kaspersky

Informe analítico

Vías de propagación del malware: un análisis de la ubicación de infostealers en sistemas de archivos infectados

Análisis de la ubicación de los infostealers dentro de los sistemas de archivos

Introducción

Los programas de robo de información ("infostealers" o "stealers") siguen siendo una de las categorías de malware más extendidas y de más rápida evolución. Como su nombre indica, su objetivo principal es robar contraseñas y otra información confidencial de los dispositivos de los usuarios. Toda la información recopilada se envía a los servidores de comando y control de los atacantes en forma de archivos de registro.

Un **archivo de registro** es un conjunto de archivos que contienen datos robados del dispositivo de un usuario. Se trata principalmente de archivos de texto que contienen credenciales de cuenta, configuraciones de cookies y metadatos.

Más de

5 millones

de archivos de registro que contenían información sobre la ruta de acceso a archivos maliciosos fueron analizados por la solución Kaspersky Digital Footprint Intelligence en 2025.

Kaspersky Digital Footprint Intelligence

Además de los metadatos recopilados de las estaciones de trabajo infectadas, algunos *stealers* también almacenan datos sobre la ruta del archivo ejecutable en el que se ocultaba el malware.

Nuestro análisis de los archivos de registro publicados nos da una idea del volumen y la naturaleza de las infecciones en los dispositivos de los usuarios, así como del modo en que estos dispositivos se infectaron en primer lugar. El informe analiza lo siguiente:

- Los directorios más comunes donde se puede encontrar malware.
- Técnicas para camuflar malware como archivos legítimos del sistema y del usuario.
- Nombres típicos de archivos ejecutables maliciosos.
- Relaciones entre los nombres de los archivos, los métodos de distribución y las familias específicas de infostealers.
- Situaciones de infección reales.

Las conclusiones y los hallazgos del informe son relevantes para todos los usuarios de estaciones de trabajo modernas, desde lectores particulares hasta empleados de grandes corporaciones, organismos gubernamentales y pequeñas y medianas empresas.

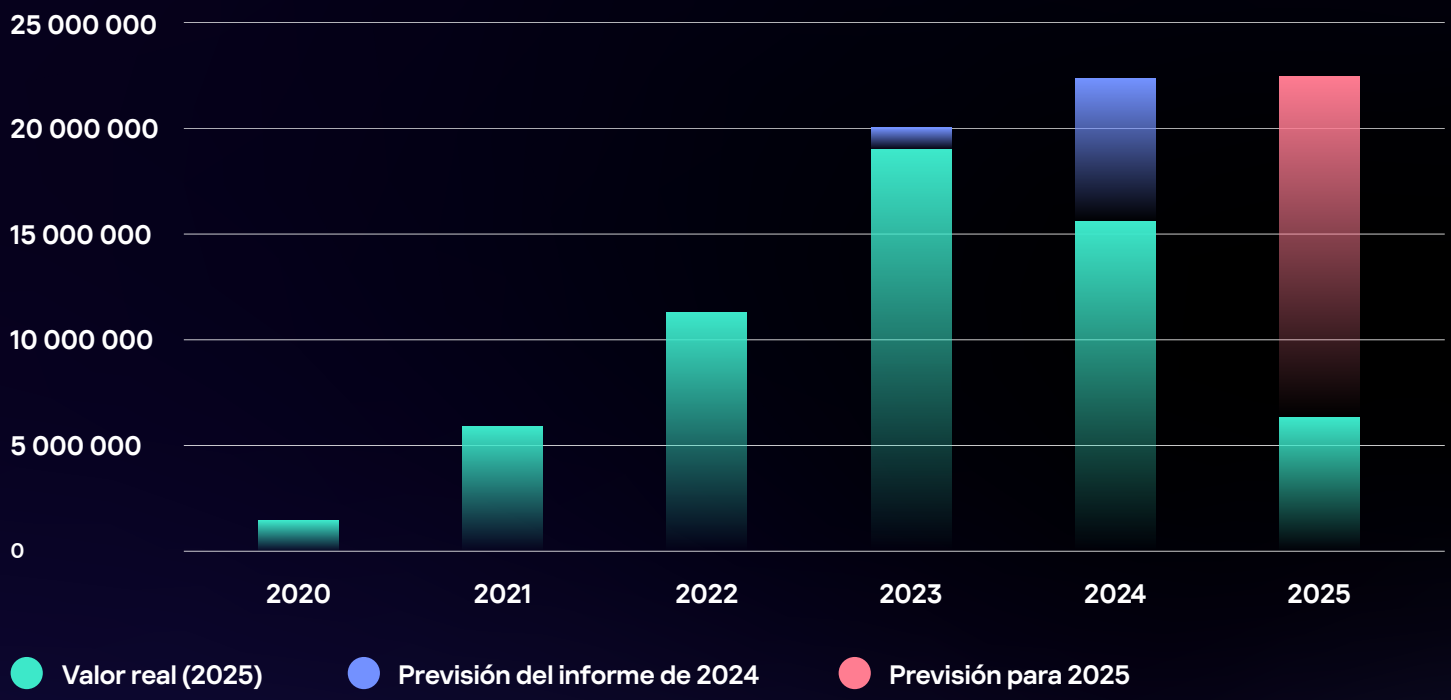
Esta es la tercera parte de nuestra serie sobre amenazas de infostealers. Haga clic en los vínculos para leer la primera y la segunda parte.

Estadísticas de infección de usuarios

Una proporción notable de los archivos de registro aparece en la red oscura después de un cierto lapso de tiempo: por ejemplo, los archivos de registro con fecha de 2024 comenzaron a publicarse más adelante ese mismo año y en 2025. Es de esperar que en 2026 se publiquen muchos archivos de registro con fecha de 2025.

En consecuencia, es posible que las estadísticas anuales de infecciones se revisen en el futuro y las estadísticas correspondientes a 2025 incluyan cifras proyectadas.

