Análisis de la amenaza Lumma Stealer

Análisis del malware, TTPs, IoCs y medidas de seguridad

Autor:

Ángel Luis Rodríguez Martín-Palomino

Índice de contenidos

Introducción.....**3**
Resumen Ejecutivo.....3
Análisis del Malware.....**4**
Virus Total.....4
Any.RUN.....8
Joe Sandbox.....11
Inteligencia y Artefactos.....**13**
Vectores de ataque.....13
TTPs.....14
IoCs.....15
Conclusiones y recomendaciones.....**16**
Referencias.....**17**

Índice de imágenes

Imagen 1. Analisis de VirusTotal para la muestra de Lumma Stealer.....4
Imagen 2. Dominios contactados por el ejecutable de LummaStealer.....5
Imagen 3. URLs contactadas por la muestra.....6
Imagen 4. Resumen de la actividad de la muestra de Lumma Stealer.....6
Imagen 5. Táctica de descubrimiento utilizada por la muestra.....6
Imagen 6. Lectura del portapapeles por un proceso del ejecutable.....7
Imagen 7. Intento de establecerse como un AutoRun de la muestra.....7
Imagen 8. Alertas generadas por reglas IDS.....7
Imagen 9. Llamadas al sistema operativo sospechosas.....8
Imagen 10. Alertas generadas por ANY.RUN al ejecutar la muestra.....8
Imagen 11. Gráfico de procesos de ANY.RUN.....9
Imagen 12. Análisis del proceso core.exe desde ANY.RUN.....10
Imagen 13. Comunicaciones del proceso core.exe en ANY.RUN.....10
Imagen 14, Dominio C2 contactado por la muestra en ANY.RUN.....11
Imagen 15. Tipos de reportes de Joe Sandbox.....11
Imagen 16. Clasificación del malware en diagrama de Joe Sandbox.....12
Imagen 17. Claves de registro accedidas por la muestra en Joe Sandbox.....12
Imagen 18. Creación del proceso core.exe por KMSPico.....13
Imagen 19. Ejemplo de mensaje ClickFix.....14
Imagen 20. TTPs de Lumma Stealer en ANY.RUN.....14

Introducción

El presente informe pretende realizar un análisis básico sobre una muestra del malware *Lumma Stealer* mediante el uso de herramientas en línea y *sandbox* como ANY.RUN, Joe Sandbox o VirusTotal, de tal manera que se pueda realizar un estudio detallado del comportamiento del malware de forma segura en un entorno virtualizado.

En concreto la muestra se ha obtenido del *Malware Bazaar* en el siguiente enlace.

Nombre Fichero	KMSPico.exe
MD5	56c6b5cb4714c8754c2721a4fd794522
SHA256	fcf8d40fe2db604954c51451d753a0e965996c43154bf506fdbdfbb3885ffce4

Se ha elegido esta muestra sobre otras por su elevado número de víctimas recientemente que, según fuentes oficiales, entre el 16 de marzo y el 16 de mayo de 2025 han sido más de 394.000 equipos Windows los que se han visto afectados por esta familia.

Resumen Ejecutivo

AMENAZA	***Lumma Stealer***
MODELO	MaaS
PAÍS ORIGEN	Rusia
FECHA INICIAL	2022
MOTIVACIÓN	Robo de Información
VECTOR ATAQUE	*Phishing / Fake Captcha / Trojan*
SISTEMA OBJETIVO	Windows
IMPACTO	**ALTO**

Lumma Stealer es un malware del tipo *Info Stealer*, es decir, cuyo principal objetivo es el robo de información de carácter confidencial en los dispositivos infectados. Generalmente se suele camuflar como una aplicación o fichero aparentemente benigno como una extensión del navegador o, en el caso de esta muestra, un activador de licencias de Windows, con el objetivo de acceder a los sistemas y desplegar sus acciones maliciosas.

Se trata de un MaaS (*Malware-as-a-Service*) y según investigadores oficiales se cree que su procedencia es rusa ya que se empezó a distribuir en foros ruso-parlantes desde al menos agosto del 2022. La información a la que intenta acceder es muy variada y depende de la muestra, pero generalmente se centra en:

- Carteras de criptomonedas.
- Extensiones de navegador de 2FA.
- Captura de información sensible como credenciales o tarjetas de crédito mediante registro de pulsaciones de teclado.

- Documentos, fotos y vídeos sensibles.
- Contenido del portapapeles.

Una vez obtenidos los datos objetivo los datos se exfiltran a un C2 mediante peticiones `HTTP POST` utilizando el agente de usuario "`TeslaBrowser/5.5`".
Adicionalmente, tiene otras capacidades a parte del robo de información como el control del dispositivo infectado para descargar e instalar otros malware, técnicas de evasión como ofuscación y cifrado e incluso es capaz de añadir una puerta trasera al dispositivo para que pase a formar parte de una *botnet* de equipos infectados.

Análisis del Malware

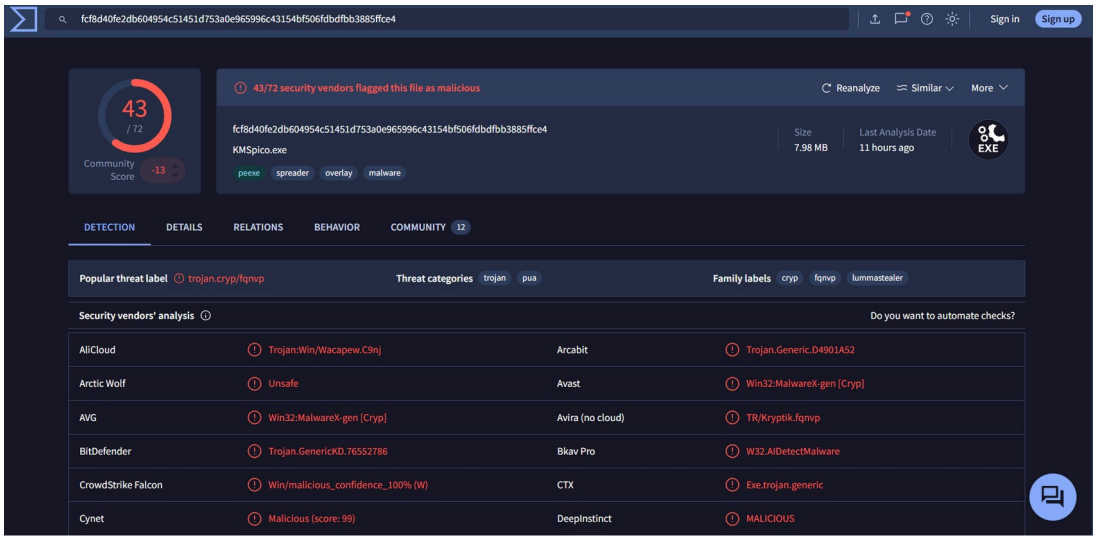
En este apartado se realizará un análisis del malware utilizando distintas plataformas en línea para identificar sus capacidades, etapas de la infección, TTPs, IoCs, vectores de ataque y en general cómo funciona a alto nivel esta amenaza y que cambios realiza en el sistema.

