



27 DE NOVIEMBRE DE 2024

INFORME DE ANÁLISIS DE MALWARE

TROJAN.WIN32.MAKOOB.GEN

MARÍA RODRÍGUEZ



Contenido

1. Introducción.....	2
1.1. Objeto y objetivos del Estudio	2
1.2. Metodología	2
1.4. Herramientas utilizadas	3
1.5. Información general de la muestra.....	4
2. Análisis estático	6
2.1. Indicadores.....	6
2.2. Evaluación de la estructura del archivo	8
2.2. Análisis de entropía	14
2.3. Empaquetador	15
2.4. Análisis de comportamiento con strings	16
2.5. Análisis con Virustotal	18
3. Análisis dinámico	18
3.1. Análisis de procesos.....	18
3.3. Análisis de red.....	20
3.3. Análisis del comportamiento	25
Conclusiones	26

1. Introducción

1.1. Objeto y objetivos del Estudio

Objeto del estudio

En este trabajo se analiza el comportamiento del malware Makoob, aplicando tanto técnicas de análisis estático como dinámico para entender su funcionalidad, origen e impacto potencial. El objetivo es diseccionar las características clave de este troyano y comprender cómo opera en los sistemas que compromete.

Para este estudio, se utiliza una muestra de Makoob que será evaluada mediante herramientas especializadas de análisis. Estas herramientas permiten explorar el comportamiento del malware desde dos perspectivas: una inspección estática para identificar atributos internos del archivo y una dinámica que simula su ejecución en un entorno controlado. El laboratorio empleado para las pruebas consta de una máquina virtual con el sistema operativo Windows 7, configurado para capturar su actividad de manera segura y detallada.

Objetivos del estudio

Los objetivos específicos de este estudio son los siguientes:

- Comprender la funcionalidad de Makoob
- Analizar su estructura interna
- Evaluar su comportamiento dinámico
- Determinar su origen y propósito
- Medir su impacto potencial
- Proponer medidas de mitigación y detección

1.2. Metodología

Los métodos utilizados en este análisis de malware son de dos tipos:

Análisis estático

El análisis estático de malware es una técnica de ciberseguridad para estudiar el comportamiento y las características de un malware sin ejecutarlo en un sistema. Su objetivo es obtener información sobre el comportamiento potencial del malware, sus capacidades, y las amenazas que representa, todo esto sin activar su código. Este tipo de análisis se realiza examinando el archivo malicioso directamente, utilizando herramientas y técnicas para extraer información sobre su

estructura, funcionalidad y posibles impactos. Este enfoque es seguro porque no expone el entorno de análisis al riesgo de infección.

Análisis dinámico

El análisis dinámico de malware es el proceso de ejecutar un archivo malicioso en un entorno controlado para observar y registrar su comportamiento en tiempo real. A diferencia del análisis estático, que examina el malware sin ejecutarlo, este enfoque permite identificar cómo interactúa el malware con el sistema, sus objetivos y las acciones que lleva a cabo, como cambios en el sistema, comunicaciones en red, y procesos iniciados.

El análisis dinámico de malware es una técnica clave en ciberseguridad para entender cómo se comporta un archivo malicioso en un sistema. Al complementarlo con el análisis estático, se obtiene una visión más completa del malware, sus objetivos y sus métodos, ayudando a desarrollar contramedidas efectivas.

1.4. Herramientas utilizadas

Hardenización del entorno virtual:

- Pafish: Simula actividades de malware para detectar entornos virtuales o sandbox.
- VBoxHardener: Endurece la configuración de VirtualBox para hacerla menos detectable por malware que busca evitar máquinas virtuales.

Análisis estático:

- Portex Analyzer: Analiza características de archivos binarios, como patrones de código, empaquetado, y comportamiento. Ideal para detectar malware empaquetado.
- Resource Hacker: Permite editar y explorar los recursos de un archivo ejecutable (íconos, cadenas, imágenes, etc.).
- PE Studio: Realiza análisis estático de archivos PE para detectar secciones sospechosas, cadenas, importaciones y comportamientos maliciosos.
- Strings: Extrae cadenas de texto de un archivo binario.
- Protection ID: Detecta empaquetadores y herramientas de protección en archivos ejecutables. Ayuda a identificar cómo un archivo PE ha sido protegido o empaquetado.
- PEiD: herramienta para analizar ejecutables y detectar si están empaquetados o comprimidos.

- Detect It Easy (Die): identificar empaquetadores, compiladores, protectores y otros aspectos técnicos relacionados con archivos binarios.

Análisis dinámico

- Any.run: plataforma de análisis dinámico en línea que permite ejecutar y analizar archivos sospechosos, incluidas muestras de malware, en un entorno aislado y seguro.

1.5. Información general de la muestra

Se analiza un archivo ejecutable de tipo Portable Executable (PE) con extensión .exe. El archivo tiene un tamaño de 1.2 MB y su hash SHA-256 es 915903938dd1c51abd0f1e2f35e0fca67040694d9f5b1edd5825533a70a7269f. Ha sido identificado preliminarmente como un posible troyano del tipo Makoob.

Trojan.Win32.Makoob.gen es un programa malicioso diseñado para espiar electrónicamente las actividades del usuario (interceptar la entrada del teclado, tomar capturas de pantalla, capturar una lista de aplicaciones activas, etc.). La información recopilada se envía al cibercriminal por diversos medios, incluido el correo electrónico, FTP y HTTP (mediante el envío de datos en una solicitud).

Opera en la plataforma Win32, que es una API de los sistemas operativos basados en Windows NT (Windows XP, Windows 7, etc.) que permite la ejecución de aplicaciones de 32 bits.

Históricamente, este malware ha sido asociado con campañas diseñadas para distribuir cargas útiles adicionales o para disfrazarse de software legítimo. Una característica clave es su capacidad para evitar detección mediante el uso de técnicas de ofuscación, además de emplear métodos como la manipulación de tokens de acceso para operar con mayores privilegios y evadir restricciones del sistema.

Su distribución frecuentemente incluye vectores de infección como descargas maliciosas, correos electrónicos de phishing y empaquetamiento dentro de otros archivos aparentemente legítimos. Este troyano puede realizar tareas como modificar configuraciones del sistema y desactivar herramientas de seguridad, lo que lo convierte en una amenaza persistente y peligrosa.

Aunque la fecha exacta de su aparición inicial no está claramente definida, su detección se intensificó entre 2019 y 2021, cuando analistas comenzaron a identificar muestras asociadas a este malware en plataformas como VirusTotal.

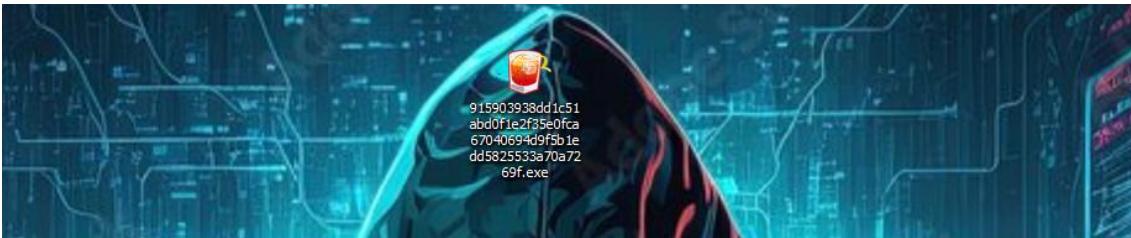


Imagen 1. Muestra utilizada en este estudio.

pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\master\desktop\915903938dd1c51abd0f1e2f35e0fca67040694d9f5b1ed0]

file settings about

property	value
md5	BCF1B4C359D89892CBDEDDCAC52FD4D7
sha1	3C12D1EFE6438FED0BCEC88C23C5994C44066E43
sha256	915903938DD1C51ABD0F1E2F35E0FCA67040694D9F5B1EDD5825533A70A7269F
md5-without-overlay	04CBFC423F9C21800572262E75A5E606
sha1-without-overlay	D132E38A13B9837875ECF5673E1B66EA993D9DF6
sha256-without-over...	84D8DBD4ACD1C9585D7DCAF1F17FEF49F0EBAD5E29C08223F74E8CB5FF33AAA5
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 40 00 00...
first-bytes-text	M Z @
file-size	1135960 (bytes)
size-without-overlay	392160 (bytes)
entropy	7.054
imphash	n/a
signature	n/a
entry-point	81 EC 84 01 00 00 53 56 57 33 DB 68 01 80 00 00 89 5C 24 18 C7 44 24 10 98 91 4...
file-version	2.2.0.0
description	taus
file-type	executable
cpu	32-bit
subsystem	GUI
compiler-stamp	0x57807BB9 (Sat Jul 09 06:21:13 2016)
debugger-stamp	n/a
resources-stamp	
exports-stamp	n/a
version-stamp	empty
certificate-stamp	0x0655ED80 (Sat Aug 10 09:22:15 2024)

Imagen 2. Información sobre la muestra obtenida de PESTudio.

