Los ciberdelincuentes están engañando a usuarios incautos con versiones gratuitas o pirateadas de software comercial para distribuir un cargador de malware llamado Hijack Loader, que luego implementa un ladrón de información conocido como Vidar Stealer.

> *«Los atacantes lograron engañar a los usuarios para que descargaran archivos comprimidos protegidos con contraseña que contenían copias troyanizadas de una aplicación de Cisco Webex Meetings (ptService.exe)»,* explicó Ale Houspanossian, investigador de seguridad de Trellix, en un análisis publicado el lunes.
>
> *«Cuando las víctimas desprevenidas extraían y ejecutaban un archivo binario 'Setup.exe', la aplicación de Cisco Webex Meetings cargaba discretamente un cargador de malware sigiloso, lo que conducía a la ejecución de un módulo de robo de información.»*

El punto de partida es un archivo comprimido RAR que contiene un ejecutable llamado «Setup.exe», que en realidad es una copia del módulo ptService de Cisco Webex Meetings.

Lo que hace que esta campaña sea destacable es el uso de técnicas de carga lateral de DLL para lanzar subrepticiamente Hijack Loader (también conocido como DOILoader o IDAT Loader), que luego actúa como un conducto para descargar Vidar Stealer mediante un script de AutoIt.

> *«El malware utiliza una técnica conocida para eludir el Control de Cuentas de Usuario (UAC) y explotar la interfaz COM CMSTPLUA para la escalada de privilegios. Una vez lograda la escalada de privilegios, el malware se añadía a la lista de exclusión de Windows Defender para evadir las defensas»,* indicó Houspanossian.

La cadena de ataque, además de usar Vidar Stealer para sustraer credenciales sensibles de

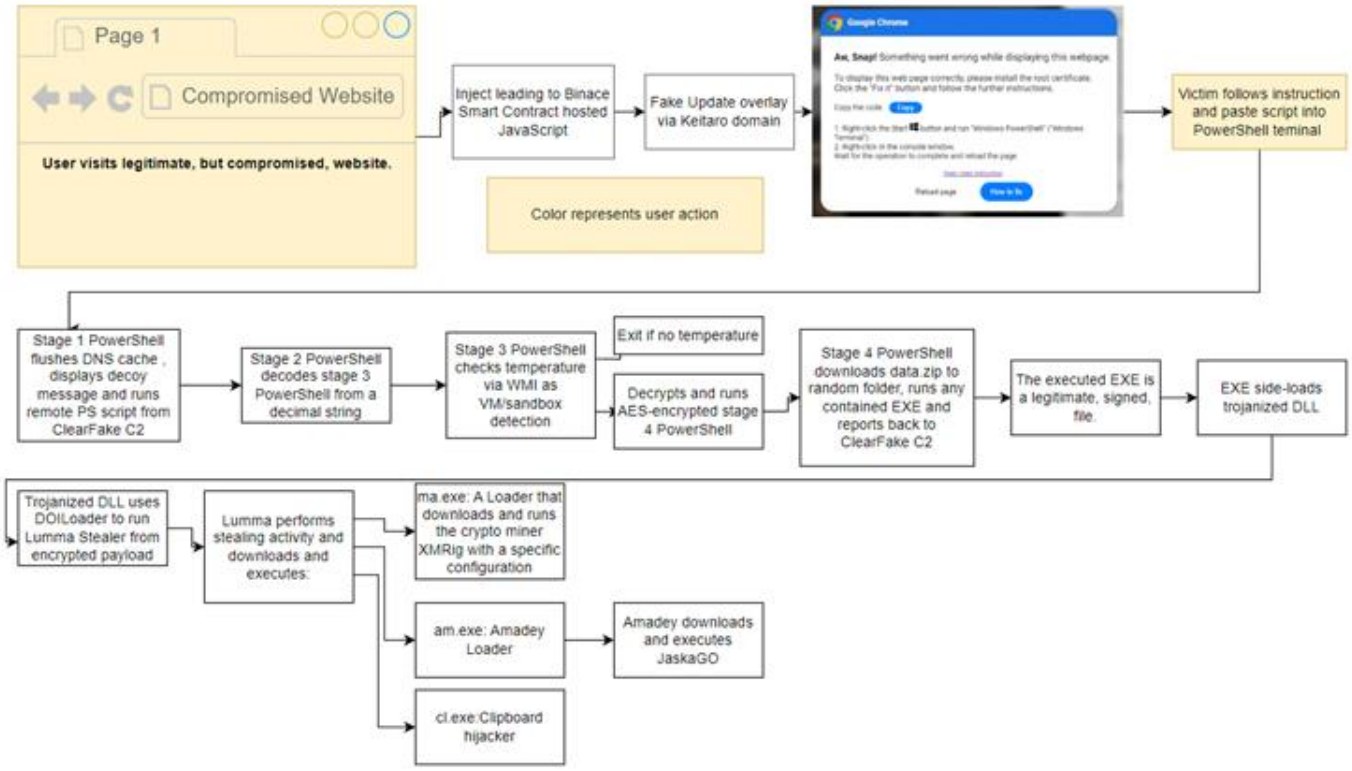
navegadores web, emplea cargas adicionales para desplegar un minero de criptomonedas en el sistema comprometido.