Virus Total

VirusTotal es una plataforma *online* que permite escanear archivos en base a su hash de tal manera que se puede obtener el veredicto de gran cantidad de marcas de antivirus sobre la legitimidad del recurso. Así mismo, integra apartados de *sandboxing* que permiten extraer *insights* sobre el comportamiento de la aplicación, en este caso, como sus conexiones de red o acceso/modificación de archivos. En definitiva, es una opción muy útil como primer contacto con una muestra para obtener una visión general sobre lo que se está tratando y sirve para obtener de manera rápida TTPs e IoCs.

A continuación, se muestra una imagen del resultado del escaneo de la muestra en VirusTotal.

Imagen 1. *Analisis de VirusTotal para la muestra de Lumma Stealer.*



Como se puede ver los resultados no son muy esperanzadores, la muestra ha sido catalogada como maligna por 43 de los 75 proveedores de seguridad de VirusTotal y por 13 usuarios de la comunidad.

Además, a simple vista podemos ver que la muestra ha sido catalogada como troyano y se han añadido etiquetas que pueden indicar métodos que utiliza el malware como *overlays* y *spreader*, es decir, que tiene capacidades de propagación a otros dispositivos.

En el apartado de relaciones podemos ver las comunicaciones que realiza el ejecutable a nivel de IP o dominio.

Imagen 2. *Dominios contactados por el ejecutable de LummaStealer.*

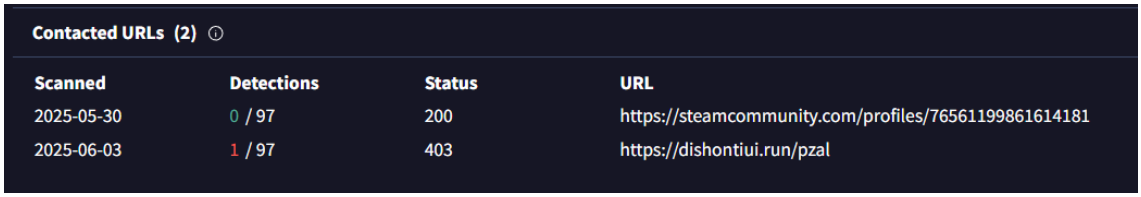
Contacted Domains (20)

Domain	Detections	Created	Registrar
0.pool.ntp.org	0 / 94	1997-01-18	TUCOWS, INC.
1.pool.ntp.org	0 / 94	1997-01-18	TUCOWS, INC.
2.pool.ntp.org	0 / 94	1997-01-18	TUCOWS, INC.
3.pool.ntp.org	0 / 94	1997-01-18	TUCOWS, INC.
c.pki.goog	0 / 94	2016-06-13	MarkMonitor Inc.
citellcagt.top	21 / 94	2025-05-10	-
diecam.top	20 / 94	2025-05-19	-
dishontiui.run	12 / 94	2025-05-21	-
ecs-office.s-0005.dual-s-msedge.net	0 / 94	2022-12-02	CSC CORPORATE DOMAINS, INC.
escczlv.top	21 / 94	2025-05-19	-
joshuagrde.shop	16 / 94	2025-05-21	-
korxddl.top	21 / 94	2025-05-19	-
localixbiw.top	21 / 94	2025-05-21	-
narrathfpt.top	21 / 94	2025-05-10	-
s-0005.dual-s-msedge.net	0 / 94	2022-12-02	CSC CORPORATE DOMAINS, INC.
screhwc.live	19 / 94	2025-05-31	-
steamcommunity.com	0 / 94	2006-05-28	MarkMonitor Inc.
tinklertjp.bet	20 / 94	2025-05-21	-
witchdbhy.run	21 / 94	2025-05-21	-
www.microsoft.com	0 / 94	1991-05-02	MarkMonitor Inc.

En este caso al tratarse de un `KMSPico.exe` que se ejecuta en sistemas Windows para activar licencias, algunos de los dominios contactados son legítimos como el de Microsoft, msedge o los servidores NTP. Sin embargo, la mayoría de los dominios tienen nombres algo extraños y están marcados como maliciosos por varios fabricantes. De hecho, al entrar a los comentarios de la comunidad en dichos dominios es común encontrarse referencias a *Lumma Stealer*, lo que parece indicar que pueden ser parte de la infraestructura utilizada por el malware.

En este apartado de relaciones también destacan las URLs contactadas, entre las que se encuentra una de la famosa plataforma de distribución de videojuegos Steam, en concreto, el perfil de un usuario de la comunidad.

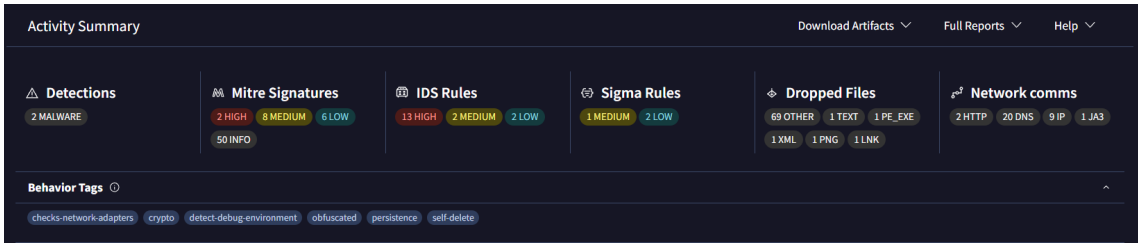
Imagen 3. *URLs contactadas por la muestra.*



En principio, parece que esta URL es totalmente legítima ya que Steam es una compañía con varios años en el sector, pero tras haberlo investigado más detenidamente, parece ser que es uno de los servidores «*de reserva*» que se utilizan para exfiltrar información según apuntan reportes oficiales de Microsoft[1].

