

Alerta ID:	118
Fecha del reporte:	01/07/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Campaña Silent Swap distribuye Crypto Clipper mediante extensiones falsas de Google Notes e instaladores fraudulentos para comprometer transacciones de criptomonedas
Herramienta de detección	N/A
Activo involucrado:	Estaciones de trabajo Windows, navegadores Chromium (Google Chrome, Microsoft Edge, Brave, Opera), perfiles de usuario, extensiones del navegador, portapapeles del sistema operativo, billeteras de criptomonedas, plataformas de intercambio de activos digitales, equipos administrativos y dispositivos utilizados para operaciones financieras institucionales.
Tipo de alerta:	Alerta
Nivel de riesgo:	Critico

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre una campaña activa de distribución de malware denominada **Silent Swap**, identificada por investigadores de McAfee Labs, la cual emplea instaladores fraudulentos desarrollados en **.NET** y **Golang** para desplegar un malware tipo **Crypto Clipper** mediante una extensión maliciosa para navegadores Chromium que suplanta la funcionalidad de **Google Notes**.

La campaña se caracteriza por combinar múltiples técnicas de ingeniería social, manipulación de reputación digital y distribución de software malicioso utilizando sitios web fraudulentos, proyectos publicados en plataformas legítimas como GitHub y SourceForge, videos promocionales generados mediante inteligencia artificial, reseñas falsas y comentarios manipulados en VirusTotal con el propósito de generar confianza en las víctimas antes de la descarga del software malicioso.

Una vez instalado, el malware monitoriza permanentemente el portapapeles del sistema operativo y sustituye de manera automática las direcciones de billeteras de criptomonedas copiadas por el usuario por direcciones controladas por los atacantes, desviando las transferencias financieras sin generar indicios visibles durante la operación. Además, modifica los archivos **Preferences** y **Secure Preferences** de navegadores Chromium para forzar la instalación persistente de la extensión maliciosa.

Aunque la campaña tiene como objetivo principal el robo de activos digitales, las técnicas empleadas representan un riesgo significativo para organizaciones del sector salud debido a que evidencian capacidades avanzadas de compromiso de estaciones de trabajo, alteración de configuraciones de navegadores, persistencia mediante extensiones maliciosas, manipulación del sistema operativo y aprovechamiento de la confianza depositada por los usuarios en plataformas ampliamente utilizadas para distribución de software.

El propósito de esta alerta es que las entidades evalúen el impacto potencial que esta amenaza podría generar sobre:

- estaciones de trabajo administrativas;
- equipos utilizados para procesos financieros;
- navegadores corporativos basados en Chromium;
- equipos utilizados para administración de infraestructura tecnológica;
- sistemas empleados para operaciones con activos digitales;
- credenciales almacenadas en navegadores;
- plataformas de autenticación corporativa;
- infraestructura utilizada por personal administrativo;
- perfiles de usuario del sistema operativo;
- activos críticos conectados a estaciones comprometidas.

En el sector salud, la ejecución de software obtenido desde fuentes no verificadas continúa siendo uno de los principales vectores de compromiso inicial utilizados por actores maliciosos para establecer persistencia, comprometer credenciales institucionales y facilitar ataques posteriores contra infraestructura tecnológica crítica.

Descripción:



Investigadores de McAfee Labs identificaron una campaña activa denominada Silent Swap, diseñada para distribuir un malware especializado en el secuestro de transacciones de criptomonedas mediante la instalación de extensiones maliciosas para navegadores Chromium. La operación combina múltiples técnicas de ingeniería social con mecanismos avanzados de persistencia y manipulación de configuraciones internas del navegador, incrementando considerablemente la probabilidad de éxito frente a usuarios con conocimientos técnicos limitados o moderados.

A diferencia de campañas tradicionales que distribuyen malware mediante documentos ofimáticos o archivos comprimidos, Silent Swap utiliza un ecosistema completo de infraestructura fraudulenta destinado a construir credibilidad alrededor del software distribuido. Los atacantes emplean proyectos falsos alojados en GitHub y SourceForge, sitios web desarrollados sobre WordPress, artículos patrocinados en portales legítimos, videos tutoriales narrados mediante inteligencia artificial, reseñas falsas y comentarios coordinados publicados en VirusTotal para convencer a las víctimas de que las herramientas distribuidas son legítimas y ampliamente utilizadas.

