

Informe Módulo 8

Practica – Análisis de Malware

Fecha: 31 de Mayo de 2024

Autor: **Azael Ramírez Pérez**

Mail: **keepcoder_test@gmail.com (ficticio)**

Empresa: **KeepCoder.inc (ficticio)**

Contenido

Ámbito y alcance.....	3
Entorno Sandbox utilizado.....	4
Datos generales de la muestra de malware.....	5
Análisis Estático.....	7
Análisis Dinámico.....	16
Análisis con herramientas Online.....	24
Comportamiento.....	33
Mitigación.....	34
Recomendaciones.....	36
Registro en MISP.....	38

Ámbito y alcance

El presente trabajo está enfocado en realizar el análisis de una muestra de Malware llamada **SmokeLoader**, el principal objetivo es comprender el funcionamiento y las capacidades de este tipo de software.

Recordemos que el análisis de malware se clasifica en 2 tipos:

- Análisis estático
 - o Este tipo de análisis se caracteriza por inspeccionar el malware sin ejecutarlo, es decir se utilizan herramientas y técnicas para examinar el código, los datos y las estructuras del malware, esto permite a los analistas identificar las características y el comportamiento del malware sin correr el riesgo de infectar sus sistemas, cabe destacar que es muy habitual tener un entorno Sandbox para realizar este tipo de análisis.
- Análisis Dinámico
 - o Generalmente este tipo de análisis es mucho mas atractivo para los analistas debido a que pueden observar el funcionamiento del malware, la característica central es que es necesario ejecutar el malware en el entorno Sandbox con conexión a internet para que de esta manera pueda el malware lograr su objetivo y podamos extraer los datos que posteriormente se tendrán que analizar con más detalle.

Entorno Sandbox utilizado

Inicialmente presentamos un diagrama en el cual se muestra como está compuesto el entorno SandBox, mismo que fue utilizado para poder realizar el análisis de la muestra de Malware.

Nuestro host anfitrión se compone de un Sistema Operativo Windows, la plataforma de virtualización que se uso fue VMWare de modo que a través de esta misma nos sirvió para montar el host virtual siendo Ubuntu, finalmente al interior del host de Ubuntu se utilizo KVM como plataforma de virtualización para poder usar una máquina de Windows 7 y de esta manera tener un ambiente de análisis de Malware seguro.

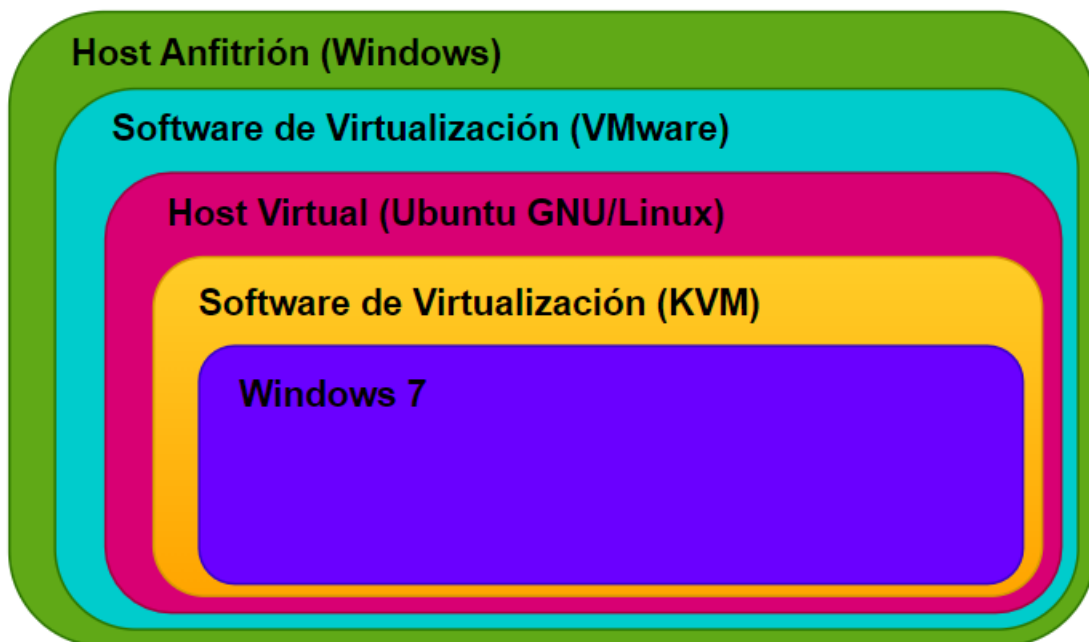
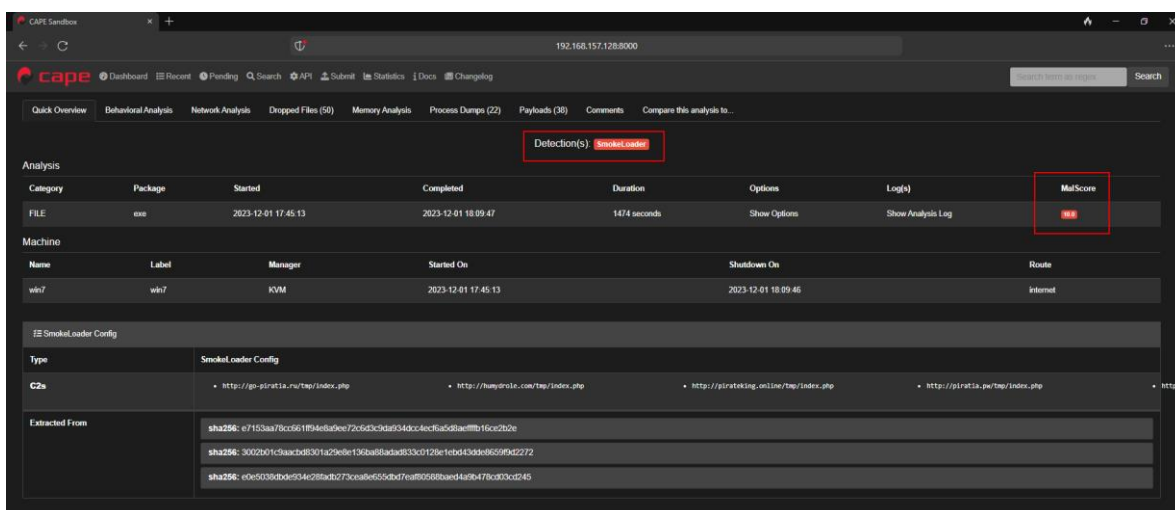


Imagen 1. Entorno Sandbox para Análisis de Malware

Datos generales de la muestra de malware

A continuación, se muestran la información básica de **SmokeLoader** siendo la muestra de malware, es necesario identificar el tipo de malware, para así poder combatir eficazmente las amenazas, mitigar el daño, prevenir futuras infecciones, ayudar a mejorar la seguridad general.



