Nro. Alerta:	AL-2025-059	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	18-nov-2025	SmoKeLoader	Pág.: **1** of **10**

I. DATOS GENERALES:

Clase de alerta: Amenaza activa – Malware Loader
Tipo de Incidente: Distribución de malware / potencial ransomware
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- SmoKeLoader - Figura referencial

Se ha identificado un repunte significativo de actividad del SmokeLoader, que es un popular y asociado distribuidor de múltiples tipos de malware, de entrega de payloads como troyanos, familias de ransomware como MedusaLocker y Phobos e incluyendo Stealers (robo de información). Durante noviembre de 2025, diferentes fuentes de inteligencia (Microsoft Threat Intelligence, Zscaler ThreatLabz, SOC Prime y Unit 42) reportaron nuevas campañas activas de este malware en América Latina y Europa del Este, empleando técnicas actualizadas de ingeniería social y explotación de vulnerabilidades recientes.

III. INTRODUCCIÓN

Activo desde 2011, SmokeLoader es un malware de tipo Backdoor, sin embargo, por su diseño está orientado al envió de malware para la entrega de payload de segunda etapa, que son aquellos que contiene las instrucciones maliciosas completas, como un control remoto (Meterpreter) para, exfiltrar datos, tomar control del SO, browser hijacking, desplegar más malware, ransomware o troyano, con el fin de llevar a cabo el ataque deseado una vez que el exploit inicial ha abierto el camino.

Por el método que utiliza para el despliegue de otros payloads, fue categorizado como un gusano.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

En el 2014, tenía capacidades de creación de botnets, que luego son explotadas para ataque DDoS lo que permite a los ordenadores infectados ejecutar los comandos enviados desde el servidor de comandos (C2).

Otro aspecto específico relacionado con este Backdoor es la forma en que está codificado. En primer lugar, los lenguajes de bajo nivel como Asm rara vez se utilizan para la creación de malware, aunque C se encuentra con bastante frecuencia. Profundamente ofuscado y cifrado, el código permanece ilegible incluso durante la ejecución del malware. Cuando necesita realizar otra llamada a la API, cifra la parte que ha dejado de utilizar y descifra la que necesita. Este enfoque proporciona una gran seguridad contra la ingeniería inversa, pero la ejecución suele tardar más de lo habitual.

El payload que este malware envía al dispositivo objetivo NO contiene un PE header (es una estructura de datos fundamental en el SO Windows, esencial para entender cómo funcionan los archivos ejecutables .exe y las librerías de enlace dinámico (.dll) y otros componentes del sistema), por lo que no se puede ejecutar de forma habitual. Esto confunde a algunos antivirus, que lo consideran un archivo dañado y, por lo tanto, lo ignoran. Para ejecutarse y proporcionar persistencia, vacía el código en un proceso del sistema y enumera las ubicaciones de las DLL para poder utilizarlas cuando sea necesario.

SmokeLolader resurge a principios de 2025, la compañía ThreatLabz identificó una nueva versión que incluía correcciones de errores y otras mejoras a esta nueva variante se la denomino la versión 2025 alfa.

Para julio de 2025, el autor de SmokeLoader anunció una nueva versión en un foro de ciberdelincuentes. ThreatLabz identificó una variante adicional con más cambios y un protocolo de red ligeramente modificado que rompe la compatibilidad con las versiones anteriores, esta variante denominada versión 2025 que coincide con el número de versión que informa en las beacons (comunicación maliciosa) al servidor de comando y control (C2).

SmokeLoader en 2025 sigue siendo una amenaza importante tanto para las empresas como para los usuarios individuales. Sus características de diseño le permiten actuar de forma sigilosa y ser invisible e invencible para los programas antivirus.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