Si bien el apartado de relaciones es muy útil, quizá el apartado más interesante de VirusTotal sea el de *Behaviour* ya que ahí es donde se acumula toda la inteligencia generada por los distintos proveedores de *sandbox*. En la siguiente imagen podemos ver un resumen de la actividad de la muestra.

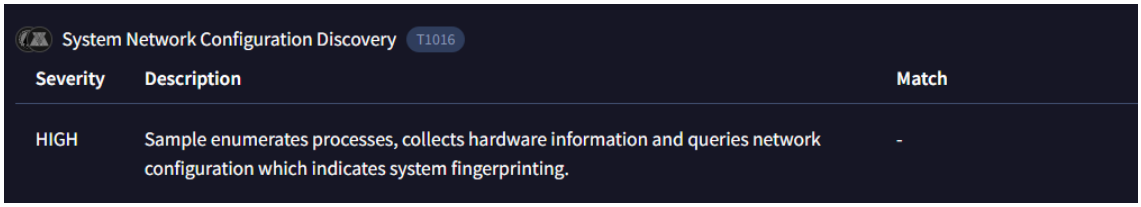
Imagen 4. *Resumen de la actividad de la muestra de Lumma Stealer.*



En la anterior imagen se puede ver como el ejecutable ha hecho saltar varias firmas de tácticas y técnicas de MITRE, 13 reglas de riesgo alto de IDS y como ha instalado varios ficheros y realizado comunicaciones con varios equipos.

A continuación, se muestran algunas de las técnicas catalogadas como más peligrosas por MITRE en VirusTotal.

Imagen 5. *Táctica de descubrimiento utilizada por la muestra.*

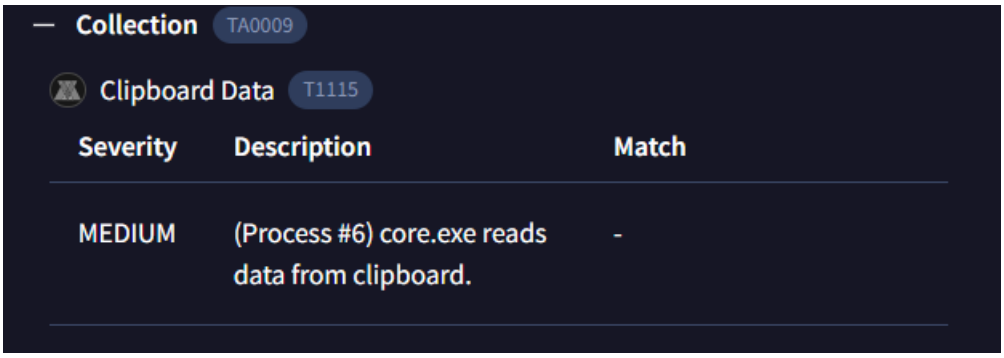


En la anterior imagen se puede ver como la muestra utiliza la técnica `T1016` para obtener información sobre procesos internos en la máquina, información del hardware, configuración de red y en general acciones de *fingerprinting* lo cual suele ser utilizado como una de las primeras fases para reconocer la víctima y saber cómo actuar en consecuencia.

[1] En el apartado de «C2 Communication» del siguiente enlace se puede ver cómo se menciona el servidor Steam como C2 alternativo, https://www.microsoft.com/en-us/security/blog/2025/05/21/lumma-stealer-breaking-down-the-delivery-techniques-and-capabilities-of-a-prolific-infostealer/

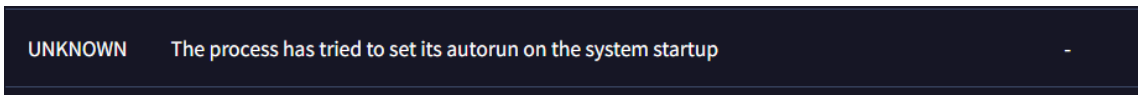
También podemos ver que uno de los procesos creados accede a leer los contenidos del portapapeles que a menudo contienen información sensible copiada.

Imagen 6. *Lectura del portapapeles por un proceso del ejecutable.*



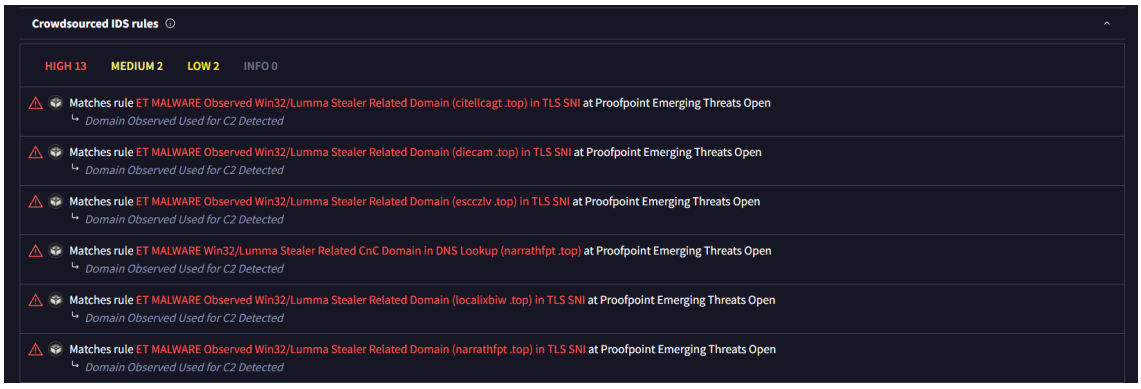
O por ejemplo como ha intentado establecerse como un `AutoRun`, lo cual suele ser una manera de obtener persistencia en el sistema.

Imagen 7. *Intento de establecerse como un AutoRun de la muestra.*



En cuanto a las reglas IDS que se muestran en la siguiente imagen, la mayoría parecen ser provocadas por interacciones con dominios marcados como parte de la infraestructura de *Lumma Stealer* detectados a través del campo SNI de TLS.

