| | |
|---|---|
| **Alerta ID:** | 087 |
| **Fecha del reporte:** | 26/03/2026 |
| **Entidad:** | Todas las Entidades del Ecosistema Digital |
| **Título:** | Malware Kiss Loader con inyección Early Bird APC |
| **Herramienta de detección** | N/A |
| **Activo involucrado:** | Microsoft Windows |
| **Tipo de alerta:** | Boletín informativo |
| **Nivel de riesgo:** | Alta |

## Resumen ejecutivo

Informar a las entidades del Ecosistema Digital sobre la existencia y comportamiento de Kiss Loader, un malware loader de nueva generación identificado en marzo de 2026 por investigadores de G DATA.

## Descripción:

Kiss Loader es un loader malicioso de reciente creación, diseñado específicamente para infiltrarse en sistemas Windows de forma sigilosa mediante técnicas avanzadas de inyección de código en memoria. Su descubrimiento fue el resultado de una investigación de rutina realizada por analistas de G DATA, quienes encontraron que el directorio WebDAV del atacante estaba completamente abierto sin restricciones de acceso, lo que reveló que la campana se encontraba aún en fase activa de desarrollo al momento de su detección.

**Características principales:**

- Herramienta completamente nueva, sin precedentes en bases de datos públicas de malware.
- Campana activa y en desarrollo al momento de su descubrimiento en marzo de 2026.



CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Usa infraestructura legítima (TryCloudflare) para alojar y actualizar sus payloads.
- Implementa inyección Early Bird APC dentro de explorer.exe (proceso de confianza de Windows).
- El shellcode se genera con Donut, operando exclusivamente en memoria sin escribir archivos en disco.
- Entrega dos payloads secundarios: VenomRAT (RAT tipo AsyncRAT) y Kryptik (malware protegido con .NET Reactor).
- Durante el análisis, el actor de la amenaza respondió activamente a mensajes del investigador, confirmando presencia en tiempo real en la máquina comprometida.

## Consecuencias de la explotación

La ejecución exitosa de Kiss Loader tiene consecuencias críticas para la organización o usuario afectado:

| | |
|---|---|
| **ACCESO REMOTO TOTAL** | VenomRAT permite al atacante controlar el sistema comprometido de forma completa: exfiltración de datos, ejecución de comandos, captura de pantalla y keylogging. |
| **PERSISTENCIA AUTOMÁTICA** | El malware se garantiza ejecución tras cada reinicio mediante la inserción de archivos en la carpeta de inicio de Windows (Startup), dificultando su eliminación manual. |
| **EVASIÓN DE ANTIVIRUS** | Al operar exclusivamente en memoria (sin escritura en disco) y mediante inyección en procesos legítimos como explorer.exe, los antivirus tradicionales no lo detectan. |



CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

| | |
|---|---|
| ENTREGA DE MALWARE ADICIONAL | La arquitectura modular permite al atacante desplegar cualquier payload adicional: ransomware, infostealers, minería de criptomonedas, etc. |
| PRESENCIA ACTIVA DEL ATACANTE | Se confirmó interacción en tiempo real del actor de amenaza durante el análisis forense, lo que indica capacidades de respuesta activa post-compromiso. |

## Modo de explotación y cadena de infección

Kiss Loader implementa una cadena de infección multi-etapa altamente sofisticada. A continuación se describe cada fase:

### Entrega del Vector Inicial

La víctima recibe o descarga un archivo llamado DKM_DE000922.pdf.url. Este archivo es en realidad un Windows Internet Shortcut (.url), no un PDF, pero su nombre está diseñado para engañar al usuario haciéndole creer que es un documento PDF legítimo. Al hacer clic sobre el archivo, el sistema operativo Windows procesa silenciosamente la URL embebida en el shortcut.

### Conexión a Infraestructura TryCloudflare

El shortcut apunta a un servidor remoto alojado mediante un tunel TryCloudflare. TryCloudflare es un servicio legítimo de Cloudflare que permite crear conexiones temporales a internet sin necesitar un dominio registrado. Esta técnica le permite al atacante: (a) operar bajo dominios de confianza que raramente son bloqueados por proxies corporativos, (b) actualizar o reemplazar payloads en tiempo real sin alterar el vector inicial, y (c) dificultar el rastreo y bloqueo de la infraestructura maliciosa.



CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

**Descarga de Componentes y Persistencia**

Una vez establecida la conexión, el sistema descarga múltiples componentes adicionales: scripts de tipo .bat, .js y .wsh, y un archivo comprimido .zip con los módulos del loader. Un script Batch (gg.bat / pol.bat) copia un archivo de persistencia dentro de la carpeta de inicio de Windows (C:\Users\[usuario]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\), garantizando que el malware se ejecute automáticamente en cada reinicio del sistema. Paralelamente, se despliega un PDF señuelo para que la víctima no sospeche de la actividad maliciosa en segundo plano.

**Carga del Python Loader (Kiss Loader / so.py)**

El archivo comprimido contiene un loader escrito en Python (so.py), que constituye el núcleo de Kiss Loader. Este componente: (a) lee archivos de configuración en formato JSON que contienen las claves de descifrado, (b) descifra los payloads cifrados almacenados como archivos binarios (ov.bin, tv.bin), y (c) pasa el shellcode descifrado al siguiente módulo para su inyección en memoria. Al operar con claves externas en JSON, el código fuente del loader no contiene información sensible por sí solo, complicando el análisis estático.

**Conversión a Shellcode con Donut**

Los payloads (.NET assemblies — VenomRAT y Kryptik) son convertidos a shellcode puro usando Donut, una herramienta de código abierto que transforma ensamblados .NET en shellcode que puede ejecutarse directamente en memoria. Esta técnica garantiza que ningún archivo malicioso sea escrito en disco en esta etapa, haciendo que los antivirus tradicionales basados en firmas sean prácticamente ineficaces.

**Inyección Early Bird APC en explorer.exe**

Esta es la técnica central de evasión de Kiss Loader. El proceso se ejecuta de la siguiente manera:

1. Kiss Loader lanza explorer.exe en estado suspendido (CreateProcess con CREATE_SUSPENDED), lo que significa que el proceso inicia pero no ejecuta ninguna instrucción.



CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

2. Asigna un bloque de memoria dentro del espacio de proceso de explorer.exe usando VirtualAllocEx.
3. Escribe el shellcode descifrado en ese bloque de memoria mediante WriteProcessMemory.
4. En lugar de crear un nuevo hilo (técnica monitoreada por EDRs), encola una Asynchronous Procedure Call (APC) en el hilo principal del proceso suspendido usando QueueUserAPC.
5. Al reanudar la ejecución del proceso con ResumeThread, la APC se dispara primero, ejecutando el shellcode antes de que explorer.exe realice sus operaciones normales.
6. El resultado es que el payload (VenomRAT/Kryptik) se ejecuta completamente dentro del contexto de un proceso legítimo del sistema operativo, sin dejar rastros en disco y sin crear hilos nuevos detectables.

**Ejecución de Payloads Finales**

- VenomRAT: RAT (Remote Access Trojan) similar a AsyncRAT, que permite control remoto completo de la máquina: ejecución de comandos, exfiltración de archivos, captura de pantalla, keylogging y más.
- Kryptik: Archivo .NET protegido con .NET Reactor (ofuscador comercial), cuya función exacta aún se investiga. Se presume que actúa como dropper o infostealer adicional.

## Vulnerabilidades explotadas

Kiss Loader no explota vulnerabilidades de software con CVE asignado. En su lugar, abusa de funcionalidades legítimas del sistema operativo Windows y de servicios en la nube confiables:

- **Abuso de Windows Internet Shortcut (.url)**

Los archivos .url son procesados silenciosamente por Windows Shell sin interacción visible adicional del usuario. Renombrar un archivo .url con una extensión enganhosa (.pdf.url) explota la confianza del usuario en extensiones de archivo familiares. Windows por defecto puede ocultar extensiones, agravando este engaño.



CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- **Abuso de TryCloudflare (Living off Trusted Sites)**

TryCloudflare es un servicio gratuito de Cloudflare. El atacante lo usa para tunelizar tráfico malicioso a través de dominios *.trycloudflare.com, que generalmente están en listas blancas corporativas y raramente son bloqueados. Esto le otorga al atacante dominio de confianza sin registro, anonimato de infraestructura y capacidad de actualización de payloads en tiempo real.

- **Early Bird APC Injection (Técnica de Evasión Avanzada)**

Esta técnica abusa de la API de Windows APC (Asynchronous Procedure Calls), un mecanismo legítimo del sistema operativo para ejecutar código de forma asíncrona. Al inyectar código en un proceso antes de que este inicie su ejecución normal (Early Bird), el atacante evade la mayoría de las herramientas de seguridad que monitorizan la creación de hilos y llamadas al sistema post-inicio de proceso.

- **Evasión por Operación en Memoria (Fileless Malware)**

El uso de Donut para convertir ensamblados .NET a shellcode en memoria elimina la necesidad de escribir archivos maliciosos en disco. Los antivirus basados en firmas no pueden detectar código que nunca existe como archivo. Solo las soluciones con inspección de memoria en tiempo real (EDR avanzados) pueden detectar esta técnica.

## Indicadores de compromiso

A continuación se listan los hashes SHA-256 y archivos asociados a Kiss Loader, publicados por G DATA en su investigación del 26 de marzo de 2026:

| Hash / Indicador | Archivo / Descripción | Payload |
|---|---|---|
| 6abd118a0e6f5d67bfe1a79dacc1fd198059d8d66381563678f4e27ecb413fa7 | DKM_DE000922.pdf.url | Vector inicial (acceso) |
| e8f83d67a6b894399fad774ac196c71683de9ddca3cf0441bb95318f5136b553 | oa.wsh | Script WSH auxiliar |
| 549c1f1998f22e06dde086f70f031dbf5a3481bd3c5370d7605006b6a20b5b0b | ccv.js | Script JavaScript malicioso |



CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

| Hash / Indicador | Archivo / Descripción | Payload |
|---|---|---|
| 6d62b39805529aefe0ac0270a0b805de6686d169348a90866bf47a07acde2284 | gg.bat | Script de persistencia (Batch) |
| b4525711eafbd70288a9869825e5bb3045af072b5821cf8fbc89245aba57270a | pol.bat | Script Batch secundario |
| e8dbdab0afac4decce1e4f8e74cc1c1649807f791c29df20ff72701a9086c2a0 | vwo.zip | Archivo comprimido con componentes |
| 5cab6bf65f7836371d5c27fbfc20fe10c0c4a11784990ed1a3d2585fa5431ba6 | so.py | Kiss Loader (Python) |
| 130ca411a3ef6c37dbd0b1746667b1386c3ac3be089c8177bc8bee5896ad2a02 | ov.bin (descifrado) | VenomRAT — Payload primario |
| 2b40a8a79b6cf90160450caaad12f9c178707bead32bcc187deb02f71c25c354 | tv.bin (descifrado) | Kryptik — Payload secundario |

**Indicadores de red / comportamientos adicionales:**

- Conexiones salientes a dominios *.trycloudflare.com a través de WebDAV.
- Proceso explorer.exe lanzado en estado suspendido por un proceso no nativo.
- Archivos .url con extensión doble (ej. archivo.pdf.url) descargados desde correos o enlaces.
- Directorios WebDAV accesibles públicamente sin autenticación que alojan archivos .zip, .py, .bat y .js.

## Recomendaciones

Para identificar una posible infección por Kiss Loader, los equipos de seguridad deben monitorear las siguientes señales:

- Bloquear o alertar sobre conexiones WebDAV a dominios *.trycloudflare.com no autorizados.
- Monitorear transferencias de archivos .zip, .py, .bat y .js desde dominios de túnel.



CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Detectar tráfico inusual hacia TryCloudflare fuera del horario laboral normal.
- Implementar inspección SSL/TLS para identificar payloads cifrados en tránsito.
- Buscar el nombre de archivo DKM_DE000922.pdf.url en historiales de descarga y correo electrónico.
- Verificar la existencia de so.py, gg.bat, pol.bat, vwo.zip en sistemas de producción.

**Medidas inmediatas:**

1. Bloquear en proxy/firewall todas las conexiones hacia *.trycloudflare.com que no estén explícitamente autorizadas.
2. Revisar y eliminar cualquier archivo presente en la carpeta Startup no autorizado por el equipo de TI.

**Medidas a largo plazo:**

- Configurar políticas de grupo (GPO) para deshabilitar la ejecución automática de archivos .url desde correo electrónico o descargados de internet.
- Implementar Application Whitelisting para restringir la ejecución de Python a rutas y usuarios autorizados.
- Capacitar a usuarios finales en la identificación de archivos con extensiones dobles o engañosas.
- Requerir autenticación en todos los servidores WebDAV internos y externos para evitar hosting abierto de payloads.
- Mantener actualizados los sistemas operativos Windows y todos los runtimes instalados (.NET, Python).
- Implementar reglas YARA basadas en las características de so.py (descifrado JSON + APC injection) en plataformas de análisis de malware.
- Revisar y reforzar las políticas de correo electrónico para bloquear adjuntos con extensión .url en los gateways de email.



CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

## Fuentes:


- G DATA Blog — 'Analysis: Kiss Loader' (marzo 2026): https://blog.gdatasoftware.com/2026/03/38399-analysis-kissloader
- CyberSecurityNews — 'New Kiss Loader Malware Uses Early Bird APC Injection' (26 marzo 2026): https://cybersecuritynews.com/new-kiss-loader-malware-uses-early-bird-apc-injection/
- MITRE ATT&CK — Process Injection: APC Injection (T1055.004): https://attack.mitre.org/techniques/T1055/004/
- MITRE ATT&CK — Boot or Logon Autostart: Startup Folder (T1547.001): https://attack.mitre.org/techniques/T1547/001/
- Donut — Shellcode Generator: https://github.com/TheWover/donut
- TryCloudflare — Documentación oficial: https://developers.cloudflare.com/cloudflare-one/connections/connect-networks/do-more-with-tunnels/trycloudflare/


En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 3168931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.



CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570