Esta revelación sigue a un aumento en las campañas de ClearFake, que atraen a los visitantes de sitios web a ejecutar manualmente un script de PowerShell para resolver un supuesto problema con la visualización de páginas web, una técnica previamente divulgada por ReliaQuest a finales del mes pasado.

El script de PowerShell luego sirve como plataforma de lanzamiento para Hijack Loader, que finalmente entrega el malware Lumma Stealer. Este ladrón de información también está diseñado para descargar tres cargas adicionales, incluyendo Amadey Loader, un descargador que lanza el minero XMRig, y un malware clipper para redirigir transacciones de criptomonedas a billeteras controladas por los atacantes.

> *«Se observó que Amadey descargaba otras cargas, como un malware basado en Go que se cree que es JaskaGO,»* afirmaron los investigadores de Proofpoint Tommy Madjar, Dusty Miller y Selena Larson.

La firma de seguridad empresarial también detectó a mediados de abril de 2024 otro grupo de actividades denominado ClickFix, que utilizaba cebos de actualizaciones defectuosas de navegadores para atraer a los visitantes de sitios web comprometidos y propagar Vidar Stealer usando un mecanismo similar que implicaba copiar y ejecutar código PowerShell.



Otro grupo de ciberdelincuentes que ha adoptado la misma estrategia de ingeniería social en sus campañas de correo no deseado (malspam) es TA571, que se ha visto enviando correos electrónicos con archivos HTML adjuntos. Al abrirlos, aparece un mensaje de error que dice: *«La extensión 'Word Online' no está instalada en su navegador».*

En el mensaje también hay dos opciones disponibles: «Cómo solucionarlo» y «Reparación automática». Si la víctima elige la primera opción, se copia un comando PowerShell codificado en Base64 al portapapeles de la computadora, seguido de instrucciones para abrir una terminal PowerShell, hacer clic derecho en la ventana de la consola para pegar el contenido del portapapeles y ejecutar un código que lanza un instalador MSI o un Script Básico de Visual (VBS).

Del mismo modo, quienes optan por la «Reparación automática» ven archivos alojados en WebDAV llamados «fix.msi» o «fix.vbs» en el Explorador de Windows, aprovechando el

manipulador de protocolo «search-ms:».

Independientemente de la opción elegida, la ejecución del archivo MSI resulta en la instalación de Matanbuchus, mientras que la ejecución del archivo VBS conduce al despliegue de DarkGate.

Otras versiones de la campaña también han llevado a la distribución de NetSupport RAT, lo que destaca los intentos de modificar y actualizar los señuelos y cadenas de ataque, a pesar de requerir una interacción significativa por parte del usuario para tener éxito.

> *«El uso legítimo y las múltiples formas de almacenar el código malicioso, y el hecho de que la víctima ejecute manualmente el código malicioso sin conexión directa a un archivo, hacen que la detección de este tipo de amenazas sea difícil»*, comentó Proofpoint.
>
> *«Dado que el software antivirus y los EDR pueden tener dificultades para inspeccionar el contenido del portapapeles, la detección y el bloqueo deben implementarse antes de que se presente el HTML/sitio malicioso a la víctima».*

Este desarrollo también coincide con la revelación de eSentire sobre una campaña de malware que utiliza sitios web similares a Indeed[.]com para distribuir el malware de robo de información SolarMarker mediante un documento señuelo que supuestamente ofrece ideas para fortalecer equipos.

> *«SolarMarker emplea técnicas de envenenamiento de optimización de motores de búsqueda (SEO) para manipular resultados de búsqueda y aumentar la visibilidad de enlaces engañosos»*, señaló la empresa canadiense de ciberseguridad.

> *«El uso de tácticas SEO por parte de los atacantes para dirigir a usuarios a sitios maliciosos subraya la importancia de ser cauteloso al hacer clic en resultados de búsqueda, incluso si parecen legítimos».*