IV. VECTOR DE ATAQUE

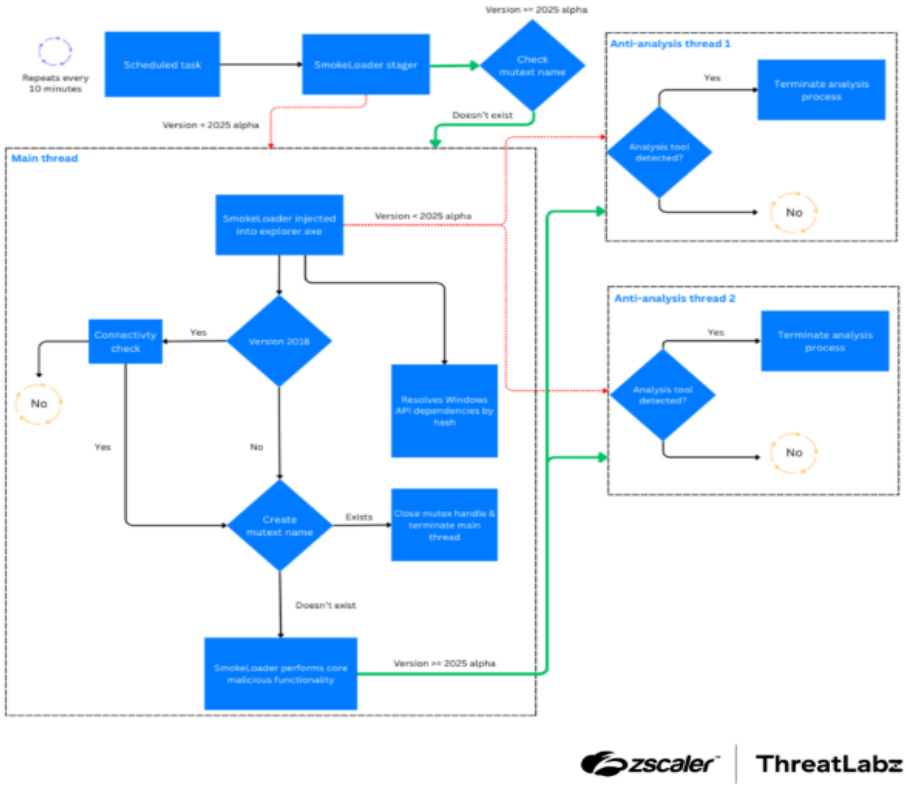


Figura 2. - Comparación del flujo de control del proceso de ejecución con las versiones anteriores versión alfa 2025 (rojo) y la posterior versión 2025 (verde) - SmoKeLoader

Análisis de SmokeLoader, versión 2025 alfa y la versión 2025.

La versión 2025 alfa se identifica también como versión 2022 cuando se comunica con el servidor C2. Sin embargo, las marcas de tiempo de compilación de estas muestras se remontan aproximadamente a febrero de 2025. SmokeLoader consta de dos componentes principales: un stager y un main module.

El stager tiene dos funciones principales, la de dificultar el análisis, detectar entornos virtuales (y terminarlos si están presentes) e inyectar el módulo principal de SmokeLoader en explorer.exe.

El main module realiza la mayor parte de la funcionalidad maliciosa, incluyendo el establecimiento de la persistencia, la señalización al servidor C2 y la ejecución de tareas y complementos.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Las versiones de SmokeLoader del 2018 a 2022 causaban una degradación del rendimiento en los SO infectados. Esto se debía a varios factores, entre ellos una tarea programada (utilizada para la persistencia) que ejecutaba el stager de SmokeLoader cada 10 minutos. Dado que el stager de SmokeLoader no comprobaba si el módulo principal ya se estaba ejecutando (a través de un mutex), el stager asignaba memoria en explorer.exe e inyectaba una nueva copia del main module de SmokeLoader cada 10 minutos. Además, el main module creaba dos subprocesos para identificar y desactivar las herramientas de análisis antes de comprobar si SmokeLoader ya se estaba ejecutando. Como resultado, también se creaban dos nuevos subprocesos en explorer.exe cada 10 minutos.

Stager

El stager de la versión 2025 alpha corrigió el error de inyectar SmokeLoader continuamente en el proceso explorer.exe, el resto del código se mantuvo prácticamente sin cambios. Sin embargo, en el stager de la versión 2025 de SmokeLoader se introdujeron cambios adicionales, entre los que se incluyen los siguientes:

- Se implementó una nueva función para descifrar bloques de código añadiendo un valor codificado a cada byte antes de la ejecución.
- Calcula dinámicamente los RVA (realizando una operación XOR con una constante) al descifrar el código.
- Añadió un nuevo código shell de 64 bits para inyectar el módulo principal en explorer.exe.