El malware se distribuye principalmente mediante instaladores no firmados desarrollados en .NET y Go, diseñados para identificar automáticamente navegadores basados en Chromium presentes en el sistema comprometido. Una vez detectados los perfiles de usuario, el instalador finaliza los procesos activos del navegador para evitar bloqueos de archivos y procede a modificar directamente los archivos Secure Preferences y Preferences, responsables del almacenamiento de configuraciones internas y extensiones instaladas. Esta manipulación permite forzar la carga automática de una extensión maliciosa denominada “Google Notes”, sin requerir interacción adicional del usuario.

Desde una perspectiva técnica, el objetivo principal de la extensión consiste en monitorizar continuamente el contenido del portapapeles utilizando las interfaces de programación del sistema operativo y del navegador. Cuando detecta que el usuario copia una dirección correspondiente a una billetera de criptomonedas soportada, la reemplaza instantáneamente por otra perteneciente a la infraestructura controlada por los atacantes. Debido a que la

sustitución ocurre en milisegundos y mantiene el mismo formato sintáctico de la dirección original, la víctima normalmente no percibe la modificación antes de confirmar la transacción.

La campaña evidencia un cambio significativo en la evolución de las amenazas financieras dirigidas a usuarios de criptomonedas. En lugar de centrarse exclusivamente en el robo de credenciales o en la instalación de troyanos bancarios tradicionales, los atacantes explotan directamente el comportamiento habitual de los usuarios durante las operaciones de transferencia, reduciendo la necesidad de comprometer plataformas de intercambio o vulnerar mecanismos criptográficos de las billeteras digitales.

Desde el punto de vista defensivo, Silent Swap representa una amenaza relevante porque demuestra la convergencia entre técnicas avanzadas de ingeniería social, manipulación de reputación digital, persistencia mediante extensiones de navegador, modificación de configuraciones internas de Chromium y automatización del robo financiero mediante monitoreo permanente del portapapeles. La combinación de estos elementos incrementa considerablemente la superficie de ataque de organizaciones cuyos usuarios descargan herramientas desde fuentes no verificadas o mantienen privilegios administrativos sobre sus estaciones de trabajo.

Consecuencias de la explotación

La explotación exitosa de la campaña **Silent Swap** puede generar impactos significativos sobre la confidencialidad, integridad y disponibilidad de la información almacenada en las estaciones de trabajo comprometidas. Aunque el objetivo principal del malware consiste en el desvío fraudulento de transacciones de criptomonedas, los mecanismos utilizados para lograr dicho objetivo proporcionan al atacante capacidades adicionales que incrementan considerablemente la superficie de exposición de los equipos afectados.

Uno de los principales riesgos corresponde a la modificación no autorizada de la configuración interna de los navegadores basados en Chromium mediante la alteración directa de los archivos **Preferences** y **Secure Preferences**. Esta técnica permite instalar extensiones persistentes sin utilizar los mecanismos tradicionales de la Chrome Web Store, evadiendo parcialmente los controles implementados por el navegador y dificultando su identificación por parte del usuario.

La capacidad de monitorizar permanentemente el portapapeles constituye otro de los elementos más críticos de esta campaña. El malware inspecciona continuamente el contenido copiado por el usuario y aplica expresiones regulares y algoritmos de validación para identificar direcciones pertenecientes a múltiples redes blockchain. Una vez detectada una dirección compatible, ésta es sustituida de manera inmediata por otra controlada por los actores de amenaza, sin alterar el formato ni la longitud esperada de la cadena, reduciendo significativamente la probabilidad de detección durante el proceso de copia y pegado.

Adicionalmente, la manipulación de procesos del navegador durante la instalación permite modificar archivos de configuración que normalmente permanecen bloqueados cuando la aplicación está en ejecución. Esta capacidad evidencia que el malware posee un conocimiento detallado de la arquitectura interna de Chromium y de la forma en que administra perfiles de usuario, extensiones instaladas y políticas locales.

En escenarios donde los usuarios poseen privilegios administrativos sobre sus estaciones de trabajo, la ejecución del instalador fraudulento puede facilitar la incorporación de componentes adicionales de malware, la modificación de parámetros del sistema operativo, la instalación de nuevas tareas persistentes y la ampliación del compromiso hacia otros activos tecnológicos de la organización.