Estadísticas anuales de infecciones, 2020-2025 (datos observados y proyecciones)



En nuestro informe de 2024, se hicieron las siguientes previsiones sobre infecciones:

- **2023: 20 millones de usuarios.**
- **2024: 22.5 millones de usuarios.**

El número real de infecciones en 2023 fue de 19 millones (con una desviación respecto a la previsión del –4.61 %) y, en 2024, la cifra fue de 15 millones (con una desviación del –30.80 %). En cuanto al año 2025, nuestro análisis incluyó archivos de registro recientemente descubiertos con fecha de 2023, lo que dio lugar a un aumento del 11.46 %. Y, en 2024, se incluyeron en el análisis los archivos de registro con fecha de 2022, lo que dio lugar a un aumento del 4.48 %.

Esta diferencia numérica apunta a un aumento en el tiempo necesario para recopilar datos completos. Teniendo en cuenta esta tendencia, la previsión de infecciones para 2024 se mantiene sin cambios en unos 22.5 millones de dispositivos de usuarios.

La previsión de infecciones para 2025 es similar a la de 2024: entre 20 y 25 millones de dispositivos infectados (22.5 millones en promedio).

Análisis de metadatos en los registros de infostealers

Uno de los parámetros que se encuentran en los registros de infostealers es la **ruta del malware**: la ruta al directorio que contiene el archivo ejecutable del malware (la ubicación exacta en la que se instaló cuando se infectó el dispositivo), así como el nombre del archivo.

La siguiente tabla muestra la frecuencia con que se encontraron rutas específicas a directorios, en relación con la cantidad total de registros de infostealers analizados en 2025.

Análisis de las rutas a los infostealers ubicados en los directorios de los usuarios, % (datos correspondientes a 2025)

Ruta	%
C:\Usuarios\<Usuario>\AppData\Local\Temp*	35,53 %
C:\<Windows>\Microsoft.NET\Framework\<versión>*	32,33 %
C:\Usuarios\<Usuario>\AppData\Roaming*	8,40 %
C:\Usuarios\<Usuario>\Descargas*	6,60 %
C:\Usuarios\<Usuario>\Documentos*	3,23 %
C:\Usuarios\<Usuario>\Escritorio*	3,00 %
Otros directorios en C:\Usuarios\<Usuario>\AppData\	2,56 %
C:\<Windows>\Installer*	1,98 %
C:\Archivos de programa*	1,77 %
Otros directorios en C:\Usuarios\<Usuario>\	1,28 %
C:\Usuarios\<Usuario>\OneDrive*	0,71 %
D:*	0,60 %
C:\<Windows>\Temp*	0,56 %
Otros directorios del disco C:\	0,50 %
C:\Archivos de programa**	0,40 %
E:*	0,17 %
Otra letra de unidad	0,16 %
C:\Usuarios\<Usuario>\Música*	0,12 %
C:\Usuarios\<Usuario>\Imágenes*	0,10 %
Recurso compartido en red	0,01 %

Como podemos ver, una parte notable de las rutas corresponde a los directorios **C:\Usuarios\<Usuario>\AppData\Local\Temp*** y **C:\<Windows>\Microsoft.NET\Framework\<versión>***.

La ruta C:\Usuarios\<Usuario>\AppData\Local\Temp se utiliza para almacenar archivos temporales, incluidos los datos temporales del navegador. Al abrir un archivo ejecutable desde un navegador, es posible que dicho archivo se guarde en **C:\Usuarios\<Usuario>\AppData\Local\Temp**.

La presencia de numerosas entradas que hacen referencia a este directorio puede ser un indicio de que se está ejecutando malware sin guardarlo primero en un directorio específico.

También analizamos los nombres de los archivos ejecutables del infostealer que se encontraron en la ruta del malware en **C:\<Windows>\Microsoft.NET\Framework\<versión>***.

Los 20 nombres de archivo más frecuentes son los siguientes:

Nombre de archivo	Conde
MSBuild.exe	661 638
RegAsm.exe	537 034
AppLaunch.exe	123 292
AddInProcess32.exe	50 724
[A-Za-z0-9]{10}\.exe	48 699
aspnet_regiis.exe	46 891
NETFXSBS10.exe	30 270
aspnet_compiler.exe	25 424
InstallUtil.exe	21 523
vbc.exe	20 886
aspnet_wp.exe	20 801
RegSvcs.exe	11 385
jsc.exe	7814
ServiceModelReg.exe	6077
csc.exe	6050
System.dll	2342
maxerste.exe	1762
father121.exe	1687
ilasm.exe	1525
cvtres.exe	1256

Observamos que muchas de las entradas con la ruta **C:\<Windows>\Microsoft.NET\Framework\<versión>*** están relacionadas con el mecanismo de malware que consiste en inyectarse en un proceso legítimo para eludir las medidas de seguridad. Esta técnica se utilizó, por ejemplo, en el stealer Lumma.

Encuentre más detalles sobre el malware Lumma en Securelist.com

Las campañas de Lumma utilizaron varios métodos de distribución, especialmente la inyección de una carga útil en la sección superpuesta de software gratuito legítimo.

En el caso de **C:\Usuarios\<Usuario>\AppData\Local\Temp***, guardar archivos en este directorio es una acción habitual para el usuario; sin embargo, en el caso de **C:\<Windows>\Microsoft.NET\Framework\<versión>**, se trata de un indicio de malware que se hace pasar por componentes de Microsoft (cuyos nombres coinciden con los de paquetes legítimos). Para obtener estadísticas más relevantes, excluimos de la muestra dos categorías principales de rutas: **(C:\Usuarios\<Usuario>\AppData\Local\Temp*** y **C:\<Windows>\Microsoft.NET\Framework\<versión>*)** y agrupamos las categorías con menos entradas.