The screenshot shows the CAPE Sandbox interface. The top navigation bar includes links for Dashboard, Recent, Search, Submit, Statistics, Docs, and Changelog. The sidebar on the left lists analysis categories: Quick Overview, Behavioral Analysis, Network Analysis, Dropped Files (50), Memory Analysis, Process Dumps (22), Payloads (38), Comments, and Compare this analysis to... The main content area displays the analysis results for a file named 'SmokeLoader'. A red box highlights the 'SmokeLoader' detection, and another red box highlights the 'MalScore' field. The table below shows the analysis results:

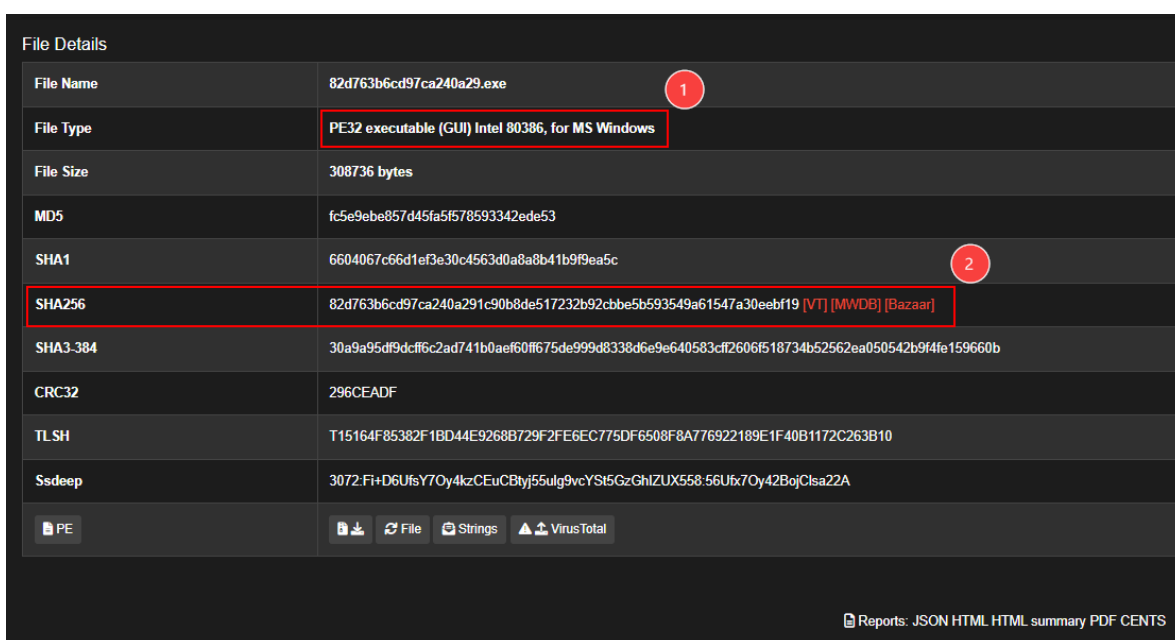
Category	Package	Started	Completed	Duration	Options	Log(s)	MalScore
FILE	exe	2023-12-01 17:45:13	2023-12-01 18:09:47	1474 seconds	Show Options	Show Analysis Log	100

The 'Machine' section shows the following details:

Name	Label	Manager	Started On	Shutdown On	Route
win7	win7	KVM	2023-12-01 17:45:13	2023-12-01 18:09:46	Internet

The 'SmokeLoader Config' section shows the following details:

Type	SmokeLoader Config
C2s	http://ip-piratis.ru/Tap/index.php http://ruymrslie.com/Tap/index.php http://pirateking.online/Tap/index.php http://piratis.pw/Tap/index.php http://ip-piratis.ru/Tap/index.php
Extracted From	sha256: e7153aa76cc561894e6a9ee72c6d3c9da934dccc6c6a6d8a6f1b15c2b2e sha256: 3002b01c5a6c8b301a29e6e136ba8b8ada833c012be1ebd43dd86609f9d2272 sha256: c0e033b0d934c28ad273ca8e615d8d7eaff0568b8d4a86478d303cd43



The screenshot shows the File Details section for the file 'SmokeLoader'. The section displays various file hashes and metadata. A red box highlights the SHA256 hash, and another red box highlights the File Type.

File Name	82d763b6cd97ca240a29.exe
File Type	PE32 executable (GUI) Intel 80386, for MS Windows
File Size	308736 bytes
MD5	fc5e9ebe857d45fa5f578593342ede53
SHA1	6604067c66d1ef3e30c4563d0a8a8b41b9f9ea5c
SHA256	82d763b6cd97ca240a291c90b8de517232b92cbbe5b593549a61547a30eebf19 [VT] [MWDB] [Bazaar]
SHA3-384	30a9a95df9dcff6c2ad741b0aef60f675de999d8338d6e9e640583cfd2606f518734b52562ea050542b9f4fe159660b
CRC32	296CEADF
TLSH	T15164F85382F1BD44E9268B729F2FE6EC775DF6508F8A776922189E1F40B1172C263B10
Ssdeep	3072:Fi+D6UfsY7Oy4kzCEuCBtyj5sulg9vcYsI5GzGhIZUX558:56Ufx7Oy42BojCIsa22A

The bottom section shows the file type 'PE' and the VirusTotal link.

Imagen 2. Información básica de SmokeLoader

Se ha identificado que el archivo del malware es un ejecutable para Windows específicamente para una arquitectura i386.

Se ha logrado obtener la función hash del malware con 3 distintos algoritmos (MD5, SHA1 Y SHA256), estos Hashes son de mucha ayuda para poder identificar al malware con herramientas online y poder ver si el malware ha sido reportado por algún analista de seguridad.

Análisis Estático

Para el análisis estático analizamos el código del programa sin ejecutarlo, esto nos permitirá tener una visión preliminar acerca de su funcionamiento y composición.

Extracción y el análisis de cadenas (strings)

Para ello analizamos utilizamos la herramienta de CAPE con esta misma logramos la extracción y el análisis de cadenas (strings) pues es fundamental poder identificar y examinar las cadenas de caracteres presentes dentro de un archivo binario malicioso.

A continuación, listamos las cadenas que con base a nuestra experiencia son las mas relevantes y las cuales nos arrojan información valiosa.

OpenFile	Función útil que facilita que los usuarios abran archivos en aplicaciones de Windows.
english-caribbean french-canadian spanish-bolivia	Se encontraron distintos lenguajes que utiliza el malware para diversos fines, una conjetura podría ser que identifique la región en la que se encuentra y de

spanish-puerto rico spanish-ecuador	esta manera poder adaptarse y lograr su objetivo.
GetFileType	Se utiliza para determinar el tipo de un archivo en Windows.
HeapAlloc	Se utiliza para asignar memoria en un montón. Un montón es un área de memoria dinámica que se utiliza para almacenar datos asignados por el programador.
GetCurrentProcess	Se utiliza para obtener un identificador de proceso (PID).
GetCommandLineA	Se utiliza para recuperar la línea de comandos utilizada para iniciar un proceso. La línea de comandos incluye el nombre del ejecutable y cualquier argumento que se le haya pasado.
StringFileInfo	Es una estructura de datos en Windows que se utiliza para almacenar información de cadena sobre un archivo ejecutable o una biblioteca de enlace dinámico (DLL).
InternalName	El nombre interno es el nombre que utiliza el sistema operativo para identificar el archivo o módulo, y

	generalmente es diferente del nombre de archivo que ve el usuario.
HeapSetInformation	tiene dos propósitos principales, Asignación de memoria en el montón Obtener el tamaño de un bloque de memoria asignado
msimg32.dll KERNEL32.dll mscoree.dll USER32.dll WUSER32.DLL	Se utilizan distintas librerías para distintos fines, además existen 2 tipos principales de DLL en Windows: <ul style="list-style-type: none"> • DLL de sistema • DLL de aplicación
IsWow64Process	Se utiliza para determinar si un proceso específico se está ejecutando en WoW64 (Windows-on-Windows 64) , un subsistema que permite que las aplicaciones de 32 bits se ejecuten en un sistema operativo Windows de 64 bits.
GetUserObjectInformationW	Se utiliza para recuperar información específica acerca de un objeto de usuario existente en el sistema. "W" al final del nombre indica que se trata de una

	función específica para Unicode, permitiendo manejar caracteres de distintos idiomas.
@Microsoft Visual C++ Runtime Library	Es un conjunto de bibliotecas que contienen funciones y código precompilado que son esenciales para ejecutar aplicaciones desarrolladas con los compiladores de C y C++ de Microsoft Visual C++.

