Los navegadores web basados en Chromium están siendo objetivo de un nuevo malware llamado Rilide, que se hace pasar por una extensión aparentemente legítima para recopilar datos confidenciales y desviar criptomonedas.

> *«El malware Rilide se disfraza como una extensión legítima de Google Drive y permite a los hackers realizar un amplio espectro de actividades maliciosas, incluida la supervisión del historial, tomar capturas de pantalla e inyectar scripts maliciosos para retirar fondos de varios intercambios de criptomonedas»*, dijo Trustwave SpiderLabs Research.

Además, el malware ladrón puede mostrar diálogos falsificados para engañar a los usuarios para que ingresen un código de autenticación de dos factores para retirar activos digitales.

Trustwave dijo que identificó dos campañas distintas que involucraban a Ekipa RAT y Aurora Stealer, que condujeron a la instalación de la extensión maliciosa del navegador.

Aunque Ekipa RAT se distribuye a través de archivos de Microsoft Publisher con trampas explosivas, los anuncios deshonestos de Google actúan como el vector de entrega de Aurora Stealer, una técnica que se ha vuelto cada vez más común en los últimos meses.

Ambas cadenas de ataque facilitan la ejecución de un cargador basado en Rust, que a su vez, modifica el archivo de acceso directo LNK del navegador y utiliza el interruptor de línea de comando *«–load-extension»* para iniciar el complemento.

Se desconocen los orígenes exactos de Rilide, pero Trustwave dijo que pudo encontrar una publicación clandestina en un foro realizada en marzo de 2022 por un actor de amenazas que anunciaba la venta de una botnet con funcionalidades similares.

Desde entonces, una parte del código fuente del malware llegó a los foros después de lo que parece ser una disputa de pago sin resolver.

Una característica notable implementada en el código fuente filtrado es la capacidad de intercambiar direcciones de billetera de criptomonedas en el portapapeles con una dirección controlada por el hacker codificada en la muestra.

Además, una dirección de comando y control (C2) especificada en el código de Rilide ha hecho posible identificar varios respositorios de GitHub pertenecientes a un usuario llamado gualantin, que contienen cargadores para la extensión.

> *«El ladrón de Rilide es un excelente ejemplo de la creciente sofisticación de las extensiones de navegador maliciosas y los peligros que representan»*, dijo Trustwave.

> *«Si bien la próxima aplicación del manifiesto v3 puede dificultar la operación de los actores amenazas, es poco probable que resuelve el problema completamente, ya que la mayoría de las funcionalidades aprovechadas por Rilide seguirán estando disponibles».*