PROYECTO FIN DE CURSO

Análisis Forense de un Incidente de Seguridad

Investigación de conexión no autorizada

REALIZADO POR:

/ Juan Carlos Vico / Ignacio Camacho / Luis Delgado /Jesica Julia Olortegui / Joan Navinés /

ÍNDICE

INFORME PERICIAL DE CIBERSEGURIDAD

Número de Expediente: 170625
Juzgado/Cliente: Cayetano de Juan
Perito: CyberSherlock SL
Fecha: 17/6/2025

DECLARACIÓN DE CONFORMIDAD

Los peritos firmantes del presente informe manifiestan que el contenido del mismo ha sido elaborado con rigor técnico y conforme a los principios de objetividad, imparcialidad y veracidad exigidos legalmente.

La elaboración de este informe pericial se ha realizado conforme a lo establecido en los **Artículos 335 a 339 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil**, y en particular en cumplimiento del **Artículo 335.2**, en el que se exige que los peritos actúen con la máxima objetividad posible, considerando tanto lo que pueda favorecer como perjudicar a cualquiera de las partes.

Asimismo, se declara que la metodología aplicada se ha basado en estándares reconocidos, tales como:

- **UNE 197010:2015**, sobre criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC).
- **UNE 71506:2013**, relativa a la metodología para el análisis forense de evidencias electrónicas.
- **ISO/IEC 27037**, referente a las directrices para la identificación, recogida, adquisición y preservación de evidencias digitales.

En los casos en que la investigación haya implicado el análisis de incidentes relacionados con el acceso o tratamiento de datos personales, se ha observado lo dispuesto en la **Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)** y el **Reglamento (UE) 2016/679 (RGPD)**.

Asimismo, si la entidad afectada por el incidente pertenece al sector público, se han tenido en cuenta los principios y medidas establecidos en el **Esquema Nacional de Seguridad (ENS)**, conforme al **Real Decreto 311/2022, de 3 de mayo**.

En caso de haberse detectado conductas que pudieran constituir delito, como el acceso ilegítimo a sistemas o datos, se han considerado las previsiones del **Artículo 197 ter del Código Penal español**.

Finalmente, los peritos declaran que este informe representa fielmente las evidencias obtenidas y los análisis realizados, actuando en todo momento conforme a su leal saber y entender, y conscientes de las responsabilidades legales que asumirían en caso de falsedad o parcialidad.

ESTRUCTURA Y FINALIDAD DEL INFORME

Este informe se ha elaborado con el objetivo de facilitar una comprensión clara y progresiva del incidente de ciberseguridad analizado.

En primer lugar, se presenta un Informe Ejecutivo, redactado de forma sencilla y accesible, para que pueda ser entendido por personas sin formación técnica.

A continuación, se incorpora un Informe Técnico Pericial, más detallado, donde se exponen los aspectos informáticos y las evidencias recopiladas, dirigido a un público con conocimientos técnicos especializados.

INFORME EJECUTIVO

Explicación Simplificada del Incidente de Ciberseguridad

El presente apartado tiene como objetivo explicar de manera clara y concisa el incidente de ciberseguridad detectado y analizado, facilitando su comprensión a personas sin conocimientos técnicos especializados.

1. Detección de la Anomalía:

El incidente se originó a partir de la detección de una **conexión no autorizada** desde un equipo corporativo de la empresa hacia una dirección IP externa perteneciente a **spyrix.net** y localizada en **Montreal, Canadá**. Esta conexión anómala fue observada aproximadamente el **17 de septiembre de 2020**.

2. Identificación del Software Malicioso:

La investigación forense determinó que la conexión era generada por un **software malicioso clasificado como "keylogger"**.

Este tipo de software tiene la capacidad de **capturar todas las pulsaciones de teclado (keystrokes)** realizadas en el equipo, así como de **realizar grabaciones de la pantalla (monitor)**.

Su funcionalidad principal es la **extracción de información sensible**, incluyendo nombres de usuario, contraseñas, y comunicaciones privadas.

La información recolectada es posteriormente **enviada a un servidor remoto**, donde la IP es identificada como **spyrix.net** en su servidor de Montreal.

Se identificó un programa en los datos analizados: **Spyrix Free Keylogger**

3. Cronología y Autoría de la Instalación:

La instalación del programa malicioso **Spyrix Free Keylogger** se produjo el **16 de septiembre de 2020** alrededor de las **11:18**

El usuario responsable de la instalación fue identificado como **"UsuarioMalo"**.

4. Método de Instalación (Escalada de Privilegios):

A pesar de que la política de la empresa **prohíbe la instalación de software por parte de los usuarios**, "UsuarioMalo" logró instalar el keylogger.

Esto se realizó mediante:

- La ejecución de un **software diseñado para la escalada de privilegios** dentro del sistema operativo.
- Se identificó el uso de un ejecutable que explota una **vulnerabilidad en el sistema para efectuar una Elevación de Privilegios**.
- Esta acción fue posible debido a que los equipos **no estaban actualizados con los últimos parches de seguridad**.
- Una vez efectuada la escalada, "UsuarioMalo" obtuvo **permisos de administrador**, lo que le permitió instalar el software no autorizado.

5. Vector de Infección (Origen del Programa):

El programa malicioso llegó al equipo principalmente a través de:

Descarga directa: "UsuarioMalo" realizó búsquedas en internet para encontrar herramientas de escalada de privilegios y el keylogger, descargando un archivo comprimido (software.rar) que contenía el keylogger desde la plataforma Mega.

Conclusión del Incidente: Se confirma la **instalación no autorizada de un keylogger** en un equipo corporativo, lo que permitió la **potencial exfiltración de información confidencial** de la empresa. Este incidente fue consecuencia directa de la **acción de un usuario (UsuarioMalo)**, quien explotó **vulnerabilidades existentes en el sistema operativo** (falta de actualizaciones) y las aprovechó para instalar el software malicioso.

INFORME TÉCNICO PERICIAL

1. Objeto del Informe

La presente investigación forense fue solicitada en torno al **día 17/9/2020** por el cliente Alex P, Quim M y Cayetano DJ, debido a sospechas de la existencia de software malicioso en un equipo corporativo. Se detectó una conexión desde este equipo a una IP que no se corresponde con ningún servicio legítimo, en concreto la **158.69.117.119**.

El objeto del presente informe pericial es determinar los siguientes puntos:

1.1. Existencia de software malicioso (malware) y qué programa ha realizado la conexión a la IP sospechosa.

1.2. Fecha y autoría de la instalación del programa, es decir, desde cuándo lleva el programa en la máquina.

1.3. Vector de infección y posibles vulnerabilidades explotadas, incluyendo cómo llegó al equipo el programa y cómo fue instalado, considerando la política de empresa que prohíbe a los usuarios instalar software.

1.4. Justificación de las respuestas con las evidencias obtenidas.

2. Metodología

Para la realización de esta investigación forense, se procedió a realizar una **adquisición en caliente de la máquina comprometida** mediante la herramienta **BrimorLabs**. Esta adquisición proporcionó una serie de evidencias sobre las que trabajar y analizar. Las conclusiones están respaldadas por las herramientas usadas, los comandos ejecutados y las pruebas documentadas, como capturas de pantalla.

Las herramientas y estándares utilizados incluyen:

Análisis forense digital:

Extracción segura de logs y análisis del sistema de archivos con **FTK Imager**, específicamente para volcar información del archivo **$MFT** en formato legible como '.csv'.

Análisis de información detallada del sistema obtenida de **WinAudit.html**.

Análisis de conexiones de red y procesos mediante **netstat_anb_results.txt**, **TCPView.txt** y **cports.html**.

Análisis de procesos y archivos ejecutables relacionados con el programa malicioso a través de **PrcView_extended** y la carpeta **prefetch (Winprefetch)**.