En un entorno hospitalario, una estación de trabajo inicialmente comprometida podría convertirse en el punto de partida para campañas posteriores orientadas al robo de credenciales institucionales, acceso no autorizado a aplicaciones corporativas, compromiso de cuentas privilegiadas, distribución de malware adicional o utilización del equipo como plataforma para ejecutar ataques contra infraestructura interna.

En escenarios de explotación exitosa, un atacante podría:

- instalar extensiones maliciosas persistentes en navegadores Chromium;
- modificar archivos **Preferences** y **Secure Preferences** de perfiles de usuario;
- monitorizar continuamente el contenido del portapapeles;
- sustituir direcciones de billeteras de criptomonedas por direcciones controladas por el atacante;
- obtener beneficios económicos mediante el desvío de transacciones financieras;
- mantener persistencia incluso después del reinicio del navegador;

- utilizar repositorios y plataformas legítimas para dificultar la atribución de la campaña;
- comprometer la confianza del usuario sobre herramientas aparentemente legítimas;
- preparar la instalación de componentes maliciosos adicionales;
- utilizar la estación comprometida como punto inicial para movimientos laterales dentro de la organización.

Aunque la finalidad inmediata de la campaña está orientada al robo de activos digitales, las técnicas observadas demuestran un elevado grado de sofisticación que podría adaptarse fácilmente para distribuir otras familias de malware, incluyendo troyanos de acceso remoto (RAT), infostealers, ransomware o herramientas utilizadas por grupos APT.

Modo de explotación del ataque

Fase 1 – Construcción de la infraestructura maliciosa y manipulación de la reputación digital

La campaña Silent Swap inicia con la construcción de una infraestructura diseñada para generar confianza y reducir la percepción de riesgo de las víctimas antes de la descarga del malware. A diferencia de campañas tradicionales basadas únicamente en correos electrónicos de phishing o sitios web fraudulentos, los actores de amenaza desarrollan un ecosistema completo de distribución compuesto por páginas web falsas, repositorios públicos, contenido multimedia generado mediante inteligencia artificial y publicaciones en plataformas ampliamente utilizadas por la comunidad tecnológica.

Como parte de esta estrategia, los atacantes crean proyectos aparentemente legítimos en plataformas como GitHub y SourceForge, donde publican instaladores que simulan corresponder a herramientas relacionadas con inteligencia artificial, productividad y gestión de criptomonedas. Paralelamente, registran dominios con nombres similares a proyectos legítimos, implementan sitios web desarrollados sobre gestores de contenido como WordPress y utilizan certificados TLS válidos para incrementar la confianza del usuario durante el proceso de descarga.

Con el propósito de fortalecer la credibilidad de la campaña, los operadores publican videos promocionales generados mediante inteligencia artificial, crean reseñas falsas en diferentes

plataformas y realizan publicaciones en foros especializados y sitios de análisis de malware, generando una falsa percepción de legitimidad alrededor del software distribuido.

Las actividades realizadas durante esta fase pueden incluir:

- registro de dominios similares a proyectos legítimos;
- creación de repositorios fraudulentos en plataformas públicas;
- publicación de documentación técnica falsa;
- generación de contenido audiovisual mediante inteligencia artificial;
- posicionamiento de sitios web mediante técnicas de optimización para motores de búsqueda (SEO);
- utilización de certificados digitales válidos;
- publicación de comentarios y reseñas falsas para incrementar la reputación del software.

El objetivo principal consiste en inducir a las víctimas a descargar voluntariamente el instalador malicioso desde fuentes aparentemente confiables, evitando el uso de vectores tradicionales de distribución que suelen ser detectados con mayor facilidad por soluciones de seguridad.

Fase 2 – Descarga y ejecución del instalador fraudulento

Una vez la víctima accede al sitio web fraudulento o al repositorio manipulado, descarga un instalador desarrollado principalmente en .NET o Golang, diseñado para simular la instalación de una aplicación legítima relacionada con herramientas de inteligencia artificial o productividad.

Durante la ejecución inicial, el instalador realiza múltiples validaciones sobre el sistema operativo con el propósito de identificar el entorno donde será desplegado el malware. Entre las acciones observadas se encuentra la enumeración de navegadores basados en Chromium instalados en el equipo, la identificación de perfiles de usuario, la validación de privilegios disponibles y la localización de las rutas donde se almacenan las configuraciones internas del navegador.

