Alejandro García Gutiérrez

  alexmagximo@gmail.com

Analisis de malware

# **Resumen ejecutivo**

El objetivo de este informa es comprender mejor los mecanismo de **SmokeLoader**, identificar sus componentes maliciosos y tomar medidas preventivas para proteger sistemas y datos sensibles.

Captura de pantalla de un videojuego

El contenido generado por IA puede ser incorrecto.

**SmokeLoader** es un malware diseñado para **cargar y ejecutar otros programas maliciosos** en sistemas infectados.  
Actúa como una **puerta de entrada** para amenazas más graves como troyanos bancarios, ransomware, stealers y cryptominers.  
Su presencia suele ser **indicativa de infecciones adicionales**.

## Principales comportamientos observados

* **Persistencia:** se asegura de reiniciarse automáticamente junto con el sistema operativo.
* **Inyección de procesos:** se oculta dentro de procesos legítimos para evitar la detección.
* **Descarga de malware adicional:** conecta a servidores remotos para recibir órdenes y descargar más malware.
* **Antianálisis:** implementa mecanismos para detectar entornos de análisis o máquinas virtuales y alterar su comportamiento.
* **Comunicación cifrada:** establece comunicación cifrada personalizada con servidores de comando y control (C2).

# **Resumen técnico**

## Análisis estático

### Detalles del archivo

Identificamos el malware con sus hashes:

Imagen que contiene Texto

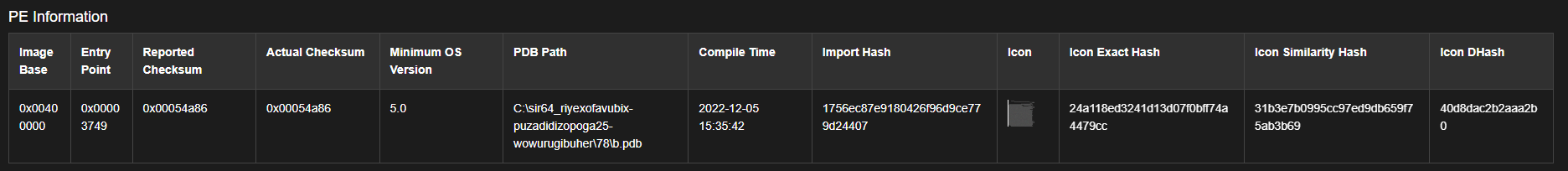
El contenido generado por IA puede ser incorrecto.



### Strings

|  |  |
| --- | --- |
| **String** | **Acción maliciosa** |
| **SetUnhandledExceptionFilter** | Técnicas anti-debugging para capturar excepciones y ocultar errores del analista. |
| **RaiseException** | Técnicas anti-debugging o control de flujo en malware. |
| **VirtualFree** | Desencripta código en memoria y luego libera el buffer. |
| **LoadResource** | El malware guarda su payload como recurso incrustado. |
| **OriginalFilename / LegalCopyright / Munpler** | Información de metadatos incrustada: revela nombres falsos o indicadores de campañas. |
| **GetNativeSystemInfo** | Detectar si la máquina es 32 o 64 bits. |
| **SetComputerNameA / GetComputerNameW** | Indican reconocimiento del sistema, útil para fingerprinting del entorno. |
| **CreateFileMappingW** | Técnicas de *process hollowing* o *injection* para mapear memoria entre procesos. |
| **OpenMutexW / OpenSemaphoreW** | Puede ser usado para asegurar que solo una instancia del malware se ejecute. |
| **CreateJobObjectW / TerminateJobObject** | Manipulación de trabajos del sistema; usado en evasión. |
| **GetCommandLineA / GetModuleFileNameA** | Identificación de ruta del propio ejecutable, usada en persistencia o auto-replicación. |
| **Microsoft Visual C++ Runtime Library / runtime error / Please contact the application's support team...** | Mensajes comunes en binarios compilados con Visual Studio, pero también útiles para identificar *packers*. |
| **SetThreadIdealProcessor** | Parte de técnicas evasivas o de manipulación de afinidad de hilos. |