Lectura de bases de datos para analizar el historial de navegación de Chrome, utilizando **DB Browser for SQLite**.

Detección de malware (implícito en la identificación de Spyrix Free Keylogger).

Fuentes de datos:

Logs de eventos de Windows (Event Viewer).

Historial de descargas y ejecutables en rutas de usuario (C:\Users\[Usuario]\AppData, y la carpeta de historial de Chrome).

Archivo **$MFT** para el histórico de registro maestro de archivos y carpetas.

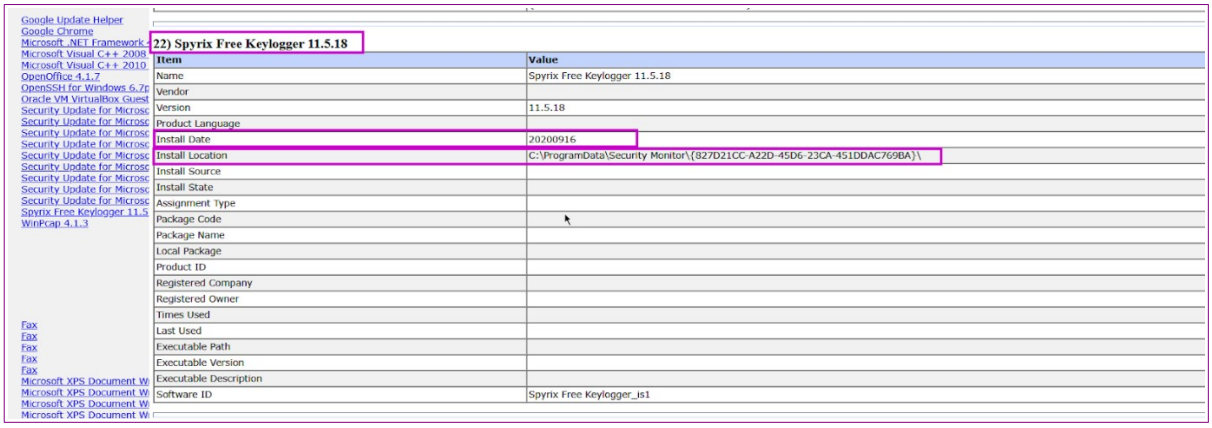
3. Hallazgos

3.1. Existencia de software malicioso

Se identificó la presencia de un software malicioso en el equipo corporativo: **Spyrix Free Keylogger**. Este programa puede ser usado de forma maliciosa para capturar pulsaciones del teclado y grabaciones del monitor, extrayendo información sensible como usuarios, contraseñas y conversaciones privadas.

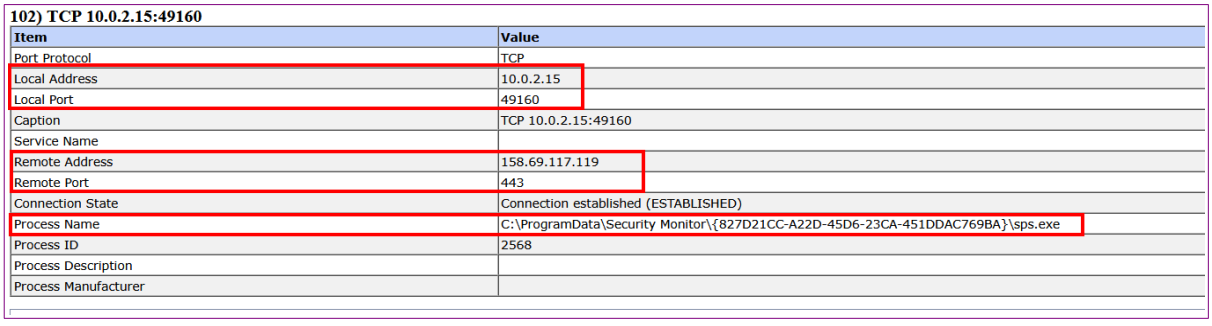
Las evidencias que confirman su existencia y actividad son:

Conexión a IP maliciosa: El archivo **WinAudit.html** proporcionó información clave del equipo, incluyendo la IP Local por el puerto 49160 y su conexión a la **IP maliciosa 158.69.117.119.443 por el puerto 443**.



22) Spyrix Free Keylogger 11.5.18

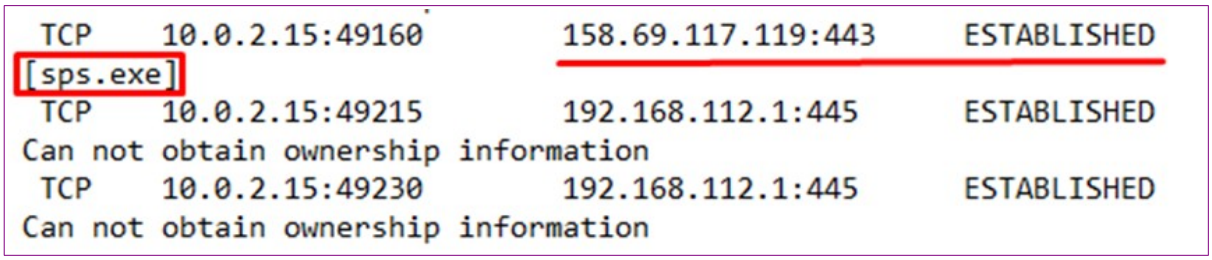
Item	Value
Name	Spyrix Free Keylogger 11.5.18
Vendor	
Version	11.5.18
Product Language	
Install Date	20200916
Install Location	C:\ProgramData\Security Monitor\{827D21CC-A22D-45D6-23CA-451DDAC769BA}\
Install Source	
Install State	
Assignment Type	
Package Code	
Package Name	
Local Package	
Product ID	
Registered Company	
Registered Owner	
Times Used	
Last Used	
Executable Path	
Executable Version	
Executable Description	
Software ID	Spyrix Free Keylogger_is1



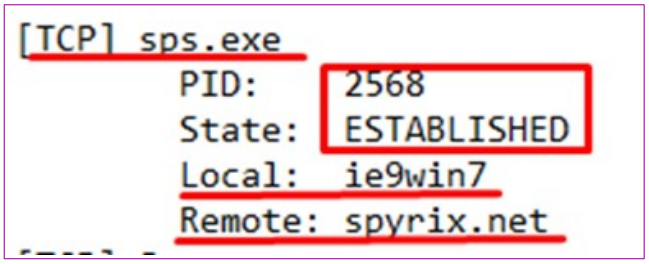
102) TCP 10.0.2.15:49160

Item	Value
Port Protocol	TCP
Local Address	10.0.2.15
Local Port	49160
Caption	TCP 10.0.2.15:49160
Service Name	
Remote Address	158.69.117.119
Remote Port	443
Connection State	Connection established (ESTABLISHED)
Process Name	C:\ProgramData\Security Monitor\{827D21CC-A22D-45D6-23CA-451DDAC769BA}\sps.exe
Process ID	2568
Process Description	
Process Manufacturer	

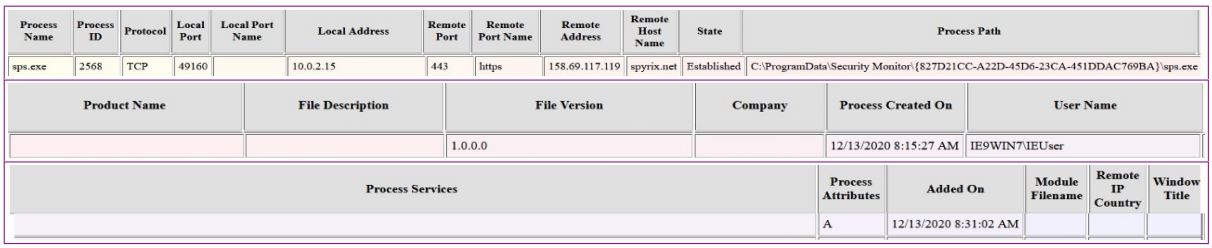
Proceso ejecutor: En el fichero **netstat_anb_results.txt** se encontró una conexión TCP establecida entre la IP local 10.0.2.15:49160 y la IP maliciosa 158.69.117.119.443, ejecutada mediante **sps.exe**.