A diferencia de otros programas maliciosos que descargan componentes adicionales desde servidores externos, algunas variantes de Silent Swap incorporan directamente los archivos requeridos para la instalación de la extensión maliciosa, reduciendo la actividad de red durante las primeras etapas de la infección y dificultando la detección basada en tráfico.

Las actividades realizadas durante esta fase pueden incluir:

- ejecución del instalador fraudulento;
- identificación del sistema operativo;
- detección de navegadores Chromium instalados;
- enumeración de perfiles de usuario;
- validación de permisos disponibles;
- extracción de componentes internos;
- preparación del entorno para la instalación.

El objetivo consiste en obtener la información necesaria para desplegar el componente malicioso dentro del navegador sin generar alertas visibles para el usuario.

Fase 3 – Modificación del navegador y establecimiento de persistencia

Después de identificar los perfiles de usuario existentes, el instalador procede a finalizar temporalmente los procesos activos del navegador con el propósito de acceder a los archivos de configuración que normalmente permanecen bloqueados mientras la aplicación se encuentra en ejecución.

Posteriormente, modifica directamente los archivos Preferences y Secure Preferences, utilizados por Chromium para almacenar información relacionada con configuraciones internas, políticas locales y extensiones instaladas. Mediante esta técnica, el malware incorpora una extensión maliciosa que se presenta como una herramienta denominada Google Notes, evitando utilizar los mecanismos oficiales de distribución de extensiones.

La modificación directa de estos archivos constituye una técnica de persistencia particularmente efectiva, ya que la extensión permanece disponible cada vez que el usuario inicia el navegador, incluso después de reiniciar el sistema operativo.

Las actividades realizadas durante esta fase pueden incluir:

- finalización de procesos activos del navegador;
- acceso a los perfiles de usuario;
- modificación de los archivos Preferences;
- modificación de los archivos Secure Preferences;
- incorporación de la extensión maliciosa;
- actualización de configuraciones internas del navegador;
- establecimiento de persistencia mediante el perfil del usuario.

El objetivo consiste en garantizar que el malware permanezca operativo durante futuras sesiones sin requerir nuevas acciones por parte de la víctima.

Fase 4 – Activación de la extensión maliciosa y monitoreo del portapapeles

Una vez el navegador vuelve a ejecutarse, la extensión maliciosa es cargada automáticamente como parte de las configuraciones persistentes del perfil comprometido. Desde este momento, inicia un proceso continuo de supervisión del contenido almacenado en el portapapeles del sistema operativo.

La extensión implementa mecanismos que permiten inspeccionar cada elemento copiado por el usuario y aplicar expresiones regulares junto con algoritmos de validación para determinar si el contenido corresponde a una dirección válida de una billetera de criptomonedas perteneciente a redes como Bitcoin, Ethereum, TRON, Litecoin u otros activos digitales soportados por la campaña.

Este proceso ocurre de forma transparente para el usuario y no requiere interacción adicional una vez completada la instalación.

Las actividades realizadas durante esta fase pueden incluir:

- carga automática de la extensión maliciosa;
- inicialización de procesos de monitoreo;
- supervisión continua del portapapeles;

- identificación de direcciones de criptomonedas;
- validación del formato de las direcciones detectadas;
- verificación del tipo de blockchain;
- preparación del proceso de sustitución.

El objetivo consiste en identificar oportunidades para modificar transacciones financieras antes de que sean enviadas por la víctima.

Fase 5 – Sustitución automática de direcciones de billeteras

Cuando la extensión identifica que el usuario ha copiado una dirección perteneciente a una billetera de criptomonedas, ejecuta de forma inmediata un proceso de sustitución mediante el cual reemplaza el contenido original del portapapeles por otra dirección previamente configurada por los operadores de la campaña.

La modificación ocurre en milisegundos y mantiene la longitud, estructura y formato esperado para cada tipo de blockchain, dificultando que la víctima identifique visualmente el cambio antes de confirmar la transferencia.

Algunas variantes incorporan múltiples direcciones de destino dependiendo del tipo de criptomoneda detectada, permitiendo que los atacantes administren diferentes billeteras para cada activo digital comprometido.

Las actividades realizadas durante esta fase pueden incluir:

- detección de una dirección válida de criptomoneda;
- identificación del tipo de blockchain;
- selección de la dirección controlada por el atacante;
- reemplazo del contenido del portapapeles;
- validación del formato de la nueva dirección;
- mantenimiento de la estructura sintáctica original;
- preparación para el desvío de la transacción.