Porcentaje de rutas a infostealers ubicados en los directorios de los usuarios, sin contar las categorías excluidas, % (datos de 2025)

Ruta	%
C:\Usuarios\<Usuario>\AppData\Roaming*	26,12 %
C:\Usuarios\<Usuario>\Descargas*	20,53 %
C:\Usuarios\<Usuario>\Documentos*	10,05 %
C:\Usuarios\<Usuario>\Escritorio*	9,32 %
Otros directorios en C:\Usuarios\<Usuario>\AppData\	7,97 %
C:\<Windows>\Installer*	6,17 %
C:\Archivos de programa*	5,50 %
Otros directorios en C:\Usuarios\<Usuario>\	4,00 %
C:\Usuarios\<Usuario>\OneDrive*	2,22 %
D:*	1,88 %
C:\<Windows>\Temp*	1,74 %
Otros directorios del disco C:\	1,55 %
C:\Archivos de programa**	1,23 %
Otros	1,72 %

La carpeta Roaming contiene principalmente archivos relacionados con aplicaciones, lo que en este caso se refiere a malware que podría haber penetrado en la estación de trabajo de un usuario a través de una aplicación. La probabilidad de que el usuario los descargue intencionalmente es extremadamente baja. Por lo tanto, los directorios de usuario que más nos interesan son **Descargas**, **Documentos** y **Escritorio**, ya que suelen ser los lugares donde se guarda el malware descargado que se hace pasar por archivos inofensivos.

En el apéndice del informe se pueden encontrar ejemplos de las rutas completas más comunes para estos directorios, según los archivos de registro analizados.

Comparación de los 20 nombres de archivos ejecutables más frecuentes en estos directorios:

	Descargas	Documentos	Equipos de escritorio
1	Bootstrapper.exe	[A-Za-z0-9_]{24}.exe	Bootstrapper.exe
2	Set-up.exe	PerfectouinVans.exe	Set-up.exe
3	Bootstapper.exe	Bootstrapper.exe	Licence_Version_Loader.exe
4	setup.exe	S?t_u? [U?D].exe	setup.exe
5	Licence_Version_Loader.exe	f75282f1.exe	Aura.exe
6	Aura.exe	identity_helper.exe	Kiddion's Modest Menu.exe
7	Kiddion's Modest Menu.exe	Xeno.exe	Kiddion's Modest Menu v1.0.0.exe
8	IDPнь_PђCЃtivP°tPsr.exe	BootstrapperUI.exe	Loader.exe
9	Loader.exe	S?t_u? [U?D!].exe	IDPнь_PђCЃtivP°tPsr.exe
10	Kiddion's Modest Menu v1.0.0.exe	BootstrapperAppxx.exe	Bootstapper.exe
11	Kiddions Mod.exe	Set-up.exe	S?t_u? [U?D].exe
12	Adobe_Activator.exe	setup.exe	Collapse.exe
13	activate.exe	XenoBootstrapper.exe	Adobe_Activator.exe
14	Xeno.exe	XenoIU.exe	activate.exe
15	identity_helper.exe	BootstrapperLua.exe	Xeno.exe
16	AdPsbe_Activator.exe	Xeno Release.exe	Kiddions Mod.exe
17	Verus.exe	XenoB.exe	modest-menu.exe
18	S?t_u? [U?D].exe	Licence_Version_Loader.exe	FusionLoader v2.1.exe
19	FusionLoader v2.1.exe	c06cdda6.exe	Verus.exe
20	BootstrapperUI.exe	kosdko0.exe	S?t_u? [U?D!].exe

Algunos nombres de archivo parecen generarse mediante una máscara de archivo específica, lo que significa que el nombre no es fijo ni único, sino que puede variar según una lógica preestablecida. Por ejemplo, los directorios **SimpleAdobe**, **GuardFox** y **piratemamm** pueden contener un archivo que coincida con la máscara **[A-Za-z0-9_]{24}.exe**. Ejemplos:

- C:\Usuarios\<Usuario>\Documentos\SimpleAdobe\GpQC1mCb9qtDeLNO_B1Ar08_.exe
- C:\Usuarios\<Usuario>\Documentos\SimpleAdobe\TL5EtTgS7O_di1ACG4eQaHrl.exe
- C:\Usuarios\<Usuario>\Documentos\GuardFox\Pm68igyBd5rQoMnsyLCAygRl.exe
- C:\Usuarios\<Usuario>\Documentos\piratemamm\hRAssuW6MEXEJiniYHLzXZ1l.exe

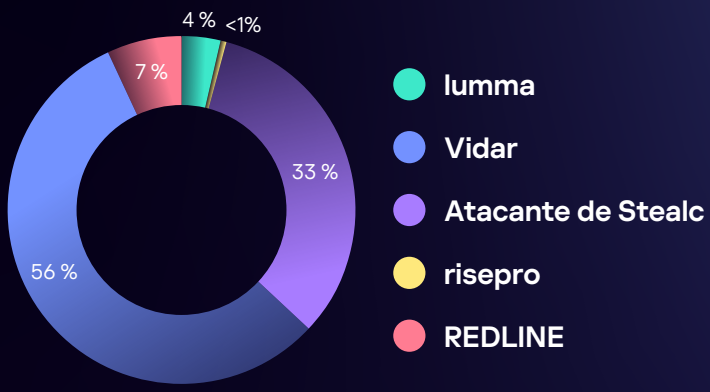
Hay otros nombres que parecen tener más sentido. Como podemos observar, el nombre de un archivo de malware suele corresponder a un archivo de instalación **(Bootstapper.exe**, **Set-up.exe**, **setup.exe)** o a un activador **(Adobe_Activator.exe**, **activate.exe)**; es decir, a programas utilizados para activar ilegalmente software o un sistema operativo. Estos programas suelen distribuirse a través de sitios web no confiables y tiendas de aplicaciones no oficiales.

La instalación de software procedente de fuentes no confiables y los intentos de activarlo de forma ilegal se encuentran entre las principales causas de infección de los sistemas de los usuarios.

