Investigadores en ciberseguridad han identificado una campaña activa que utiliza extensiones maliciosas para navegadores con el propósito de robar criptomonedas mediante la sustitución encubierta de direcciones de billeteras digitales cuando los usuarios realizan una transacción.

Esta operación de crypto clipping ha sido denominada Silent Swap por McAfee Labs.

«La campaña se distribuye mediante instaladores sin firma digital —identificados en versiones desarrolladas en .NET y Golang— que despliegan una extensión maliciosa para navegadores basados en Chromium, haciéndose pasar por una herramienta legítima denominada «Google Notes»», indicó la compañía de ciberseguridad en un informe técnico.

El instalador sin firma basado en .NET, denominado BaseZipInstaller, está diseñado para descargar un archivo comprimido en formato ZIP que contiene los componentes necesarios para la extensión maliciosa. Posteriormente, analiza el sistema en busca de navegadores basados en Chromium y, por cada perfil detectado, finaliza forzosamente el proceso del navegador antes de insertar la extensión mediante la modificación de los archivos Secure Preferences y Preferences.

El objetivo principal de la extensión consiste en actuar como un clipper, interceptando las direcciones de billeteras de criptomonedas copiadas al portapapeles del sistema para reemplazarlas por otras controladas por los atacantes, redirigiendo así los fondos hacia sus propias cuentas. Para ello, la falsa extensión Google Notes solicita permisos para acceder al portapapeles, a todas las URL visitadas y al historial de navegación.

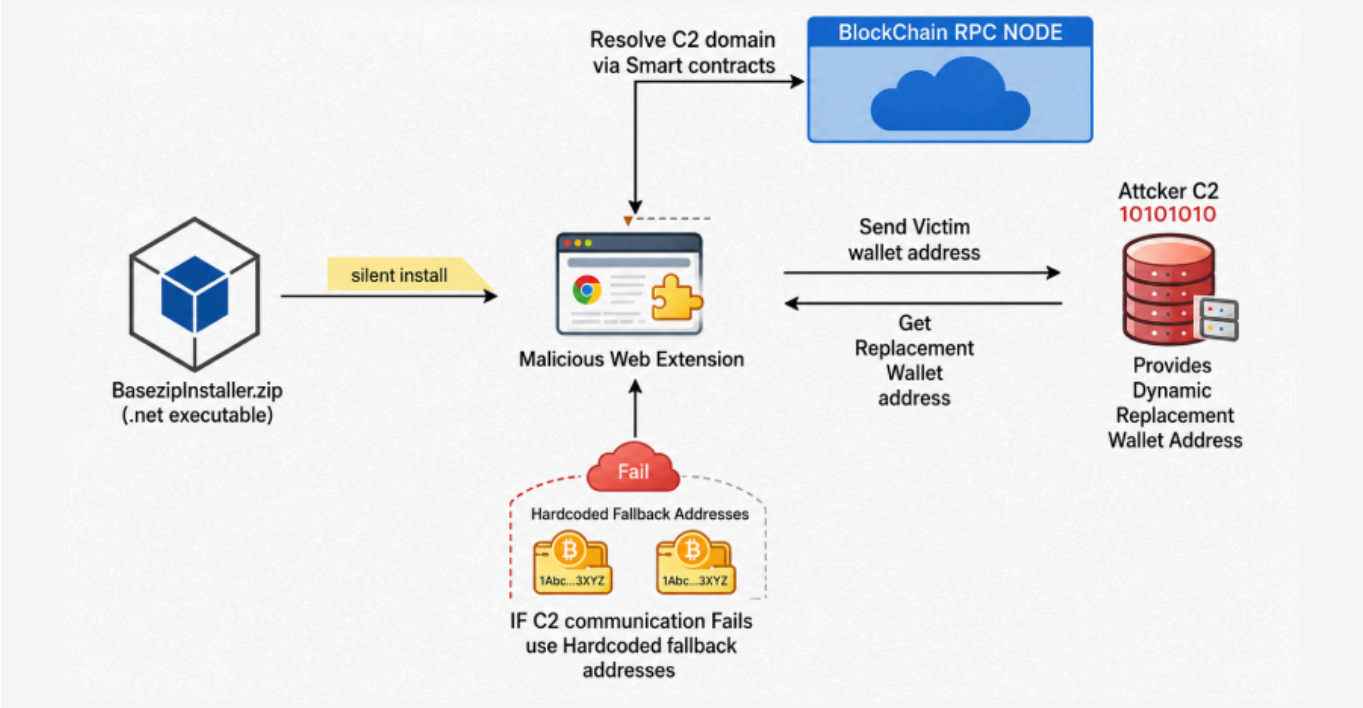
Dado que la mayoría de las transacciones realizadas sobre cadenas de bloques son irreversibles, la sustitución de una dirección puede provocar pérdidas económicas permanentes. Según McAfee Labs, esta campaña presenta similitudes con una operación anterior conocida como CountLoader, utilizada para distribuir otro malware de tipo crypto clipper, lo que sugiere que ambas actividades podrían estar siendo dirigidas por el mismo actor de amenazas.