El objetivo consiste en redirigir silenciosamente los activos digitales hacia billeteras controladas por los actores de amenaza sin comprometer directamente la plataforma de intercambio utilizada por la víctima.

Fase 6 – Evasión de mecanismos de seguridad y ocultamiento de la actividad maliciosa

Durante toda la operación, Silent Swap implementa diversas técnicas destinadas a reducir la probabilidad de detección tanto por parte del usuario como de las soluciones tradicionales de seguridad.

Entre estas técnicas se encuentra la utilización de nombres de extensiones aparentemente legítimos, la reducción del tráfico de red durante la instalación, el empleo de plataformas ampliamente reconocidas para la distribución inicial del malware y la ejecución de actividades que imitan el comportamiento normal de aplicaciones legítimas.

La ausencia de actividades ruidosas, como el cifrado de archivos o la ejecución masiva de comandos administrativos, permite que el malware permanezca activo durante períodos prolongados sin despertar sospechas.

Las actividades realizadas durante esta fase pueden incluir:

- utilización de nombres legítimos para la extensión instalada;
- reducción de conexiones hacia infraestructura externa;
- ejecución de procesos compatibles con el comportamiento esperado del navegador;
- utilización de plataformas públicas para distribuir el malware;
- limitación de actividades visibles para el usuario;
- permanencia silenciosa dentro del navegador;
- ocultamiento de la manipulación del portapapeles.

El objetivo consiste en prolongar la permanencia del malware dentro del equipo comprometido maximizando el número de transacciones fraudulentas antes de ser descubierto.

Fase 7 – Monetización y posible expansión del compromiso

Una vez que las transacciones son redirigidas exitosamente hacia las billeteras controladas por los atacantes, la campaña obtiene el beneficio económico esperado sin necesidad de comprometer directamente los servicios financieros utilizados por la víctima.

Sin embargo, el acceso obtenido sobre la estación de trabajo y el conocimiento adquirido sobre el entorno tecnológico permiten que la infraestructura utilizada por Silent Swap pueda evolucionar hacia campañas más complejas. Una estación inicialmente comprometida podría convertirse en un punto de partida para la distribución de malware adicional, el robo de credenciales corporativas, la instalación de herramientas de acceso remoto o la ejecución de ataques dirigidos contra otros activos tecnológicos de la organización.

En organizaciones del sector salud, donde las estaciones de trabajo administrativas suelen mantener acceso a sistemas clínicos, aplicaciones financieras, plataformas de gestión documental y servicios de autenticación corporativa, este escenario incrementa considerablemente el riesgo de compromiso de información institucional y de afectación de procesos críticos.

Las actividades realizadas durante esta fase pueden incluir:

- desvío de activos digitales hacia billeteras controladas por el atacante;
- monitoreo continuo de nuevas transacciones;
- permanencia de la extensión maliciosa en el navegador;
- recopilación de información sobre el entorno comprometido;
- preparación para la instalación de componentes adicionales;
- utilización del equipo como punto inicial para ataques posteriores;
- ampliación del compromiso hacia otros activos tecnológicos de la organización.

El objetivo consiste en maximizar el beneficio económico obtenido mediante el fraude y conservar una posición privilegiada dentro del entorno comprometido que permita desarrollar futuras operaciones maliciosas con un impacto potencialmente mayor.

Vulnerabilidades asociadas



Instalación de software desde fuentes no confiables

- **Descripción:** La campaña Silent Swap distribuye instaladores fraudulentos que suplantan aplicaciones legítimas mediante sitios web maliciosos, anuncios patrocinados (malvertising) y resultados manipulados en motores de búsqueda. El usuario ejecuta voluntariamente el instalador, permitiendo la ejecución de código malicioso sin necesidad de explotar vulnerabilidades del sistema operativo. Posteriormente, el malware instala componentes adicionales, establece mecanismos de persistencia y despliega el Crypto Clipper encargado de manipular las transacciones con criptomonedas.
- **Impacto:** La ejecución de software procedente de fuentes no confiables puede permitir la instalación de malware, el compromiso del equipo, la ejecución de código arbitrario, el robo de información, la descarga de cargas maliciosas adicionales y la utilización del dispositivo como punto de acceso para nuevos ataques dentro de la infraestructura tecnológica.
- **Referencias técnicas:**
 - MITRE ATT&CK: T1189 – Drive-by Compromise; T1204.002 – User Execution: Malicious File.
 - CWE: CWE-494 – Download of Code Without Integrity Check; CWE-829 – Inclusion of Functionality from Untrusted Control Sphere.