Estadísticas por tipo de stealer para los nombres de archivo de malware más frecuentes ubicados en los directorios Descargas, Documentos y Escritorio:

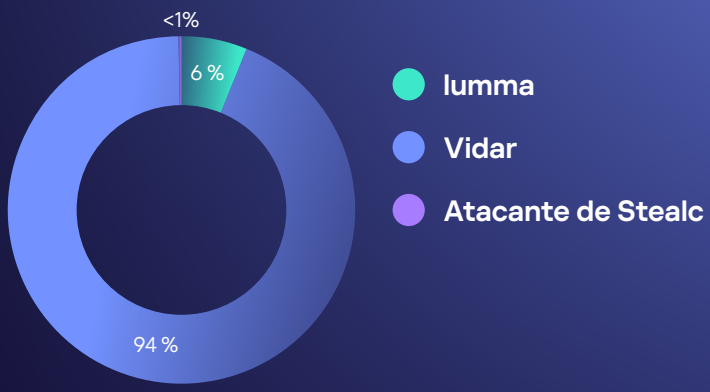
Como se muestra en el gráfico, los nombres que coincidían con la máscara **[A-Za-z0-9_]{24}.exe** fueron los que se encontraron con mayor frecuencia en las rutas del malware de los stealers **RisePro** y **Stealc**.

[A-Za-z0-9_]{24}.exe



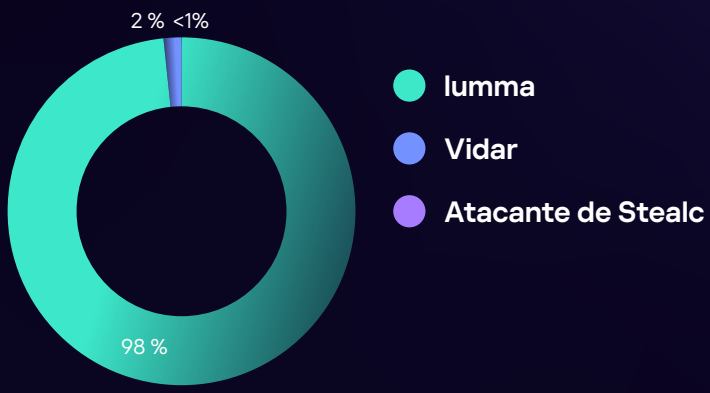
El nombre **Bootstrapper.exe** aparece con mayor frecuencia en los archivos de registro de los stealers **Vidar** y **Lumma**.

Bootstrapper.exe



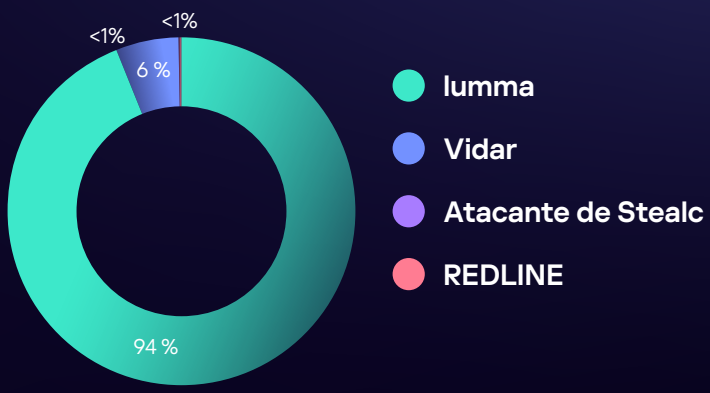
El nombre **Set-up.exe** aparece con mayor frecuencia en los archivos de registro del stealer **Lumma**.

Set-up.exe



El nombre **setup.exe** suele aparecer en los archivos de registro del stealer **Lumma**, aunque también se encuentra en un pequeño porcentaje de los archivos de registro del stealer **Vidar**.

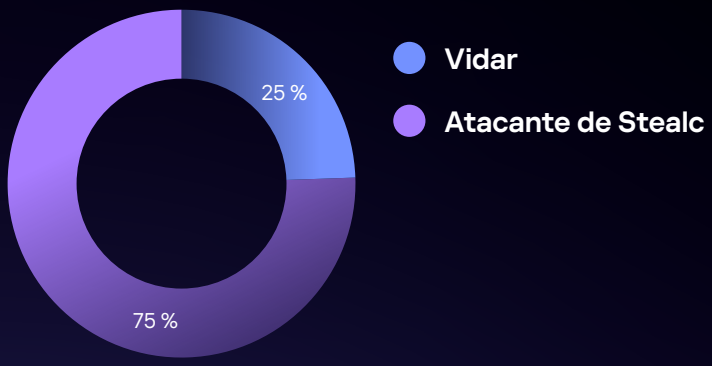
setup.exe



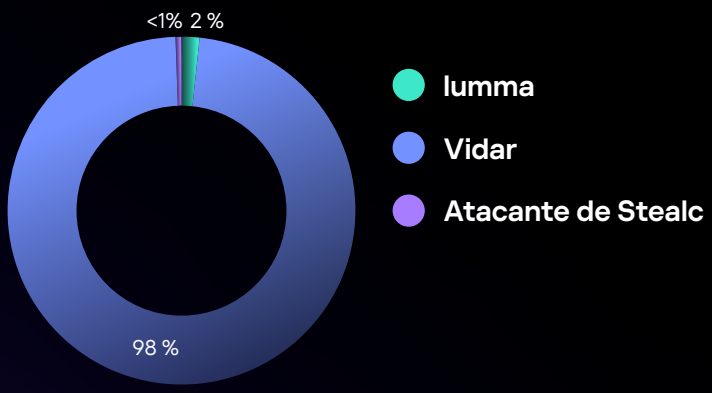
Como se ve en el gráfico, el nombre **Licence_Version_Loader.exe** fue el que más se encontró en los archivos de registro de los stealers **Stealc** y **Vidar**.

El nombre **Bootstapper.exe** aparece con mayor frecuencia en los archivos de registro del stealer **Vidar**.

Licence_Version_Loader.exe



Bootstapper.exe



Tenga en cuenta que el nombre de un archivo de malware depende menos del tipo de stealer y más del método de distribución y las acciones del atacante en cuestión.

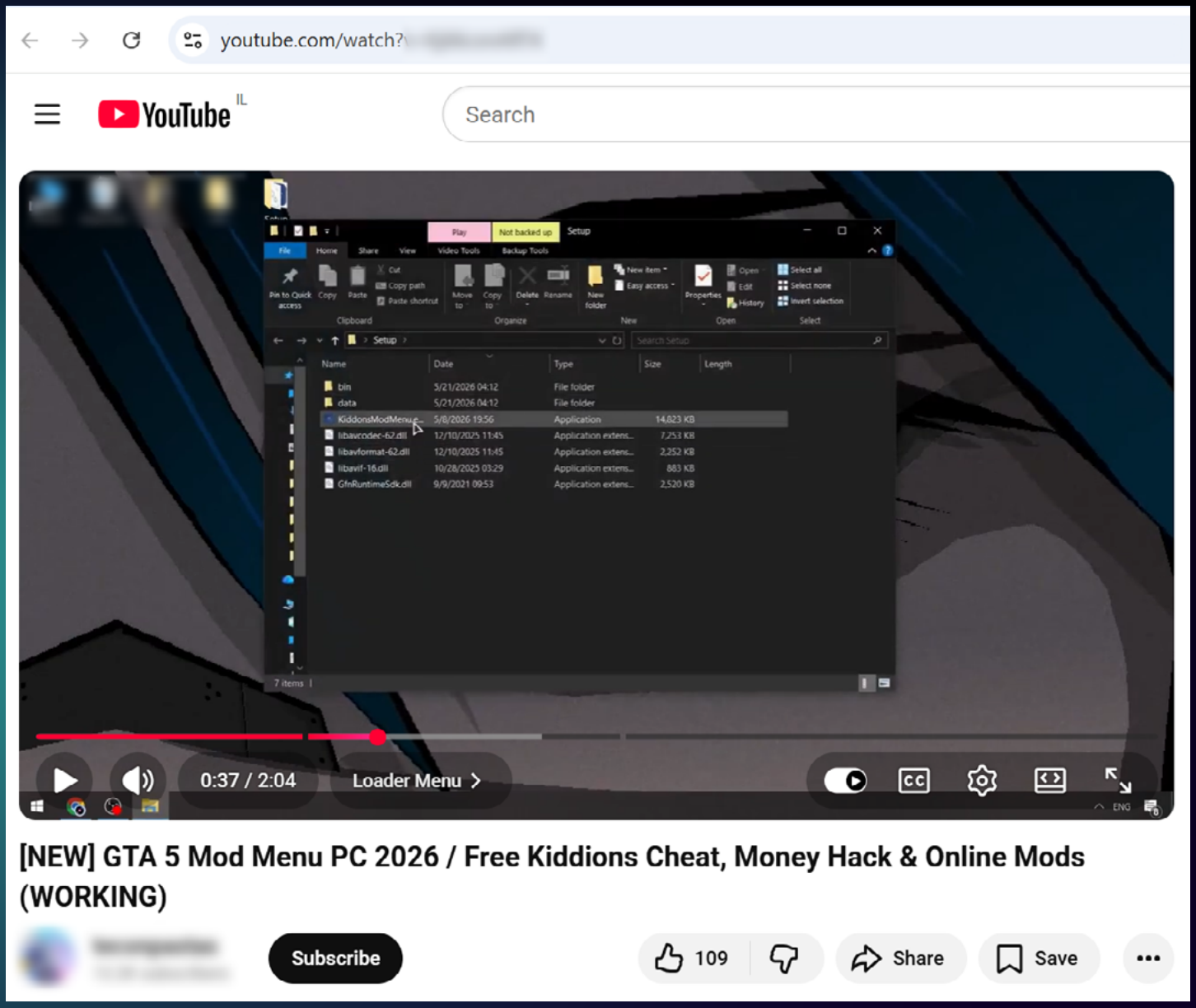
Además de los archivos de instalación y los activadores, es igualmente habitual que el malware se distribuya bajo la apariencia de diversas modificaciones (mods) y complementos para juegos populares.

Por ejemplo, **Modest Menu de Kiddion** es un mod para Grand Theft Auto (GTA). Los usuarios que buscan este tipo de mods para videojuegos en Internet suelen ser víctimas de malware disfrazado de software legítimo. Por ejemplo, la palabra "kiddion" aparece en muchos de los nombres de archivos ejecutables más frecuentes que se enumeran más arriba.

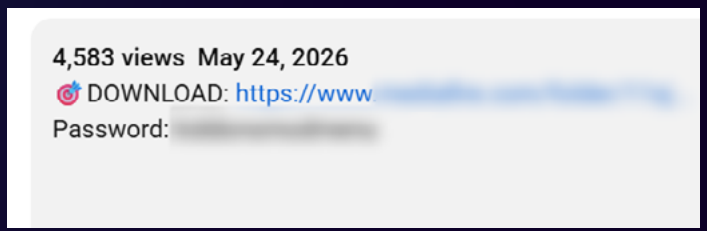
MPGPH131.exe, **MPGPH1.exe**, **MSIUpdaterV1.exe** y **MSIUpdaterV131.exe** son nombres de archivos ejecutables que suelen estar relacionados con el stealer **RisePro**. Representan el 22 % de todas las infecciones por el virus **RisePro**.

Ejemplo de un mecanismo de distribución de malware

El análisis de los métodos de distribución es uno de los factores clave para detectar el malware. Una táctica habitual consiste en convencer a los usuarios para que descarguen y abran un archivo ejecutable. Para ello, los atacantes suben videos a plataformas populares con instrucciones para instalar y ejecutar software o complementos (como mods de videojuegos). Estos videos parecen mostrar al atacante ejecutando la aplicación y obteniendo el resultado deseado.

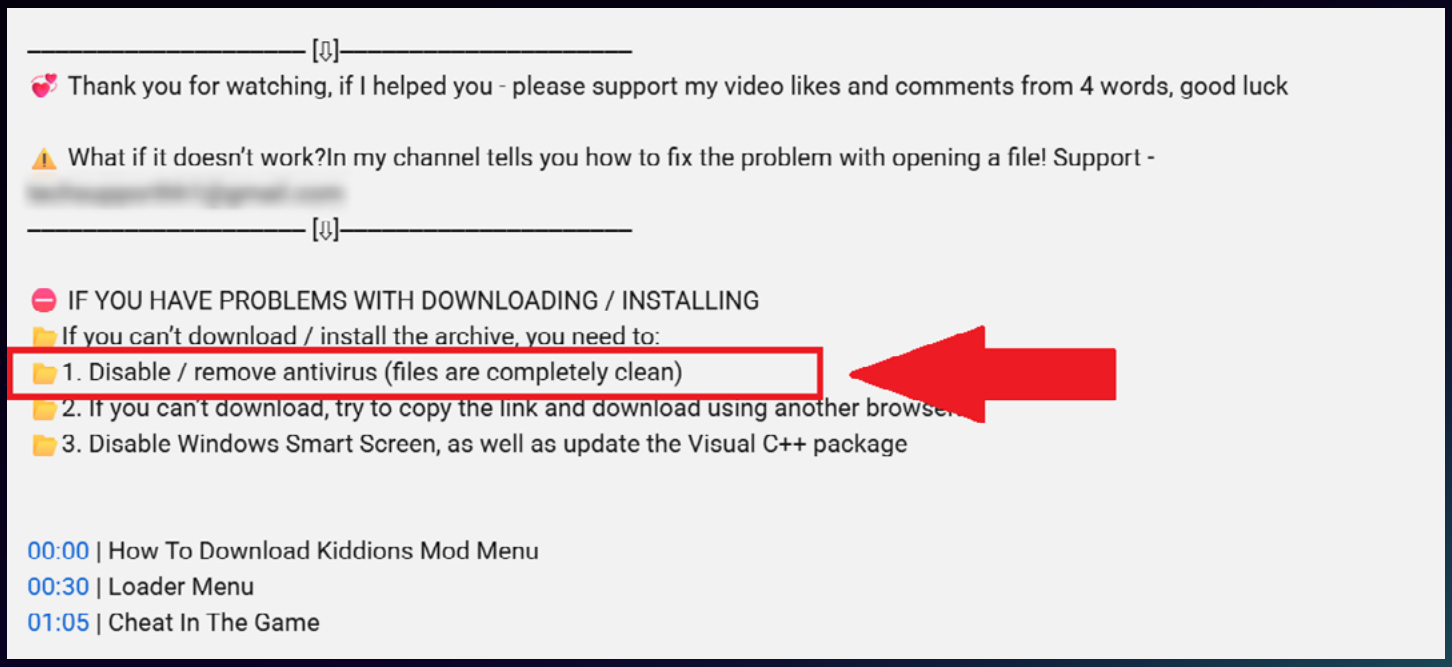


Luego, publican un vínculo de descarga de la aplicación en la sección de comentarios. No hace falta decir que el video es falso y que el vínculo de descarga conduce a un malware.



Como regla:

- **El archivo descargable es un archivo comprimido protegido con contraseña que contiene malware**
- **Las instrucciones le recomiendan al usuario que deshabilite temporalmente cualquier programa antivirus.**



Lamentablemente, muchos usuarios confían en las instrucciones y ejecutan el archivo malicioso. Tenga en cuenta que el malware puede camuflarse como casi cualquier tipo de software, no solo como mods de videojuegos.

Conclusión

Nuestro análisis muestra que la distribución de los infostealers es generalizada y, en gran medida, estandarizada, y que el comportamiento de los usuarios, más que las vulnerabilidades técnicas, desempeña un papel clave.

Una parte significativa de las rutas que se encuentran en los archivos de registro se refieren a software legítimo instalado en la estación de trabajo de destino, lo que refleja el funcionamiento de dicho software. El malware se infiltra en procesos legítimos y elude las medidas de seguridad.

Conclusión: los directorios de usuarios siguen siendo un área de riesgo clave.

Hay dos tipos de directorios que representan la mayor parte de las ubicaciones de archivos maliciosos:

- **C:\Usuarios\<Usuario>\AppData\Local\Temp\ (aproximadamente el 35 %)**
  Esta ruta indica una situación en la que los archivos se ejecutan directamente desde el navegador sin guardarlos explícitamente. Esto confirma que una proporción significativa de los ataques no requiere un encubrimiento complejo: son los propios usuarios quienes inician la ejecución.
- **C:\Windows\Microsoft.NET\Framework\ (~32%)**
  Esta ruta está relacionada con las técnicas de inyección de procesos y de living-off-the-land, en las que el malware se infiltra en procesos legítimos. Este comportamiento es característico de familias más avanzadas, como Lumma.

