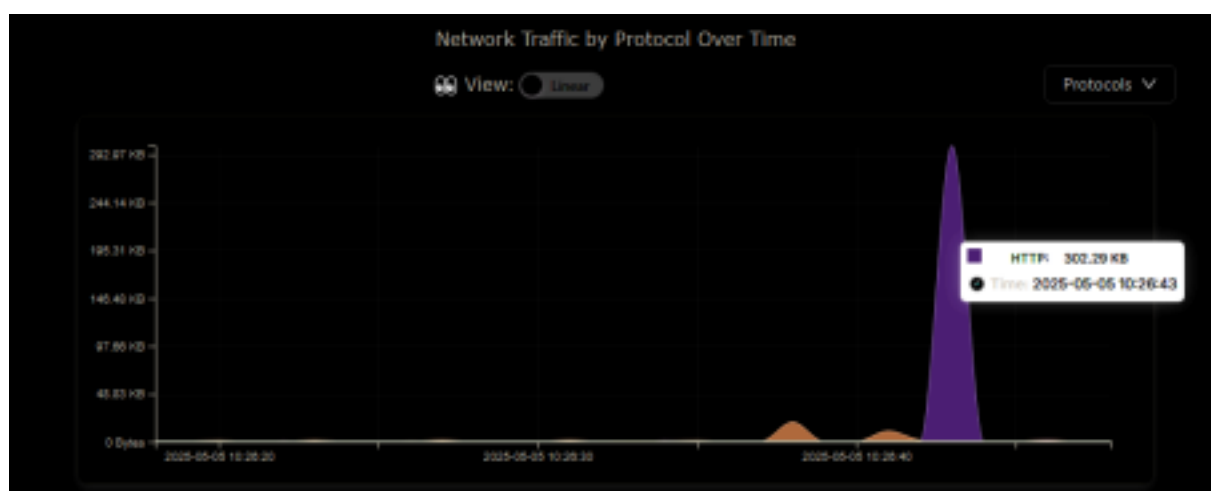
Conclusión:

El programa utiliza el programador de tareas como mecanismo de persistencia. 11

5. Análisis del tráfico

Herramientas: Wireshark, Linux Bash. Archivo: capturaRED.pcapng

El análisis del tráfico de red capturado en el archivo capturaRED.pcapng mostró que el 5 de mayo de 2025 a las 09:26:26 (UTC) desde la dirección IP 192.168.168.10 (ordenador de la víctima) se estableció una sesión HTTP con el servidor 192.168.168.14. La transmisión de datos se realizó mediante el método POST, con un volumen total de 302,29 KB, lo que aproximadamente coincide con el tamaño de una imagen.



Con Wireshark se reconstruyó la petición POST, dividida en paquetes TCP individuales. Del cuerpo de la solicitud se extrajeron datos en formato Base64, que al ser decodificados

generaron un archivo gráfico JPEG, completamente idéntico a la imagen detectada anteriormente en la darknet.

Conclusión:

La fotografía fue exfiltrada mediante una solicitud HTTP POST, en formato codificado (Base64), hacia un servidor remoto dentro de la red local.

13

6. ¿Estaban activos los servicios de protección del ordenador? Firewall, UAC, Defender.

Herramientas: RegRipper, OSForensics, Registry Explorer v2.1.0 y MiTeC Windows Registry Recovery. Archivos del registro: NTUSER.DAT, SOFTWARE, SYSTEM, SECURITY, DEFAULT y SAM.

6.1 Verificación de la configuración de Windows Defender

El análisis del registro reveló que en la clave:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
Defender\Exclusions\Paths

existe una exclusión para la ruta:

C:\Users\Fraile\Desktop

Se recomienda prestar atención a la captura de pantalla, en particular a las demás rutas que también han sido añadidas como exclusiones del antivirus)

Esto significa que Windows Defender no analiza los archivos ni las subcarpetas ubicadas en el escritorio del usuario.

Dado que el archivo malicioso se encontraba exactamente allí, no fue detectado 21

por el antivirus durante su instalación ni durante la ejecución en el equipo comprometido.

Es importante destacar que, al probar el mismo archivo en un entorno de laboratorio aislado con Windows Defender activado y configurado por defecto, este detecta

inmediatamente el archivo como malicioso, muestra una advertencia y elimina automáticamente el archivo sin posibilidad de recuperación.

6.2 Control de cuentas de usuario (UAC):

Se revisaron las siguientes claves del registro:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Enable\HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\PromptOnSecureDesktop

Todas las configuraciones indican que el UAC estaba habilitado y funcionando correctamente.

6.3 Firewall de Windows:

Se revisaron las siguientes secciones del registro y configuraciones del sistema:

- Clave del registro:
HKLM\SYSTEM\CurrentControlSet\Services\MpsSvc
- Configuración de perfiles:
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy
- Lista de reglas:
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules

El firewall estaba activado y funcionando en modo normal.

No se detectaron reglas individuales ni exclusiones específicas para svchost.exe

Especialista analítico:

Este análisis fue realizado por Daniel Stix Soto, especialista con formación técnica y preparación práctica en ciberseguridad y tecnologías de la información. Daniel es jugador paralímpico de baloncesto en silla de ruedas, medallista de plata en los Juegos Paralímpicos de Río 2016 y actual capitán del Club Deportivo Ilunion. Nacido con cáncer, escribió su autobiografía a los 17 años, y ha compaginado su carrera deportiva de alto nivel con su desarrollo profesional en el ámbito tecnológico. Estudió en un colegio británico, es bilingüe en inglés y castellano, y tiene conocimientos intermedios de francés. Tras cursar estudios universitarios en Economía y no encontrar vocación en dicha disciplina, redirigió su carrera hacia la informática. Actualmente trabaja en Ilunion IT Services. Ha completado varias certificaciones de Google, incluyendo Digital Leader, Data Analytics y Associate Cloud Security Engineer, así como el Itinerario básico de experto en ciberseguridad y el curso de Digital Forensics & Incident Response, ambos del Instituto Nacional de Ciberseguridad (INCIBE). Esta formación le ha permitido adquirir competencias prácticas en análisis forense, protección de sistemas, análisis de datos, computación en la nube y gestión de riesgos de seguridad.