Imagen 8. *Alertas generadas por reglas IDS.*

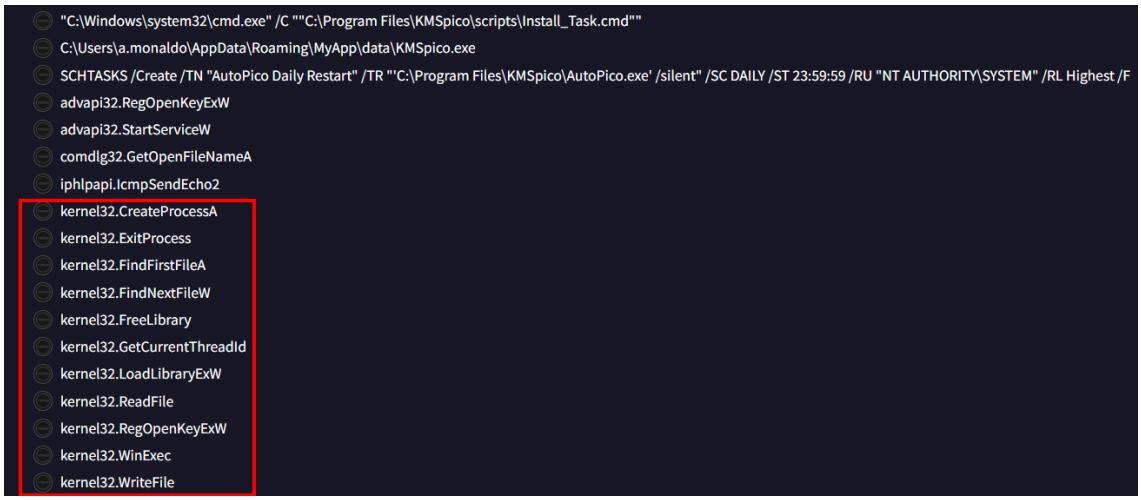


Por último, se destacará el apartado de *Highlighted Actions* en Virus Total el cual nos muestra acciones ejecutadas por la muestra que se consideran sospechosas ya sea por el uso de criptografía o por realizar ciertas llamadas al sistema operativo.

En la siguiente imagen se muestra un extracto de esas acciones, en las que destacan la creación de un servicio de *AutoPico* con privilegios de administrador y ciertas llamadas a la API de Windows `kernel32`. La creación del servicio puede ser algo «normal» ya que la muestra es de un archivo `KMSPico.exe` por lo que puede ser una acción necesaria para realizar su función. Sin embargo, el uso de llamadas a `kernel32` como `CreateProcessA`, `LoadLibraryExW`, `RegOpenKeyExW` o `WinExec` es muy común en el malware para crear otros procesos maliciosos o modificar claves del

registro, si bien no es totalmente concluyente, ya que estas llamadas se pueden utilizar de manera legítima, es notorio y necesario de mencionar.

Imagen 9. *Llamadas al sistema operativo sospechosas.*

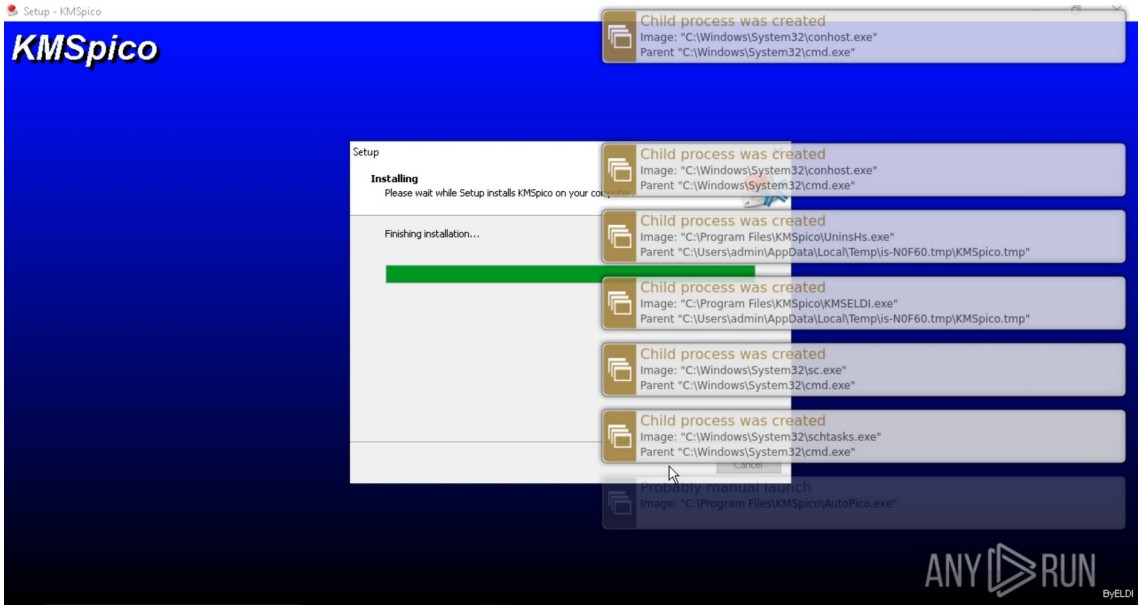


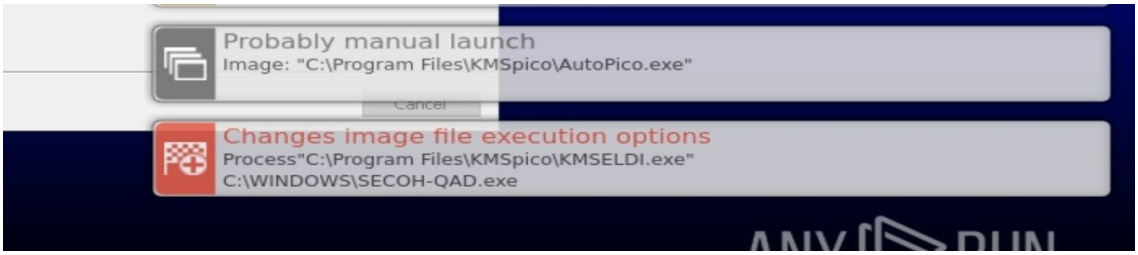
Any.RUN

Otra de las herramientas que se puede utilizar tras haber hecho un análisis preliminar con VirusTotal, es ANY.RUN. El punto fuerte de esta solución es, entre otras cosas, que permite interactuar a través del navegador con el escritorio de la máquina desplegada y visualizar los cambios en el sistema de forma gráfica.

A continuación, se puede observar la interacción con el programa `KMSPico.exe` de la muestra y como al finalizar el proceso aparecen múltiples alertas en ANY.RUN.