Estructura PE (Portable Executable)

Se logro obtener el nombre del malware original y el nombre interno, ver la figura siguiente:

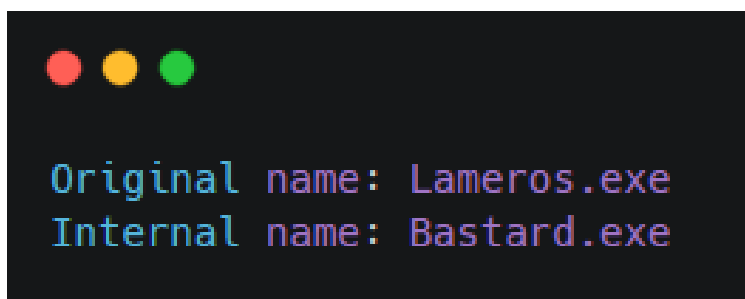


Imagen 3. Nombre original y nombre interno

Nombre original: El nombre original del archivo suele ser un nombre genérico o aleatorio que no proporciona ninguna información sobre la funcionalidad del malware. Sin embargo, puede ser útil para identificar el malware si se conoce el nombre de la familia a la que pertenece o si se ha visto en otras campañas de malware.

Nombre interno: El nombre interno del malware suele ser un nombre más descriptivo que proporciona información sobre la funcionalidad del malware o el objetivo del ataque. Esta información puede ser útil para los investigadores de seguridad para clasificar el malware y comprender su propósito.

Además de estas dos finalidades principales, el nombre original y el nombre interno de un malware PE32 también pueden usarse para otros propósitos, como:

- Comunicación entre los autores del malware: Los autores del malware pueden usar los nombres para comunicarse entre sí sobre el malware y su desarrollo.
- Ocultar la verdadera funcionalidad del malware: Los autores del malware pueden usar los nombres para ocultar la verdadera funcionalidad del malware y hacer que parezca un archivo legítimo.
- Rastrear la distribución del malware: Los investigadores de seguridad pueden usar los nombres para rastrear la distribución del malware y determinar cómo se está propagando.

Entropía del archivo

En esencia la entropía en un archivo de Malware se refiere a la medida de aleatoriedad de sus datos. Se calcula utilizando una fórmula matemática que analiza la distribución de bytes en el archivo. La entropía se expresa en una escala de 0 a 8, donde:

- **0** indica que los datos son completamente **predecibles** (por ejemplo, un archivo de texto sin comprimir).
- **8** indica que los datos son completamente **aleatorios** (por ejemplo, un archivo cifrado).

Encabezados

Observando la información que arrojo cape, en la parte de los encabezados tenemos lo siguiente:

.text se observa una mayor puntuación de entropía teniendo un valor de 6.84.

Sections						
Name	Raw Address	Virtual Address	Virtual Size	Size of Raw Data	Characteristics	Entropy
text	0x0000400	0x0001000	0x00028f56	0x00029000	IMAGE_SCN_CNT_CODE IMAGE_SCN_MEM_EXECUTE IMAGE_SCN_MEM_READ	6.84
data	0x00029400	0x0002a000	0x0267557c	0x0001800	IMAGE_SCN_CNT_INITIALIZED_DATA IMAGE_SCN_MEM_READ IMAGE_SCN_MEM_WRITE	2.84
rsic	0x0002ac00	0x026a0000	0x00020800	0x00020a00	IMAGE_SCN_CNT_INITIALIZED_DATA IMAGE_SCN_MEM_READ	4.22

Imagen 4. Valor de entropía encontrado en el encabezado .text

Es necesario entender que la entropía no es una herramienta perfecta para la detección o el análisis de malware. Algunos archivos legítimos, como los archivos multimedia comprimidos, también pueden tener una alta entropía.

Sin embargo, la entropía puede ser una herramienta valiosa cuando se utiliza junto con otros métodos de análisis de malware.

Imports en la muestra de Malware

Los imports permiten que los programas interactúen con el sistema operativo y realicen operaciones básicas, por lo que son referencias a funciones y variables que se encuentran en otras bibliotecas o módulos. Estos imports son necesarios para que el ejecutable pueda acceder a la funcionalidad proporcionada por las bibliotecas o módulos.

Los imports que encontramos al analizar la muestra de Malware son Kernel32 y User32, cada una de ellas tiene un rol específico.

Kernel32

Es la base sobre la que se construye todo el sistema operativo Windows. Es responsable de las tareas fundamentales del sistema, como la gestión de la memoria, la ejecución de programas y la comunicación con el hardware.

Algunas de las funciones que la muestra de malware utiliza son las siguientes:

- **GetComputerNameA:** Obtiene el nombre de la computadora local.
- **CreateFileA:** Abre un archivo o crea un nuevo archivo.
- **OpenFile:** Abre un archivo existente para su lectura o escritura.

- **SetLocaleInfoA:** Establece la configuración regional actual para la entrada y salida de texto.
- **WriteConsoleInputW:** Escribe datos en el búfer de entrada de la consola.

User32

Se encarga de la interfaz gráfica de usuario, sin ella, el sistema operativo no podría mostrar una interfaz y sería imposible para los usuarios interactuar con las aplicaciones.

Algunas de las funciones que la muestra de malware utiliza son las siguientes:

- **CharToOemBuffW:** Convierte una cadena de caracteres Unicode de ancho doble (UTF-16) a una cadena de caracteres OEM de ancho doble.
- **CharUpperW:** Convierte todos los caracteres en mayúsculas en una cadena de caracteres Unicode de ancho doble (UTF-16).

Análisis Dinámico

Es una técnica valiosa en la detección y análisis de malware, ya que permite observar el comportamiento real del software sospechoso en un entorno controlado. Esto ayuda a identificar amenazas que pueden evadir la detección mediante análisis estáticos y proporciona información útil para la respuesta a incidentes y la mitigación de riesgos.

MITRE ATT&CK

Es un marco de referencia creado por la organización MITRE cuyo fin es modelar, detectar, prevenir y combatir las amenazas de ciberseguridad. Se basa en el comportamiento real de los adversarios y proporciona una visión común para que los defensores comprendan y respondan a los ataques cibernéticos.

Sirve esencialmente como una base de conocimiento global, está abierta y disponible para que cualquier persona u organización lo utilice sin costo alguno.

En nuestro caso a través de la herramienta CAPE logramos obtener datos muy relevantes debido a que nos mostró una matriz de MITRE la cual tiene información muy específica, a continuación, listamos las tácticas y técnicas que utiliza la muestra de Malware que se está analizando.

Etapa de Discovery

En esta etapa, los atacantes recopilan información sobre su objetivo potencial para comprender mejor su entorno, identificar activos valiosos y encontrar vulnerabilidades que puedan explotar.

- **T1082 - System Information Discovery:** Se refiere al proceso de recopilación de información sobre un sistema informático, como el hardware, el software instalado, la configuración del sistema y detección de máquinas virtuales (VM).
- **T1497 - Virtualization/Sandbox Evasion:** Se enfoca en las técnicas utilizadas por malware para eludir la detección y el análisis en entornos virtuales o de sandbox.
- **Enumerates_running_processes:** Esta función probablemente se utiliza en el contexto de la programación o la seguridad informática para recopilar información sobre los procesos que se están ejecutando actualmente en un sistema operativo.
- **Query Registry:** Consulta el registro de Windows en busca de información específica, como configuraciones de aplicaciones, opciones del sistema, valores de configuración.

Etapa de Command and Control

Es una táctica utilizada por los ciberatacantes para establecer y mantener comunicaciones bidireccionales con los sistemas que han comprometido. Esta comunicación les permite a los atacantes:

Controlar los sistemas comprometidos, ejecutar comandos, instalar malware adicional, robar datos y realizar otras acciones maliciosas.

A continuación, se listan las técnicas que la muestra de malware está intentando realizar.

- **Application Layer Protocol:** En el contexto de la seguridad informática, el análisis de los protocolos de capa de aplicación es importante para comprender cómo se comunican las aplicaciones y qué tipos de datos están intercambiando.
- **Injection_network_traffic:** La inyección de tráfico de red es una técnica utilizada por los atacantes para modificar o insertar datos en el tráfico de red, generalmente con el objetivo de realizar ataques, robar información sensible o comprometer sistemas.
- **network_http:** Es una función comúnmente utilizada por el malware para comunicarse con servidores remotos controlados por los atacantes.

Defense Evasion

Se refiere a un conjunto de técnicas y tácticas utilizadas por los ciberdelincuentes para eludir o deshabilitar los sistemas de seguridad e infectar con éxito un sistema informático logrando pasar desapercibido.

A continuación, se listan los puntos más relevantes de evasión de defensa que utiliza la muestra de malware.

- **Masquerading:** técnica utilizada en seguridad informática donde un actor malintencionado se disfraza o se hace pasar por otro usuario, sistema, proceso o entidad legítima con el fin de evadir la detección, obtener acceso no autorizado o llevar a cabo actividades maliciosas sin ser detectado.
- **Process Injection:** es una técnica utilizada en seguridad informática en la que un proceso malicioso (o a veces legítimo) introduce código o datos en el espacio de memoria de otro proceso en ejecución en un sistema informático. Esta técnica se utiliza con frecuencia en el desarrollo de malware y herramientas de hacking, así como en aplicaciones legítimas para varios fines, como la depuración y la interoperabilidad entre procesos.
- **Abuse Elevation Control Mechanism:** es una técnica o método utilizado por atacantes para abusar de los mecanismos de control de elevación de privilegios en un sistema. Los atacantes pueden intentar abusar de estos mecanismos para obtener privilegios más altos de los que les corresponderían normalmente.

Podrían intentar explotar vulnerabilidades conocidas en el sistema operativo o en aplicaciones para obtener acceso de administrador o root. También podrían intentar engañar a los usuarios o administradores para que les otorguen acceso elevado utilizando técnicas de ingeniería social o phishing.

Privilege Escalation

La escalada de privilegios es una técnica utilizada por el malware para obtener acceso a un mayor nivel de permisos en un sistema informático. Esto permite al malware realizar acciones que normalmente no podría, por ejemplo:

- **Instalar software malicioso adicional:** El malware puede instalar otro software malicioso en el sistema con acceso elevado, lo que le da un mayor control.
- **Robar datos confidenciales:** El malware puede acceder y robar datos confidenciales, como contraseñas, información financiera o datos personales.
- **Deshabilitar o eludir los sistemas de seguridad:** El malware puede deshabilitar o eludir los sistemas de seguridad, como antivirus, firewalls e IDS.
- **Controlar el sistema:** El malware puede tomar el control completo del sistema, lo que le permite realizar cualquier acción que desee.

Análisis de Red

El análisis de red tiene como finalidad principal identificar y comprender cómo el malware interactúa con las redes informáticas. Esto implica observar cómo se comunica el malware, qué datos transfiere, a dónde los envía y cómo utiliza la red para propagarse o llevar a cabo sus objetivos maliciosos.

Durante este tipo de análisis se analizaron solo 10 IP's siendo las siguientes:

- **190.218.32.77**

- o Esta primera IP fue identificada por SOCRadar y Fortinet
- o Presenta actividad maliciosa y se presenta relación con RecordBreaker 20-11-2023
- o Cabe destacar que RecordBreaker es un software malicioso clasificado como **stealer**. Este tipo de malware está diseñado para extraer y exfiltrar datos y contenidos vulnerables, además se ha propagado activamente a través de varios sitios web que ofrecen software "crackeado"

- **93.184.220.29**

- o Esta IP fue identificada por Abusix
- o Esta misma ha sido reportada 160 veces
- o Se reporta en su mayoría que hace un escaneo de puertos
- o Tiene una relación estrecha con archivos de tipo
 - **.exe - .docx - .dll - .xml**

- **192.36.38.33**
 - o Esta IP fue identificada por CriminalIP como maliciosa en VT
 - o Esta misma ha sido reportada 3 veces en abuse IP
- **165.227.174.150**
 - o No se encontró actividad relevante de esta IP
- **143.107.229.210**
 - o Esta relacionada directamente con Malware
 - o IP reportada por CyRadar como maliciosa
 - o Esta misma ha sido reportada 3 veces abuse IP
- **95.86.30.3 (*)**
 - o Esta IP ha sido reportada por Fortinet
 - o Esta relacionada directamente con malware
- **91.215.85.17 (*Relacionada con México)**
 - o Se ha reportado que esta IP ha tenido actividad maliciosa y está relacionada con Relacionada con **Amadey 11-09-2023 TIPO: RAT Amadey**
- **34.143.166.163**
 - o Esta ip ha sido reportada por proveedores como CriminalIP, ESET, Vipre, CyRadar, G-Data, Zcitiium Verdict Cloud
 - o Tiene agrupación archivos, tiene relación con repositorios de GitHub.oi
 - o En abuse IP esta relacionada con Hackeo y Ataques a aplicaciones web

- **104.198.2.251**

- o Esta IP ha sido encontrada por muchos proveedores y se ha detectado como maliciosa, estos proveedores son:

- alphaMountain.ai
- Antiy-AVL
- Criminal IP
- ESET
- G-Data
- MalwareURL
- Webroot
- Abusix
- VIPRE
- Lionix
- Fortinet
- CyRadar
- BitDefender
- AlphaSOC
- La comunidad de analistas ha asociado esta IP con el grupo Hive0065

- **34.94.245.237**

- o Esta Ip ha sido reportada por 4 proveedores, Criminal IP, Xcitium Verdict Cloud, CyRadar y Gridinsoft.
- o Se ha utilizado en varios ataques ciberdelictivos durante más de una década.

- **8.8.4.4**

- o Esta IP es el DNS de Google
- o Esta **IP** ha sido reportada por **ArcSight Threat Intelligence**

Análisis con herramientas Online

Se analizo también la muestra de malware con 2 herramientas online las cuales son: **Virus Total**, **Any.Run** y **Joe Sanbox**.

Se utilizo el hash (sha256) de la muestra de malware para buscarlo en las anteriores herramientas mencionadas, la herramienta en la que hemos encontrado rastro de la muestra fue en Virus Total, Joe Sand Box y Any.Run.

Análisis con Virus Total

VirusTotal es una plataforma en línea gratuita que proporciona servicios de análisis de archivos y URLs para detectar malware y otras amenazas de seguridad en línea. Fue adquirida por Google en 2012 y desde entonces ha sido una herramienta popular tanto para usuarios individuales como para empresas en la lucha contra el malware.

Módulo de Detección

Esta herramienta nos muestra información muy valiosa, pues empresas como ESET-NOD32, Microsoft, Malwarebytes, TrendMicro etc, han detectado la muestra como maliciosa, a continuación, se muestra evidencia de lo que se menciona.

Q

82d763b6cd97ca240a291c90b8de51732b92cbb5b593549a61547a30eebf19

Security vendors' analysis ⓘ

Do you want to automate checks?

