Las personas que tributan en México y Chile han sido el blanco de un grupo de ciberdelincuencia radicado en México que se autodenomina Fenix para vulnerar las redes seleccionadas y sustraer datos valiosos.

Un rasgo distintivo de la operación consiste en copiar los portales oficiales del Servicio de Administración Tributaria (SAT) en México y el Servicio de Impuestos Internos (SII) en Chile y redireccionar a las potenciales víctimas a esos sitios.

> *«Estos sitios web falsos solicitan a los usuarios que bajen una supuesta herramienta de seguridad, asegurando que aumentará la seguridad de su navegación por el portal»*, dijeron los investigadores de seguridad de Metabase Q, Gerardo Corona y Julio Vidal en un reciente análisis.

> *«Sin embargo, sin que las víctimas lo sepan, esta bajada instala en realidad la etapa inicial del software malicioso, lo que permite finalmente el hurto de información sensible como credenciales».*

La meta de Fenix, según la empresa de seguridad cibernética enfocada en América Latina, es actuar como un intermediario de acceso inicial y obtener una presencia en distintas empresas de la región, y vender el acceso a asociados de ransomware para una mayor monetización.

Las evidencias recabadas hasta ahora indican que el actor de la amenaza organiza campañas de phishing coincidiendo con las actividades gubernamentales durante el año desde al menos el cuarto trimestre de 2022.

La mecánica de la campaña se desarrolla así: Los visitantes que llegan a los sitios web falsificados son instados a descargar un software que supuestamente resguarda sus datos mientras navegan por el portal. Alternativamente, los usuarios son seducidos por sitios de phishing configurados para descargar aplicaciones legítimas como AnyDesk.

> *«[Fenix] vulnera sitios web débiles utilizando motores WordPress expuestos y también crea nuevos dominios para lanzar campañas de phishing. El grupo crea dominios de typosquatting similares a aplicaciones conocidas como AnyDesk, WhatsApp, etc.».* dijeron los investigadores,

Pero en realidad, el archivo ZIP que contiene el supuesto software se utiliza como un punto de partida para activar una secuencia de infección que conduce a la ejecución de un script PowerShell ofuscado, que, a su vez, carga y ejecuta un binario .NET, después de lo cual se muestra el mensaje *«Ahora se encuentra protegido»* para mantener el engaño.

El ejecutable .NET posteriormente prepara el camino para establecer la persistencia en el host vulnerado y desplegar un malware botnet que es capaz de ejecutar comandos recibidos desde un servidor remoto, cargar un módulo stealer que exfiltra credenciales almacenadas en navegadores web y billeteras criptográficas, y finalmente borrarse a sí mismo.

> *«Estamos viendo nuevos grupos maliciosos creados en LATAM para proporcionar acceso inicial a bandas de ransomware. Estos actores locales no son aficionados y aumentarán su pericia técnica y por lo tanto más difíciles de rastrear, detectar y erradicar, es importante anticiparse a sus acciones»,* concluyeron los investigadores.