Main module

El main module de SmokeLoader ha recibido varias actualizaciones tanto en la versión 2025 alpha como en la 2025, con un solapamiento significativo entre ambas versiones. Dado que el algoritmo de generación de mutex se trasladó al stager, la cadena mutex se pasa al módulo principal, donde se crea el mutex si aún no existe. Si el nombre del mutex existe (lo que en teoría nunca debería ocurrir debido a la comprobación en el stager), SmokeLoader se cierra.

En ambas versiones, varias constantes se ofuscan utilizando una función simple que realiza una operación XOR con un valor codificado (que cambia por muestra). En la versión 2025, se ofuscan constantes como el valor 0xF001F (SECTION_ALL_ACCESS) que se pasa a la función NtCreateSection. Sin embargo, en la versión 2025 alfa, se ofuscan diferentes constantes, incluido el número de versión de SmokeLoader, como se muestra a continuación.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

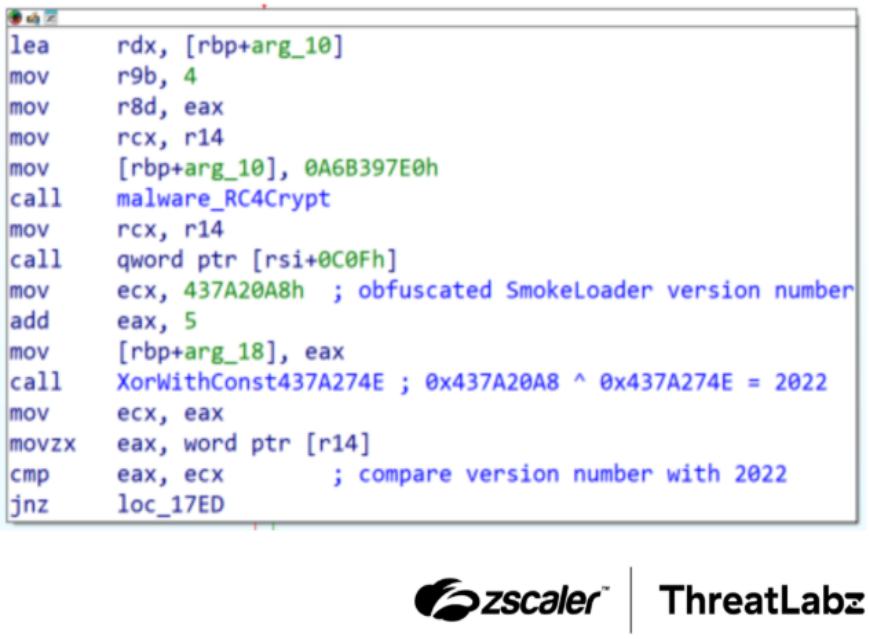


Figura 3.- Ejemplo de la ofuscación constante alfa versión 2025 - SmoKeLoader

En la versión 2025, hay una comprobación adicional del idioma que compara si la distribución del teclado de la víctima es rusa (y no ucraniana). Si se detecta una distribución de teclado rusa, SmokeLoader se cierra automáticamente. Curiosamente, ya existe una comprobación muy similar en el stager de SmokeLoader, por lo que este código es algo redundante.

Otro cambio en el main module en las versión a alfa 2025 y anteriores, es que el nombre de asignación de archivos consistía en el ID del bot seguido de los caracteres "FF". En la versión 2025, el nombre de asignación de archivos es ahora el hash del ID del bot (como cadena) convertido a caracteres hexadecimales en mayúscula (sin los caracteres "FF" añadidos).