AhnLab-V3	ⓘ Trojan:Win.Tofsee.R626309	Alibaba	ⓘ Trojan:Win32/RedLine.649979f4
AllCloud	ⓘ Trojan:Win/RedLine.SPGQIMTB	Antiy-AVL	ⓘ Trojan:Win32.Kryptik.hvkj
Arcabit	ⓘ Trojan.Mint.Zard.59	Avast	ⓘ Win32-DropperX-gen [Drp]
Avert Labs	ⓘ Artemis!FC5E9EBE85TD	AVG	ⓘ Win32-DropperX-gen [Drp]
Avira (no cloud)	ⓘ HEUR/AGEN.1371585	BitDefender	ⓘ Gen:Heur.Mint.Zard.59
Bkav Pro	ⓘ W32.AIDetectMalware	ClamAV	ⓘ Win.Packer.pkr_ce1a-9980177-0
Cylance	ⓘ Unsafe	Cynet	ⓘ Malicious (score: 100)
DrWeb	ⓘ Trojan.Siggen22.21050	Elastic	ⓘ Malicious (high Confidence)
Emsisoft	ⓘ Gen:Heur.Mint.Zard.59 (B)	eScan	ⓘ Gen:Heur.Mint.Zard.59
ⓘ 1 → ESET-NOD32	ⓘ A Variant Of Win32/Kryptik.HVKW	Fortinet	ⓘ W32/GenKryptik.ERHNltr
GData	ⓘ Gen:Heur.Mint.Zard.59	Google	ⓘ Detected
Ikarus	ⓘ Trojan.Win32.Azorult	Jiangmin	ⓘ Trojan.Chapak.rrz
K7AntiVirus	ⓘ Trojan (0056f9be1)	K7GW	ⓘ Trojan (0056f9be1)
Kingsoft	ⓘ Win32.Trojan.Convagent.gen	Lionic	ⓘ Trojan.Win32.Chapak.4lc
ⓘ 2 → Malwarebytes	ⓘ Trojan.MalPack.GS	MAX	ⓘ Malware (ai Score=83)
ⓘ 3 → Microsoft	ⓘ Trojan:Win32/RedLine.SPGQIMTB	NANO-Antivirus	ⓘ Trojan.Win32.Kryptik.kerqkx
Palo Alto Networks	ⓘ Generic.ml	Panda	ⓘ Trj/RansomGen.A

Imagen 5. Modulo de detección, ciertos proveedores han identificado como a la muestra como maliciosa.

Módulo de Details

En este módulo la información más relevante que nos arroja es: la función Hash usando 3 tipos de algoritmos MD5, SHA1 y SHA256. Nos indica también el tipo de archivo siendo un archivo ejecutable para una arquitectura de 32 bits i386 para la plataforma de Windows. Particularmente usa el compilador Microsoft Visual C/C++, finalmente nos muestra el tamaño del archivo 304.50 KB.

A continuación, se muestra evidencia de lo mencionado, ver punto 2.

82d763b6cd97ca240a291c90b8de517232b92cbb5b593549a61547a30eebf19

53 / 68

Community Score

53/68 security vendors and 4 sandboxes flagged this file as malicious

Reanalyze Similar More

82d763b6cd97ca240a291c90b8de517232b92cbb5b593549a61547a30eebf19

Size: 301.50 KB Last Modification Date: 11 days ago

EXE

poze detect-debug-environment spreader malware executes-dropped-file self-delete

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY (21)

Basic properties

MD5	fc5e9ebe857d45af5f78593342ede53
SHA-1	6604067c66d1ef3e30c4563d0a8ab41b99ea5c
SHA-256	82d763b6cd97ca240a291c90b8de517232b92cbb5b593549a61547a30eebf19
Vhash	0350366d151015c200647z1dz3fz
Authenthash	ab1ce4067f1722ffe4a7cc2e377cd18df7950633c45b47c541ed22c1176be5
ImpHash	1756ec87e9180426f9d9ce779d24407
SSDEEP	3072:FiH6Ufs7Oy4kCEuCBty55ul9vcYSt5GzGhIZUXS58-56Ufx7Oy42BojCIsa22A
TLSH	T15164F85382F18D44E9268B729F2FE6EC775DF6508F8A776922189E1F40B1172C263B10
File type	Win32 EXE executable windows win32 pe poze
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (47.3%) Win64 Executable (generic) (15.9%) Win32 Dynamic Link Library (generic) (9.9%) Win16 NE executable (generic) (0.0%)
DetectItEasy	PE32 Compiler: EP:Microsoft Visual C/C++ (2008-2010) [EXE32] Compiler: Microsoft Visual C/C++ (15.00-16.00) [libcm]
File size	301.50 KB (308736 bytes)

History

Creation Time	2022-12-05 15:35:42 UTC
First Seen In The Wild	2023-11-30 18:25:42 UTC
First Submission	2023-11-30 17:21:13 UTC
Last Submission	2023-12-09 12:05:52 UTC
Last Analysis	2024-05-13 11:01:30 UTC

Imagen 6. Modulo de detalles, se ha identificado el hash de la muestra, así como el tipo de archivo

Módulo de Relations

En este módulo principalmente permite investigar y comprender las conexiones entre diferentes archivos, URLs, dominios, direcciones IP y hashes que pueden estar relacionados con una amenaza de seguridad o un incidente de malware.

A continuación, se observan las URL's, los dominios asociados que la muestra de Malware utiliza (ver punto 2 al 4).

The screenshot displays the 'Relations' tab for a specific malware sample. The sample ID is 82d763b6cd97ca240a291c90b8de517232b92cbb5b593549a61547a30eebf19. The interface shows three sections: 'Contacted URLs (6)', 'Contacted Domains (9)', and 'Contacted IP addresses (30)'. Each section contains a table of related entities.

Contacted URLs (6)

Scanned	Detections	Status	URL
2024-05-08	18 / 92	200	http://sumagulituyo.org/
2024-05-09	17 / 92	200	http://snukerukeutit.org/
2024-01-08	18 / 91	-	http://atozrental.cc/atoz/index.php
2024-05-09	18 / 92	200	http://liuliuoumumy.org/
2024-05-18	16 / 94	200	http://lightseinsteniki.org/
2024-05-09	19 / 92	-	http://stualialuyastrelia.net/

Contacted Domains (9)

Domain	Detections	Created	Registrar
2no.co	4 / 93	2012-05-25	GoDaddy.com, LLC
atozrental.cc	10 / 93	2023-11-06	WEBCC
dns.msftncsi.com	0 / 93	2005-11-10	CSC CORPORATE DOMAINS, INC.
lightseinsteniki.org	17 / 93	2023-10-12	-
liuliuoumumy.org	19 / 93	2023-10-12	-
onualituyrs.org	19 / 93	2023-10-05	-
snukerukeutit.org	18 / 93	2023-10-12	-
stualialuyastrelia.net	20 / 93	2023-10-05	-
sumagulituyo.org	18 / 93	2023-10-12	-

Contacted IP addresses (30)

IP	Detections	Autonomous System	Country
104.198.2.251	13 / 93	396982	US
104.21.79.229	0 / 93	13335	-
109.175.29.39	4 / 93	9146	BA
131.107.255.255	3 / 93	3598	US
14.33.209.147	4 / 93	4766	KR
148.251.183.205	1 / 93	24940	DE
172.67.149.76	0 / 93	13335	-
175.119.10.231	8 / 93	9318	KR
175.120.254.9	4 / 93	9318	KR

Imagen 7. Modulo de Relations, nos muestra los dominios con los que ha tenido relación el malware

Módulo de Behavior

Este módulo está diseñado para proporcionar una evaluación dinámica del comportamiento de un archivo sospechoso o malicioso. Se centra en el análisis dinámico. Ejecuta el archivo sospechoso en un entorno virtualizado y monitorea su comportamiento en tiempo real. Esto puede incluir actividades como la creación de archivos o procesos, cambios en el registro del sistema, conexiones de red, entre otros. Todos estos datos se recopilan y analizan para determinar si el archivo tiene un comportamiento malicioso.