Instalación de extensiones de navegador no verificadas

- **Descripción:** Los actores de amenaza distribuyen extensiones falsas que imitan aplicaciones legítimas para navegadores basados en Chromium. Estas extensiones incorporan código JavaScript capaz de ejecutarse de forma persistente, interactuar con las API del navegador y acceder a diferentes recursos según los permisos otorgados durante la instalación.

- **Impacto:** Una extensión maliciosa puede acceder a información sensible del navegador, modificar contenido web, interceptar credenciales, manipular sesiones activas y ejecutar acciones persistentes que comprometan la confidencialidad e integridad de la información procesada por el usuario.
 - **Referencias técnicas:**
 - MITRE ATT&CK: T1036 – Masquerading; T1176 – Browser Extensions.
 - CWE: CWE-1357 – Reliance on Insufficiently Trustworthy Component Identification.
-

Concesión excesiva de permisos a extensiones del navegador

- **Descripción:** Las extensiones utilizadas en la campaña solicitan permisos avanzados como acceso al portapapeles, lectura y modificación de los datos de los sitios web visitados, ejecución en segundo plano y acceso al almacenamiento local del navegador. La concesión de estos privilegios permite al malware operar con amplias capacidades sin requerir mecanismos adicionales de explotación.
 - **Impacto:** El abuso de permisos privilegiados facilita la manipulación del contenido mostrado al usuario, el acceso a información confidencial, la alteración de direcciones de billeteras de criptomonedas y la ejecución de actividades maliciosas con un bajo nivel de visibilidad para las herramientas tradicionales de seguridad.
 - **Referencias técnicas:**
 - MITRE ATT&CK: T1115 – Clipboard Data; T1056 – Input Capture.
 - CWE: CWE-266 – Incorrect Privilege Assignment.
-

Ausencia de controles de lista blanca de aplicaciones (Application Allowlisting)

- **Descripción:** La inexistencia de políticas que restrinjan la instalación y ejecución de software autorizado permite que usuarios con privilegios suficientes incorporen aplicaciones y extensiones sin validación previa por parte del área de tecnología o seguridad de la información.

- **Impacto:** La falta de mecanismos de control sobre el software autorizado incrementa la superficie de ataque, facilita la ejecución de código malicioso, dificulta la administración segura de los equipos y aumenta el riesgo de compromiso de la infraestructura tecnológica.
 - **Referencias técnicas:**
 - MITRE ATT&CK: T1204 – User Execution.
 - CWE: CWE-693 – Protection Mechanism Failure.
-

Monitoreo insuficiente del portapapeles del sistema

- **Descripción:** El componente Crypto Clipper supervisa continuamente el contenido del portapapeles del sistema operativo para identificar patrones correspondientes a direcciones de billeteras de criptomonedas. Cuando detecta una coincidencia, sustituye automáticamente la dirección original por otra controlada por el atacante antes de que el usuario confirme la transacción.
 - **Impacto:** Esta técnica compromete la integridad de las transacciones financieras, permitiendo el desvío de activos digitales hacia billeteras pertenecientes a los actores maliciosos sin generar alertas visibles para el usuario.
 - **Referencias técnicas:**
 - MITRE ATT&CK: T1115 – Clipboard Data.
 - CWE: CWE-345 – Insufficient Verification of Data Authenticity.
-

Capacidades limitadas de detección basada en comportamiento

- **Descripción:** Silent Swap utiliza componentes legítimos del sistema operativo y del navegador para ejecutar parte de sus actividades, reduciendo la probabilidad de ser detectado por soluciones tradicionales de antivirus basadas exclusivamente en firmas. Adicionalmente, puede emplear técnicas de evasión para disminuir la generación de indicadores de compromiso (IoC).

- **Impacto:** La limitada capacidad para detectar actividades anómalas favorece la permanencia del malware dentro del sistema (dwell time), incrementa el riesgo de exfiltración de información, dificulta las labores de respuesta a incidentes y aumenta la posibilidad de propagación o instalación de cargas maliciosas adicionales.
- **Referencias técnicas:**
 - MITRE ATT&CK: T1027 – Obfuscated/Compressed Files and Information; T1218 – System Binary Proxy Execution.
 - CWE: CWE-693 – Protection Mechanism Failure.