### PE Estructura



#### Información de versiones

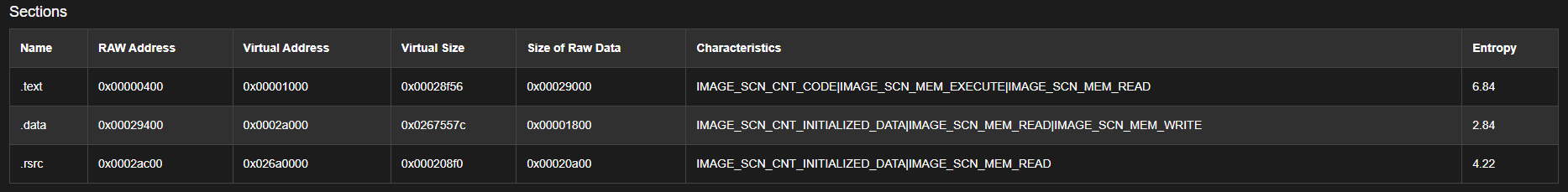
Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

La información de versión está **claramente falsificada** para despistar, con nombres absurdos e inventados y valores que no son de estándares conocidos.

#### Análisis de Sections

* **Alta entropía** en .text sugiere que el malware está **ofuscado o empaquetado**.
* **Secciones estándar** (.text, .data, .rsrc) → Sin secciones raras como .sdata, .UPX, .pack, pero eso **no descarta empaquetado**: podrían haber renombrado las secciones.
* **Tamaño de .data muy pequeño** frente a .text → sugiere que el ejecutable **no necesita muchos datos externos** o bien que **carga dinámicamente** su funcionalidad.



* + 1. MITRE ATT&CK

**MITRE ATT&CK** (Adversarial Tactics, Techniques & Common Knowledge) es un marco de referencia desarrollado por MITRE Corporation que recopila y categoriza **tácticas, técnicas y procedimientos (TTPs)** empleados por actores maliciosos en entornos reales. Este marco está diseñado para:

* **Describir comportamientos adversarios** desde el acceso inicial hasta el impacto final.
* **Establecer un lenguaje común** entre analistas de seguridad, investigadores y defensores.
* **Mejorar la detección, prevención y respuesta** ante amenazas avanzadas.

Cada técnica dentro de ATT&CK está organizada por **tácticas**, que representan las metas que un atacante desea alcanzar, como evasión de defensas, persistencia o robo de credenciales. A su vez, las técnicas están respaldadas por ejemplos del mundo real y mapeadas a herramientas y familias de malware conocidas.

En este informe, las técnicas MITRE ATT&CK observadas en la muestra analizada permiten comprender las capacidades, objetivos y modus operandi del malware, proporcionando una visión estructurada de su comportamiento.

#### Técnicas de Descubrimiento y Evasión

|  |  |  |  |
| --- | --- | --- | --- |
| **MITRE ID** | **Técnica** | **¿Qué hace?** | **Evidencia** |
| **T1033** | **System Owner/User Discovery** | El malware intenta saber quién es el usuario del sistema. | encrypt\_pcinfo — probablemente recopila el nombre del usuario y máquina. |
| **T1082** | **System Information Discovery** | Recoge info del sistema (CPU, RAM, nombre del host, etc.). | Varios módulos: antivm\_generic\_\*, recon\_fingerprint apuntan a fingerprinting detallado del entorno. |
| **T1010** | **Application Window Discovery** | Busca ventanas abiertas (aplicaciones visibles), a menudo para detectar entornos de análisis. | antidebug\_windows — identifica si hay herramientas de análisis abiertas (como OllyDbg, IDA…). |
| **T1083** | **File and Directory Discovery** | Busca archivos o directorios, probablemente para decidir qué cifrar o robar. | antiemu\_windefend — explora archivos del sistema (como Windows Defender) para evadirlo. |
| **T1497** | **Virtualization/Sandbox Evasion** | Detecta si está en VM o sandbox para abortar ejecución. | Múltiples detecciones: antivm\_generic\_\*, antivm\_vbox\_keys, antiemu\_windefend. Muy común en *SmokeLoader*. |
| **T1057** | **Process Discovery** | Enumera procesos activos del sistema. | Usa varias técnicas (CreateToolhelp32Snapshot, cmdline\_process\_discovery, etc.) para ver qué software se está ejecutando. |
| **T1012** | **Query Registry** | Lee entradas del registro de Windows, muchas veces para evadir o recolectar info. | antivm\_\*, recon\_fingerprint → acceso al registro para identificar entorno. |
| **T1518** | **Software Discovery** | Busca software instalado. | antiemu\_windefend → analiza si hay antivirus o herramientas de análisis instaladas. |