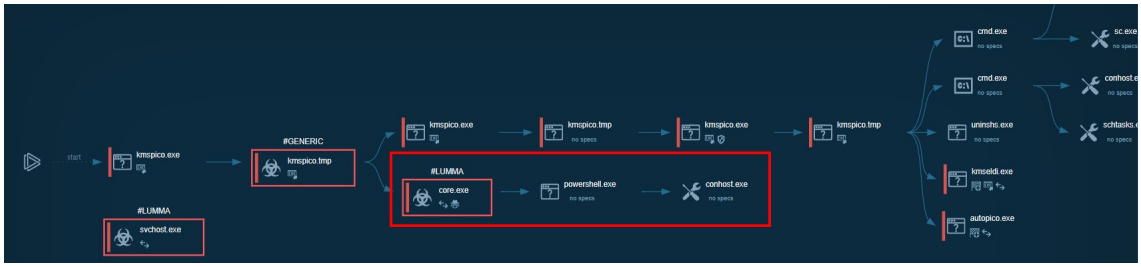
Imagen 10. *Alertas generadas por ANY.RUN al ejecutar la muestra.*





Otro de los puntos fuertes de ANY.RUN es que nos permite visualizar mediante un gráfico el flujo de creación de los distintos procesos y servicios tal y como muestra la siguiente imagen.

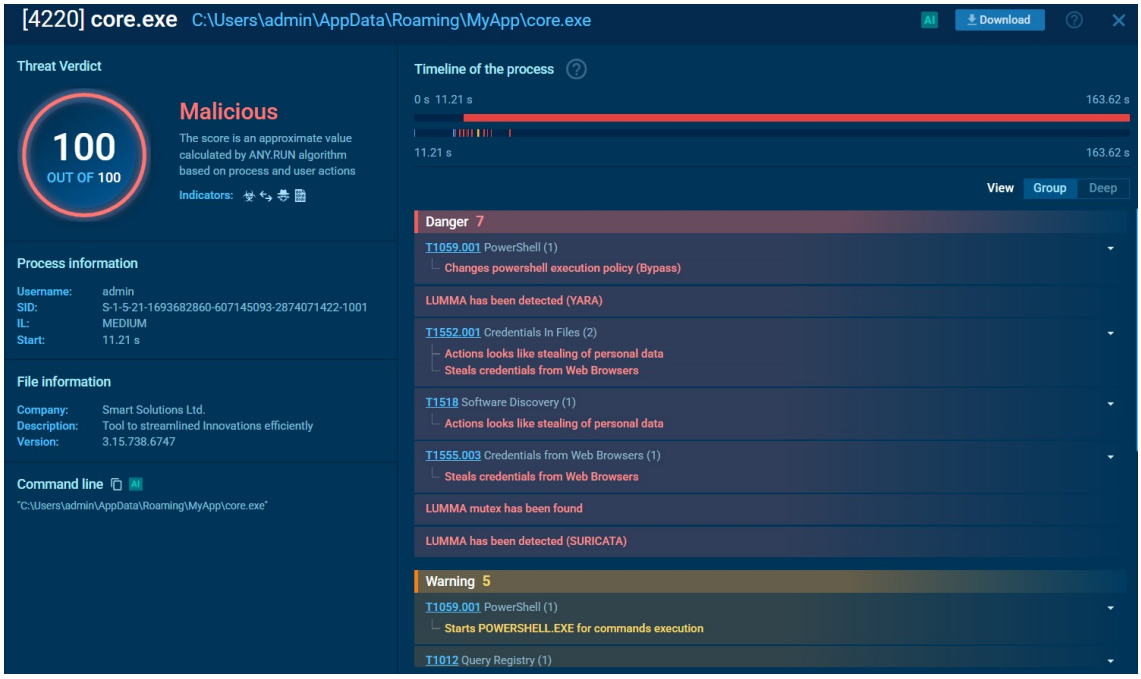
Imagen 11. *Gráfico de procesos de ANY.RUN.*



En la anterior imagen se puede ver cómo tras la ejecución del proceso de `KMSPico.exe` se crean dos ramas de procesos. La de arriba parece corresponder al flujo normal de instalación del activador de licencias KMSPico. Sin embargo, a la vez que se crea dicha rama, también lo hace el proceso `core.exe` el cual está marcado como `#LUMMA` por ANY.RUN y es malicioso 100/100.

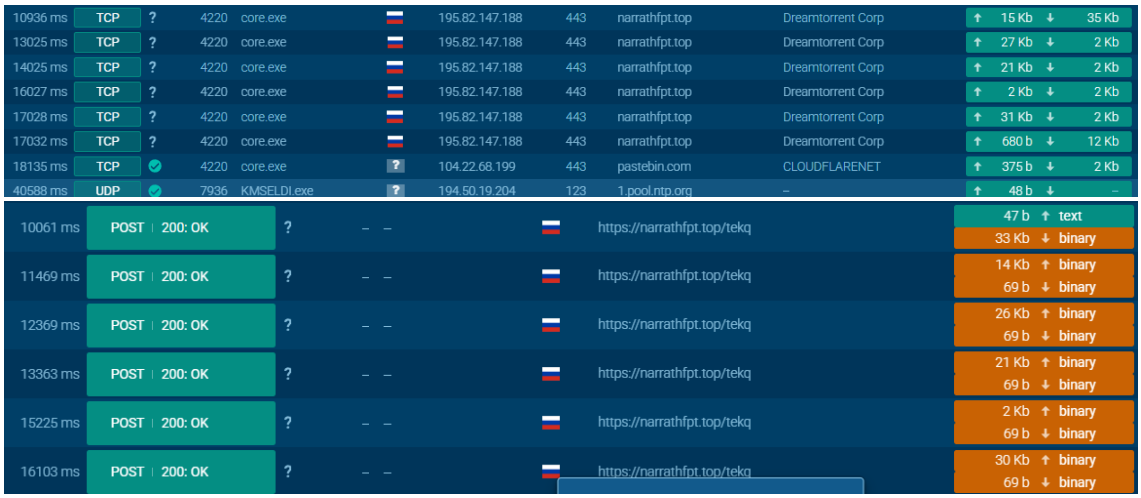
Mirando más detenidamente el proceso `core.exe` resulta que este emplea distintas técnicas MITRE como crear un proceso PowerShell con `powershell -exec bypass` para habilitar la ejecución de scripts desde la terminal y la búsqueda de datos personales sensibles en ficheros y navegadores web. También hace saltar algunas reglas YARA y alertas de SURICATA tal y como muestra la siguiente imagen.