2. Análisis estático

2.1. Indicadores

Los indicadores proporcionan información detallada sobre las características del archivo PE, específicamente sobre patrones o comportamientos que podrían indicar que el archivo es malicioso. A continuación, se detalla la información sobre los indicadores proporcionada por PESTudio:

Xml-id	Información	Nivel
1430	El archivo contiene 40 cadenas que han sido etiquetadas como blacklist. Una cadena en lista negra es un texto conocido por estar relacionado con actividades maliciosas, como comandos, URLs, nombres de dominio, rutas de archivos, o palabras clave específicas usadas por el malware.	1
1525	El archivo contiene un archivo incrustado, además de una firma que lo asocia a Nullsoft Installer. Este software se suele usar como empaquetador en malware. El archivo incrustado se encuentra en la sección overlay del archivo principal.	1
1266	El archivo importa 37 funciones (<i>symbols</i>) que están etiquetadas como maliciosos o sospechosos según una lista negra. Los símbolos son funciones o API que el archivo llama desde bibliotecas externas (como DLLs).	1
1434	El archivo contiene una referencia a la URL http://nsis.sf.net/NSIS_Error , que es una URL legítima asociada al instalador NSIS (Nullsoft Scriptable Install System). Esto es otro indicador de que el malware usa NSIS como método de empaquetado.	1
1003	La proporción alta del overlay (65,48%) sugiere que el archivo malicioso está utilizando esta sección para ocultar componentes adicionales, como payloads, scripts, o datos de configuración	
1262	El archivo importa una función anónima desde una biblioteca o recurso externo.	2
1153	El archivo contiene una sección virtualizada (.ndata), lo que sugiere que el malware utiliza técnicas avanzadas de ofuscación y ocultación. La sección .ndata probablemente contiene código o datos transformados. Dificulta el análisis estático y dinámico, ya que las instrucciones reales no están directamente visibles en el archivo.	2
1019	El archivo contiene un rich-header que hace referencia a Visual Studio, que es un bloque de metadatos que se encuentra en los archivos binarios PE, y es utilizado para	3

	almacenar información relacionada con la compilación del archivo.	
1241	Se ha encontrado una identidad de manifiesto dentro del archivo con el nombre Nullsoft.NSIS.exehead.	3
1424	El archivo tiene un nombre original que ha sido identificado: sita strengeinstruments.exe	3
1261	El archivo importa 14 funciones obsoletas. El uso excesivo de funciones obsoletas puede ser una señal de que el archivo está intentando evadir detección	3
1634 en adelante	El archivo malicioso usa funciones de la API, que están relacionadas con la manipulación de archivos, de registro, de DLLs, de ejecución, de sincronización, de memoria, de información del sistema, de almacenamiento, de diagnóstico, de windowing, de ratón y teclado, de administración, de recursos, de intercambio de datos, de seguridad y de Shell.	3
1633	El archivo malicioso hace referencia a un grupo de pistas. En este caso, la pista está relacionada con el privilegio dentro del sistema. Esto podría indicar que el archivo intenta obtener privilegios elevados o está relacionado con un exploits de escalada de privilegios.	

pestudio 9.09 - Malware Initial Assessment - www.winitior.com [c:\users\master\downloads\915903938dd1c51abd0f1e2f35e0fca67040694d9f5b1edd5825533a70a7269f.exe]

file settings about

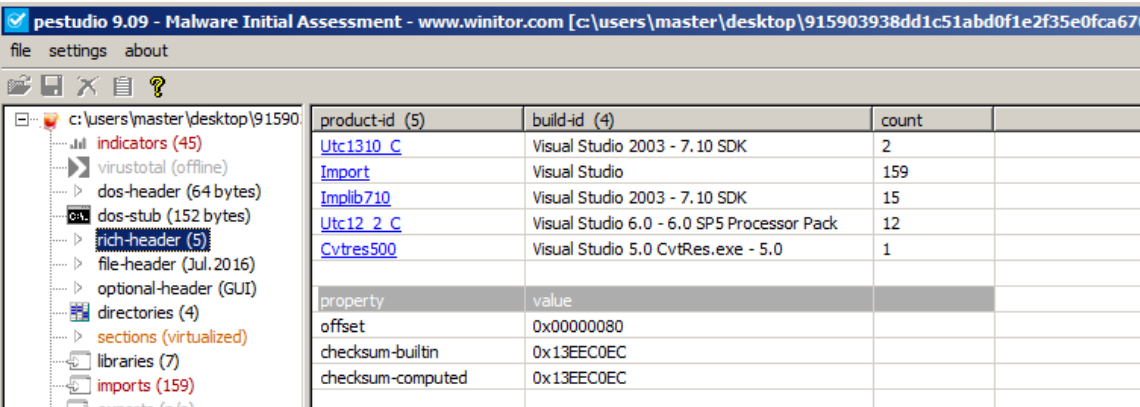
xml-id	indicator (45)	detail	level
1430	The file references string(s) tagged as blacklist	count: 40	1
1525	The file contains another file	signature: Nullsoft, location: overlay, offset: 0x0005EA0...	1
1266	The file imports symbol(s) tagged as blacklist	count: 23	1
1265	The count of imports is suspicious	count: 124	1
1434	The file references a URL pattern	url: http://nsis.sf.net/NSIS_Error	1
1003	The file-ratio of the overlay is suspicious	ratio: 65.48 %	2
1153	The file contains a virtualized section	section: .ndata	2
1120	The file is scored by virustotal	score: 51/71	3
1019	The file contains a rich-header	status: yes	3
1241	The manifest identity has been found	name: Nullsoft.NSIS.exehead	3
1424	The original name of the file has been found	name: sita strengeinstruments.exe	3
1011	The file references a certificate	size: 4576 bytes	3
1261	The file imports deprecated function(s)	count: 12	3
1634	The file references a group of API	api: file, count: 29	3
1634	The file references a group of API	api: registry, count: 12	3
1634	The file references a group of API	api: dynamic-library, count: 6	3
1634	The file references a group of API	api: execution, count: 10	3
1634	The file references a group of API	api: synchronization, count: 1	3
1634	The file references a group of API	api: memory, count: 5	3
1634	The file references a group of API	api: system-information, count: 7	3
1634	The file references a group of API	api: storage, count: 4	3
1634	The file references a group of API	api: diagnostic, count: 1	3
1634	The file references a group of API	api: windowing, count: 18	3
1634	The file references a group of API	api: keyboard-and-mouse, count: 2	3
1634	The file references a group of API	api: administration, count: 1	3
1634	The file references a group of API	api: resource, count: 1	3
1634	The file references a group of API	api: data-exchange, count: 4	3
1634	The file references a group of API	api: security, count: 3	3
1634	The file references a group of API	api: shell, count: 1	3
1633	The file references a group of hint	hint: dos-message, count: 1	3
1633	The file references a group of hint	hint: utility, count: 3	3
1633	The file references a group of hint	hint: registry, count: 1	3
1633	The file references a group of hint	hint: file, count: 15	3
1633	The file references a group of hint	hint: url-pattern, count: 1	3
1633	The file references a group of hint	hint: privilege, count: 1	3
1633	The file references a group of hint	hint: base64, count: 3	3
1268	The file references whitelisted string(s)	count: 2	4
1050	The file uses Control Flow Guard (CFG) as software security defense	status: no	4
1100	The file opts for Data Execution Prevention (DEP) as software security defense	status: yes	4
1102	The file opts for Address Space Layout Randomization (ASLR) as software security defense	status: yes	4
1043	The file contains a Manifest	status: yes	4
1106	The file opts for Stack Buffer Overrun Detection (GS) as software security defense	status: no	4
1109	The file opts for Code Integrity (CI) as software security defense	status: no	4
1287	The file subsystem has been found	type: GUI	4
1215	The file-ratio of the section(s) has been determined	ratio: 34.03%	4

Imagen 3. Indicadores de compromiso obtenidos con PESTudio.