#### Técnicas de Robo de Credenciales

|  |  |  |  |
| --- | --- | --- | --- |
| **MITRE ID** | **Técnica** | **¿Qué hace?** | **Evidencia** |
| **T1003** | **OS Credential Dumping** | Intenta extraer credenciales del sistema operativo (hashes, contraseñas en memoria). | infostealer\_mail, infostealer\_browser — podrían usar herramientas o funciones como CredEnumerate, acceso a archivos de perfil. |
| **T1539** | **Steal Web Session Cookie** | Roba cookies de sesión de navegadores para secuestrar sesiones web activas. | infostealer\_cookies — módulo dedicado a extraer cookies, útil para acceder a cuentas online. |
| **T1555** | **Credentials from Password Stores** | Extrae contraseñas almacenadas en navegadores como Chrome o Firefox. | infostealer\_browser — apunta a acceso a almacenes como Login Data o key3.db. |
| **T1552** | **Unsecured Credentials** | Busca contraseñas sin cifrar (en archivos, formularios guardados, etc.). | infostealer\_mail, infostealer\_browser — posible lectura de archivos de configuración o cache de correo. |
| **T1555.003** | **Credentials from Web Browsers** | Subtécnica que indica robo específico desde navegadores web. | infostealer\_browser — accede directamente a contraseñas guardadas por el navegador. |
| **T1552.001** | **Credentials in Files** | Subtécnica que identifica búsqueda directa de credenciales en archivos. | infostealer\_mail, infostealer\_browser — podrían revisar archivos .ini, .xml, .txt con credenciales o config. de correo. |

#### Técnicas de Ejecución de código malicioso

|  |  |  |  |
| --- | --- | --- | --- |
| **MITRE ID** | **Técnica** | **¿Qué hace el malware?** | **Evidencia clave** |
| **T1129** | **Shared Modules** | Ejecuta código malicioso a través de módulos compartidos (como DLLs). | dropper — puede usar DLL injection o cargar librerías compartidas desde el propio ejecutable. |
| **T1106** | **Native API** | Usa directamente funciones del sistema (WinAPI) para evitar herramientas de análisis. | process\_creation\_suspicious\_location, antidebug\_guardpages — técnicas para evadir debuggers y análisis. |
| **T1059.001** | **Command and Scripting Interpreter: PowerShell** | Ejecuta scripts en PowerShell para descargar o ejecutar payloads. | powershell\_download, powershell\_request — indica descarga de código malicioso vía PowerShell. |

#### Técnicas de Recolección de información del sistema

|  |  |  |  |
| --- | --- | --- | --- |
| **MITRE ID** | **Técnica** | **¿Qué hace el malware?** | **Evidencia clave** |
| **T1114** | **Email Collection** | Extrae correos o credenciales de clientes de correo electrónico. | infostealer\_mail — puede acceder a archivos de Outlook, Thunderbird, etc. |
| **T1005** | **Data from Local System** | Recolecta datos de archivos locales (documentos, contraseñas, config). | infostealer\_mail, infostealer\_browser — busca información sensible almacenada localmente. |
| **T1560** | **Archive Collected Data** | Comprime o empaqueta los datos para exfiltrarlos más fácilmente. | encrypt\_pcinfo — puede cifrar o empaquetar los datos recolectados antes de enviarlos. |

#### Técnicas de Persistencia

|  |  |  |  |
| --- | --- | --- | --- |
| **MITRE ID** | **Técnica** | **¿Qué hace el malware?** | **Evidencia clave** |
| **T1547** | **Boot or Logon Autostart Execution** | Se asegura de ejecutarse cada vez que arranca el sistema. | persistence\_autorun — clave genérica de persistencia en arranque. |
| **T1547.001** | **Registry Run Keys / Startup Folder** | Usa claves del registro para ejecutarse en el inicio del sistema. | persistence\_autorun — probablemente añade entradas en HKCU\Software\Microsoft\Windows\CurrentVersion\Run. |

#### Técnicas de Escalada de Privilegios

|  |  |  |  |
| --- | --- | --- | --- |
| **MITRE ID** | **Técnica** | **¿Qué hace el malware?** | **Evidencia clave** |
| **T1547 / T1547.001** | **Autostart Execution via Registry** | Persiste al inicio del sistema aprovechando claves de ejecución automática del Registro. | persistence\_autorun |
| **T1055** | **Process Injection** | Inyecta código malicioso en procesos legítimos para ejecutarse con sus privilegios y evadir detección. | injection\_inter\_process, explorer\_http |