Detalles del proceso: El archivo **TCPView.txt** confirmó la conexión y proporcionó el **PID del proceso: 2568**, el usuario local: **ie9win7**, y el usuario remoto: **spyrix.net**.



Confirmación de conexión HTTPS: El documento **cports.html** confirmó que, mediante el protocolo TCP, desde la IP 10.0.2.15 en el puerto 49160 se realiza una conexión **HTTPS a la IP maliciosa 158.69.117.119**, es decir, al servidor del Keylogger Spyrix.



Process Name	Process ID	Protocol	Local Port	Local Port Name	Local Address	Remote Port	Remote Port Name	Remote Address	Remote Host Name	State	Process Path
sps.exe	2568	TCP	49160		10.0.2.15	443	https	158.69.117.119	spyrix.net	Established	C:\ProgramData\Security Monitor\{827D21CC-A22D-45D6-23CA-451DDAC769BA}\sps.exe

Product Name	File Description	File Version	Company	Process Created On	User Name
		1.0.0.0		12/13/2020 8:15:27 AM	IE9WIN7\IEUser

Process Services	Process Attributes	Added On	Module Filename	Remote IP Country	Window Title
	A	12/13/2020 8:31:02 AM			

Archivos relacionados: En el documento **PrcView_extended** se observaron tres archivos .exe que comparten el mismo **GUID (spkl.exe, spmm.exe y sps.exe)**, confirmándose que son componentes o módulos de la misma aplicación, asociada con el programa **"Security Monitor"**.

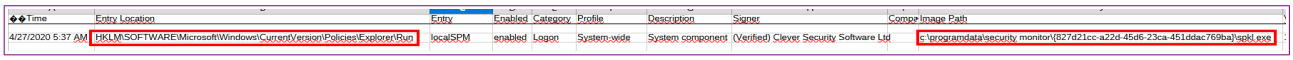
PrcView_extended.txt: Bloc de notas

Archivo Edición Formato Ver Ayuda

PROCESS	PID	PRIO	PATH
Dwm.exe	1240	Normal	C:\Windows\system32\Dwm.exe
Explorer.EXE	1256	Normal	C:\Windows\Explorer.EXE
taskhost.exe	1372	Normal	C:\Windows\system32\taskhost.exe
spkl.exe	1680	Normal	C:\ProgramData\Security Monitor\{827D21CC-A22D-45D6-23CA-451DDAC769BA}\spkl.exe
VBoxTray.exe	1696	Normal	C:\Windows\System32\VBoxTray.exe
cygrunsrv.exe	1888	Normal	C:\Program Files\OpenSSH\bin\cygrunsrv.exe
conhost.exe	896	Normal	C:\Windows\system32\conhost.exe
sshd.exe	960	Normal	C:\Program Files\OpenSSH\usr\sbin\sshd.exe
spmm.exe	2492	Normal	C:\ProgramData\Security Monitor\{827D21CC-A22D-45D6-23CA-451DDAC769BA}\spmm.exe
sps.exe	2568	Normal	C:\ProgramData\Security Monitor\{827D21CC-A22D-45D6-23CA-451DDAC769BA}\sps.exe
cmd.exe	2028	Normal	C:\Windows\system32\cmd.exe
conhost.exe	348	Normal	C:\Windows\system32\conhost.exe
cmd.exe	3384	Normal	C:\Windows\system32\cmd.exe
conhost.exe	3740	Normal	C:\Windows\system32\conhost.exe
rundll32.exe	352	Normal	C:\Windows\System32\rundll32.exe
RunDll32.exe	276	Normal	C:\Windows\system32\RunDll32.exe
pv.exe	1436	Normal	\\192.168.112.1\compartida\WINDOW~1\Tools\PrcView\pv.exe

Evidencia de ejecución: La carpeta **prefetch** contiene registros de cómo se han ejecutado los .exe relacionados directamente con el keylogger, incluyendo la fecha y hora de ejecución.

SourceCreated	SourceModified	SourceAccessed	ExecutableName	Hash	Size	Version	RunCount	LastRun
23/05/2025 11:57	13/12/2020 16:26	02/06/2025 15:45	SPKL.EXE	6B8A4D88	58488	Windows Vista or W	2	16/09/2020 11:22
23/05/2025 11:57	13/12/2020 16:26	02/06/2025 15:45	SPMM.EXE	49C4EA87	24674	Windows Vista or W	2	16/09/2020 11:22
23/05/2025 11:57	13/12/2020 16:26	02/06/2025 15:45	SPS.EXE	2FED94	44184	Windows Vista or W	2	16/09/2020 11:22



Para remarcar la persistencia del keylogger, en la siguiente imagen vemos como está instalado el archivo 'spkl.exe'en la ruta: 'HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run **la cual es usada para ejecutar programas automáticamente en cada arranque del sistema.**

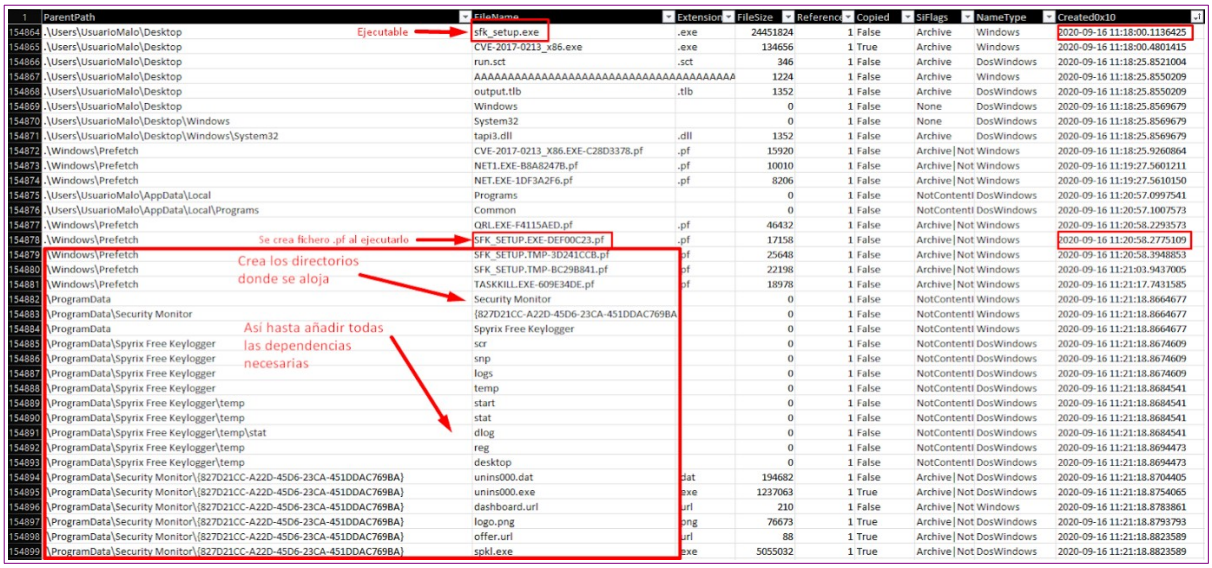
3.2. Fecha y autoría de la instalación

Para determinar la fecha de instalación, se analizó el archivo **$MFT** utilizando **FTK Imager**. Mediante el histórico de registro maestro de todos los archivos y carpetas en la partición NTFS, se pudo establecer el orden de creación/ejecución de los ficheros.