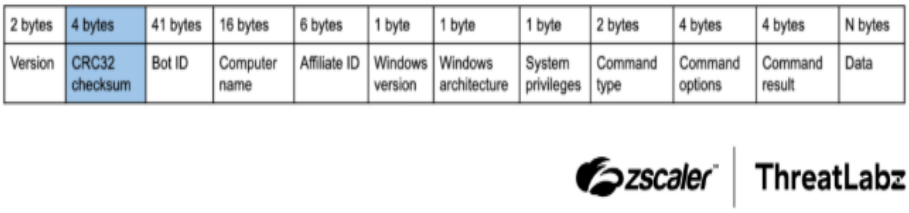
Nombre de la tarea programada

Las versiones anteriores de SmokeLoader utilizaban la cadena de formato Firefox Default Browser Agent %hs para la tarea programada que establecía la persistencia. A partir de la versión 2025 alpha, SmokeLoader utiliza ahora la cadena de formato MicrosoftEdgeUpdateTaskMachine%hs. En ambos casos, la cadena de formato %hs del nombre de la tarea son los primeros 16 caracteres del ID del bot víctima. Curiosamente, el desarrollador de SmokeLoader eliminó el espacio entre el prefijo de la cadena del navegador falso y el ID del bot, lo que probablemente sea un descuido.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Protocolo de red para la versión 2025

Aunque la variante alfa 2025 utiliza el mismo protocolo de red que la versión 2022, se han realizado algunos ajustes mínimos en la versión 2025. Por ejemplo, el número de versión de dos bytes ahora muestra el valor 2025 (0x7e9) en lugar de 2022 (0x7e6). La versión 2025 también ha actualizado la solicitud para incluir un valor CRC32 de cuatro bytes en el desplazamiento de bytes 2. La suma de comprobación CRC32 se calcula en los bytes siguientes al desplazamiento 6 (que comienza con el ID del bot), como se muestra en la siguiente figura.



2 bytes	4 bytes	41 bytes	16 bytes	6 bytes	1 byte	1 byte	1 byte	2 bytes	4 bytes	4 bytes	N bytes
Version	CRC32 checksum	Bot ID	Computer name	Affiliate ID	Windows version	Windows architecture	System privileges	Command type	Command options	Command result	Data

zscaler | ThreatLabz

Figura 4.- Formato de beacon versión 2025 - SmoKeLoader

El formato de respuesta en la versión 2025 también se modificó ligeramente. Anteriormente, los primeros 4 bytes de la respuesta C2 contenían la longitud del comando. Ahora, este valor de longitud se oculta mediante una operación XOR con la clave de cifrado RC4 de las muestras.

La siguiente tabla ofrece una comparación de los cambios más significativos de las tres últimas versiones de SmokeLoader.

	Versión 2022	Versión 2025 alpha	Versión 2025
Obfuscated constants	No	Yes	Yes
Scheduled task name	Firefox Default Browser Agent %hs	MicrosoftEdgeUpdateTaskMachine%hs	MicrosoftEdgeUpdateTaskMachine%hs
Mutex check	Main module	Stager + main module	Stager + main module
Network protocol version	2022	2022	2025
Keyboard layout check	Stager	Stager	Stager + main module
File mapping name	Bot ID + “FF"	Bot ID + “FF"	MD5(Bot ID)

Tabla 1.- Comparación de las tres últimas variantes - SmoKeLoader

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

V. IMPACTO

Categoría	Producto/ Software Afectado	Detalles/ Vulnerabilidad Asociada
Sistema Operativo	Windows (todas las versiones activas)	Objetivo principal de SmokeLoader.
Suite Ofimática	Microsoft Office	Vulnerabilidades explotadas: CVE-2017-0199 y CVE-2017-11882.
Utilidad de compresión	7-Zip (versiones antiguas)	Vulnerabilidad CVE-2025-0411 usada para desplegar malware vía archivos 7z.
Otros vectores	Keygens, cracks, instaladores falsos	Distribuidos en foros y sitios piratas; ejecutan SmokeLoader al abrirlos.
Software de seguridad	N/A	Evade detección de algunos antivirus; recomienda uso de EDR actualizado.