|  |  |  |  |
| --- | --- | --- | --- |
| **MITRE ID** | **Técnica** | **¿Qué hace el malware?** | **Evidencia clave** |
| **T1564 / T1564.003** | **Ocultación de Artefactos / Ventana Oculta** | Oculta sus ventanas para evadir la detección del usuario. | stealth\_window |
| **T1218 / T1218.004 / T1127** | **System Binary Proxy Execution** | Abusa de herramientas legítimas como InstallUtil.exe para ejecutar código. | spawns\_dev\_util |
| **T1202** | **Indirect Command Execution** | Usa herramientas legítimas del sistema para ejecutar comandos maliciosos. | suspicious\_command\_tools, uses\_windows\_utilities |
| **T1562 / T1562.001** | **Desactivar defensas** | Desactiva funciones de sandbox o unhooks de librerías para evitar análisis. | antisandbox\_unhook |
| **T1036** | **Masquerading** | Se hace pasar por procesos legítimos. | explorer\_http |
| **T1055** | **Process Injection** | Vuelve a aparecer aquí como técnica doble: ejecución + evasión. |  |
| **T1112** | **Modificación del Registro** | Cambia claves del sistema para persistencia o evasión. | powershell\_download, persistence\_autorun |
| **T1070** | **Borrado de Indicadores** | Elimina sus propios archivos tras ejecución. | deletes\_executed\_files |
| **T1497** | **Evasión de virtualización/sandbox** | Detecta si está en entornos de análisis y se adapta o detiene. | antivm\_generic\_\*, antiemu\_windefend |
| **T1027 / T1027.002** | **Obfuscation / Packing** | Usa *Themida*, un *packer* avanzado para proteger su código. | packer\_themida |

#### Técnicas de Evasión de defensas

#### Command and Control (C2)

|  |  |  |  |
| --- | --- | --- | --- |
| **MITRE ID** | **Técnica** | **¿Qué hace el malware?** | **Evidencia clave** |
| **T1071** | **C2 mediante protocolos estándar** | Usa HTTP/HTTPS, DNS y SMTP para comunicarse con sus servidores. | network\_cnc\_http, network\_smtp, powershell\_request, explorer\_http, etc. |
| **T1090 / T1090.003** | **Uso de proxies / Multi-hop proxies** | Canaliza tráfico malicioso a través de la red TOR. | network\_tor |
| **T1573** | **Canal cifrado** | Usa HTTPS cifrado para dificultar la detección del tráfico C2. | network\_cnc\_https\_\* |

#### Impacto en el sistema

|  |  |  |  |
| --- | --- | --- | --- |
| **MITRE ID** | **Técnica** | **¿Qué hace el malware?** | **Evidencia clave** |
| **T1486** | **Cifrado de datos (Ransomware)** | Cifra archivos como parte de un ataque ransomware. | ransomware\_file\_modifications |
| **T1485** | **Destrucción de datos** | Elimina archivos críticos del sistema. | anomalous\_deletefile |

## Análisis Dinámico

### Árbol de procesos

* **82d763b6cd97ca240a29.exe (PID 772):** Proceso inicial malicioso
* **explorer.exe (PID 1988) → SmokeLoader:** Carga de SmokeLoader
* **Procesos Hijos:**
  + **288D.exe, 3928.exe, 8769.exe, A89F.exe, B65B.exe, B7C1.exe, ACF7.exe**

Ejecución de múltiples payloads de nombres aleatorios → indica descarga y ejecución de malware adicional.

* **regsvr32.exe** ejecutando **942B.dll** (Persistencia e inyección):

Uso de **regsvr32.exe** con /s → carga silenciosa de DLLs maliciosas.

Técnica conocida de *Proxy Execution*

* **cmd.exe ejecutando tasklist + findstr:**

Búsqueda de procesos de antivirus (Avast, Sophos, Webroot).

* **PING.exe -n 5 localhost:** Técnica común para retrasar análisis automático.
* **cmd.exe con /c copy /b y .pif**

El malware concatena varios archivos (Infected, Tin, Excited, etc.) en un .pif, ocultando carga útil en ejecutables falsos.

* Múltiples **explorer.exe** instancias → ocultación del proceso real.

### Firmas

Tabla

El contenido generado por IA puede ser incorrecto.

Imagen que contiene Diagrama

El contenido generado por IA puede ser incorrecto.

Imagen que contiene Diagrama

El contenido generado por IA puede ser incorrecto.

Diagrama

El contenido generado por IA puede ser incorrecto.

**Firmas relevantes detectadas**

Durante el análisis dinámico de la muestra, se han identificado múltiples comportamientos maliciosos mediante firmas automáticas. A continuación, se detallan las más significativas:

**1. Robo de información (Info Stealer)**

* Recolección y cifrado de información del sistema:
  + data\_being\_encrypted: AMA-PC9D9172A010660A23
  + data\_being\_encrypted: AMA-PC04866CC210660A23
* Robo de información de navegadores:
  + C:\Users\ama\AppData\Roaming\Mozilla\Firefox\profiles.ini
  + C:\Users\ama\AppData\Roaming\Mozilla\Firefox\Profiles\32n1np5l.default-release\cookies.sqlite
* Extracción de datos de clientes de correo:
  + HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\...
  + HKEY\_CURRENT\_USER\Software\Microsoft\Office\15.0/16.0\Outlook\Profiles\Outlook\...

**2. Exfiltración de datos y comunicación remota**

* Exfiltración mediante PowerShell:  
  → *Técnicas MITRE: T1059.001, T1041*
* Conexión HTTPS a almacenamiento temporal anónimo:
  + transfer.sh con agentes tipo Mozilla/4.0 (compatible; MSIE 8.0; ...)
  + Descarga de binarios como ffoooll.exe, 2176361523.exe

**3. Persistencia y ejecución maliciosa**

* Instalación de Tor para comunicaciones C2 cifradas:  
  → *Técnica MITRE: T1090.003*
* Instalación para inicio automático en Windows:
  + HKEY\_LOCAL\_MACHINE\...\Run\CSRSS
  + HKEY\_CURRENT\_USER\...\Run\CSRSS con ruta C:\ProgramData\Drivers\csrss.exe
* Inyección de código:
  + 288D.exe(3464) → 288D.exe(3432)
* Ejecución de binarios maliciosos:
  + C:\Users\ama\AppData\Local\Temp\3928.exe, B65B.exe
* Bypass de políticas de ejecución mediante AppLaunch suspendido:
  + A89F.exe → .NET AppLaunch.exe

**4. Comportamiento tipo ransomware o wiper**

* Sobrescritura de archivos temporales, cachés y otros:
  + Múltiples archivos CabXXXX.tmp, TarXXXX.tmp
  + Archivos en Microsoft\CryptnetUrlCache, Canon\_Inc\_IC, ribagga, vhbagga, etc.
* Evidencias de cifrado de archivos legítimos del sistema y creación de nuevos artefactos

**5. Evasión y técnicas anti-análisis**

* Modificación de funciones de Windows monitoreadas por CAPE:
  + IsDebuggerPresent, CopyFileW, LoadLibraryExW, etc.
* Detección de herramientas como Avast, Windows Defender, VirtualBox o Sandboxie:  
  → *Técnica MITRE: T1497*
* Eliminación del binario original tras ejecución: → *Técnica MITRE: T1070*

### Análisis de comportamientos de red

Imagen que contiene Texto

El contenido generado por IA puede ser incorrecto.Analizando las conexiones de forma automática con un script y con ABUSEIPDB encontramos ips que han sido muy reportadas, ejemplos:

Relacionada con actividades cibercriminales:

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.Texto

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

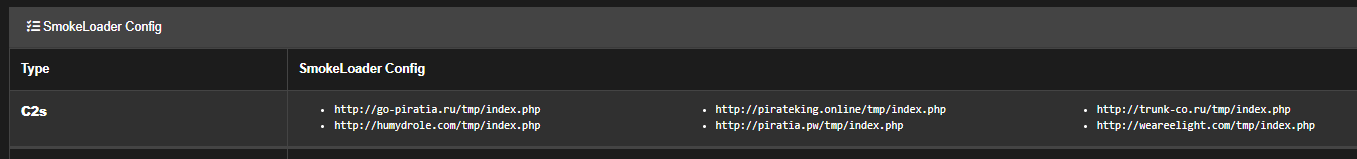
Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.Texto

El contenido generado por IA puede ser incorrecto.

Las que mayores reportes tienen vienen relacionadas con conexiones a la red TOR.

#### Comunicaciones de Comando y Control (C2)

El malware intenta establecer conexión con múltiples servidores C2 ubicados en dominios sospechosos, la mayoría con temáticas relacionadas con piratería y alojados en dominios con baja reputación. Todos usan un endpoint común /tmp/index.php, lo cual sugiere el uso de una infraestructura compartida o una plantilla de backend típica de campañas de malware.