Recomendaciones

Restringir la instalación de software y extensiones

Implementar políticas de control de aplicaciones (Application Allowlisting) que permitan únicamente la instalación y ejecución de software previamente autorizado por la organización. Asimismo, restringir la instalación de extensiones de navegador únicamente a aquellas aprobadas por el área de tecnología o seguridad de la información mediante mecanismos de administración centralizada.

Descargar software únicamente desde fuentes oficiales

Establecer políticas institucionales que prohíban la descarga de aplicaciones, instaladores y extensiones desde sitios web de terceros, anuncios patrocinados o enlaces recibidos por correo electrónico, mensajería instantánea o redes sociales. Antes de instalar cualquier software, verificar que provenga del sitio oficial del fabricante y validar, cuando sea posible, su firma digital e integridad.

Fortalecer la protección de los endpoints

Mantener implementadas soluciones de protección de endpoints (EPP/EDR/XDR) con capacidades de análisis de comportamiento, detección basada en inteligencia de amenazas y

respuesta automatizada. Configurar dichas herramientas para identificar actividades relacionadas con la modificación del portapapeles, la ejecución de procesos anómalos, la instalación de extensiones no autorizadas y la creación de mecanismos de persistencia.

Aplicar el principio de mínimo privilegio

Restringir los privilegios administrativos de los usuarios finales para impedir la instalación de software y extensiones sin autorización. Utilizar cuentas con privilegios diferenciados para tareas administrativas y aplicar controles de elevación de privilegios cuando sea estrictamente necesario.

Implementar controles sobre navegadores corporativos

Administrar de forma centralizada los navegadores utilizados dentro de la organización mediante políticas que permitan controlar las extensiones autorizadas, deshabilitar la instalación manual de complementos, restringir permisos de alto riesgo y mantener actualizadas las configuraciones de seguridad recomendadas por los fabricantes.

Supervisar el comportamiento del portapapeles y de los procesos

Incorporar reglas de monitoreo en las plataformas EDR, SIEM o XDR para detectar procesos que accedan de forma continua al portapapeles del sistema, modifiquen su contenido o presenten comportamientos compatibles con malware tipo Crypto Clipper. Correlacionar estos eventos con la instalación reciente de aplicaciones o extensiones del navegador para facilitar la identificación temprana de actividades maliciosas.

Fortalecer los controles de navegación y filtrado web

Implementar soluciones de filtrado DNS, Secure Web Gateway (SWG) o plataformas SASE que permitan bloquear dominios maliciosos, sitios de phishing, repositorios utilizados para distribuir malware y páginas identificadas como origen de campañas de malvertising.

Complementar estas medidas con listas de reputación de dominios e indicadores de compromiso (IoC) actualizados.

Mantener actualizados los indicadores de compromiso (IoC)

Incorporar de manera permanente los indicadores de compromiso publicados por fabricantes, CERT, CSIRT y proveedores de inteligencia de amenazas en las plataformas de monitoreo y detección de la organización. Esto permitirá identificar de forma temprana archivos, dominios, direcciones IP, hashes y comportamientos asociados con la campaña Silent Swap.

Capacitar al personal sobre ingeniería social

Desarrollar campañas periódicas de sensibilización dirigidas a funcionarios, personal asistencial, contratistas y terceros, enfocadas en la identificación de sitios web fraudulentos, anuncios patrocinados maliciosos, instaladores falsificados y extensiones de navegador no confiables. Reforzar la importancia de verificar cuidadosamente cualquier dirección de billetera de criptomonedas antes de confirmar una transacción.

Establecer procedimientos de respuesta ante incidentes

Definir procedimientos específicos para la atención de incidentes relacionados con malware distribuido mediante extensiones de navegador o instaladores fraudulentos. En caso de sospecha de compromiso, aislar inmediatamente el equipo afectado de la red, preservar las evidencias digitales, realizar un análisis forense, eliminar los componentes maliciosos identificados, restablecer las configuraciones de seguridad y revisar otros equipos que hayan podido verse afectados por la misma campaña.