Imagen 12. *Análisis del proceso core.exe desde ANY.RUN.*



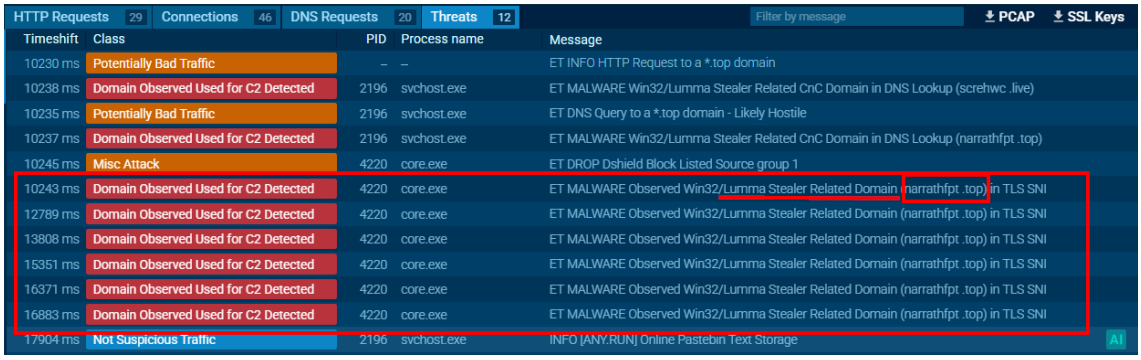
Destaca también como este proceso parece comunicarse con una serie de IPs rusas a través del dominio `narrathtfpt[.]top` lo cual tiene sentido conociendo la procedencia de esta amenaza.

Imagen 13. *Comunicaciones del proceso core.exe en ANY.RUN.*



De hecho, dicho dominio está marcado como servidor C2 utilizado por *LummaStealer* en ANY.RUN.

Imagen 14. *Dominio C2 contactado por la muestra en ANY.RUN.*

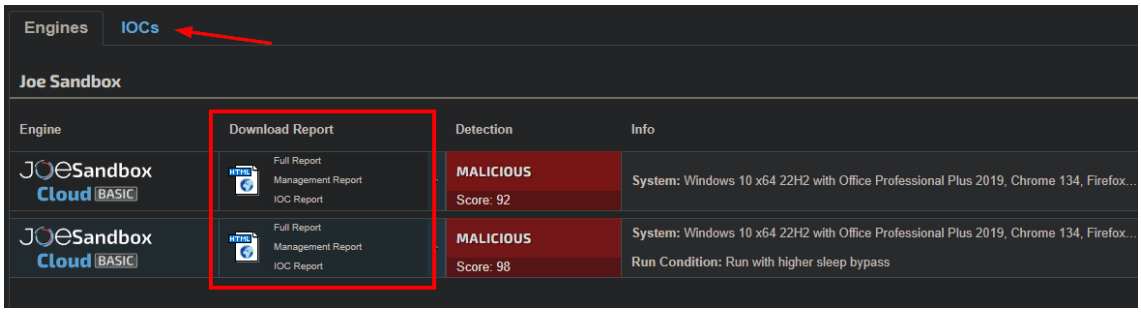


Joe Sandbox

A parte de VirusTotal y ANY.RUN, existen multitud de herramientas online que permiten realizar análisis básicos de malware en un *sandbox*. Por destacar uno de ellos, quizá el más conocido entre las alternativas, en esta sección se utilizará Joe Sandbox. No obstante, al tratarse de la misma muestra los resultados obtenidos por las distintas herramientas son muy similares, por lo que tan sólo se aportarán algunos apartados interesantes de esta herramienta.

Una de las ventajas de Joe Sandbox es que es capaz de generar un reporte en línea en formato HTML con el resumen de los hallazgos del análisis en varios niveles con información más o menos reducida y con una presentación distinta.

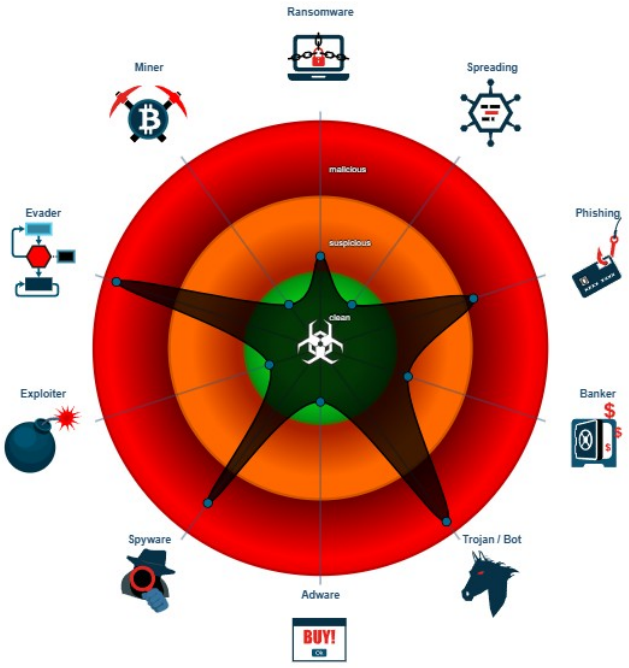
Imagen 15. *Tipos de reportes de Joe Sandbox.*



En la anterior imagen de pueden ver que existe un reporte completo con toda la información (*Full Report*), otro más escueto para gestión (*Management Report*) y otro para los IoCs así como otra pestaña específica.

En los hallazgos del reporte completo podemos ver información de más general a más específica según la necesidad. Por ejemplo, en la primera sección se nos muestra la clasificación del *malware* en un diagrama para que rápidamente podamos conocer con qué tipo de muestra estamos tratando y sus capacidades.

Imagen 16. *Clasificación del malware en diagrama de Joe Sandbox.*



En el caso de la muestra, como se puede ver en la imagen anterior, se trata de un troyano/spyware con capacidades de evasión y que utiliza técnicas como el phishing para la intrusión.

También se puede obtener información mucho más especifica como las claves de registro accedidas o modificadas en el reporte de IoCs de la herramienta.