Uno de los elementos que distingue a Silent Swap es la utilización de una técnica denominada EtherHiding, la cual emplea la cadena de bloques como un mecanismo de dead drop resolver para recuperar la información del servidor activo de comando y control (C2). Gracias a este enfoque, el atacante únicamente necesita modificar el valor de un contrato inteligente para apuntar hacia un nuevo dominio, evitando redistribuir el malware.

Otro aspecto relevante de la campaña es la instalación encubierta de la extensión maliciosa en navegadores basados en Chromium, como Google Chrome, Microsoft Edge, Brave y Vivaldi, mediante la alteración de archivos protegidos de configuración del navegador. No obstante, el ataque requiere habilitar previamente el modo desarrollador en las versiones más recientes de estos navegadores, una acción que los actores de amenazas pueden lograr mediante técnicas de ingeniería social.

«Normalmente, estos navegadores almacenan datos de verificación de seguridad (valores hash/HMAC) junto con configuraciones sensibles para detectar modificaciones no autorizadas. El malware recalcula y actualiza dichos valores tras alterar los archivos, engañando al navegador para que considere que la extensión maliciosa fue instalada de forma legítima», explicó McAfee.

«Esto permite que la extensión eluda el proceso habitual de instalación desde la tienda oficial de extensiones y se cargue silenciosamente sin requerir la aprobación del usuario.»



Los investigadores describen la estrategia de persistencia y evasión de esta campaña como deliberada y compuesta por múltiples capas, priorizando una baja visibilidad para el usuario y una elevada resistencia frente a intentos de desmantelamiento o análisis estático. La persistencia se consigue registrando la extensión mediante modificaciones en el archivo Secure Preferences, permitiendo que esta se cargue automáticamente cada vez que el navegador es iniciado, sin depender de mecanismos adicionales.

Asimismo, el malware intenta habilitar de forma programática el modo desarrollador en Brave y Opera. Una vez ejecutado el instalador, este elimina automáticamente su propio archivo, dificultando la identificación del punto inicial de compromiso. Como técnica adicional de evasión, utiliza un sistema dinámico de sustitución de billeteras, encargado de obtener una dirección fraudulenta específica para reemplazar la dirección original copiada por la víctima.

«El malware envía la dirección de la billetera interceptada al servidor controlado por los atacantes y utiliza la respuesta recibida para sustituir dinámicamente la dirección original. Si

la comunicación con el servidor falla, recurre a una dirección predefinida codificada en el propio malware, garantizando que la actividad maliciosa continúe sin interrupciones», indicó McAfee.