Fecha de llegada e instalación: Se determinó que el programa malicioso **sfk_setup.exe**, que es el ejecutable de instalación de Spyrix Free Keylogger (verificado mediante prueba de concepto), llegó al sistema el **día 16/9/2020 sobre las 11:18.**

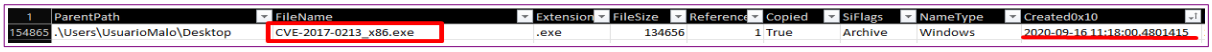
ParentPath	FileName	Extension	FileSize	Reference	Copied	SIFlags	NameType	Created0x10
.\Users\UsuarioMalo\Desktop	sfk_setup.exe	.exe	24451824	1	False	Archive	Windows	2020-09-16 11:18:00.1136425

Corroboración de instalación: El seguimiento del orden de instalación/ejecución en el **$MFT** confirma la creación de los ficheros y rutas donde se aloja y ejecuta el programa malicioso.



	ParentPath	FileName	Extension	FileSize	Reference	Copied	SiFlags	NameType	Created0x10
154864	.\Users\UsuarioMalo\Desktop	sfk_setup.exe	.exe	24451824	1	False	Archive	Windows	2020-09-16 11:18:00.1136425
154865	.\Users\UsuarioMalo\Desktop	CVE-2017-0213_x86.exe	.exe	134656	1	True	Archive	Windows	2020-09-16 11:18:00.4801415
154866	.\Users\UsuarioMalo\Desktop	run.sct	.sct	346	1	False	Archive	DosWindows	2020-09-16 11:18:25.8521004
154867	.\Users\UsuarioMalo\Desktop	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		1224	1	False	Archive	Windows	2020-09-16 11:18:25.8550209
154868	.\Users\UsuarioMalo\Desktop	output.tlb	.tlb	1352	1	False	Archive	DosWindows	2020-09-16 11:18:25.8550209
154869	.\Users\UsuarioMalo\Desktop	Windows		0	1	False	None	DosWindows	2020-09-16 11:18:25.8569679
154870	.\Users\UsuarioMalo\Desktop\Windows	System32		0	1	False	None	DosWindows	2020-09-16 11:18:25.8569679
154871	.\Users\UsuarioMalo\Desktop\Windows\System32	tapi3.dll	.dll	1352	1	False	Archive	DosWindows	2020-09-16 11:18:25.8569679
154872	.\Windows\Prefetch	CVE-2017-0213_X86.EXE-C28D3378.pf	.pf	15920	1	False	Archive|Not	Windows	2020-09-16 11:18:25.9260864
154873	.\Windows\Prefetch	NET1.EXE-B8A8247B.pf	.pf	10010	1	False	Archive|Not	Windows	2020-09-16 11:19:27.5601211
154874	.\Windows\Prefetch	NET.EXE-1DF3A2F6.pf	.pf	8206	1	False	Archive|Not	Windows	2020-09-16 11:19:27.5610150
154875	.\Users\UsuarioMalo\AppData\Local	Programs		0	1	False	NotContentI	DosWindows	2020-09-16 11:20:57.0997541
154876	.\Users\UsuarioMalo\AppData\Local\Programs	Common		0	1	False	NotContentI	DosWindows	2020-09-16 11:20:57.1007573
154877	.\Windows\Prefetch	QRL.EXE-F4115AED.pf	.pf	46432	1	False	Archive|Not	Windows	2020-09-16 11:20:58.2293573
154878	.\Windows\Prefetch	SFK_SETUP.EXE-DEF00C23.pf	.pf	17158	1	False	Archive|Not	Windows	2020-09-16 11:20:58.2775109
154879	.\Windows\Prefetch	SFK_SETUP.TMP-3D241CCB.pf	pf	25648	1	False	Archive|Not	Windows	2020-09-16 11:20:58.3948853
154880	.\Windows\Prefetch	SFK_SETUP.TMP-BC29B841.pf	pf	22198	1	False	Archive|Not	Windows	2020-09-16 11:21:03.9437005
154881	.\Windows\Prefetch	TASKKILL.EXE-609E34DE.pf	pf	18978	1	False	Archive|Not	Windows	2020-09-16 11:21:17.7431585
154882	.\ProgramData	Security Monitor		0	1	False	NotContentI	Windows	2020-09-16 11:21:18.8664677
154883	.\ProgramData\Security Monitor	{827D21CC-A22D-45D6-23CA-451DDAC769BA		0	1	False	NotContentI	Windows	2020-09-16 11:21:18.8664677
154884	.\ProgramData	Spyrix Free Keylogger		0	1	False	NotContentI	Windows	2020-09-16 11:21:18.8664677
154885	.\ProgramData\Spyrix Free Keylogger	scr		0	1	False	NotContentI	DosWindows	2020-09-16 11:21:18.8674609
154886	.\ProgramData\Spyrix Free Keylogger	snp		0	1	False	NotContentI	DosWindows	2020-09-16 11:21:18.8674609
154887	.\ProgramData\Spyrix Free Keylogger	logs		0	1	False	NotContentI	DosWindows	2020-09-16 11:21:18.8674609
154888	.\ProgramData\Spyrix Free Keylogger	temp		0	1	False	NotContentI	DosWindows	2020-09-16 11:21:18.8684541
154889	.\ProgramData\Spyrix Free Keylogger\temp	start		0	1	False	NotContentI	DosWindows	2020-09-16 11:21:18.8684541
154890	.\ProgramData\Spyrix Free Keylogger\temp	stat		0	1	False	NotContentI	DosWindows	2020-09-16 11:21:18.8684541
154891	.\ProgramData\Spyrix Free Keylogger\temp\stat	dlog		0	1	False	NotContentI	DosWindows	2020-09-16 11:21:18.8684541
154892	.\ProgramData\Spyrix Free Keylogger\temp	reg		0	1	False	NotContentI	DosWindows	2020-09-16 11:21:18.8694473
154893	.\ProgramData\Spyrix Free Keylogger\temp	desktop		0	1	False	NotContentI	DosWindows	2020-09-16 11:21:18.8694473
154894	.\ProgramData\Security Monitor\{827D21CC-A22D-45D6-23CA-451DDAC769BA}	unins000.dat	dat	194682	1	False	Archive|Not	DosWindows	2020-09-16 11:21:18.8704405
154895	.\ProgramData\Security Monitor\{827D21CC-A22D-45D6-23CA-451DDAC769BA}	unins000.exe	exe	1237063	1	True	Archive|Not	DosWindows	2020-09-16 11:21:18.8754065
154896	.\ProgramData\Security Monitor\{827D21CC-A22D-45D6-23CA-451DDAC769BA}	dashboard.url	url	210	1	False	Archive|Not	Windows	2020-09-16 11:21:18.8783861
154897	.\ProgramData\Security Monitor\{827D21CC-A22D-45D6-23CA-451DDAC769BA}	logo.png	png	76673	1	True	Archive|Not	DosWindows	2020-09-16 11:21:18.8793793
154898	.\ProgramData\Security Monitor\{827D21CC-A22D-45D6-23CA-451DDAC769BA}	offer.url	url	88	1	True	Archive|Not	DosWindows	2020-09-16 11:21:18.8823589
154899	.\ProgramData\Security Monitor\{827D21CC-A22D-45D6-23CA-451DDAC769BA}	spkl.exe	exe	5055032	1	True	Archive|Not	DosWindows	2020-09-16 11:21:18.8823589

Usuario ejecutor: Se ha podido determinar que el usuario **UsuarioMalo** estuvo implicado en la instalación, ya que realizó la escalada de privilegios necesaria para la instalación del software.