Verificar la integridad de las transacciones con criptomonedas

En los casos en que la organización utilice activos digitales o interactúe con servicios basados en criptomonedas, implementar procedimientos de doble verificación de las direcciones de

destino antes de confirmar cualquier transferencia. Cuando sea posible, utilizar listas de direcciones confiables (whitelists), mecanismos de validación fuera de banda y procesos de doble aprobación para minimizar el riesgo de manipulación del portapapeles.

Realizar actividades de búsqueda proactiva (Threat Hunting)

Ejecutar actividades periódicas de Threat Hunting orientadas a identificar indicadores asociados con la campaña Silent Swap, incluyendo la presencia de extensiones no autorizadas, modificaciones persistentes en los navegadores, procesos que interactúan con el portapapeles, conexiones hacia dominios de baja reputación y mecanismos de persistencia establecidos en los equipos comprometidos.

La implementación conjunta de estas recomendaciones fortalece la capacidad de las organizaciones para prevenir, detectar y responder oportunamente frente a campañas como Silent Swap, reduciendo la probabilidad de compromiso de los equipos, la pérdida de información y el impacto derivado de la manipulación de transacciones financieras mediante malware tipo Crypto Clipper.

Conclusiones

La campaña Silent Swap evidencia la evolución de las amenazas dirigidas a los usuarios finales, combinando técnicas de ingeniería social, distribución de software fraudulento y abuso de funcionalidades legítimas de los navegadores para comprometer los equipos sin necesidad de explotar vulnerabilidades conocidas. Este enfoque incrementa la probabilidad de éxito de los ataques al apoyarse principalmente en errores de configuración, debilidades en los controles de seguridad y la interacción del usuario con contenido aparentemente legítimo.

Aunque el objetivo principal de la campaña es la manipulación de direcciones de billeteras de criptomonedas mediante malware tipo Crypto Clipper, los mecanismos empleados para lograr la infección pueden representar un riesgo significativo para las organizaciones del sector salud. La instalación de software o extensiones maliciosas puede facilitar la ejecución de código arbitrario, el robo de credenciales, la exfiltración de información sensible, el establecimiento de

mecanismos de persistencia y la descarga de cargas maliciosas adicionales que amplíen el alcance del compromiso.

Las entidades del sector salud deben considerar este tipo de campañas como una amenaza relevante, especialmente debido a la amplia utilización de navegadores web, servicios en la nube y aplicaciones de terceros en los procesos administrativos y asistenciales. La ausencia de controles sobre la instalación de software, la administración de extensiones de navegador y la supervisión de los equipos finales puede incrementar significativamente la superficie de ataque y favorecer la materialización de incidentes de ciberseguridad con impacto operacional.

La mitigación de esta amenaza requiere un enfoque de defensa en profundidad que combine controles técnicos, administrativos y de concienciación. La implementación de políticas de control de aplicaciones, la administración centralizada de navegadores, el uso de soluciones EDR/XDR, el monitoreo continuo mediante plataformas SIEM, la incorporación de inteligencia de amenazas y la capacitación permanente del personal constituyen medidas fundamentales para reducir la probabilidad de compromiso y fortalecer la capacidad de detección y respuesta frente a campañas similares.

El CSIRT Salud recomienda a las organizaciones mantenerse atentas a la publicación de nuevos indicadores de compromiso (IoC), tácticas, técnicas y procedimientos (TTP) asociados con esta campaña, actualizar periódicamente sus mecanismos de detección y respuesta, e integrar la información proveniente de fuentes confiables de inteligencia de amenazas en sus procesos de monitoreo y gestión de incidentes. La adopción de un enfoque preventivo y de mejora continua permitirá fortalecer la postura de ciberseguridad institucional y disminuir el impacto potencial de amenazas emergentes como Silent Swap.

Fuentes:

- <https://www.mcafee.com/blogs/?p=231741>
- <https://thehackernews.com/2026/06/silent-swap-crypto-clipper-uses-fake.html>
- <https://attack.mitre.org/>
- <https://cwe.mitre.org/>
- <https://chromeenterprise.google/policies/>
- <https://developer.chrome.com/docs/extensions/>

- <https://cheatsheetseries.owasp.org/>
- <https://www.cisa.gov/>
- <https://csrc.nist.gov/>
- <https://www.microsoft.com/en-us/security/blog/2026/06/17/crypto-clipper-uses-tor-worm-like-propagation-for-persistence-control/>

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) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.