Dentro del resumen de actividad se puede observar que se han detectado firmas de Mire, se han encontrado Reglas IDS (Sistema de Detección de Intrusiones (4 con criticidad alta), también se han encontrado Reglas Sigma (1 con criticidad alta), se ha detectado que el malware hace eliminación de archivos y se detalla también las comunicaciones a nivel de red.

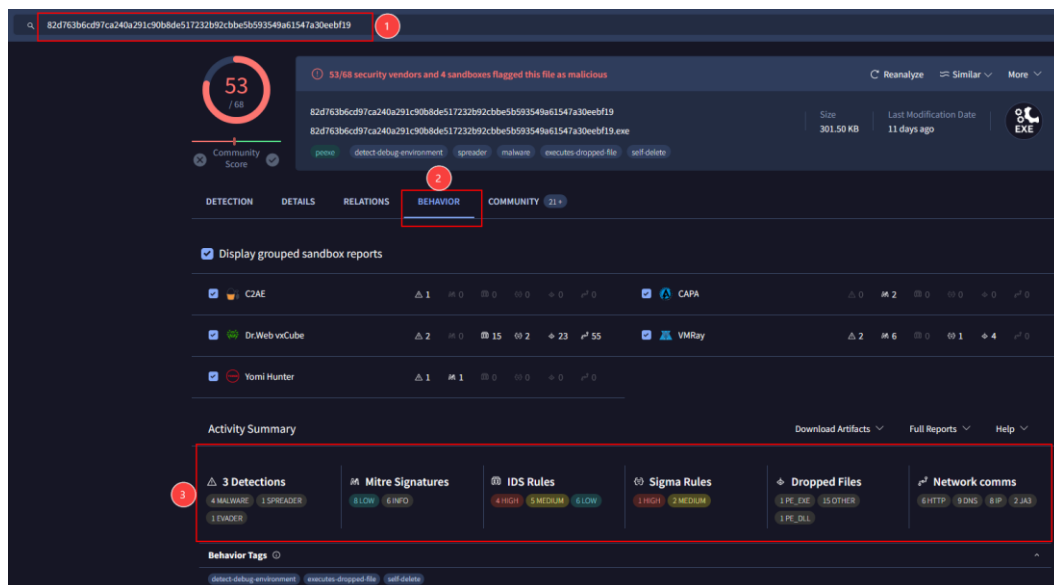


Imagen 8. Módulo de Behavior, nos muestra parte del comportamiento que ha tenido el malware

Análisis con Joe Sandbox

Joe Sandbox una plataforma avanzada de análisis de malware y seguridad cibernética. Permite a los investigadores de seguridad analizar archivos y URL's sospechosos en un entorno controlado para comprender su comportamiento y determinar si representan una amenaza. Utiliza técnicas de análisis dinámico y estático para identificar malware, incluyendo análisis de sandboxing, análisis de comportamiento, y análisis de firmas. Joe Sandbox es utilizado por profesionales de la seguridad cibernética, empresas y agencias gubernamentales para investigar y combatir el malware y otras amenazas en línea.

En la siguiente imagen se muestra la búsqueda del hash de la muestra de **SmokeLoader**, Joe Sandbox ya tiene identificada la muestra, por lo que se nos arroja información valiosa, se ha detectado como Maliciosa la muestra, ver punto 2.

JoeSandbox Cloud BASIC 82d763b6cd97ca240a291c90b8de5172 Analyze Results Register Login

Deep Malware Analysis

MALWARE TRENDS

Agenttesla Redline Njrat LummaC Formbook Amadey Snake Keylogger Xworm Vidar RisePro Remcos

Not found what you are looking for? Try: Advanced Search

5 search results for "82d763b6cd97ca240a291c90b8de517232b92cbbe5b593549a61547a30eebf19" (limited to max. 20 search results)

Detection	Sample Info	Download Report	Classification & Info	Graph
MALICIOUS Glupteba, Petite Virus, R... AV: 87%	etNheGz9UQ.exe 2023-12-10 09:40:06 +01:00	Full Report Management Report IOC Report	Info Class	
MALICIOUS Glupteba, LummaC Steal... AV: 87%	lkYqsQV4ty.exe 2023-12-09 12:54:34 +01:00	Full Report Management Report IOC Report	Info Class	
MALICIOUS Glupteba, LummaC Steal... AV: 87%	NQ8lktjil.exe 2023-12-08 19:04:07 +01:00	Full Report Management Report IOC Report	Info Class	
MALICIOUS RedLine, SmokeLoader, ... AV: 87%	aHB5nXdi3C.exe 2023-12-03 19:43:49 +01:00	Full Report Management Report IOC Report	Info Class	
MALICIOUS RedLine, SmokeLoader AV: 83%	file.exe 2023-11-30 18:21:06 +01:00	Full Report Management Report IOC Report	Info Class	

Windows:
Injects
Writes Registry keys
Drops PE Files
Has more than one Process

Android:
Receives SMS
Sends SMS
Reboot
Native CMD

Common:
Generates Internet Traffic
Generates HTTP Network Traffic
Expired Sample
Creates malicious files

Customization
☐ Show ID column

Imagen 9. Match del hash de la muestra de malware en Joe Sandbox

En la siguiente pantalla nos muestra los datos que ya hemos identificado con CAPE como el hash (MD5, SHA1 y SHA256), adicionalmente se observa que la muestra se clasifica como maliciosa, también nos arroja una descripción detallada del malware y nos indica las Signatures (por ejemplo yara) que han detectado al malware.

Overview
Signatures
Screenshots
Behavior Graph
Network Map

Windows Analysis Report

file.exe

Overview

General Information

Sample Name:	file.exe
Analysis ID:	1350693
MD5:	fc5e9ebe857d4...
SHA1:	6604067c66d1e...
SHA256:	82d763b6cd97c...
Tags:	exe, SmokeLoader
Infos:	info

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

RedLine, SmokeLoader

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Yara detected SmokeLoader
- System process connects to network (li...
- Detected unpacking (changes PE secti...
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Snort IDS alert for network traffic
- Found malware configuration
- Multi AV Scanner detection for submitte...
- Benign windows process drops PE files
- Malicious sample detected (through co...
- Antivirus / Scanner detection for submitt...
- Multi AV Scanner detection for dropped ...
- Tries to steal Mail credentials (via file / r...
- Maps a DLL or memory area into anoth...

Classification

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
RedLine Stealer	RedLine Stealer is a malware available on underground forums for sale apparently as standalone (\$100/\$150 depending on the version) or also on a subscription basis (\$100/month). This malware harvests information from browsers such as saved credentials, autocomplete data, and credit card information. A system inventory is also taken when running on a target machine, to include details such as the username, location data, hardware configuration, and information regarding installed security software. More recent versions of RedLine added the ability to steal cryptocurrency. FTP and IM clients are also apparently targeted by this family, and this malware has the ability to upload and download files, execute commands, and periodically send	No Attribution	<ul style="list-style-type: none"> https://apophis133.mediu... https://asec.ahnlab.com/e... https://asec.ahnlab.com/e... https://asec.ahnlab.com/k... https://bartblaze.blogspot.... 	https://malpedia.caad.fkie.fr...

Imagen 10. Reporte de análisis de la muestra de malware

Análisis con Any.Run

En Any.Run se ha encontrado la muestra de Malware **SmokeLoader**, la función principal es lanzar otro malware más destructivo en las máquinas infectadas. Sin embargo, a diferencia de muchos cargadores, este se puede ampliar mediante complementos para incluir funciones destructivas y de robo de información.

En la siguiente imagen podemos observar los datos básicos de la muestra de Malware, cabe destacar que un cargador es software malicioso que se infiltra en los dispositivos para entregar cargas útiles maliciosas. Este malware es capaz de infectar los ordenadores de las víctimas, analizar la información de su sistema e instalar otro tipo de amenazas, como troyanos o ladrones. Los delincuentes suelen entregar cargadores a través de correos electrónicos y enlaces de phishing, confiando en la ingeniería social para engañar a los usuarios para que descarguen y ejecuten sus ejecutables.