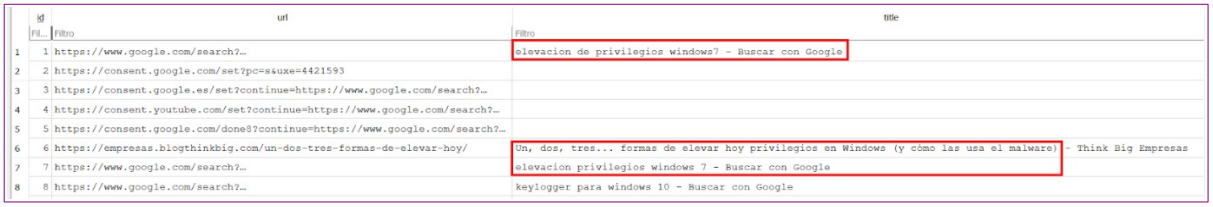


	ParentPath	FileName	Extension	FileSize	Reference	Copied	SiFlags	NameType	Created0x10
154865	.\Users\UsuarioMalo\Desktop	CVE-2017-0213_x86.exe	.exe	134656	1	True	Archive	Windows	2020-09-16 11:18:00.4801415

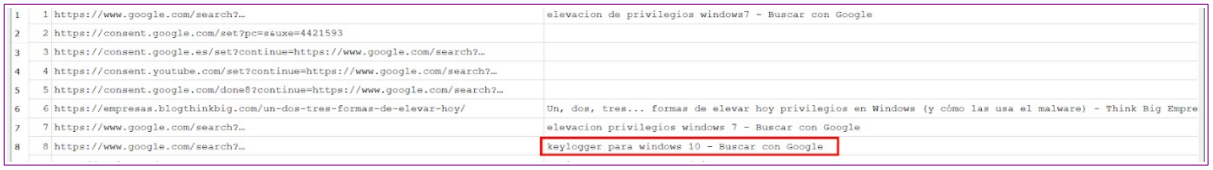
3.3. Vector de infección

El programa llegó al equipo a través de los siguientes pasos llevados a cabo por el usuario **UsuarioMalo**:

Búsquedas previas: El historial de Chrome del usuario **UsuarioMalo** muestra una serie de búsquedas en internet relacionadas con la realización de una escalada de privilegios y la búsqueda de una herramienta de keylogger. Para leer esta carpeta, se utilizó el programa **DB Browser for SQLite**.



	id	url	title
	Fil…	Filtro	Filtro
1	1	https://www.google.com/search?…	elevacion de privilegios windows7 - Buscar con Google
2	2	https://consent.google.com/set?pc=s&uxe=4421593	
3	3	https://consent.google.es/set?continue=https://www.google.com/search?…	
4	4	https://consent.youtube.com/set?continue=https://www.google.com/search?…	
5	5	https://consent.google.com/done8?continue=https://www.google.com/search?…	
6	6	https://empresas.blogthinkbig.com/un-dos-tres-formas-de-elevar-hoy/	Un, dos, tres... formas de elevar hoy privilegios en Windows (y cómo las usa el malware) - Think Big Empresas
7	7	https://www.google.com/search?…	elevacion privilegios windows 7 - Buscar con Google
8	8	https://www.google.com/search?…	keylogger para windows 10 - Buscar con Google



1	1	https://www.google.com/search?…	elevacion de privilegios windows7 - Buscar con Google
2	2	https://consent.google.com/set?pc=s&uxe=4421593	
3	3	https://consent.google.es/set?continue=https://www.google.com/search?…	
4	4	https://consent.youtube.com/set?continue=https://www.google.com/search?…	
5	5	https://consent.google.com/done8?continue=https://www.google.com/search?…	
6	6	https://empresas.blogthinkbig.com/un-dos-tres-formas-de-elevar-hoy/	Un, dos, tres... formas de elevar hoy privilegios en Windows (y cómo las usa el malware) - Think Big Empre
7	7	https://www.google.com/search?…	elevacion privilegios windows 7 - Buscar con Google
8	8	https://www.google.com/search?…	keylogger para windows 10 - Buscar con Google

Recepción del malware: El malware llegó al sistema a través de un **correo electrónico**. Este archivo estaba previamente alojado en los **servidores de Mega**.

Recibidos (26) - miguel.buyer@gmail.com - Gmail	1
Recibidos (26) - miguel.buyer@gmail.com - Gmail	1
Recibidos (26) - miguel.buyer@gmail.com - Gmail	1
Recibidos (26) - miguel.buyer@gmail.com - Gmail	2
Software - miguel.buyer@gmail.com - Gmail	1
	1

https://mega.nz/folder/D9hiHKyB#Ud3xsiAKz2BYHjTYjTrm2w
Google Chrome bloquea las descargas - Ayuda de Google Chrome

Descarga y ejecución: Acto seguido, en la carpeta de descargas, se encontraron los programas descargados, llamados **software.rar** y **COMPARTIDA.zip**, de los cuales salen el keylogger y el ejecutable de la escalada de privilegios **CVE-2017-0213_x86.exe.**

C:\Users\UsuarioMalo\Downloads\WinRAR Portable Unplugged.exe
C:\Users\UsuarioMalo\Downloads\software.rar
C:\Users\UsuarioMalo\Downloads\COMPARTIDA.zip
C:\Users\UsuarioMalo\Downloads\wrar591es.exe

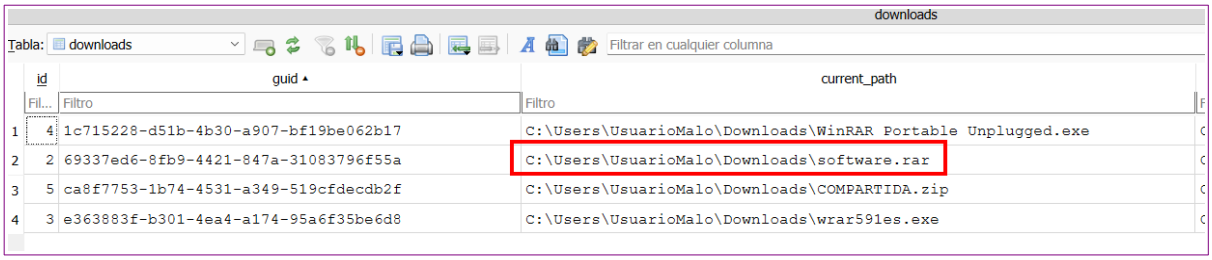

downloads

Tabla: downloads

Filtrar en cualquier columna

	id	guid	current_path
1	4	1c715228-d51b-4b30-a907-bf19be062b17	C:\Users\UsuarioMalo\Downloads\WinRAR Portable Unplugged.exe
2	2	69337ed6-8fb9-4421-847a-31083796f55a	C:\Users\UsuarioMalo\Downloads\software.rar
3	5	ca8f7753-1b74-4531-a349-519cfdecdb2f	C:\Users\UsuarioMalo\Downloads\COMPARTIDA.zip
4	3	e363883f-b301-4ea4-a174-95a6f35be6d8	C:\Users\UsuarioMalo\Downloads\wrar591es.exe

3.4. Instalación sin permisos de administrador y vulnerabilidades explotadas

A pesar de la política de empresa que prohíbe a los usuarios instalar software, el programa fue instalado en la máquina debido a la explotación de una vulnerabilidad:

Escalada de privilegios: El usuario **UsuarioMalo** obtuvo un ejecutable llamado **CVE-2017-0213_x86.exe**. Este ejecutable realiza una escalada de privilegios dentro del sistema mediante una **explotación del COM de Windows**.

Vulnerabilidad del sistema: Esta explotación, a pesar de haber sido parcheada poco después de su aparición en 2017, pudo llevarse a cabo porque los equipos de la empresa **no estaban actualizados con los últimos parches de seguridad**.

Instalación posterior: Una vez que UsuarioMalo efectúa la escalada de privilegios y obtiene permisos de administrador, pudo instalar el keylogger.

4. Conclusiones

De la investigación forense realizada, se extraen las siguientes conclusiones:

1. Software identificado: El software malicioso presente en el equipo es **Spyrix Free Keylogger**, el cual estuvo activo desde el **16/09/2020**.