Cada dirección de billetera que coincide con los formatos de Bitcoin (BTC), Ethereum, Bitcoin Cash, Ripple y Dash se asocia en el servidor con una dirección única controlada por los atacantes. En cambio, todas las direcciones correspondientes a Solana son redirigidas hacia una única billetera maliciosa. Al momento de elaborarse el informe, dicha dirección de Solana mantenía un saldo de 1.902,45 dólares estadounidenses.

«Cada dirección enviada es asociada a una dirección única controlada por los atacantes. Si una misma dirección original vuelve a enviarse, el sistema devuelve siempre la misma dirección de reemplazo, lo que demuestra la existencia de una correspondencia determinística uno a uno gestionada desde el servidor.»

Los datos de telemetría indican que las infecciones se distribuyen a nivel mundial, aunque existe una mayor concentración de víctimas en India. Otros países afectados incluyen Estados Unidos, Brasil, Indonesia y España.

«Esta campaña representa claramente la evolución del robo de criptomonedas dirigido a usuarios finales. Las direcciones estáticas utilizadas anteriormente por los atacantes han sido sustituidas por un sistema de asignación individual para cada víctima gestionado desde el servidor. Del mismo modo, los dominios estáticos de comando y control han sido reemplazados por un mecanismo basado en blockchain que permite al operador cambiar la infraestructura mediante una única transacción», concluyó McAfee.

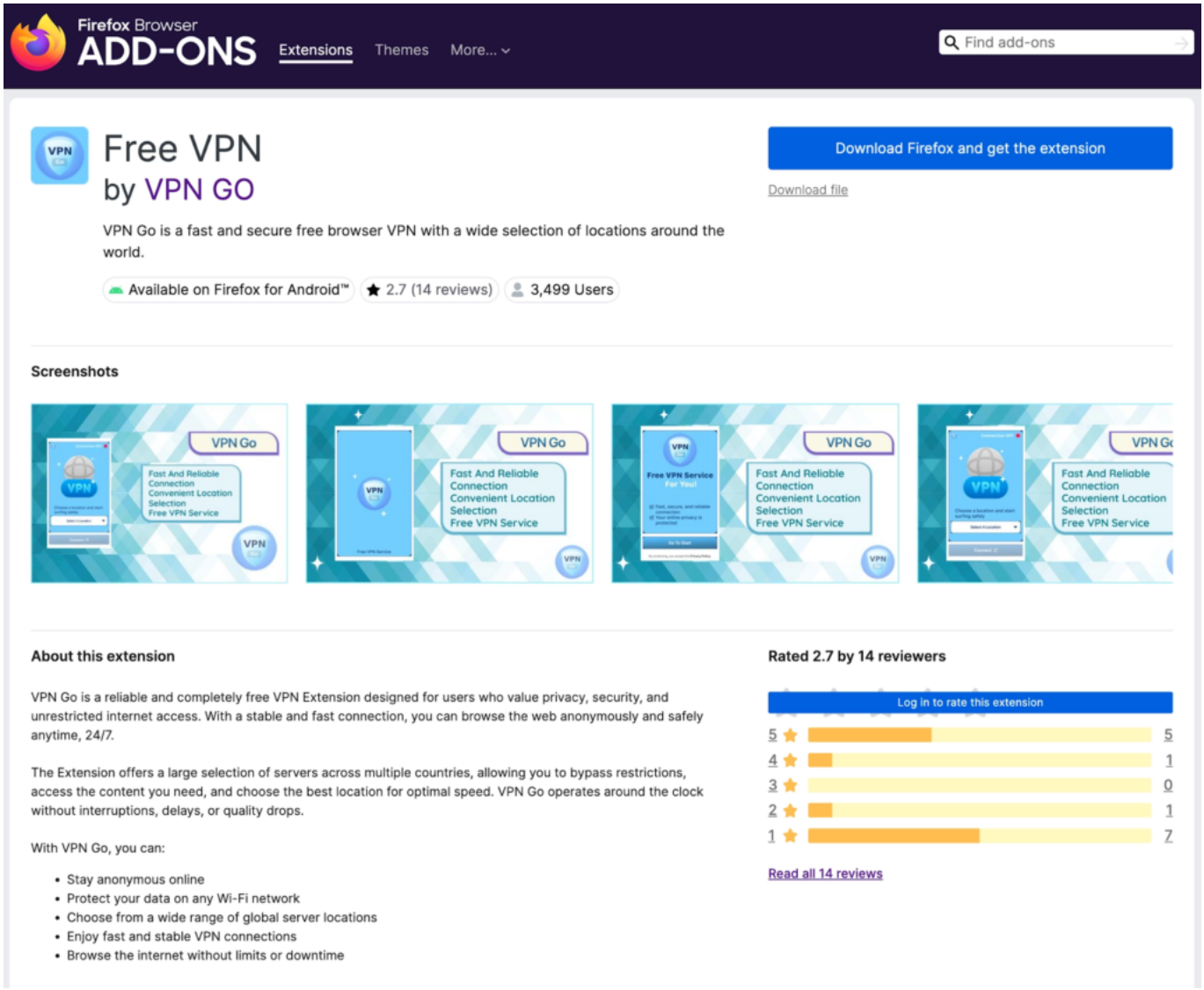
Extensiones de Chrome y Firefox disfrazadas de VPN gratuitas incorporan malware para robar información del portapapeles

La publicación de estos hallazgos coincide con un informe de Socket, que reveló la existencia de dos extensiones maliciosas para Google Chrome y Mozilla Firefox, ambas distribuidas bajo el nombre «VPN Go: Free VPN» a través de la Chrome Web Store y el catálogo de

complementos de Firefox.

«Ambas extensiones se presentan como herramientas VPN gratuitas e incluyen una funcionalidad visible de servidor proxy. Sin embargo, internamente incorporan un mecanismo malicioso de robo del portapapeles que supervisa continuamente el texto copiado y lo envía a una infraestructura controlada por los actores de amenazas», afirmaron los investigadores de Socket, Kirill Boychenko y Kush Pandya.

El comportamiento malicioso va más allá del robo de direcciones de billeteras de criptomonedas, ya que permite a los operadores capturar cualquier tipo de información confidencial almacenada temporalmente en el portapapeles, incluyendo contraseñas, códigos de autenticación, claves de API, tokens OAuth y frases semilla utilizadas para recuperar billeteras digitales.



El análisis detallado de estas extensiones también reveló un patrón de actualización maliciosa por etapas. Inicialmente, el desarrollador publicó una versión completamente legítima en las tiendas oficiales de extensiones. Posteriormente, mediante una actualización, incorporó las funciones destinadas al robo de información del portapapeles.

Las versiones 1.1 y 1.2 de la extensión para Chrome enviaban la información robada al servidor 178.236.252[.]133, mientras que la versión 1.3 modificó el canal de exfiltración

hacia la dirección IP 77.91.123[.]187. En el caso de Firefox, la versión 1.3.3 fue la primera en integrar el módulo de robo del portapapeles y transmitir los datos al servidor 178.236.252[.]133; posteriormente, la actualización 1.3.4 trasladó la infraestructura de recepción a 77.91.123[.]187.

Los usuarios que tengan instalada cualquiera de estas extensiones deben desinstalarlas de inmediato y asumir que toda la información confidencial manipulada mientras permanecieron activas ha quedado comprometida.

«El análisis del código estático demuestra que estas extensiones fueron desarrolladas para funcionar realmente como herramientas proxy y no únicamente para mostrar una interfaz falsa de VPN. No obstante, esa funcionalidad incrementa el riesgo, ya que puede redirigir el tráfico del navegador a través de infraestructura controlada por los atacantes, exponer tráfico HTTP sin cifrar y metadatos de conexión, además de hacer que la extensión parezca útil mientras el monitor del portapapeles opera de forma paralela», concluyó Socket.