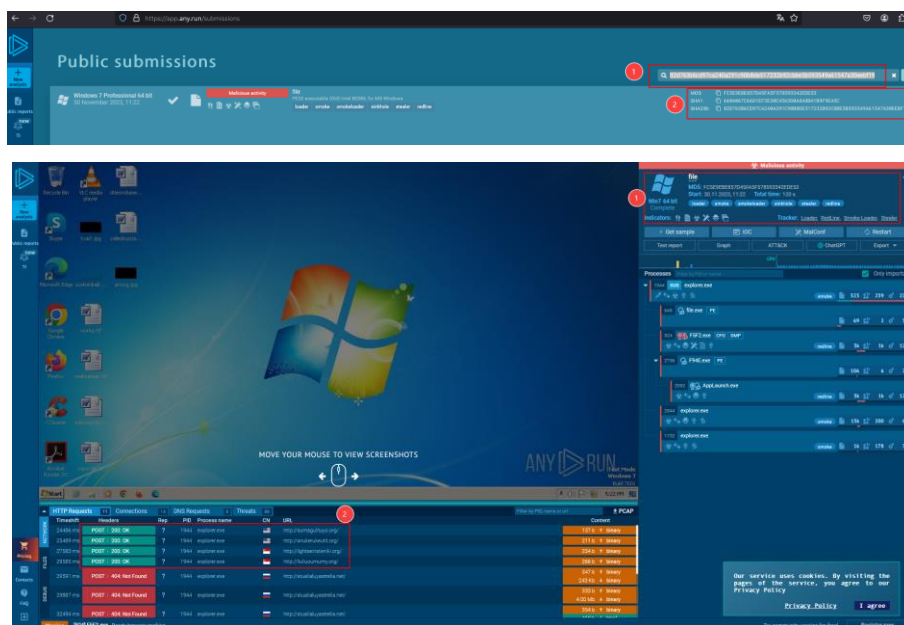


Imagen 11. Any.run nos muestra detalles de la muestra

Comportamiento

Generalmente la familia de Malware **SmokeLoader** es una puerta trasera genérica con una variedad de capacidades que dependen de los módulos incluidos en cualquier versión determinada del malware. El malware se distribuye de diversas formas y está ampliamente asociado con actividades delictivas. El malware frecuentemente intenta ocultar su actividad C2 generando solicitudes a sitios legítimos como microsoft.com, bing.com, adobe.com y otros. Normalmente, la descarga real devuelve un HTTP 404 pero aún contiene datos en el cuerpo de la respuesta.

Mitigación

Para las actividades de mitigación hay algunas medidas que se pueden tomar para protegerse contra el malware SmokeLoader, listamos algunas de ellas:

- **Software Antivirus/Antimalware:** Asegúrate de tener un software antivirus o antimalware actualizado y activo en todos los dispositivos. Esto puede ayudar a detectar y eliminar el malware antes de que pueda causar daño.
- **Firewall:** Utiliza un firewall de red para controlar el tráfico de entrada y salida de tu red. Configura reglas adecuadas para bloquear el tráfico malicioso conocido y desconocido.
- **Actualizaciones de Software:** Mantén todos los programas y sistemas operativos actualizados con los últimos parches de seguridad. Esto ayuda a cerrar las vulnerabilidades conocidas que podrían ser explotadas por malware como Smoke Loader.
- **Conciencia de la Seguridad:** Educa a los usuarios sobre las prácticas de seguridad cibernética, como no hacer clic en enlaces sospechosos o descargar archivos adjuntos de fuentes no confiables.
- **Filtrado de Contenido Web:** Implementa filtros de contenido web para bloquear el acceso a sitios web maliciosos conocidos que podrían distribuir malware.
- **Monitoreo de Red:** Utiliza herramientas de monitoreo de red para detectar patrones de tráfico inusuales que podrían indicar la presencia de malware.

- **Análisis de Comportamiento:** Emplea soluciones de seguridad que puedan analizar el comportamiento de los programas en tiempo de ejecución para detectar actividades maliciosas.
- **Segmentación de Red:** Divide tu red en segmentos para limitar la propagación del malware en caso de una infección.
- **Copias de Seguridad:** Realiza copias de seguridad regulares de tus datos importantes y asegúrate de que estén almacenadas de forma segura fuera del alcance de cualquier malware.

Recomendaciones

Tomar en cuenta las recomendaciones para evitar el malware es fundamental para proteger la privacidad, seguridad financiera, integridad del sistema y reputación en línea. Estas medidas ayudan a prevenir las consecuencias negativas asociadas con la infección por malware y a mantener tus dispositivos y datos seguros.

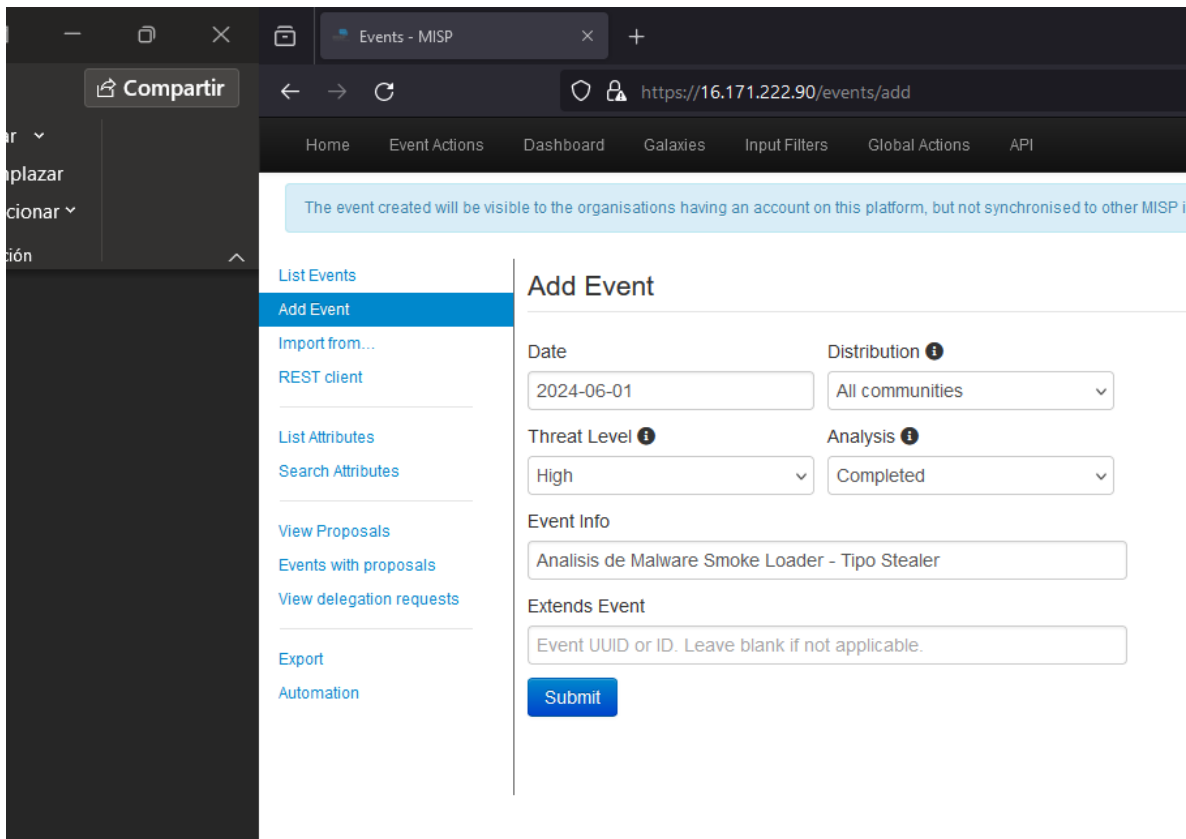
- **Protección de datos personales:** El malware puede robar información personal y confidencial, como contraseñas, números de tarjetas de crédito, información bancaria, y más. Siguiendo las recomendaciones de seguridad, puedes proteger tus datos personales de ser comprometidos.
- **Seguridad financiera:** El malware a menudo se utiliza para realizar fraudes financieros, como el robo de identidad o la realización de transacciones no autorizadas. Al evitar el malware, reduces el riesgo de sufrir pérdidas financieras debido a actividades fraudulentas.
- **Mantenimiento del funcionamiento del sistema:** El malware puede ralentizar o dañar el funcionamiento de tu dispositivo, lo que puede afectar tu productividad y rendimiento. Al seguir las mejores prácticas de seguridad, puedes mantener tu sistema funcionando de manera óptima.

- **Integridad de los archivos y programas:** El malware puede infectar y corromper archivos y programas en tu dispositivo, lo que puede causar la pérdida de datos importantes o incluso la inutilización de tu sistema. Al evitar el malware, proteges la integridad de tus archivos y programas.
- **Reputación en línea:** Si tu dispositivo se infecta con malware, podría utilizarse para enviar spam, realizar ataques a otros sistemas o participar en otras actividades maliciosas sin tu conocimiento. Esto podría dañar tu reputación en línea y tener consecuencias negativas para ti tanto a nivel personal como profesional.

Registro en MISP

Se ha registrado el análisis de la muestra de Malware en MISP, el id que se nos ha asignado es:

- **Event ID:** 14
- **UUID:** bfb2a40c-747f-4d2f-a547-507d3b27260c
- **Url:** <https://16.171.222.90/events/view/14>



The screenshot shows a web browser window with the address bar displaying `https://16.171.222.90/events/add`. The browser's tab is labeled "Events - MISP". The page has a dark-themed sidebar on the left with a "Compartir" button and a menu containing options like "List Events", "Add Event" (which is highlighted), "Import from...", "REST client", "List Attributes", "Search Attributes", "View Proposals", "Events with proposals", "View delegation requests", "Export", and "Automation". The main content area is titled "Add Event" and contains a form with the following fields:

- Date:** A text input field containing "2024-06-01".
- Distribution:** A dropdown menu set to "All communities".
- Threat Level:** A dropdown menu set to "High".
- Analysis:** A dropdown menu set to "Completed".
- Event Info:** A text input field containing "Análisis de Malware Smoke Loader - Tipo Stealer".
- Extends Event:** A text input field with the placeholder text "Event UUID or ID. Leave blank if not applicable."

At the bottom of the form is a blue "Submit" button. A light blue notification banner at the top of the form area states: "The event created will be visible to the organisations having an account on this platform, but not synchronised to other MISP instances".

Event #14 - MISP

https://16.171.222.90/events/view/14

Home Event Actions Dashboard Galaxies Input Filters Global Actions API

The event has been saved

View Event

View Correlation Graph
View Event History

Edit Event
Delete Event
Add Attribute
Add Object
Add Attachment
Add Event Report
Populate from...
Enrich Event
Merge attributes from...

Contact Reporter
Download as...

List Events
Add Event

Analisis de Malware Smoke Loader - Tipo Stealer

Event ID	14
UUID	bfb2a40c-747f-4d2f-a547-507d3b27260c
Creator org	Keepcoding
Creator user	alumno05@keepcoding.io
Protected Event (experimental)	Event is in unprotected mode.
Tags	
Date	2024-06-01
Threat Level	High
Analysis	Completed
Distribution	All communities

Warnings

Content:
Your event has neither attributes nor objects, whilst this can have legitimate reasons (such as purely creating an event with an event report or galaxy clusters), in most cases it's a sign that the event has yet to be fleshed out.

Contextualisation:
Your event has neither tags nor galaxy clusters attached - generally adding context to an event allows for quicker decision making and more accurate filtering, it is highly recommended that you label your events to the best of your ability.

Info Analisis de Malware Smoke Loader - Tipo Stealer

Published	No
#Attributes	0 (0 Objects)
First recorded change	
Last change	2024-06-01 01:40:31
Modification map	
Sightings	0 (0) - restricted to own organisation only

—Pivots —Galaxy +Event graph +Event timeline +Correlation graph +ATT&CK matrix +Event reports —Attributes —Discussion

14: Analisis de Mal...

Workspace creado en VIPER

Se subieron las muestras de Malware al framework de Viper.

16.170.61.110:8080/project/Azael/

Projects Yara Rules CLI

Search in all Projects Name Search

More Logout (alumno15)

Home Azael

Upload new Sample File Upload Sample(s) Archive Download Sample from URL Download Sample from VirusTotal

Choose file Tags for Sample (comma separated) Upload

Samples in Project: Azael

Show 10 entries Search:

#	SHA256	Name	Mime Type	Size	Tags
3	72486ec12b191d2fa211c1899e62c9257379d5bd1d850c66cc546685f3d8ea	wannacry_72406ec12b191d2fa211c1899e62c9257379d5bd1d850c66cc546685f3d8ea.exe	application/x-dosexec; charset=binary	2.2 MB	
2	35a9558eeb948ab7b943ac15b3712da7d349422c2be490c018f55d686dea59	imagen_35a9558eeb948ab7b943ac15b3712da7d349422c2be490c018f55d686dea59.png	application/x-iso9660-image; charset=binary	254.0 KB	
1	b9575221797dae0ee2baa74764e986e4a2988b8bcc6cc782060584c4c8c2ee	excel_b9575221797dae0ee2baa74764e986e4a2988b8bcc6cc782060584c4c8c2ee.xlsm	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet; charset=binary	2.5 MB	

Showing 1 to 3 of 3 entries

First Previous 1 Next Last

Event #14 - MSP

Viper - File

16.170.61.110:8000/project/Azael/file/b9575221797dae0ee2baa74764e906e4ad2988b0bcc6ecd782060584c4c8c2ee#nav-static

Search in all Projects

Name

Search

More Logout (alumno13)

Home / Azael / b9575221797dae0ee2baa74764e906e4ad2988b0bcc6ecd782060584c4c8c2ee

Sample Info

Notes

Modules

Hex View

excel_b9575221797dae0ee2baa74764e906e4ad2988b0bcc6ecd782060584c4c8c2ee.xlsm

DownloadDelete

Meta	File ID	1
	Uploaded	Sat, 01 Jun 2024 01:37:25 +0000
File Info	Name	excel_b9575221797dae0ee2baa74764e906e4ad2988b0bcc6ecd782060584c4c8c2ee.xlsm
	Size	2.5 MB (2655659 bytes)
	Type	Microsoft Excel 2007+
	Mime	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet; charset=binary
Hashes	MD5	9acd26176423fd95bae030ae9f154548
	SHA1	272cebdd8a63e7963034fe41a369b00980b83a7b
	SHA256	b9575221797dae0ee2baa74764e906e4ad2988b0bcc6ecd782060584c4c8c2ee
	SHA512	dff7f59824cde97aa2247e78931f6e1eb7cc1e44d7fcea61d05c49801a2b68aee88afe0c1461cb9650692279418c4ed7e9624a37fa8d30527f64091b4bc66170
	CRC32	C76F2B91
	Ssdeep fuzzy	49152:jE1G/iKauH5zH5msxxbIxikumYXn1z4xgRyvY88WVkyVQh2r::jEo/iK77FsXbIxmY40VKH
Relations	Parent	
	Children	

Fuzzy Search