Tabla 2.- Productos y Software Afectados - SmoKeLoader

VI. INDICADORES DE COMPROMISO

hashes SHA-256	
Troyano.Win32.Cargador de humo.bot	a7f605d4110bba430e02c7c5240e656fb3f1dd7f02dce985e9e5677169c9de55
Troyano.Win32.Cargador de humo.bot	cc58ad1f7a097f077f06b78e21c1f5a01007cd98613b602bb22b95751920ba80
Troyano.Win32.Cargador de humo.bot	143310670009099214b1b1a812e98a485db3e2879ab35dca8ba63005a62a610c
Troyano.Win32.Cargador de humo.bot	109d9077e847550b471e717986dec00400d4a49cccf438a462ec9630eda654c5
Troyano.Win32.Cargador de humo.bot	0c1f4caa4168d458ffedcd65213253b42d972964ea78d042d4c560d8a71973bc

Tabla 3.- hashes SHA-256 – SmoKeLoader

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

URL de C2
monsutiur4[.]com
cucumbetuturel4[.]com
nikogminut88[.]en
eyecosl[.]ga
paishancho17[.]arriba
xpowebs[.]ga
lilisjjoer44[.]com
nusurionuy5ff[.]en
samnutu11nuli[.]com
limo00ruling[.]org
lingotes[.]tk
ydiannetter18[.]arriba
nunuslushau[.]com
venis[.]ml
moroitomo4[.]net
archivo-host-host6[.]com
mini55tunull[.]com
mizangs[.]tw
azarehanelle19[.]arriba
linislominyt11[.]en
mbologwuholing[.]co[.]ug
susuerulianita1[.]net
host-host-file8[.]com
tootoo[.]ga
fiskahlilian16[.]arriba
quericeriant20[.]top
luxulixionus[.]net
quadoil[.]ru

Tabla 4.- URL de C2 - SmokeLoader

Direcciones IP
5[.]149[.]253[.]100
185[.]174[.]173[.]116
137[.]74[.]151[.]148
94[.]103[.]82[.]216
213[.]183[.]51[.]54
37[.]230[.]112[.]146
185[.]117[.]88[.]96
185[.]174[.]173[.]241
185[.]223[.]95[.]66
185[.]20[.]187[.]13
62[.]109[.]24[.]176
185[.]174[.]174[.]72
185[.]174[.]173[.]34
62[.]109[.]26[.]121
85[.]143[.]221[.]60
185[.]242[.]179[.]118
62[.]109[.]27[.]196
65[.]55[.]252[.]93

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Direcciones IP
162[.]247[.]155[.]114
185[.]68[.]93[.]27
195[.]123[.]216[.]115
62[.]109[.]26[.]208
185[.]174[.]174[.]156

Tabla 5.- Direcciones ip - SmokeLoader

VII. RECOMENDACIONES:

- Mantener el software actualizado, especialmente parchear vulnerabilidades explotadas como la de 7-Zip utilizada para desplegar SmokeLoader.
- Implementar filtros de correo electrónico y controles de entrada que bloqueen archivos adjuntos sospechosos (ZIP, 7Z, LNK) y deshabiliten ejecución automática de macros o scripts provenientes de fuentes no confiables.
- Monitorizar constantemente la red y los endpoints para detectar tareas programadas inusuales, procesos inyectados, mutexes desconocidos o conexiones hacia servidores de comando y control (C2).
- Implementar segmentación de red, privilegios mínimos y controles de acceso para reducir la propagación lateral del malware.
- Usar herramientas de análisis forense y remediación especializadas para detectar y eliminar SmokeLoader de los sistemas comprometidos.
- Realizar copias de seguridad regulares, verificar su integridad y ensayar los procedimientos de restauración.
- Capacitar al personal sobre buenas prácticas de seguridad: cuidado al abrir archivos adjuntos, evitar software de fuentes no oficiales y reportar comportamientos anómalos.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

ZSCALER (2025). SmokeLoader Rises from the Ashes. https://www.zscaler.com/blogs/security-research/smokeloader-rises-ashes

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

GRIDINSOFT (2025). SmokeLoader Backdoor Description. https://gridinsoft.com/backdoor/smokeloader

MICROSOFT (2025). Threat Encyclopedia — Trojan:JS/SmokeLoader.KKZ!MTB. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan%3AJS%2FSmokeLoader.KKZ%21MTB&ThreatID=2147956875

HOPLON INFOSEC (2025). SmokeLoader Malware, Plugins, and DDoS Capabilities. https://hoploninfosec.com/smokeloader-malware-plugins-data-dos-attacks?utm_source

G DATA SOFTWARE (2025). Emmental: SmokeLoader Malware Campaign. https://www.gdatasoftware.com/blog/2025/03/38160-emmenhtal-smokeloader-malware?utm_source

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec