Se ha observado que una extensión maliciosa para los navegadores web basados en Chromium se distribuye por medio de un antiguo ladrón de información de Windows llamado ViperSoftX.

La empresa de seguridad cibernética con sede en República Checa, Avast, apodó el plugin de navegador como VenomSoftX, debido a sus características independientes que le permiten acceder a visitas a sitios web, robar credenciales y datos del portapapeles e incluso, intercambiar direcciones de criptomonedas a través de un ataque de adversario en el medio (AiTM).

ViperSoftX, que salio a la luz por primera vez en febrero de 2020, fue caracterizado por Fortinet como un troyano de acceso remoto basado en JavaScript y un ladrón de criptomonedas. El analista de amenazas de Sophos, Colin Cowie, documentó a inicios de este año el uso que hace el malware de una extensión del navegador para avanzar en sus objetivos de recopilación de información.

> *«Este ladrón de múltiples etapas exhibe interesantes capacidades de ocultación, ocultas como pequeños scripts de PowerShell en una sola línea en medio de grandes archivos de registro que de otra forma, parecen inocentes, entre otros»,* dijo el investigador de Avast, Jan Rubín.

> *«ViperSoftX se enfoca en robar criptomonedas, intercambiar portapapeles, tomar huellas dactilares de la máquina infectada, así como descargar y ejecutar cargas útiles adicionales arbitrarias o ejecutar comandos».*

El vector de distribución utilizado para propagar ViperSoftX generalmente se realiza mediante software hackeado para Adobe Illustrator y Microsoft Office, que se alojan en sitios de intercambio de archivos.

El archivo ejecutable descargado viene con una versión limpia del software descifrado junto con archivos adicionales que configuran la persistencia en el host y albergan el script ViperSoftX PowerShell.

Las variantes más nuevas del malware también pueden cargar el plugin VenomSoftX, que se recupera de un servidor remoto, en navegadores basados en Chromium como Google Chrome, Microsoft Edge, Opera, Brave y Vivaldi.

Esto se logra buscando archivos LNK para las aplicaciones del navegador y modificando los accesos directos con un interruptor de línea de comando «–load-extension» que apunta a la ruta donde se almacena la extensión desempaquetada.

> *«La extensión intenta disfrazarse de extensiones de navegador conocidas y comunes como Google Sheets. En realidad, VenomSoftX es otro ladrón de información implementado en la víctima desprevenida con permisos de acceso completo a cada sitio web que el usuario visita desde el navegador infectado»,* explicó Rubín.

Cabe mencionar que la táctica –load-extension también ha sido usada por otro ladrón de información basado en navegador, denominado ChromeLoader (también conocido como Choziosi Loader o ChromeBack).

VenomSoftX, como ViperSoftX, también está orquestado para robar criptomonedas de sus víctimas. Pero a diferencia de este último, que funciona como un recortador para redirigir las transferencias de fondos a una billetera controlada por un atacante, VenomSoftX manipula las solicitudes de API a los intercambios de cifrado para drenar los activos digitales.

Los servicios a los que se dirige la extensión incluyen Blockchain.com, Binance, Coinbase,

Gate.io y Kucoin.

El desarrollo marca un nuevo nivel de escalada al intercambio de portapapeles tradicional, al mismo tiempo que no levanta ninguna sospecha inmediata ya que la dirección de la billetera se reemplaza a un nivel mucho más fundamental.

Avast dijo que ha detectado y bloqueado más de 93,000 infecciones desde principios de 2022, con la mayoría de los usuarios afectados ubicados en India, Estados Unidos, Italia, Brasil, Reino Unido, Canadá, Francia, Pakistán y Sudáfrica.

Un análisis de las direcciones de billetera codificadas en las muestras revela que la operación ha generado para sus autores una suma total de aproximadamente $130,421 dólares al 8 de noviembre de 2022, en varias criptomonedas. Desde entonces, la ganancia monetaria colectiva se ha reducido a $104,500.

> *«Debido a que las transacciones en blockchains/libros mayores son inherentemente irreversibles, cuando el usuario verifica el historial de transacciones de pagos después, ya es demasiado tarde»,* dijo Rubín.