2. Responsable: El usuario **UsuarioMalo** es el responsable de la instalación del software, ya que realizó las búsquedas, descargó el malware y efectuó la escalada de privilegios necesaria para su instalación.

3. Vector de infección: El vector inicial de infección fue un **correo electrónico**, desde donde se descargó el keylogger (identificado como software.rar) después de que **UsuarioMalo** realizara búsquedas de herramientas de escalada de privilegios.

4. Vulnerabilidad explotada: La instalación fue posible debido a la explotación de la vulnerabilidad **CVE-2017-0213** en el COM de Windows 7, lo que permitió una escalada de privilegios. Esto se debió a que los equipos no estaban actualizados con los últimos parches de seguridad. Adicionalmente, se identifica una **falta de filtrado de adjuntos en el correo corporativo y ausencia de segmentación de permisos** que permitieron la ejecución del malware.

RECOMENDACIONES

Basado en los resultados de la investigación, se emiten las siguientes recomendaciones para mejorar la seguridad del sistema:

Técnicas:

Parchear vulnerabilidades críticas: Es fundamental asegurar que todos los sistemas operativos y aplicaciones corporativas estén **actualizados con los últimos parches de seguridad**, previendo explotaciones conocidas como la **CVE-2017-0213**.

Implementar whitelisting de aplicaciones: Considerar el uso de herramientas como **AppLocker** para **restringir la ejecución de software no autorizado** y solo permitir la ejecución de aplicaciones aprobadas.

Mejorar el filtrado de correo electrónico: Implementar soluciones robustas de **filtrado de adjuntos en el correo corporativo** para detectar y bloquear archivos potencialmente maliciosos, incluso aquellos que puedan estar alojados en servicios de almacenamiento en la nube.

Segmentación de permisos: Revisar y ajustar las políticas de permisos de los usuarios para **limitar la capacidad de instalación de software** y la ejecución de procedimientos que requieran elevación de privilegios sin la debida autorización.

Legales/Organizativas:

Notificación a la AEPD: Si se confirmó la filtración de datos personales, evaluar la necesidad de realizar una notificación a la Agencia Española de Protección de Datos (AEPD) según el Art. 33 del RGPD.

Acción disciplinaria: Evaluar la aplicación de acciones disciplinarias contra UsuarioMalo según las políticas internas de la empresa, dada su posible implicación voluntaria o negligente en la instalación del software malicioso.

ANEXO TÉCNICO KEYLOGGER

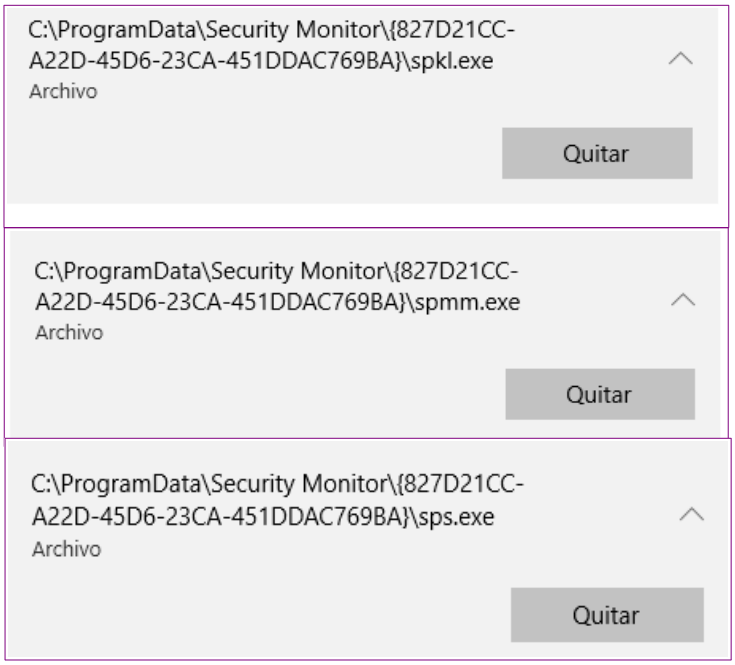
Spyrix Free Keylogger es una herramienta de monitoreo desarrollada por Spyrix Inc., compatible con sistemas Windows (7, 8, 10, 11). Si bien su propósito declarado es el control parental o empresarial, sus características de funcionamiento en segundo plano, persistencia y capacidad de ocultamiento lo convierten en una herramienta con potencial uso malicioso, encuadrable dentro del espectro del spyware.

1. Instalación

Para su instalación se puede hacer mediante la descarga de un ejecutable '.exe' desde su página oficial 'https://www.spyrix.com'o a través de terceros. El instalador puede ser personalizado permitiendo así parámetros para que se ejecute en modo sigiloso. Si se instala con privilegios de administrador, permite una instalación en modo persistente, que se inicie automáticamente cada vez que se inicia el sistema operativo donde se encuentra instalado.

Está diseñado para que sea una herramienta que pueda mantenerse activa en el sistema sin ser detectada fácilmente.

Una vez instalado, en nuestro caso en la ruta 'C:\ProgramData\SecurityMonitor' no sin antes excluir esta ruta para que el antivirus no lo detectara como malicioso, el software nos crea los siguientes directorios, que fueron observados en nuestras evidencias.



2. Persistencia

La **persistencia** es una técnica usada comúnmente por software malicioso para asegurarse de que se ejecuta automáticamente cada vez que se inicia el sistema operativ**o. Los métodos comunes para lograrlo suelen ser:**

- **Claves del Registro para su ejecución automática:** En el Registro de Windows, que es una base de datos del sistema operativo que almacena configuraciones, algunos valores especiales permiten ejecutar programas al inicio del sistema.

El programa malicioso puede escribir su ruta en:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run → Es una clave que aplica a todos los usuarios del sistema y se ejecutará cada vez que cualquier usuario inicie sesión.

HKCU\Software\Microsoft\Windows\CurrentVersion\Run → Es una clave que aplica solo al usuario actual. Aquí no es necesario tener permisos de administrador, y es una forma más discreta de iniciar software malicioso.

- **Tareas programadas (schtasks):** Tiene la capacidad mediante la herramienta de Windows schtasks de tomar capturas de pantalla de manera automática y puede configurarse para hacerlo en momentos específicos. También puede configurarse para registrar imágenes cada vez que una ventana cambia o cuando se copia algo al portapapeles.
- **Servicios de Windows disfrazados:** Un atacante puede registrar el keylogger como si fuera un servicio del sistema, usando un nombre parecido a servicios legítimos (como podrian ser UpdateService, WinUpdate, etc). Dichos servicios se ejecutan con privilegios altos y se inician con el sistema, lo que los hace ideales para persistencia silenciosa.
- **Archivos ocultos en rutas: %AppData%** (carpeta de configuración del usuario), **%SystemRoot%** (normalmente en C:\Windows, es una carpeta sensible y poderosa para el ocultamiento) o **%ProgramData%** (carpeta usada para programas para almacenar datos accesibles para todos los usuarios)