#### Gestión de ficheros

SmokeLoader **creó varios archivos nuevos**, principalmente en las carpetas temporales del sistema y en las áreas de almacenamiento de usuarios.

Ejemplos:

82d763b6cd97ca240a29.exe, 288D.exe, 3928.exe, 8769.exe, 942B.dll, A89F.exe, B65B.exe

El malware también **cambio archivos en las carpetas temporales** y registros de informes de error de Windows, así como archivos relacionados con el navegador.

Ejemplos:

State, unverified-microdesc-consensus, cached-certs, cached-microdesc-consensus.

SmokeLoader **eliminó algunos archivos temporales** y otros archivos creados previamente para ocultar su rastro y dificultar la detección.

Ejemplos:

82d763b6cd97ca240a29.exe, 288D.tmp, 3928.tmp, 8769.tmp, 942B.tmp, A89F.exe, B65B.tmp

#### Payloads Identificados

* **Injected PE Image: 32-bit executable**
  + **Descripción:** Ejecutable PE de 32 bits comprimido con UPX, inyectado en un proceso temporal (288D.exe) y vinculado a SmokeLoader.
  + **Función principal:** Actuar como payload secundario para robar información, descargar más malware o mantener persistencia en el sistema.
* **Unpacked Shellcode**
  + **Descripción:** Shellcode desempaquetado detectado en memoria, sin formato PE, asociado al proceso 288D.exe y con patrones de código malicioso embebido.
  + **Función principal:** Cargar o ejecutar código malicioso adicional en memoria (como un payload o PE embebido) eludiendo detección mediante técnicas de evasión como la inyección directa.
* **Unpacked PE Image: 32-bit executable**
  + **Descripción:** Ejecutable PE .NET desempaquetado cargado desde 8769.exe, identificado como ofuscado con *ConfuserEx*, una herramienta común para evadir análisis.
  + **Función principal:** Actuar como módulo o componente .NET ofuscado del malware, posiblemente encargado de funciones específicas como persistencia, carga dinámica o comunicación con C2.
* **PE image**
  + **Descripción:** Ejecutable DOS (COM) con presencia de shellcode y un PE32 incrustado, posiblemente utilizado como *dropper* o cargador de segunda etapa.
  + **Función principal:** Desplegar o inyectar un payload PE en memoria para ejecución posterior, actuando como componente inicial del malware para evadir detección.

## Conclusión del Análisis: SmokeLoader

SmokeLoader es un *loader* modular diseñado para eludir la detección y facilitar la descarga e inyección de payloads maliciosos adicionales. En esta muestra, el malware ejecuta múltiples técnicas ofensivas, entre ellas:

* **Inyección en procesos legítimos (process hollowing)**
* **Descarga de payloads adicionales (PE y shellcode)**
* **Persistencia y evasión (uso de packers, nombres ofuscados, alto entropy)**
* **Conexión a múltiples C2 activos,** con dominios sospechosos y rutas /tmp/index.php
* **Carga de componentes .NET obfuscados (ConfuserEx)**
* **Uso de shellcode y ejecutables COM para eludir antivirus**

Esta campaña muestra comportamiento típico de una primera fase de infección para despliegue de malware más destructivo como stealers, backdoors o ransomware.

## Mitigación

1. **Bloqueo de IoCs**
   * Añadir todos los hashes, dominios y direcciones IP a los sistemas de detección y listas negras.
   * Usar servicios como **AbuseIPDB** para alimentar reglas de firewall.
2. **Segmentación de red**
   * Aislar equipos infectados y segmentar los entornos críticos para contener la propagación.
3. **Revisión de logs y tráfico**
   * Analizar tráfico saliente HTTP no cifrado a rutas sospechosas (/tmp/index.php) y dominios inusuales.
4. **Fortalecer detección**
   * Implementar herramientas de EDR con capacidades de análisis de comportamiento.
   * Reforzar el análisis estático y dinámico mediante sandboxes tipo CAPE.

## Recomendaciones

* **Actualización de sistemas**: Garantizar que todos los sistemas operativos y aplicaciones estén actualizados con parches de seguridad.
* **Control de macros y scripts**: Restringir ejecución automática de macros en documentos ofimáticos.
* **Educación y concienciación**: Formar a los usuarios sobre phishing y archivos sospechosos.
* **Uso de entornos virtuales para análisis**: Como prácticas estándar para investigar posibles amenazas.
* **Backups periódicos**: Desconectados o en entornos de solo lectura para mitigar posibles daños por ransomware secundario.