Expertos en ciberseguridad han alertado sobre una nueva campaña de fraude que utiliza aplicaciones falsas de videollamadas para distribuir un software malicioso conocido como Realst, diseñado para robar información confidencial. Este ataque está dirigido principalmente a personas que trabajan en el sector Web3 y se presenta bajo la apariencia de reuniones de negocios ficticias.

> *«Los responsables del malware han creado compañías ficticias utilizando inteligencia artificial para hacerlas parecer más legítimas. Estas empresas contactan a las víctimas para organizar una videoconferencia, solicitándoles descargar la aplicación desde su sitio web, que en realidad contiene el infostealer Realst»*, señaló Tara Gould, investigadora de Cado Security.

La actividad ha sido denominada Meeten por la empresa de seguridad debido al uso de nombres como Clusee, Cuesee, Meeten, Meetone y Meetio en los sitios web fraudulentos.

El ataque comienza contactando a las víctimas potenciales a través de Telegram, donde se les propone una posible oportunidad de inversión y se les invita a unirse a una videollamada alojada en una de estas plataformas sospechosas. Los usuarios que acceden al sitio son dirigidos a descargar una versión para Windows o macOS, según el sistema operativo que utilicen.

Al instalarse y ejecutarse en macOS, el programa muestra un mensaje afirmando que *«La versión actual de la aplicación no es completamente compatible con su versión de macOS»* y solicita la contraseña del sistema para que funcione correctamente.

Esta técnica utiliza el comando osascript, una estrategia que ya ha sido empleada por otras familias de malware para macOS como Atomic macOS Stealer, Cuckoo, MacStealer, Banshee Stealer y Cthulhu Stealer. El propósito principal es obtener diversos tipos de información sensible, incluidos datos de billeteras de criptomonedas, y enviarlos a un servidor remoto.

Adicionalmente, el malware tiene la capacidad de robar credenciales de Telegram,

información financiera, datos almacenados en el llavero de iCloud y cookies de navegadores como Google Chrome, Microsoft Edge, Opera, Brave, Arc, Cốc Cốc y Vivaldi.

La versión para Windows de la aplicación Nullsoft Scriptable Installer System (NSIS) contiene un archivo firmado con una certificación legítima, aparentemente sustraída de Brys Software Ltd.. Este instalador incluye una aplicación basada en Electron, configurada para descargar un programa ladrón de datos, escrito en Rust, desde un dominio bajo control de los atacantes.

> *«Los ciberdelincuentes están recurriendo cada vez más a la inteligencia artificial para crear contenido en sus campañas. El uso de IA les permite generar rápidamente sitios web convincentes que otorgan credibilidad a sus fraudes, dificultando la identificación de páginas sospechosas»*, afirmó Gould.

No es la primera vez que se emplean marcas falsas de software de reuniones virtuales para distribuir malware. En marzo, Jamf Threat Labs descubrió un sitio web falso llamado meethub[.]gg, utilizado para distribuir un malware ladrón de datos que comparte características con el Realst.

En junio, Recorded Future informó sobre una campaña denominada markopolo, dirigida a usuarios de criptomonedas. Los atacantes emplearon programas falsos de reuniones virtuales para robar fondos utilizando malware como Rhadamanthys, Stealc y Atomic.

Este panorama coincide con el cierre de las operaciones del grupo detrás del malware para macOS Banshee Stealer, tras la filtración de su código fuente. Aún no se sabe qué originó esta filtración. Este malware se ofrecía en foros clandestinos por un costo mensual de $3,000.

Además, han surgido nuevas familias de programas maliciosos diseñados para robar información, como Fickle Stealer, Wish Stealer, Hexon Stealer y Celestial Stealer. Al mismo tiempo, tanto usuarios como empresas que buscan software pirateado o herramientas de

inteligencia artificial están siendo atacados con malware como RedLine Stealer y Poseidon Stealer.

> *«Los responsables de esta campaña buscan claramente infiltrarse en organizaciones de emprendedores de habla rusa que utilizan software para optimizar sus procesos empresariales»*, señaló Kaspersky al referirse a la campaña de RedLine Stealer.