El análisis de los nombres de los archivos revela un patrón de agrupación claro:

1. Instaladores y programas de descarga que imitan la instalación de software legítimo:
   - setup.exe
   - Set-up.exe
   - Bootstrapper.exe
2. Los activadores y cracks, que están directamente vinculados al software pirateado y constituyen uno de los principales vectores de infección:
   - Adobe_Activator.exe
   - activate.exe
   - Licence_Version_Loader.exe
3. Software que imita mods y utilidades de videojuegos:
   - Modest Menu de Kiddion
   - FusionLoader

Aunque el nombre del archivo suele venir determinado más por el escenario del ataque que por el propio stealer, se observan patrones recurrentes:

1. Lumma
   - setup.exe/Set-up.exe
   - Uso activo del enmascaramiento en .NET
   - Inyección en procesos legítimos
2. Vidar
   - Bootstrapper.exe
   - Bootstapper.exe
   - Loaders clásicos
3. Stealc
   - Licence_Version_Loader.exe
   - Generación de nombres aleatorios
4. RisePro
   - MPGPH*.exe
   - MSIUpdater*.exe
   - Patrones de nombres característicos y únicos (aproximadamente el 22 % de los casos)

Conclusión: el nombre del archivo es un indicador poco confiable pero útil, sobre todo si se combina con la ruta y el contexto.

El factor clave en la infección es el comportamiento de los usuarios. Casi todos los casos detectados se pueden atribuir a dos acciones del usuario: instalar software procedente de fuentes no confiables e intentar activarlo de manera ilegal. Lamentablemente, los usuarios suelen seguir las instrucciones de los atacantes y deshabilitan su software antivirus antes de ejecutar el archivo malicioso.

Las medidas para prevenir estas infecciones deben ser integrales y deben incluir el perfeccionamiento de los criterios de detección, el desarrollo de programas de sensibilización y, por supuesto, la creación de un sistema de protección basado en los escenarios de uso de los usuarios.

Proteja a su empresa de amenazas ocultas

Kaspersky Digital Footprint Intelligence

Kaspersky Threat Intelligence

Nuestro estudio sobre las rutas de los archivos de malware identificó las carpetas de descargas estándar, que a menudo se instalan de manera predeterminada, como las ubicaciones más comunes para el malware. Además, estos programas intentan hacerse pasar por procesos legítimos para eludir la detección por parte de los usuarios y los sistemas de seguridad.

A medida que evolucionan las tecnologías de la información y las redes, la higiene digital cobra cada vez más importancia para proteger a los usuarios particulares y a las empresas de todos los tamaños frente al malware que se distribuye a través de archivos descargados.

Kaspersky Digital Footprint Intelligence

Kaspersky Threat Intelligence

Apéndice

Ejemplos de las rutas completas más frecuentes para los directorios de usuario, según los archivos de registro analizados:

- C:\Usuarios\<Usuario>\Descargas\Kiddions Modest Menu\ Kiddion's Modest Menu\Kiddion's Modest Menu.exe
- C:\Usuarios\<Usuario>\Descargas\Aura\Aura\Aura.exe
- C:\Usuarios\<Usuario>\Descargas\LicPµnce.LPsadPµr(P A$$.- 2025)\Licence_Version_Loader.exe
- C:\Usuarios\<Usuario>\Descargas\Kiddions Modest Menu v1.0.0\Kiddion's Modest Menu v1.0.0\Kiddion's Modest Menu v1.0.0.exe
- C:\Usuarios\<Usuario>\Descargas\ui\Bootstapper.exe
- C:\Usuarios\<Usuario>\Descargas\Kiddions_v2\Kiddions_v2\Kiddions Mod.exe
- C:\Usuarios\<Usuario>\Descargas\Aura\Aura.exe
- C:\Usuarios\<Usuario>\Descargas\FusionHacks\FusionHacks\FusionLoader v2.1.exe
- C:\Usuarios\<Usuario>\Descargas\Adobe Photoshop\Adobe Photoshop\Set-up.exe
- C:\Usuarios\<Usuario>\Documentos\SimpleAdobe\[A-Za-z0-9_]{24}.exe
- C:\Usuarios\<Usuario>\Documentos\GuardFox\[A-Za-z0-9_]{24}.exe
- C:\Usuarios\<Usuario>\Documentos\piratemamm\[A-Za-z0-9_]{24}.exe
- C:\Usuarios\<Usuario>\Documentos\Perfectouin\Bin\PerfectouinVans.exe
- C:\Usuarios\<Usuario>\Documentos\iofolko5\[A-Za-z0-9_]{24}.exe
- C:\Usuarios\<Usuario>\Documentos\Minor Policy\[A-Za-z0-9_]{24}.exe
- C:\Usuarios\<Usuario>\Documentos\App\App\Bootstrapper.exe
- C:\Usuarios\<Usuario>\Documentos\UIBoot\UIBoot\BootstrapperUI.exe
- C:\Usuarios\<Usuario>\Documentos\Release\Release\XenoIU.exe
- C:\Usuarios\<Usuario>\Escritorio\Aura\Aura.exe
- C:\Usuarios\<Usuario>\Escritorio\Kiddion's Modest Menu\Kiddion's Modest Menu.exe
- C:\Usuarios\<Usuario>\Escritorio\Kiddion's Modest Menu v1.0.0\Kiddion's Modest Menu v1.0.0.exe
- C:\Usuarios\<Usuario>\Escritorio\Setup.exe
- C:\Usuarios\<Usuario>\Escritorio\Set-up.exe
- C:\Usuarios\<Usuario>\Escritorio\Nueva carpeta\Licence_Version_Loader.exe
- C:\Usuarios\<Usuario>\Escritorio\Collapse\Collapse\Collapse.exe
- C:\Usuarios\<Usuario>\Escritorio\Adobe Photoshop\Set-up.exe
- C:\Usuarios\<Usuario>\Escritorio\Satu-p_32--64Bit\setup.exe
- C:\Usuarios\<Usuario>\Escritorio\UI\Bootstapper.exe
- C:\Usuarios\<Usuario>\Escritorio\Adobe Premiere Pro\Set-up.exe

Otras rutas que se encuentran con frecuencia y que pueden resultar de interés para fines de detección:

- C:\Usuarios\<Usuario>\1000029002\[a-f0-9]{10}.exe (например: C:\Usuarios\<Usuario>\1000029002\9379a8d3cc.exe)
- C:\Users\<User>\1000037002\[a-f0-9]{10}.exe
- C:\Users\<User>\1000115002\[a-f0-9]{10}.exe
- C:\Users\<User>\nM3kfb2gn5k.exe
- C:\Users\<User>\PicoCo.exe
- C:\Users\<User>\1000350002\[a-f0-9]{10}.exe
- C:\Users\<User>\PlaneExplore.exe
- C:\Users\<User>\11154530102\[a-f0-9]{10}.exe
- C:\Users\<User>\Db94kfDkdls.exe
- C:\Users\<User>\Bn5kgJsa2sf5n.exe

- C:\Windows\Installer\$PatchCache$\Managed\68AB67CA330133017706CB5110E47A00\21.1.20135_32bitmapibroker.exe
- C:\Windows\Installer\$PatchCache$\Managed\68AB67CA7DA73301B744BA0000000010\11.0.0\AcroRd32.exe
- C:\Windows\Installer\$PatchCache$\Managed\68AB67CA430133017706CB5110E47A00\21.1.20135_32bitmapibroker.exe
- C:\Windows\Installer\$PatchCache$\Managed\68AB67CA3301FFFF7706CB5110E47A00\21.1.20135_32bitmapibroker.exe
- C:\Windows\Installer\$PatchCache$\Managed\68AB67CA7DA73301B744CAF070E41400\15.7.20033\AcroRd32.exe
- C:\Windows\Installer\$PatchCache$\Managed\68AB67CA330100FF7706CB5110E47A00\21.1.20135_32bitmapibroker.exe
- C:\Windows\Installer\$PatchCache$\Managed\68AB67CA640133017706CB5110E47A00\21.1.20135_32bitmapibroker.exe
- C:\Windows\Installer\$PatchCache$\Managed\68AB67CA7DA73301B744CAF070E41400\15.7.20033\ADNotificationManager.exe
- C:\Windows\Installer\{307032B2-6AF2-46D7-B933-62438DEB2B9A}\ARPPRODUCTICON.exe
- C:\Windows\Installer\{4487064C-F31E-4499-A1EF-9B8E809A0358}\ARPPRODUCTICON.exe
- C:\Windows\Installer\{21DE6405-91DE-4A69-A8FB-483847F702C6}\ARPPRODUCTICON.exe
- C:\Windows\Installer\$PatchCache$\Managed\68AB67CA630133017706CB5110E47A00\21.1.20135_32bitmapibroker.exe
- C:\Windows\Installer\{42e5a8d4-8fb0-48a1-9063-fc159c7566a0}\ARPPRODUCTICON.exe
- C:\Windows\Installer\{18373B57-4FC3-4B1A-95B3-A7E5DCA577F7}\ARPPRODUCTICON.exe
- C:\Windows\Installer\{067039C9-A41C-42F5-9571-B06E0700AAA4}\icon.exe
- C:\Windows\Installer\{370C1839-B7D8-425E-8D3F-C79638E7D09C}\ARPPRODUCTICON.exe
- C:\Windows\Installer\{18469ED8-8C36-4CF7-BD43-0FC9B1931AF8}\ARPPRODUCTICON.exe
- C:\Windows\Installer\{06CD45E6-FF5E-4D8E-BC01-B276A90DADF2}\ARPPRODUCTICON.exe
- C:\Windows\Installer\$PatchCache$\Managed\68AB67CA3301FFFF7706C0F070E41400\15.7.20033\Acrobat_Elements.exe
- C:\Windows\Installer\{1E5C3247-B6FF-47F2-AEE9-A921B21E914F}\ARPPRODUCTICON.exe

- C:\Archivos de programa (x86)\UltraStar Deluxe\songs\ultrastar deluxe songs pack
- C:\Archivos de programa\Dassault Systemes\DraftSight\draftsight
- C:\Archivos de programa (x86)\KONAMI\Pro Evolution Soccer 2013\crack pes
- C:\Archivos de programa (x86)\VictorVal\Pro Evolution Soccer 2013 Repack\rld.dll pes
- C:\Archivos de programa (x86)\Vital Office\Hasp\hardlock hasp hl emulator
- C:\Archivos de programa (x86)\Sports Interactive\Football Manager 2005\fm
- C:\Archivos de programa (x86)\Microsoft\EdgeUpdate\1.3.195.15\MicrosoftEdgeUpdateCore.exe
- C:\Archivos de programa\Windows NT\[A-Za-z0-9]{43}.exe
- C:\Archivos de programa\Lumion 4.5.1\Channels\lumion
- C:\Archivos de programa\Google\Chrome\Application\updater.exe

- C:\Windows\Temp\Fb94JnkgmTbi.exe
- C:\Windows\Temp\[A-Za-z0-9]{13}.exe
- C:\Windows\Temp\[a-z0-9]{8}.[a-z0-9]{3}.exe
- C:\Windows\Temp\nM5Gkugn5b.exe
- C:\Windows\Temp\Gko5Kmko4n.exe

- C:\ProgramData\MPGPH131\MPGPH131.exe
- C:\ProgramData\MPGPH1\MPGPH1.exe
- C:\ProgramData\Lawai.com
- C:\ProgramData\MSIUpdaterV131_f09ac2d587354c6431bf93812ba7548f\MSIUpdaterV131.exe
- C:\ProgramData\MSIUpdaterV1\MSIUpdaterV1.exe
- C:\ProgramData\MSIUpdaterV1_b169c3872385b2c3c15a1f5f96f34ffe\MSIUpdaterV1.exe
- C:\ProgramData\MSIUpdaterV131_eeb341036f887f8bfa41fe84e80e9357\MSIUpdaterV131.exe
- C:\ProgramData\MSIUpdaterV131_c743bb12f321204aca6c69356124da3d\MSIUpdaterV131.exe
- C:\ProgramData\waf.com
- C:\ProgramData\Update\[A-Za-z0-9]{7}.exe