Imagen 17. *Claves de registro accedidas por la muestra en Joe Sandbox.*

Registry

Path	Value	Malicious
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\...	EnableSmartScreen	

Details	
TargetID:	5
Path:	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System
Value name:	EnableSmartScreen
Value data:	0

Signature Hits	Behavior Group	Mitre Attack

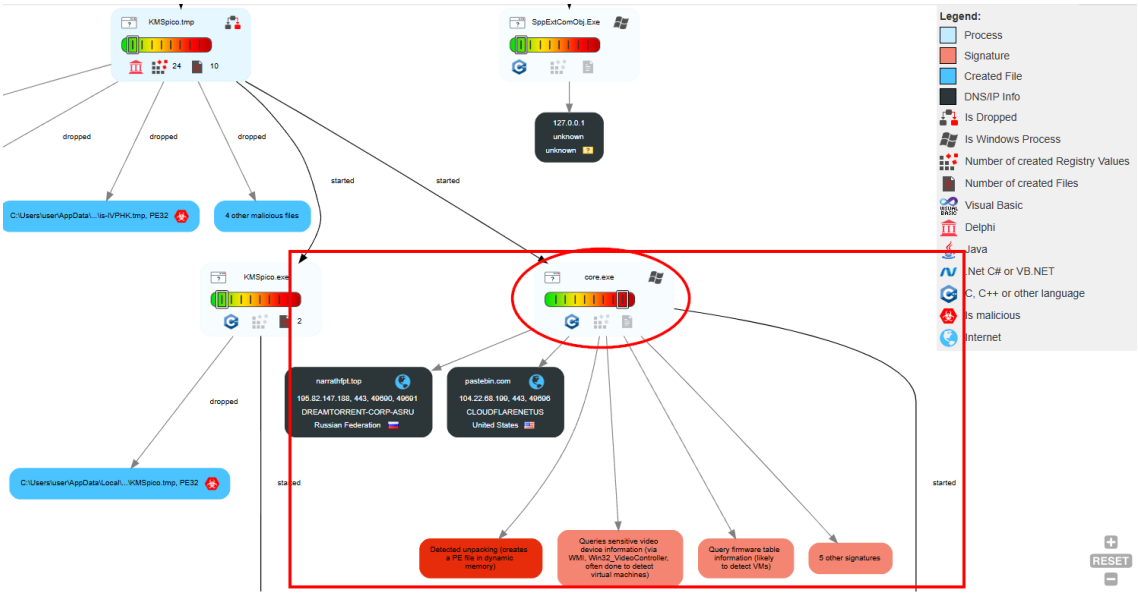
Path	Value	Malicious
HKEY_LOCAL_MACHINE\SOFTWARE\Microsof...	SmartScreenEnabled	

Details	
TargetID:	5
Path:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
Value name:	SmartScreenEnabled
Value data:	Off

En la anterior imagen se puede ver que se han accedido a las claves relacionadas con la funcionalidad de *SmartScreen* del dispositivo Windows infectado con el objetivo de deshabilitar su protección, pues esta es una característica de Microsoft Defender que bloquea sitios maliciosos o de phishing y evita la descarga de ficheros de fuentes no confiables de Internet.

Por último, una de las mayores funcionalidades de esta herramienta es el gráfico de comportamiento en el que se puede ver los distintos procesos creados por la muestra, las conexiones y sus acciones y capacidades en texto. Dado las dimensiones de este gráfico, simplemente se mostrará un extracto de la creación del proceso core.exe y sus acciones, no obstante, se adjunta un enlace al reporte para poder visualizar el gráfico completo.

Imagen 18. *Creación del proceso core.exe por KMSPico.*



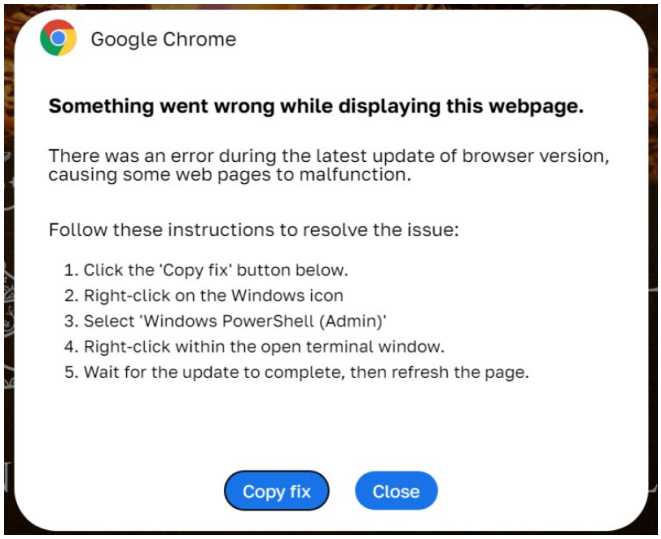
Inteligencia y Artefactos

Vectores de ataque

Lumma Stealer despliega multitud de técnicas de entrega que van evolucionando y adaptándose a lo largo del tiempo con el objetivo de evadir defensas y mejorar el éxito de las infecciones. A continuación, se listan algunos de los vectores de ataque utilizados por esta amenaza para infectar a sus víctimas.

- **Phishing/Email:** Suelen ser correos en los que se hace pasar por una entidad conocida y en las que hay algún enlace o adjunto que contiene la carga útil. Normalmente se caracterizan por provocar urgencia o contener algún tipo de incentivo para interactuar rápido con el *email*.
- **Malvertising**: En ocasiones se utilizan anuncios fraudulentos en los que se promociona una actualización de alguna aplicación como el navegador web Chrome, pero que en realidad llevan a una página web clonada que descarga el *stealer*.
- **ClickFix**: Consiste en engañar al usuario mediante ingeniería social para que ejecute un script PowerShell codificado en base64 en la ventana Run del sistema generalmente como método de verificación de un captcha o para corrección de errores. En realidad, esto lanza un comando que descarga Lumma Stealer y lo ejecuta en memoria.