2.2. Evaluación de la estructura del archivo

Encabezados

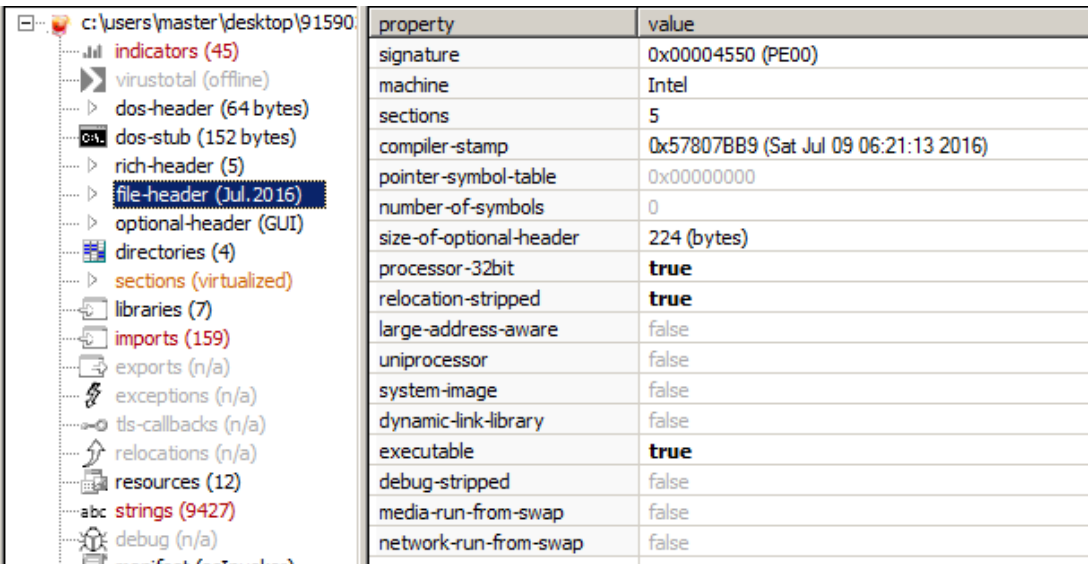
El rich header es un encabezado opcional que se encuentra al comienzo de algunos archivos PE. una forma de almacenar metadatos relacionados con la herramienta de compilación que se utilizó para crear el archivo, en este caso Visual Studio.



product-id (5)	build-id (4)	count	
Utc1310_C	Visual Studio 2003 - 7.10 SDK	2	
Import	Visual Studio	159	
Implib710	Visual Studio 2003 - 7.10 SDK	15	
Utc12_2_C	Visual Studio 6.0 - 6.0 SP5 Processor Pack	12	
Cvtres500	Visual Studio 5.0 CvtRes.exe - 5.0	1	
property	value		
offset	0x00000080		
checksum-builtin	0x13EEC0EC		
checksum-computed	0x13EEC0EC		

Imagen 4. Información sobre el rich header obtenida con PESTudio.

Por otro lado, la cabecera del archivo sugiere que es un ejecutable Portable Executable (signature: 0x00004550 (PE00) diseñado para procesadores Intel de 32 bits. Muestra la fecha y hora en que el archivo fue compilado: 0x57807BB9 (Sat Jul 09 06:21:13 2016). Esto puede ayudar a determinar cuándo fue creado el malware.



property	value
signature	0x00004550 (PE00)
machine	Intel
sections	5
compiler-stamp	0x57807BB9 (Sat Jul 09 06:21:13 2016)
pointer-symbol-table	0x00000000
number-of-symbols	0
size-of-optional-header	224 (bytes)
processor-32bit	true
relocation-stripped	true
large-address-aware	false
uniprocessor	false
system-image	false
dynamic-link-library	false
executable	true
debug-stripped	false
media-run-from-swap	false
network-run-from-swap	false

Imagen 5. Información sobre la cabecera del archivo.

Secciones

Las secciones de un archivo ejecutable son diferentes partes en las que se organiza el contenido del archivo. Cada sección tiene un propósito específico y contiene diferentes tipos de datos.

A continuación, examinamos las secciones internas del malware en busca de datos inusuales o permisos anómalos; a excepción de la entropía que será analizada en profundidad más adelante.

Sección .text

Esta sección contiene el código de la aplicación, es decir, las instrucciones que la CPU ejecutará.

- **Tamaño de archivo:** 20480 bytes
- **Tamaño virtual:** 23976 bytes
- **Características:** 0x60000020

El tamaño de la sección .text es considerable, lo que indica que el archivo contiene una cantidad significativa de código ejecutable. El tamaño virtual es ligeramente mayor que el tamaño del archivo, lo cual es normal.

Las características indican que esta sección es legible y ejecutable, pero no escribible, lo cual es estándar para secciones de código.

Sección .rdata

Almacena datos de lectura que no deben modificarse durante la ejecución del programa, como cadenas de texto y tablas de funciones importadas.

- **Tamaño de archivo:** 5120 bytes
- **Tamaño virtual:** 4878 bytes
- **Características:** 0x40000040

Esta sección no es escribible ni ejecutable, lo que protege los datos almacenados contra modificaciones y ejecución no deseada.

Sección .data:

Almacena datos globales y estáticos que el programa usa y puede modificar durante su ejecución. A diferencia de la sección .text (que contiene el código ejecutable del programa), los datos en .data son variables inicializadas y generalmente modificables.

- **Tamaño de archivo:** 1024 bytes
- **Tamaño virtual:** 377472 bytes
- **Características:** 0xC0000040

Esta sección es tanto legible como escribible, pero no ejecutable, lo que permite que los datos sean modificados durante la ejecución del programa.

La discrepancia significativa entre el tamaño de archivo y el tamaño virtual en la sección .data sugiere que esta sección contiene muchos datos que ocuparán más espacio en memoria una vez que el programa esté en ejecución. Esta característica es típica en malware que requiere grandes cantidades de datos en memoria.

Sección .rsrc

La sección .rsrc contiene recursos no ejecutables del programa, como iconos, imágenes, menús y cadenas de texto que forman parte de la interfaz gráfica o de configuración del programa.

- **Tamaño de archivo:** 356352 bytes
- **Tamaño virtual:** 356096 bytes
- **Características:** 0x40000040

Esta sección es de solo lectura, protegiendo los recursos almacenados contra modificaciones durante la ejecución.

El gran tamaño de la sección .rsrc indica que el archivo contiene muchos recursos, como iconos, imágenes, menús, etc. En malware, esta sección a veces se usa para esconder datos maliciosos, como scripts o payloads adicionales.

Analizamos el contenido con ResourceHacker:

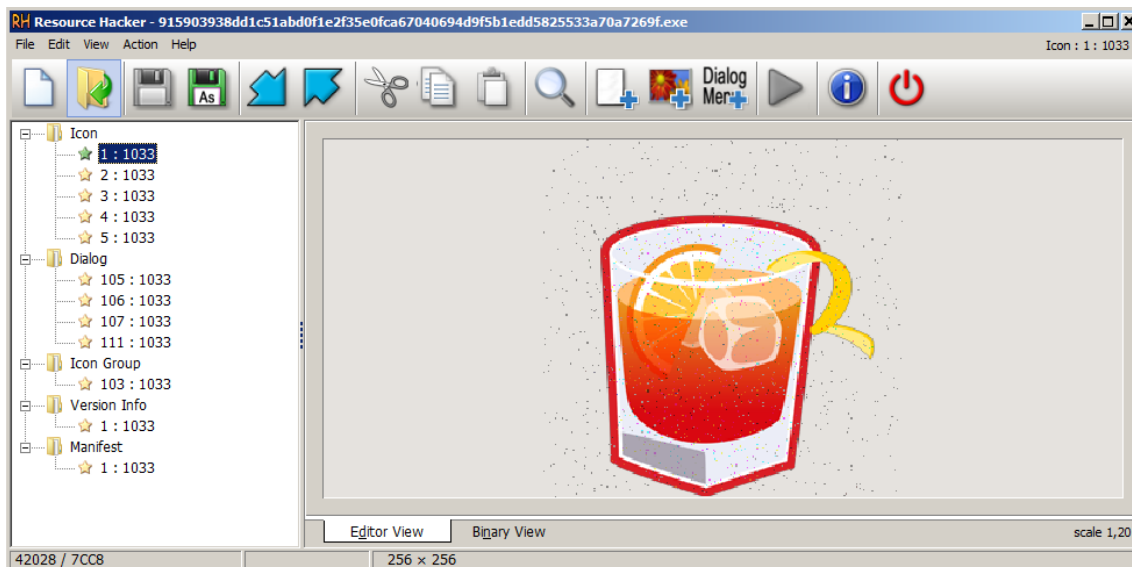


Imagen 6. Análisis de recursos con ResourceHacker.

pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\master\downloads\915903938dd1c51abd0f1e2f35e0ca67040694d9f5b1edd5825533a70a7269f.exe]												
file settings about												
	Type (5)	name	file offset (12)	signature (3)	non-standard	size (35372 bytes)	file ratio (31.28%)	md5	entropy	language (1)	first bytes hex	first bytes text
indicators (45)	version	D:\000SE368	version	-	600	0.05 %		FAD3D42C5C03A8AAB872843C401E	3.153	English-Lit...	58 02 34 00 00 00 56 00 53 00 5F 00 58	X - 4 ... V ... V ... E ...
	manifest	D:\000SE3C0	manifest	-	832	0.07 %		6C3B0E0F20A2C3C3B0FAA8B8A892	3.299	English-Lit...	3C 3F 78 60 4C 20 76 6F 72 7A 69 4E	<?xml version="1
	dos-header (64 bytes)	con-group	D:\000SE318	con-group	-	76	0.01 %	0645E3174602F9C3C4E8345D011540	2.647	English-Lit...	00 00 01 00 05 00 00 00 00 01 00 20	(
	rich-header (152 bytes)	con	D:\00007C08	con	-	276376	23.80 %	6C86170FAD04FAC79F5D0414979044	3.289	English-Lit...	28 00 00 00 00 01 00 00 00 02 00 01	{
	file-header (Jul 20 16)	con	D:\000H0C00	con	-	67624	5.16 %	8803B842A449F8B05966F4A32060C	2.493	English-Lit...	28 00 00 00 00 00 00 01 00 00 01	{
optional-header (502)	con	D:\0005A318	con	-	9640	0.85 %		0C0A374E7136C74438662CFAC40	3.611	English-Lit...	28 00 00 30 00 00 00 00 00 00 01	{
directories (4)	con	D:\0005AC03	con	-	4264	0.38 %		A4DE4A8B039E13F5F3681614E7F7F8	3.714	English-Lit...	28 00 00 20 00 00 00 40 00 00 01	{
sections (virtualized)	con	D:\000SE368	con	-	1128	0.10 %		22A4A7B0C033F7367D5C3C362611	3.800	English-Lit...	28 00 00 00 20 00 00 20 00 00 01	{
libraries (7)	diaglog	D:\000SPF00	diaglog	-	256	0.02 %		240F14855161697F3C395CCF555325	2.662	English-Lit...	01 00 FF FF 00 00 00 00 00 00 48	{
imports (count)	diaglog	D:\000SE800	diaglog	-	284	0.03 %		201AC45DCAC02644A4F716714C36066	2.881	English-Lit...	01 00 FF FF 00 00 00 00 00 00 48	{
exports (n/a)	diaglog	D:\000SEFP0	diaglog	-	196	0.02 %		690759A3A456A32CF4F5F55A4D3006	2.623	English-Lit...	01 00 FF FF 00 00 00 00 00 00 48	{
tls-callbacks (n/a)	diaglog	D:\000SE2B8	diaglog	-	96	0.01 %		69E4E13B7036C7395D6E45C0C0E8100	2.488	English-Lit...	01 00 FF FF 00 00 00 00 00 00 C8	{
resources (12)												
strings (9427)												
manifest (edrvoker)												
version (Sita stringinstruments.exe)												
certificate (10/08/2024 - 10/08/2027)												
overlay (Nullsoft)												

Imagen 7. Contenido de la sección recursos con PESTudio.

Sección virtualizada .ndata

La sección. ndata no es una sección estándar en el formato PE (Portable Executable) utilizado por los archivos ejecutables en sistemas Windows. Su presencia sugiere que una sección personalizada introducida por el atacante o un empaquetador malicioso.

La virtualización de secciones es una técnica avanzada utilizada para proteger o esconder código malicioso. En este proceso, el código original se transforma en instrucciones de bajo nivel que se ejecutan en un entorno controlado por un intérprete o máquina virtual personalizada.

El archivo contiene una sección virtualizada (.ndata), lo que sugiere que el malware utiliza técnicas avanzadas de ofuscación y ocultación. La sección. ndata probablemente contiene código o datos transformados que requieren de una máquina virtual para ejecutarse. Esto dificulta el análisis estático y dinámico, ya que las instrucciones reales no están directamente visibles en el archivo.

En conclusión, estas observaciones indican que el malware puede ser complejo y multifuncional, con técnicas potenciales de evasión y almacenamiento oculto de datos maliciosos.

pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\master\downloads\915903938dd1c51abd0f1e2f35e0ca67040694d9f5b1edd5825533a70a7269f.exe]					
file settings about					
	property	value	value	value	value
name	.text	.ndata	.data	.ndata	.rsrc
md5	F367801E475B6529E2B53203...	43FAB6A80651BD97A9F34E...	29FBCBEC0B078D0FECB3D29...	n/a	ABC24A3634178E270F45B1...
entropy	6.508	5.005	5.108	n/a	3.379
file-ratio (34.03%)	2.12 %	0.45 %	0.09 %	n/a	31.37 %
raw-address	0x00000400	0x00006200	0x00007600	0x00000000	0x00007A00
raw-size (386560 bytes)	0x00005E00 (24064 bytes)	0x00001400 (5120 bytes)	0x00000400 (1024 bytes)	0x00000000 (0 bytes)	0x000057000 (356352 bytes)
virtual-address	0x00401000	0x00407000	0x00409000	0x007A3000	0x007BC000
virtual-size (4259636 bytes)	0x00005D66 (23990 bytes)	0x0001246 (4678 bytes)	0x00399038 (3772472 bytes)	0x00019000 (102400 bytes)	0x00056F00 (356096 bytes)
entry-point	0x000030EC				
characteristics	0x00000020	0x40000040	0xC0000040	0xC0000080	0x40000040
writable	-	-	X	X	-
executable	X	-	-	-	-
shareable	-	-	-	-	-
discardable	-	-	-	-	-
initialized-data	-	X	X	-	X
uninitialized-data	-	-	X	-	-
unreadable	-	-	-	-	-
self-modifying	-	-	-	-	-
virtualized	-	-	-	X	-
file	n/a	n/a	n/a	n/a	n/a

Imagen 8. Información sobre las secciones obtenidas con PESTudio.

Overlay

El overlay es cualquier dato que se encuentra después de la última sección definida en la cabecera del archivo PE. Este contenido no forma parte de las secciones estándar (como .text, .data, .rsrc) y puede incluir:

- Datos añadidos intencionalmente, como recursos adicionales o configuraciones específicas.
- Código o datos insertados maliciosamente, como payloads de malware.
- Información legítima, como firmas digitales, aunque estas suelen tener una entropía más baja.

Bibliotecas o funciones compartidas

Las librerías en las que ha habido importaciones son las siguientes:

- Kernel32.dll contiene funciones esenciales para la gestión de procesos, archivos y memoria. Su uso es crucial para que el malware manipule estos recursos del sistema operativo. Por ejemplo, funciones como CreateFile, WriteFile, y ReadFile son fundamentales para las operaciones de entrada/salida de archivos.
- User32.dll contiene funciones para la gestión de la interfaz de usuario (ventanas, menús, etc.). El malware puede usar esta librería para manipular ventanas y eventos del usuario, lo que permite la creación de ventanas emergentes engañosas o la captura de entradas del usuario.
- Gdi32.dll proporciona funciones para el manejo de gráficos y dispositivos. El malware puede usar esta librería para dibujar elementos gráficos en la pantalla, manipular imágenes o crear interfaces visuales maliciosas.
- Shell32.dll contiene funciones relacionadas con el shell de Windows, como la gestión de archivos y la ejecución de programas. El malware puede utilizar esta librería para lanzar otros programas maliciosos o manipular el sistema de archivos.
- Advapi32.dll proporciona funciones avanzadas de gestión de seguridad y registro. El malware puede usar esta librería para modificar permisos de seguridad, crear procesos con privilegios elevados o acceder y modificar el registro de Windows.
- Comctl32.dll contiene controles comunes de interfaz de usuario, como botones y cuadros de texto. El malware puede usar esta librería para crear interfaces de usuario que imiten aplicaciones legítimas y engañen al usuario.

- Ole32.dll permite la creación y gestión de objetos OLE (Object Linking and Embedding). El malware puede usar esta librería para integrar componentes de otras aplicaciones o manipular objetos embebidos.

pestudio 9.09 - Malware Initial Assessment - www.winator.com [c:\users\master\downloads\915903938dd1c51abd0f1e2f35e0fca67040694d9f5b1edd5825533a70a7269f.exe]

file settings about

c:\users\master\downloads\915903938dd1c51abd0f1e2f35e0fca67040694d9f5b1edd5825533a70a7269f.exe

library (7)	blacklist (0)	type (1)	imports (124)	description
kernel32.dll	-	implicit	61	Windows NT BASE API Client DLL
user32.dll	-	implicit	63	Multi-User Windows USER API Client DLL
gdi32.dll	-	implicit	0	GDI Client DLL
shell32.dll	-	implicit	0	Windows Shell Common Dll
advapi32.dll	-	implicit	0	Advanced Windows 32 Base API
comctl32.dll	-	implicit	0	Common Controls Library
ole32.dll	-	implicit	0	Microsoft OLE for Windows

Imagen 9. Información sobre las librerías obtenida con PESTudio.