3. Ocultación

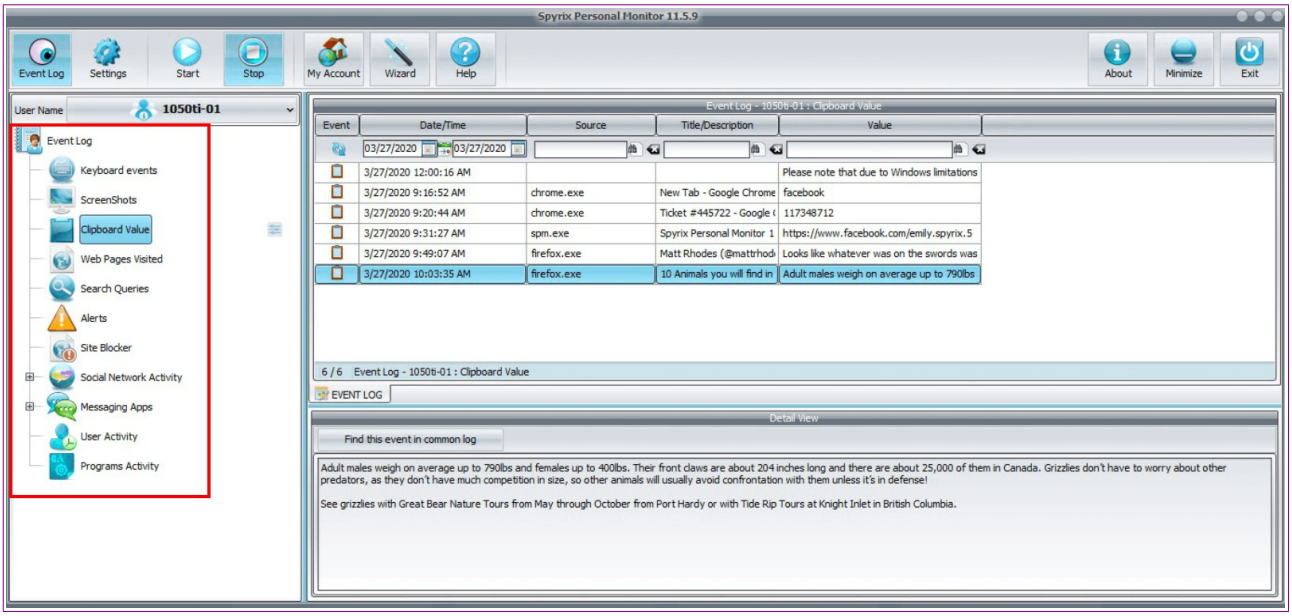
Spyrix Keylogger opera en segundo plano, no aparece en el Administrador de tareas convencional y puede configurarse para no mostrar iconos ni accesos directos. Su activación puede depender de atajos de teclado o contraseñas predefinidas, accesibles solo al operador que lo haya configurado.

4. Funciones de monitoreo

Spyrix Keylogger incorpora un amplio conjunto de funciones orientadas al monitoreo constante y detallado de la actividad del usuario en el equipo instalado. Abarca múltiples vectores de

recolección de datos, lo que la convierte en una herramienta altamente intrusiva y potencialmente peligrosa si se usa con fines no autorizados o maliciosos. Algunas de sus funcionalidades más interesantes son las siguientes:

Funcionalidad	Descripción
Captura de teclas (Keylogging)	Intercepta y registra todas las pulsaciones de teclado mediante hooking (SetWindowsHookEx), almacenando información potencialmente sensible.
Capturas de pantalla	Realiza capturas periódicas o bajo eventos, que pueden almacenarse localmente o transmitirse remotamente.
Registro de aplicaciones y ventanas activas	Monitorea la actividad del usuario sobre aplicaciones y ventanas, incluyendo horarios de uso.
Captura del portapapeles	Registra el contenido copiado y pegado, incluyendo credenciales y fragmentos sensibles.
Seguimiento de redes sociales	Detecta actividad en plataformas como Facebook, WhatsApp Web, Skype o Instagram.
Registro de navegación web	Almacena URLs visitadas, búsquedas realizadas y tiempo de permanencia en sitios web.



5. Almacenamiento y transmisión

5.1 Almacenamiento local

Spyrix Keylogger almacena localmente los datos capturados de forma estructurada, aunque con métodos diseñados para evitar su detección por parte del usuario común o incluso de algunas herramientas antivirus básicas.

Los datos recolectados se almacenan en directorios como %AppData%\Spyrix o %ProgramData%\Spyrix, utilizando extensiones no convencionales y técnicas de cifrado u ofuscación para evitar su detección. Los archivos suelen portar atributos como "oculto" (+h) y "de sistema" (+s).

Desde un punto de vista forense**,** esto implica que para acceder a estos registros es necesario activar la visualización de archivos ocultos y protegidos del sistema operativo, y en muchos casos utilizar herramientas especializadas para desencriptar o decodificar los datos registrados.

5.2 Transmisión remota

Aunque la versión gratuita de **Spyrix Keylogger** puede limitarse al almacenamiento local, las versiones comerciales del programa incluyen mecanismos de transmisión remota automática de los registros, lo que supone un riesgo significativo en términos de exfiltración de información confidencial. Entre los métodos habilitados para esta transmisión se encuentran:

- **Envío por correo electrónico:** el software permite configurar una cuenta de correo **SMTP** (por ejemplo, Gmail, Outlook, etc.) a la que envía periódicamente los registros capturados. El contenido puede ir adjunto en forma de archivos comprimidos o embebido en el cuerpo del mensaje.
- **Transferencia vía FTP:** también se puede configurar un servidor **FTP** externo para que el software cargue los registros automáticamente.
- **Integración con servicios en la nube**: Spyrix ofrece compatibilidad con plataformas como **Google Drive** y **Dropbox**, permitiendo al usuario (o atacante) vincular una cuenta en la nube en la que se subirán los datos sin necesidad de acceso físico al equipo.

Esta funcionalidad remota, si no es detectada a tiempo, facilita la exfiltración silenciosa y continua de datos sensibles, lo que agrava la situación desde una perspectiva de ciberseguridad y legalidad.

6. Usos legítimos (según el fabricante)

El fabricante de dicho software nos dice que sus posibles usos legítimos **podrían ser:** Control parental, supervisión de empleados **previamente avisados y firmado un documento de conformidad y** auditorias de actividad en empresas**.**

7. Usos maliciosos

A causa de la naturaleza del programa y en manos de un actor malicioso **podría recurrir a prácticas poco éticas como:** robo de credenciales, robo de propiedad intelectual**,** vigilancia de empleados **o compañeros sin consentimiento legal (lo que implica una violación de la privacidad y RGPD),** espionaje corporativo y acceso a información confidencial de valor**, como podría ser información financiera.**

8. Medidas de prevención y contramedidas

8.1 Controles periódicos del sistema

Es conveniente realizar revisiones regulares para identificar software sospechoso antes que cause daños. Algunas acciones específicas que podrían llevarse a cabo podrían ser:

- Verificar procesos en ejecución en el administrador de tareas
- Usar herramientas avanzadas como Process Explorer para detectar procesos desconocidos o sin firma digital
- Realizar auditorías del inicio del sistema: Revisar aplicaciones que se ejecutan al iniciar el sistema operativo usando el atajo 'Windows+r' y en ejecutar> 'msconfig' o desde el Visor de Eventos de Windows
- Revisar los servicios y tareas programadas, ya que algunos keyloggers se ocultan en servicios de Windows o tareas automáticas usando el atajo 'Windows+r' y en ejecutar > 'services.msc'
- Explorar manualmente las rutas**:** C:\ProgramData, C:\Users\Usuario\AppData\Roaming, C:\Users\Usuario\AppData\Local\Temp
- Usar comandos como 'netstat' o herramientas como 'TCPView' para detectar conexiones sospechosas salientes

8.2 Usar software antimalware y escaneos proactivos

- Instalar un antivirus confiable
- Usar herramientas legítimas y confiables como Malwarebytes, Zemana AntiMalware
- Realizar escaneos en Modo Seguro para aumentar las probabilidades de detección.