Imagen 19. *Ejemplo de mensaje ClickFix.*

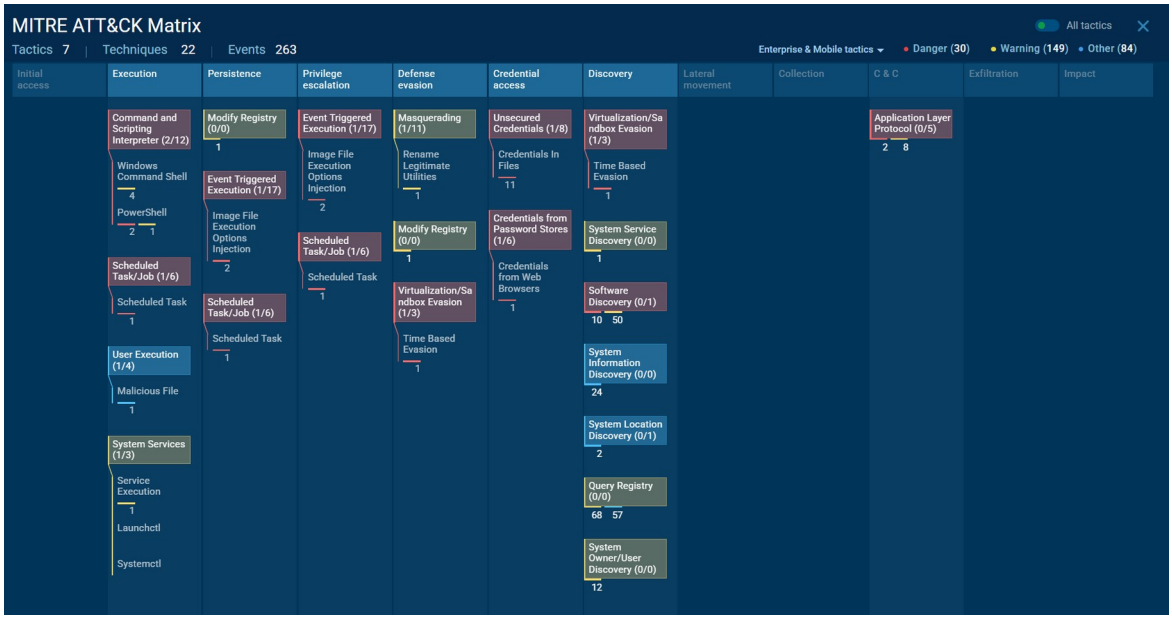


- **Aplicaciones troyanizadas**: En algunas campañas se utiliza software *pirata* de versiones de software legítimo donde se incluye el *stealer* empaquetado y se distribuye a través de plataformas de compartición de archivos. Estas campañas son más sigilosas ya que no tienen ningún elemento visible al ejecutar el software objetivo. Es el caso de la muestra con KMSPico.

TTPs

A continuación, se muestra la matriz de MITRE con las Tácticas, Técnicas y Procedimientos utilizados por el malware de la muestra durante la ejecución en ANY.RUN.

Imagen 20. *TTPs de Lumma Stealer en ANY.RUN*



IoCs

Indicador	Tipo	Descripción
`escczlv[.]top`	Dominio	Dominio Lumma Infraestructura
`narrathtfpt[.]top`	Dominio	Dominio Lumma Infraestructura
`screhwc[.]live`	Dominio	Dominio Lumma Infraestructura
TeslaBrowser/5.5	User Agent	Lumma C2 POST Request
144.76.173[.]247	IP	Infraestructura C2 Lumma Stealer
45.9.74[.]78	IP	Infraestructura C2 Lumma Stealer
77.73.134[.]68	IP	Infraestructura C2 Lumma Stealer
82.117.255[.]127	IP	Infraestructura C2 Lumma Stealer
`C:\Users\user\AppData\Roaming\MyApp\core.exe`	Proceso	Proceso `core.exe` del malware.
`HKLM\SOFTWARE\Policies\Microsoft\Windows\System`	Registro	Clave de registro accedida por Lumma Stealer
`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer`	Registro	Clave de registro accedida por Lumma Stealer
`C:\Users\user\AppData\Local\Temp\is-00FUR.tmp\KMSpico.tmp`	Fichero	Fichero instalado por la muestra.

Conclusiones y recomendaciones

Tras haber realizado el análisis sobre una muestra del malware *Lumma Stealer* utilizando distintas herramientas online de *sandboxing* como ANY.RUN, VirusTotal o Joe Sandbox se han obtenido una serie de conclusiones.

Se trata de una amenaza sofisticada diseñada para extraer credenciales, datos de navegación y archivos críticos de los sistemas infectados. Su capacidad para evadir detecciones mediante ofuscación, cifrado y técnicas de persistencia resalta la importancia de contar con soluciones de seguridad avanzadas, así como procesos de monitoreo continuo. La rapidez con la que este malware puede comprometer cuentas de usuario y facilitar movimientos laterales en la red subraya el riesgo de interrupciones operativas y posibles filtraciones de información estratégica, lo que podría derivar en un impacto reputacional y económico significativo para la organización.

Para mitigar el impacto que puede tener una infección de este tipo de malware se recomienda seguir un enfoque de defensa en profundidad, comenzando por un plan de formación y concienciación continua del personal en materia de ciberseguridad para evitar vectores de ataque como el *phishing*, *fake captcha*, *clickflix* o aplicaciones troyanizadas.

También se recomienda la implantación de sistemas de seguridad avanzada en equipos como EDR que permitan no sólo detectar y bloquear ataques conocidos basándose en firmas sino aprovechar el poder de la inteligencias artificial para detectar anomalías y prevenir infecciones. Así mismo se deberá de segmentar de manera adecuada las redes para evitar una rápida expansión del *malware*. Por último, se recomienda aplicar listas de control de acceso, segregación de permisos basados en roles (RBAC) y contar con al menos un segundo factor de autenticación. No obstante, esta medidas han de ser adaptadas e implementadas según las necesidades y capacidades específicas de la organización.

Referencias

- Reporte de Inteligencia sobre métodos de entrega de Lumma Stealer, *Microsoft*, https://www.microsoft.com/en-us/security/blog/2025/05/21/lumma-stealer-breaking-down-the-delivery-techniques-and-capabilities-of-a-prolific-infostealer/
- Análisis de VirusTotal, https://www.virustotal.com/gui/file/fcf8d40fe2db604954c51451d753a0e965996c43154bf506fdbdfbb3885ffce4/behavior
- Análisis de ANY.RUN, https://app.any.run/tasks/ec9a9a09-0415-4e36-8e5a-5456740a8118/
- Análisis de Joe Sandbox, https://www.joesandbox.com/analysis/1707440
- Información sobre Lumma Stealer, *Incibe*, https://www.incibe.es/servicio-antibotnet/info/LummaStealer
- Descripción del malware, *Malpedia*, https://malpedia.caad.fkie.fraunhofer.de/details/win.lumma