Importaciones

Observamos que, de los 159 importes, 37 pertenecen a una blacklist.

imports (159)

function	library	type	blacklist	description
SetForegroundWindow	windowing	implicit	x	user32.dll
FindWindowExA	windowing	implicit	x	user32.dll
GetCurrentDirectoryA	storage	implicit	x	kernel32.dll
SearchPathA	storage	implicit	x	kernel32.dll
OpenProcessToken	security	implicit	x	advapi32.dll
LookupPrivilegeValueA	security	implicit	x	advapi32.dll
AdjustTokenPrivileges	security	implicit	x	advapi32.dll
WritePrivateProfileStringA	registry	implicit	x	kernel32.dll
RegDeleteKeyA	registry	implicit	x	advapi32.dll
RegDeleteValueA	registry	implicit	x	advapi32.dll
RegSetValueExA	registry	implicit	x	advapi32.dll
RegEnumKeyA	registry	implicit	x	advapi32.dll
SetFileAttributesA	file	implicit	x	kernel32.dll
RemoveDirectoryA	file	implicit	x	kernel32.dll
GetTempFileNameA	file	implicit	x	kernel32.dll
MoveFileExA	file	implicit	x	kernel32.dll
MoveFileA	file	implicit	x	kernel32.dll
FindFirstFileA	file	implicit	x	kernel32.dll
FindNextFileA	file	implicit	x	kernel32.dll
DeleteFileA	file	implicit	x	kernel32.dll
SHGetSpecialFolderLocation	file	implicit	x	shell32.dll
SHGetPathFromIDListA	file	implicit	x	shell32.dll
SHBrowseForFolderA	file	implicit	x	shell32.dll
SHGetFileInfoA	file	implicit	x	shell32.dll
SHFileOperationA	file	implicit	x	shell32.dll
SetFileSecurityA	file	implicit	x	advapi32.dll
SetEnvironmentVariableA	execution	implicit	x	kernel32.dll
CreateProcessA	execution	implicit	x	kernel32.dll
GetExitCodeProcess	execution	implicit	x	kernel32.dll
ShellExecuteA	execution	implicit	x	shell32.dll
GetModuleFileNameA	dynamic-library	implicit	x	kernel32.dll
CloseClipboard	data-exchange	implicit	x	user32.dll
SetClipboardData	data-exchange	implicit	x	user32.dll
EmptyClipboard	data-exchange	implicit	x	user32.dll
OpenClipboard	data-exchange	implicit	x	user32.dll
ExitWindowsEx	administration	implicit	x	user32.dll
SystemParametersInfoA	-	implicit	x	user32.dll

Imagen 10. Información sobre las importaciones del archivo obtenida con PESTudio.

2.2. Análisis de entropía

Calcular la entropía de cada sección del archivo, identificando secciones con entropía alta en lugares inusuales, lo que puede indicar presencia de código malicioso oculto.

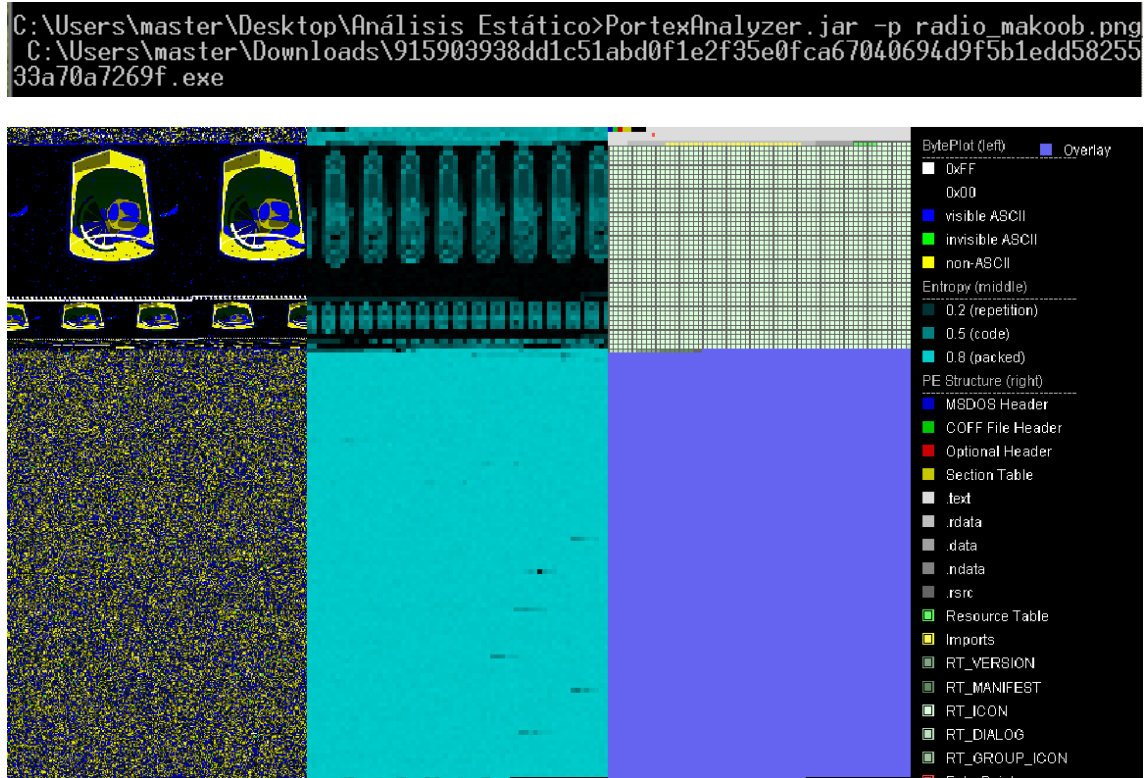


Imagen 11. Radiografía del malware con Portex Analyzer

El nivel de entropía elevado indica que este archivo podría estar empaquetado o cifrado. La sección .rsrc y otros recursos (iconos o manifestos) podrían ser un intento de suplantación de software legítimo. La mezcla de entropía alta con baja y las secciones ricas en recursos suelen ser características de malware diseñado para evadir análisis estáticos.



Imagen 12. Análisis de entropía con Die.

Entropía alta en .text: Una alta entropía (6.208) sugiere que esta sección está densamente poblada con instrucciones ejecutables. Esto es típico en malware que busca realizar múltiples acciones.

Entropía moderada en .rdata: La entropía moderada (5.005) indica un nivel moderado de aleatoriedad, coherente con datos estructurados y no ejecutables.

Entropía baja en .data: La baja entropía (1.998) sugiere que la sección contiene datos predecibles o repetitivos, como variables globales y estáticas inicializadas.

Entropía baja en .rsrc: La entropía (3.779) es más baja que en las secciones de código, lo que es consistente con el almacenamiento de datos no ejecutables.

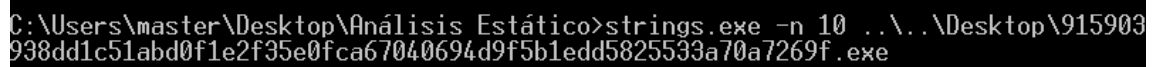
Muy alta entropía en overlay (casi 8): Un overlay con alta entropía es común en malwares que utilizan empaquetadores o técnicas de ofuscación para evitar la detección.

2.3. Empaquetador

Utiliza Nullsoft SFX Setup v3.0rc2 como empaquetador. Esto sugiere que el archivo podría estar diseñado para extraer y ejecutar un componente adicional o carga útil durante su instalación.

2.4. Análisis de comportamiento con strings

Analizamos el contenido del malware con el comando strings:



```
C:\Users\master\Desktop\Análisis Estático>strings.exe -n 10 ..\..\Desktop\915903938dd1c51abd0f1e2f35e0fca67040694d9f5b1edd5825533a70a7269f.exe
```

Imagen 13. Comando strings

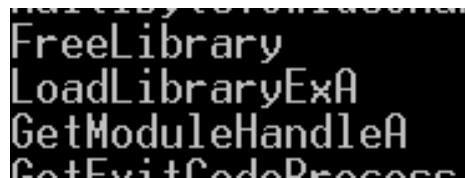
Cadenas como DeleteFileA, FindFirstFileA, FindNextFileA, SetFilePointer, SetFileAttributesA, GetFileAttributesA, GetFileSize indican que el malware interactúa con archivos del sistema. Puede buscar, leer, modificar atributos o eliminar archivos específicos.



```
\Microsoft\Internet Explorer\Quick Launch  
DeleteFileA  
FindFirstFileA  
FindNextFileA  
SetFilePointer  
GetPrivateProfileStringA
```

Imagen 14. Cadenas para manipulación del Sistema de Archivos:

LoadLibraryExA, GetModuleHandleA, FreeLibrary indican que el malware puede cargar dinámicamente bibliotecas de Windows para acceder a funciones específicas. Esto es típico en troyanos que cargan módulos adicionales.



```
FreeLibrary  
LoadLibraryExA  
GetModuleHandleA  
GetExitCodeProcess
```