8.3 Otras sugerencias

- Desactivar el uso de cuentas con permisos de administrador como uso diario
- Aplicar prácticas de seguridad como el Principio de mínimo privilegio
- Usar software de restricción como AppLocker
- Actualizar todos los programas regularmente y el sistema operativo
- No descargar software de fuentes desconocidas o pasarlo antes por herramientas como 'VirusTotal' para asegurar su autenticidad, legitimidad y seguridad.
- Usar navegadores actualizados

ANEXO TÉCNICO CVE_2017-0213

1. Introducción

CVE-2017-0213 es una vulnerabilidad de escalada de privilegios local que afecta al subsistema **Component Object Model (COM)** de Microsoft Windows. Esta vulnerabilidad reside en el proceso de desempaquetado (unmarshalling) de objetos COM dentro del componente **Aggregate Marshaler**, permitiendo la ejecución de código con privilegios elevados si no se valida correctamente el identificador de interfaz (IID) durante la deserialización de objetos serializados (OBJREFs).
Esta falla fue documentada y publicada por Microsoft en mayo de 2017, siendo clasificada como crítica debido a su capacidad para permitir que un proceso de bajo nivel obtenga acceso privilegiado al sistema.

2. Descripción Técnica

La vulnerabilidad **CVE-2017-0213** afecta al modelo de comunicación entre procesos de Windows denominado **Component Object Model (COM)**. Este sistema utiliza mecanismos de *marshalling* (empaquetado) y *unmarshalling* (desempaquetado) para permitir que diferentes procesos interactúen mediante objetos serializados conocidos como **OBJREF**.

Cuando una aplicación solicita una interfaz a través de la función QueryInterface, se genera un OBJREF que incluye el **Identificador de Interfaz (IID)** requerido. Este empaquetado lo realiza internamente la función RemQueryInterface2(). Posteriormente, el cliente que recibe este OBJREF lo deserializa usando CStdMarshal::UnmarshalInterface(), quien debe verificar que el IID incluido en el objeto coincide con el solicitado.

El problema de seguridad surge porque UnmarshalInterface() **no valida adecuadamente** este IID. Esta omisión permite que un atacante con acceso local intercepte el OBJREF y **modifique el IID**, sustituyéndolo por uno asociado a una interfaz con privilegios más altos.

Este defecto provoca lo que se denomina una **confusión de tipos**: el sistema crea un proxy creyendo que accede a una interfaz legítima (IID_IFoo), cuando en realidad está utilizando una distinta (IID_IBar), lo que permite al atacante ejecutar funciones con mayores privilegios de los que originalmente poseía.

Este comportamiento puede ser aprovechado para ejecutar código arbitrario, escalar privilegios dentro del sistema y comprometer su integridad, especialmente en entornos corporativos donde múltiples sistemas dependen de una arquitectura Windows común.

3. Impacto y Alcance

Esta vulnerabilidad se basa en un error en el proceso de deserialización utilizado por el COM Aggregate Marshaler, lo que la hace aplicable a casi todas las versiones modernas de Windows que implementan el modelo COM tal y como fue diseñado en estos sistemas. Por ello, tanto los entornos corporativos que utilizan versiones de Windows para clientes como los servidores que soportan infraestructuras empresariales pueden estar vulnerables.

Versiones afectadas:

- **Clientes**: Windows 7 SP1, Windows 8.1, Windows 10 (varias ediciones).
- **Servidores**: Windows Server 2008 SP2, 2008 R2 SP1, 2012 (Gold y R2), y 2016.

Impacto en entornos corporativos:

- **Movimientos laterales**: Posibilidad de propagarse por la red tras obtener privilegios elevados.
- **Persistencia**: Instalación de *backdoors*, *rootkits* u otros mecanismos que mantengan el acceso.
- **Compromiso de sistemas críticos**: Riesgo elevado de exfiltración de datos o interrupción de operaciones esenciales.

4. Mitigación

Para la mitigación de la amenaza se determina que la medida más eficaz es la aplicación del parche corrector del fallo del sistema que permite acceder a dicha explotación:

Aplicación del parche

- **Fecha de publicación**: 12 de mayo de 2017.
- **Solución**: Microsoft corrige el fallo en CStdMarshal::UnmarshalInterface() mediante una validación estricta del IID durante el unmarshalling.

Se recomienda verificar la instalación de este parche en todos los sistemas potencialmente vulnerables y aplicar mecanismos de auditoría para confirmar su efectividad.

5. Consideraciones Forenses

En investigaciones periciales, esta vulnerabilidad puede ser detectada a través de:

- **Análisis de memoria** con herramientas como **Volatility** o **Rekall**, que permitan la identificación de estructuras OBJREF modificadas.
- **Comparación de IIDs** embebidos vs. solicitados, para detectar desajustes indicativos de explotación.
- **Instrumentación de funciones críticas** mediante herramientas como **Microsoft Detours**, para registrar llamadas a UnmarshalInterface() y sus parámetros.
- **Centralización de logs** en plataformas como **Splunk** o **ELK Stack** para generar líneas de tiempo e indicadores de compromiso (IOCs).

6. Conclusiones

Como conclusiones podemos sacar una serie de puntos clave del estudio y análisis de esta explotación:

- CVE-2017-0213 representa una vulnerabilidad crítica con un impacto directo en la seguridad de sistemas Windows.
- La falta de validación en la deserialización de objetos COM permite a atacantes locales elevar privilegios y comprometer el sistema.
- Su explotación, combinada con otras técnicas, puede derivar en ataques complejos como la persistencia, el movimiento lateral o el control remoto total del sistema.
- La mitigación pasa por la aplicación inmediata del parche correspondiente, la restricción de accesos y la implementación de medidas de seguridad complementarias tanto técnicas como organizativas.

7. Referencias

A continuación, se adjuntan una serie de enlaces de referencia sobre la escalada de privilegios:

- MITRE CVE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0213
- INCIBE-CERT: https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2017-0213
- NVD (NIST): https://nvd.nist.gov/vuln/detail/CVE-2017-0213
- Microsoft Security Update: https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0213
- Rapid7: https://www.rapid7.com/db/vulnerabilities/msft-cve-2017-0213
- GitHub POC: https://github.com/Anonymous-Family/CVE-2017-0213
- CVE.org: https://www.cve.org/CVERecord?id=CVE-2017-0213

FUENTES

En este apartado, vamos a enumerar una serie de fuentes en las cuales nos hemos apoyado para aportar la información de este informe:

Evidencias caso:

Capturas de pantalla de los archivos **WinAudit.html**, **netstat_anb_results.txt**, **TCPView.txt**, **cports.html**, **PrcView_extended**, **$MFT**.

Información volcada del archivo **$MFT** en formato .csv.

Capturas de pantalla o exportación de datos del historial de navegación de Chrome, incluyendo las búsquedas realizadas por UsuarioMalo.

Términos Legales:

Ley Orgánica 3/2018 (LOPDGDD): https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673
Artículo 197 ter del Código Penal: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444
Esquema Nacional de Seguridad (ENS): https://www.boe.es/buscar/doc.php?id=BOE-A-2022-3206
UNE 197010:2015 y UNE 71506:2013: www.une.org
Artículo 335.2 de la Ley 1/2000 (Ley de Enjuiciamiento Civil): https://www.boe.es/buscar/act.php?id=BOE-A-2000-323
ISO/IEC 27037: https://www.iso.org/standard/44381.html
Artículos 335-339 LEC (estructura y regulación del informe pericial): https://www.boe.es/buscar/act.php?id=BOE-A-2000-323
Chat GPT

Software Keylogger:

Chat GPT
Microsoft Copilot
https://www.spyrix.com/spyrix-free-keylogger.php
https://spydrill.com/spyrix-review/

Escalada de privilegios:

Chat GPT
Microsoft Copilot
MITRE CVE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0213
INCIBE-CERT: https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2017-0213
NVD (NIST): https://nvd.nist.gov/vuln/detail/CVE-2017-0213
Microsoft Security Update: https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0213

Rapid7: https://www.rapid7.com/db/vulnerabilities/msft-cve-2017-0213
GitHub POC: https://github.com/Anonymous-Family/CVE-2017-0213
CVE.org: https://www.cve.org/CVERecord?id=CVE-2017-0213

Estructura informe:

Archivo Pericial-Borrador facilitado por Cayetano
ChatGPT