Imagen 15. Cadenas de interacción con bibliotecas y recursos

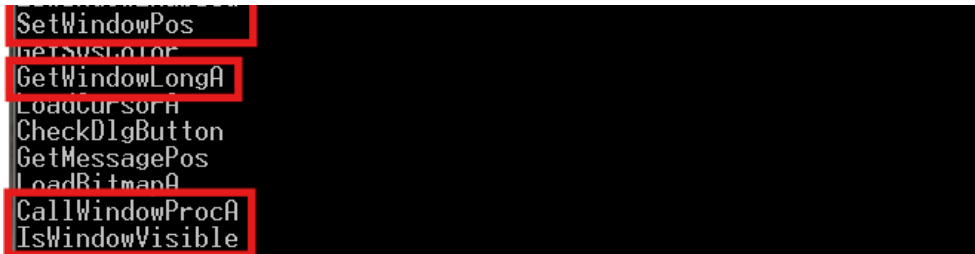
SetEnvironmentVariableA, GetWindowsDirectoryA, GetTempPathA muestran que el troyano interactúa con variables de entorno, posiblemente para localizar rutas sensibles (como %TEMP% o %WINDIR%) donde podría descargar o esconder archivos maliciosos.



```
ExitProcess  
SetEnvironmentVariableA  
GetWindowsDirectoryA  
GetTempPathA  
GetCommandLineA
```

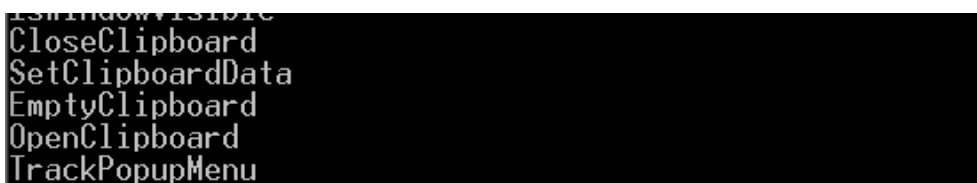
Imagen 16. Cadenas de interacción con variables del entorno

También hay varias funciones que permiten al malware interactuar con ventanas, el menú y el portapapeles. Esto podría ser usado para interactuar con elementos legítimos sin intervención del usuario o interceptar datos sensibles (como contraseñas o datos copiados por el usuario).



```
SetWindowPos  
GetSystemColor  
GetWindowLongA  
LoadCursorA  
CheckDlgButton  
GetMessagePos  
LoadBitmapA  
CallWindowProcA  
IsWindowVisible
```

Imagen 17. Cadenas de interacción con ventanas



```
IsWindowVisible  
CloseClipboard  
SetClipboardData  
EmptyClipboard  
OpenClipboard  
TrackPopupMenu
```

Imagen 18. Cadenas de interacción con el portapapeles

Observamos cadenas que indican que el malware puede recopilar información sobre ventanas activas o clases de ventanas, lo que puede ser útil para identificar aplicaciones específicas, como navegadores o software financiero.



```
ScreenToClient  
GetWindowRect  
EnableMenuItem  
GetSystemMenu  
GetClassLongA  
IsWindowEnabled
```

Imagen 19. Cadenas de espionaje y supervisión

También funciones relacionadas con el monitoreo de la actividad del usuario, como clics o botones seleccionados



```
LoadCursorA  
CheckDlgButton  
GetMessagePos  
LoadBitmapA  
LoadCursorA  
CheckDlgButton  
GetMessagePos
```

Imagen 20. Cadenas de monitoreo de actividad

2.5. Análisis con Virustotal

El archivo tiene 57 detecciones en virustotal, un porcentaje muy elevado que demuestra que es malicioso.

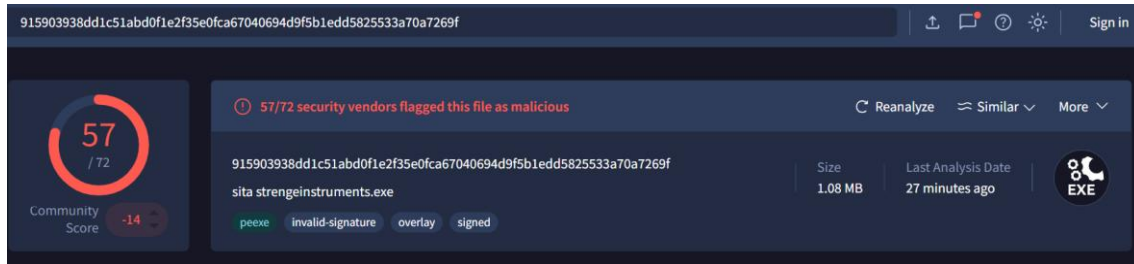


Imagen 21. Análisis con virustotal

3. Análisis dinámico

Antes de proceder, es importante mencionar que para el análisis dinámico se utilizó un escáner ya existente en any.run de este mismo malware, en la que el nombre del ejecutable es po_203-25.exe. No obstante, se trata del mismo malware que hemos estado analizando hasta ahora.

3.1. Análisis de procesos

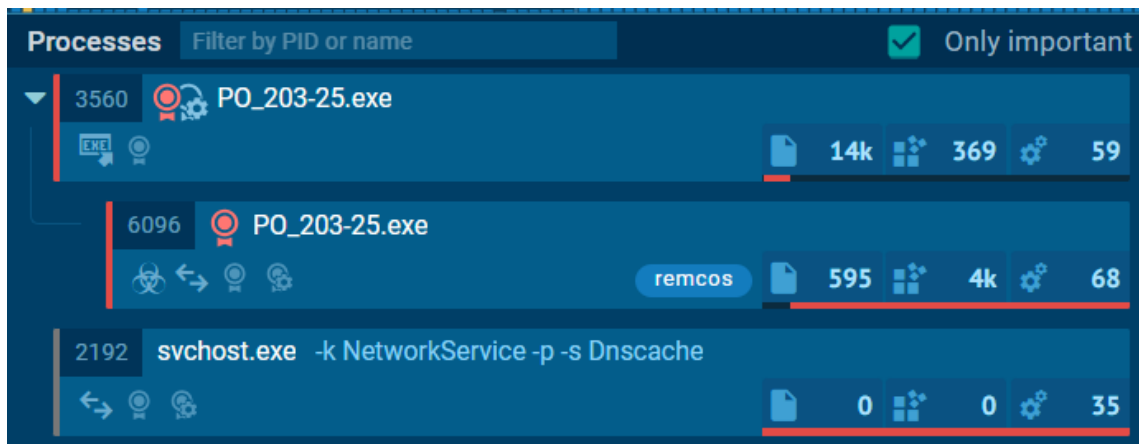


Imagen 22. Procesos obtenidos de any.run

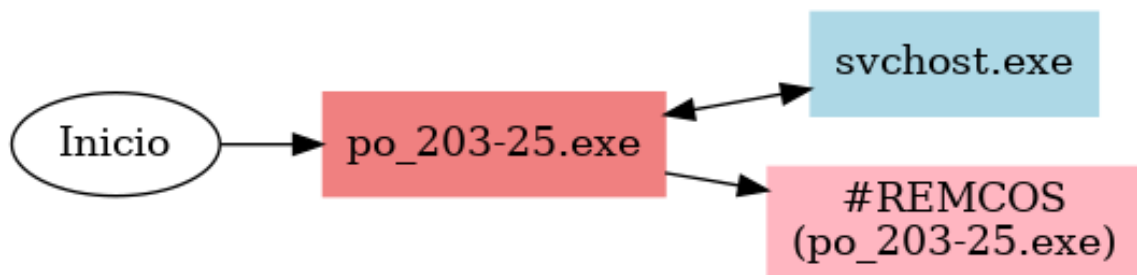


Imagen 23. Diagrama de flujo del malware

El proceso comienza con el archivo inicial, que actúa como el punto de partida del malware. Este archivo, probablemente disfrazado para no levantar sospechas, es ejecutado directamente, marcando el inicio del flujo.

El siguiente paso es la interacción del ejecutable inicial con el proceso legítimo de svchost.exe, que sugiere que el malware utiliza técnicas de inyección de procesos para ejecutar código malicioso dentro de un proceso confiable, dificultando su detección por herramientas de seguridad.

Además, el flujo muestra que el ejecutable está vinculado directamente a #REMCOS, lo que confirma que la carga útil principal del malware es una variante de este RAT (Remote Access Trojan). REMCOS es conocido por su capacidad para proporcionar acceso remoto y control sobre el sistema infectado. Esto incluye funcionalidades como capturar pulsaciones de teclado, robar credenciales, espiar a través de cámaras y micrófonos, y ejecutar comandos de forma remota. La asociación entre el ejecutable y REMCOS indica que el malware utiliza este último como un mecanismo para establecer una conexión persistente con su operador.

3.3. Análisis de red

Peticiones HTTP







HTTP Requests		6	Connections	99	DNS Requests		10	Threats	160		
Timeshift	Headers		Rep	PID	Process name	CN	URL			Content	
2861 ms	GET 200: OK	✔		2736	svchost.exe		http://crl.microsoft.com/pki/crl/produc...				
4959 ms	GET 200: OK	✔		4712	MoUsoCoreWorker.exe		http://crl.microsoft.com/pki/crl/produc...				
4963 ms	GET 200: OK	✔		2736	svchost.exe		http://www.microsoft.com/pkiops/crl/...				
4967 ms	GET 200: OK	✔		4712	MoUsoCoreWorker.exe		http://www.microsoft.com/pkiops/crl/...				
16007 ms	GET 302: Found	?		-	-		https://filetransfer.io/data-package/NO...				
17096 ms	GET 200: OK	?		-	-		https://s24.filetransfer.io/storage/down...			4k	

Imagen 24. Peticiones HTTP obtenidas de any.run

En la imagen, se observan varias solicitudes **GET** realizadas por procesos como **svchost.exe** y **MoUsoCoreWorker.exe**, ambos procesos legítimos de Windows que han sido aprovechados o inyectados por el malware. Estas solicitudes tienen como destino URLs asociadas a infraestructuras de Microsoft, como:

- <http://crl.microsoft.com/pki/crl/products/>
- <http://www.microsoft.com/pkiops/crl/>.

Esto sugiere que el malware utiliza estas conexiones para camuflarse y simular tráfico legítimo.

Además, las solicitudes vinculadas a MoUsoCoreWorker.exe y svchost.exe incluyen descargas de archivos binarios pequeños (entre 1 KB y 973 KB), que podrían ser componentes adicionales del malware o certificados manipulados para evadir análisis. El uso de tamaños pequeños también indica que el malware optimiza su carga útil para evitar detecciones basadas en anomalías de tráfico.

Llama la atención la conexión con el dominio filetransfer.io, que está fuera de las infraestructuras legítimas de Microsoft.

Aquí se registra una redirección que apunta a un archivo descargado desde <https://s24.filetransfer.io/storage/download...> Esto podría representar la descarga de una segunda etapa del malware o un payload adicional.

Conexiones

HTTP Requests		6	Connections		99	DNS Requests		10	Threats		160		
Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Tra			
BEFORE	UDP	✓	4	System	?	192.168.100.255	137	—	—	↑			
BEFORE	TCP	✓	4712	MoUsoCoreWorker.exe	🇺🇸	20.73.194.208	443	settings-win...	MICROSOFT-CO...	↑			
BEFORE	TCP	✓	2736	svchost.exe	🇺🇸	20.73.194.208	443	settings-win...	MICROSOFT-CO...	↑			
BEFORE	TCP	✓	—	—	🇺🇸	20.73.194.208	443	settings-win...	MICROSOFT-CO...				
BEFORE	TCP	✓	—	—	🇬🇧	2.23.209.131	443	www.bing.com	Akamai Internati...				
BEFORE	UDP	✓	4	System	?	192.168.100.255	138	—	—	↑			
BEFORE	TCP	✓	—	—	🇺🇸	20.73.194.208	443	settings-win...	MICROSOFT-CO...	↑			
BEFORE	TCP	✓	—	—	🇬🇧	2.23.209.131	443	www.bing.com	Akamai Internati...				
2859 ms	TCP	✓	2736	svchost.exe	🇺🇸	2.16.164.113	80	crl.microsoft...	Akamai Internati...	↑			
4959 ms	TCP	✓	4712	MoUsoCoreWorker.exe	🇺🇸	2.16.164.113	80	crl.microsoft...	Akamai Internati...	↑			
4963 ms	TCP	✓	2736	svchost.exe	🇩🇪	88.221.169.152	80	www.micros...	AKAMAI-AS	↑			
4966 ms	TCP	✓	4712	MoUsoCoreWorker.exe	🇩🇪	88.221.169.152	80	www.micros...	AKAMAI-AS	↑			
5962 ms	TCP	✓	2736	svchost.exe	🇮🇹	51.104.136.2	443	settings-win...	MICROSOFT-CO...	↑			
6956 ms	TCP	✓	4712	MoUsoCoreWorker.exe	🇮🇹	51.104.136.2	443	settings-win...	MICROSOFT-CO...	↑			
6959 ms	TCP	✓	4712	MoUsoCoreWorker.exe	🇮🇹	51.104.136.2	443	settings-win...	MICROSOFT-CO...	↑			
6965 ms	TCP	✓	4712	MoUsoCoreWorker.exe	🇮🇹	51.104.136.2	443	settings-win...	MICROSOFT-CO...	↑			
6968 ms	TCP	✓	4712	MoUsoCoreWorker.exe	🇮🇹	51.104.136.2	443	settings-win...	MICROSOFT-CO...	↑			
6979 ms	TCP	✓	4712	MoUsoCoreWorker.exe	🇮🇹	51.104.136.2	443	settings-win...	MICROSOFT-CO...	↑			
7961 ms	TCP	✓	2736	svchost.exe	🇮🇹	51.104.136.2	443	settings-win...	MICROSOFT-CO...	↑			
7966 ms	TCP	✓	3976	svchost.exe	🇮🇹	51.104.136.2	443	settings-win...	MICROSOFT-CO...	↑			
16164 ms	TCP	?	6096	PO_203-25.exe	🇺🇸	188.114.96.3	443	s24.filetransf...	CLOUDFLARENET	↑			
17263 ms	TCP	?	6096	PO_203-25.exe	🇺🇸	188.114.96.3	443	s24.filetransf...	CLOUDFLARENET	↑			
37478 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
38477 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
38478 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
38477 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
39478 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
41587 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
42583 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
44583 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
45684 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
47684 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
48683 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
50801 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
51803 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
52813 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
54889 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
55889 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
57903 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
58988 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
60991 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
61992 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
64095 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
65100 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
66104 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
68203 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
69196 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
71197 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			
72301 ms	TCP	🔥	6096	PO_203-25.exe	🇺🇸	192.3.176.134	7062	—	AS-COLOCROSS...	↑			

Imágenes 25 y 26. Conexiones obtenidas de any.run

Aquí se analizan los protocolos, IPs, puertos, dominios, y ASN (Sistemas Autónomos) involucrados.

En las primeras líneas se observa el uso del protocolo UDP desde el proceso System hacia una dirección local (192.168.100.255, puerto 137). Esta comunicación indica el uso de NetBIOS para posiblemente explorar la red local o propagar el malware a otros dispositivos, lo que puede ser una etapa de reconocimiento dentro del entorno.

Posteriormente, se presentan conexiones TCP establecidas desde procesos como MoUsoCoreWorker.exe y svchost.exe hacia dominios legítimos para camuflar actividades maliciosas, mezclando tráfico de comando y control (C2) con solicitudes normales para dificultar la detección por herramientas de monitoreo de red.

A medida que avanzamos, podemos ver IPs y dominios más sospechosos como:

1. s24.filetransfer.io (Puerto 443): Ya mencionado en el apartado anterior, este dominio es utilizado para descargar componentes adicionales del malware o para exfiltrar información.
2. 51.104.136.2 y variaciones en puertos 443 (HTTPS): Estas IPs están asociadas a ASN pertenecientes a Cloudflare. Cloudflare suele ser empleado por atacantes para ocultar las ubicaciones reales de sus servidores C2 gracias a su red de protección.
3. 192.3.176.134 (Puerto 7062): Esta conexión se establece desde el proceso po_203-25.exe, lo que indica una interacción directa con el servidor C2 del malware. El uso del puerto 7062, poco convencional, es una señal de comportamiento malicioso, ya que los atacantes tienden a usar puertos no estándar para evitar ser detectados.

El proceso po_203-25.exe, que es el ejecutable inicial del malware, establece varias conexiones directas hacia dominios y direcciones IP externas. Esto confirma que el archivo es el componente central para la interacción maliciosa en la máquina infectada.

Solicitudes DNS

HTTP Requests		6	Connections		99	DNS Requests		10	Threats		160
Timeshift	Status		Rep	Domain				IP			
BEFORE	Responded	✓		settings-win.data.microsoft.com				20.73.194.208			
								2.23.209.131			
								2.23.209.130			
								2.23.209.189			
								2.23.209.140			
BEFORE	Responded	✓		www.bing.com				2.23.209.141			
								2.23.209.133			
								2.23.209.132			
								2.23.209.135			
								2.23.209.193			
BEFORE	Responded	✓		google.com				142.250.185.142			
2849 ms	Responded	✓		crl.microsoft.com				2.16.164.113			
								2.16.164.112			
4952 ms	Responded	✓		www.microsoft.com				88.221.169.152			
5952 ms	Responded	✓		settings-win.data.microsoft.com				51.104.136.2			
6952 ms	Responded	✓		settings-win.data.microsoft.com				51.104.136.2			
16158 ms	Responded	?		filetransfer.io				188.114.96.3			
								188.114.97.3			
17259 ms	Responded	?		s24.filetransfer.io				188.114.96.3			
								188.114.97.3			
128.62 s	Responded	✓		self.events.data.microsoft.com				20.189.173.8			

Imagen 27. Solicitudes DNS obtenidas de any.run

Estas solicitudes reflejan la interacción del malware con dominios legítimos y sospechosos, revelando cómo mezcla tráfico malicioso y legítimo para evadir detecciones. Mientras las conexiones a dominios de Microsoft, Google y Bing podrían parecer inofensivas, las solicitudes hacia filetransfer.io revelan la verdadera intención del malware: comunicarse con su servidor C2 para ejecutar sus funciones maliciosas.

Alertas

HTTP Requests		6	Connections		99	DNS Requests		10	Threats		160
Timeshift	Class					PID	Process name		Message		
16273 ms	Potentially Bad Traffic					2192	svchost.exe		ET INFO Commonly Abused File Sharing Domain i...		
16277 ms	Potentially Bad Traffic					6096	PO_203-25.exe		ET INFO Commonly Abused File Sharing Domain ...		
37367 ms	A Network Trojan was detected					6096	PO_203-25.exe		REMOTE [ANY.RUN] REMCOS TLS Connection JA...		
37376 ms	Malware Command and Control Activity ...					6096	PO_203-25.exe		ET JA3 Hash - Remcos 3.x/4.x TLS Connection		
38397 ms	A Network Trojan was detected					6096	PO_203-25.exe		REMOTE [ANY.RUN] REMCOS TLS Connection JA...		
38398 ms	Malware Command and Control Activity ...					6096	PO_203-25.exe		ET JA3 Hash - Remcos 3.x/4.x TLS Connection		
39866 ms	A Network Trojan was detected					6096	PO_203-25.exe		REMOTE [ANY.RUN] REMCOS TLS Connection JA...		
39882 ms	Malware Command and Control Activity ...					6096	PO_203-25.exe		ET JA3 Hash - Remcos 3.x/4.x TLS Connection		
41587 ms	Malware Command and Control Activity ...					6096	PO_203-25.exe		ET JA3 Hash - Remcos 3.x/4.x TLS Connection		
41590 ms	A Network Trojan was detected					6096	PO_203-25.exe		REMOTE [ANY.RUN] REMCOS TLS Connection JA...		
43123 ms	A Network Trojan was detected					6096	PO_203-25.exe		REMOTE [ANY.RUN] REMCOS TLS Connection JA...		
43128 ms	Malware Command and Control Activity ...					6096	PO_203-25.exe		ET JA3 Hash - Remcos 3.x/4.x TLS Connection		
44660 ms	A Network Trojan was detected					6096	PO_203-25.exe		REMOTE [ANY.RUN] REMCOS TLS Connection JA...		
44661 ms	Malware Command and Control Activity ...					6096	PO_203-25.exe		ET JA3 Hash - Remcos 3.x/4.x TLS Connection		
46194 ms	A Network Trojan was detected					6096	PO_203-25.exe		REMOTE [ANY.RUN] REMCOS TLS Connection JA...		
46197 ms	Malware Command and Control Activity ...					6096	PO_203-25.exe		ET JA3 Hash - Remcos 3.x/4.x TLS Connection		
47729 ms	A Network Trojan was detected					6096	PO_203-25.exe		REMOTE [ANY.RUN] REMCOS TLS Connection JA...		
47733 ms	Malware Command and Control Activity ...					6096	PO_203-25.exe		ET JA3 Hash - Remcos 3.x/4.x TLS Connection		
48753 ms	A Network Trojan was detected					6096	PO_203-25.exe		REMOTE [ANY.RUN] REMCOS TLS Connection JA...		
48755 ms	Malware Command and Control Activity ...					6096	PO_203-25.exe		ET JA3 Hash - Remcos 3.x/4.x TLS Connection		
50293 ms	A Network Trojan was detected					6096	PO_203-25.exe		REMOTE [ANY.RUN] REMCOS TLS Connection JA...		
50307 ms	Malware Command and Control Activity ...					6096	PO_203-25.exe		ET JA3 Hash - Remcos 3.x/4.x TLS Connection		
51827 ms	A Network Trojan was detected					6096	PO_203-25.exe		REMOTE [ANY.RUN] REMCOS TLS Connection JA...		
51829 ms	Malware Command and Control Activity ...					6096	PO_203-25.exe		ET JA3 Hash - Remcos 3.x/4.x TLS Connection		
53360 ms	A Network Trojan was detected					6096	PO_203-25.exe		REMOTE [ANY.RUN] REMCOS TLS Connection JA...		

Imagen 28. Alertas obtenidas de any.run

Estas alertas están clasificadas principalmente como actividades relacionadas con comandos y control (C2) y detecciones de troyanos.

3.3. Análisis del comportamiento



Imagen 29. Esquema del comportamiento del malware obtenido de any.run

Evasión de defensas

1. El malware emplea empaquetado para evitar la detección por herramientas antivirus o análisis estático. Esto sugiere que el ejecutable está modificado para dificultar su análisis con herramientas de compresión o cifrado.
2. El troyano intenta hacerse pasar por un archivo legítimo (por ejemplo, usando un nombre de archivo o ubicación que parezca genuina). Esto le permite pasar desapercibido en el sistema y evitar que los usuarios o analistas de seguridad lo detecten rápidamente.

Descubrimiento (Discovery)

1. Realiza consultas en el registro de Windows para recopilar información sobre el sistema, buscando configuraciones específicas, credenciales o detalles sobre el entorno.
2. Obtiene datos sobre el sistema infectado, como versión del sistema operativo, arquitectura de hardware e información sobre el usuario y la red. Este paso es típico de malware que adapta su comportamiento al entorno o que necesita enviar esta información a un servidor C2 (Comando y Control).

Command and Control

1. Establece comunicación con el servidor de control utilizando puertos que no son los habituales (como HTTP/HTTPS en los puertos 80 o 443). Esto dificulta la detección por firewall y herramientas de monitoreo que solo revisan tráfico en puertos estándar.

2. Utiliza protocolos en la capa de aplicación (como HTTP, HTTPS, o similares) para comunicarse con su servidor de control. Este tipo de tráfico puede incluir comandos recibidos desde el servidor, así como datos exfiltrados desde el sistema infectado. Específicamente, se han registrado 209 eventos relacionados con esta técnica, lo que sugiere una comunicación activa y constante con el servidor.

Conclusiones

Makoob.gen es un troyano diseñado para espiar actividades del usuario, exfiltrar datos y realizar tareas de sabotaje en sistemas comprometidos. Sus funcionalidades incluyen capturar entradas del teclado, tomar capturas de pantalla, manipular archivos del sistema y desactivar herramientas de seguridad. Además, utiliza técnicas avanzadas como empaquetado y ofuscación para evitar la detección.

Se identificaron secciones personalizadas y con niveles de entropía altos que sugieren la inclusión de payloads cifrados. El uso de empaquetadores como Nullsoft refuerza las estrategias de ocultación. También se detectaron funciones maliciosas que sugieren actividades como espionaje, manipulación de archivos y registro del sistema.

Makoob.gen emplea técnicas de inyección en procesos legítimos como svchost.exe para ejecutar su código de manera encubierta, dificultando la detección. Establece comunicaciones con servidores C2 utilizando protocolos HTTP y HTTPS. También emplea dominios legítimos como camuflaje mientras descarga payloads adicionales o exfiltra información. Mezcla tráfico legítimo y malicioso, dificultando el monitoreo de red.

La capacidad de Makoob.gen para obtener privilegios elevados, evadir defensas y ejecutar comandos remotos lo convierte en una amenaza significativa. Su funcionalidad como herramienta de acceso remoto (RAT) permite a los atacantes realizar espionaje continuo y control total del sistema infectado.

Algunas posibles medidas de mitigación ante este troyano son implementar sistemas de detección y respuesta en tiempo real (EDR) que analicen tanto comportamientos sospechosos como cambios en el sistema; reforzar políticas de acceso y privilegios mínimos para limitar las actividades del malware; actualizar herramientas antivirus con firmas recientes y emplear técnicas heurísticas para detectar empaquetadores maliciosos y realizar auditorías periódicas de seguridad en la red para identificar tráfico no autorizado y evitar la propagación a otros dispositivos.