Presuntos hackers rusos han estado apuntando a usuarios de Europa del Este en la industria de la criptografía, con oportunidades de trabajo falsas como cebo para instalar malware que roba información en hosts comprometidos.

Los atacantes *«utilizan varios cargadores altamente ofuscados y en desarrollo para infectar a los involucrados en la industria de las criptomonedas con el ladrón Enigma»*, dijeron los investigadores de Trend Micro, Aliakbar Zahravi y Peter Girnus.

Enigma es una versión alterada de Stealerium, un malware de código abierto basado en C# que actúa como ladrón, recortador y registrador de teclas.

El proceso de infección comienza con un archivo RAR falso que se distribuye por medio de phishing o plataformas de redes sociales. Contiene dos documentos, uno de los cuales es un archivo .txt que incluye un conjunto de preguntas de entrevista de muestra relacionadas con las critpomonedas.

El segundo archivo es un documento de Microsoft Word que, si bien sirve como señuelo, tiene la tarea de iniciar el cargador Enigma de la primera etapa, que a su vez, descarga y ejecuta una carga útil ofuscada de la etapa secundaria por medio de Telegram.

> *«Para descargar la carga útil de siguiente etapa, el malware primero envía una solicitud al canal de Telegram controlado por el atacante para obtener la ruta del archivo. Este enfoque permite que el atacante actualice de forma continua y elimina la dependencia de nombres de archivos fijos»,* dijeron los investigadores.

El descargador de segunda etapa, que se ejecuta con privilegios elevados, está diseñado para deshabilitar Microsoft Defender e instalar una tercera etapa mediante la implementación de un controlador Intel en modo kernel firmado legítimamente, que además es vulnerable a CVE-2015-2291 en una técnica llamada Bring Your Own Vulnerable Driver (BYOVD).

Cabe mencionar que la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), agregó la vulnerabilidad a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV), citando evidencia de explotación activa en la naturaleza.

La carga útil de la tercera etapa finalmente allana el camino para descarga Enigma Stealer desde un canal de Telegram controlado por los hackers. El malware, al igual que otros ladrones, cuenta con capacidades para recopilar información confidencial, registrar pulsaciones de teclas y realizar capturas de pantalla, todo lo cual se extrae a través de Telegram.

Las ofertas de trabajo falsas son una táctica probada y comprobada empleada por Lazarus Group, respaldado por Corea del Norte, en sus ataques dirigidos al sector de las criptomonedas. La adopción de este modus operandi por parte de los hackers rusos *«demuestra un vector de ataque persistente y lucrativo».*

Los hallazgos se producen cuando Uptycs publicó detalles de una campaña de ataque que aprovecha el malware Stealerium para desviar datos personales, incluyendo las credenciales para billeteras de criptomonedas como Armory, Atomic Wallet, Coinomi, Electrum, Exodus, Guarda, Jaxx Liberty y Zcash, entre otros.

Unido a Enigma Stealer y Stealerium para apuntar a las billeteras de criptomonedas está otro malware denominado Vector Stealer, que también cuenta con capacidades para robar archivos .RDP, lo que permite a los hackers realizar el secuestro de RDP para acceso remoto, dijo Cyble en un artículo.

Las cadenas de ataque documentadas por las empresas de seguridad cibernética muestran que las familias de malware se entregan por medio de archivos adjuntos de Microsoft Office que contienen macros maliciosas, lo que sugiere que los atacantes aún confían en el método a pesar de los intentos de Microsoft de cerrar la brecha.

También se ha utilizado un método similar para implementar un criptominero Monero en el contexto de una campaña de criptojacking y phishing dirigida a los usuarios españoles, según

Fortinet FortiGuard Labs.

El desarrollo también es el último de una larga lista de ataques que tienen como objetivo robar los activos de criptomonedas de las víctimas en todas las plataformas.

Esto comprende un troyano bancario para Android de *«rápida evolución»* conocido como TgToxic, que roba credenciales y fondos de billeteras criptográficas, así como aplicaciones bancarias y financieras. La campaña de malware en curso, activa desde julio de 2022, está dirigida a usuarios móviles en Taiwán, Tailandia e Indonesia.

> *«Cuando la víctima descarga la aplicación falsa del sitio web proporcionado por el autor de la amenaza, o si la víctima intenta enviar un mensaje directo al autor de la amenaza por medio de aplicaciones de mensajería como WhatsApp o Viber, el hacker engaña al usuario para que se registre e instale el malware y habilite los permisos que necesita»*, dijo Trend Micro.

Las aplicaciones no autorizadas, además de abusar de los servicios de accesibilidad de Android para realizar transferencias de fondos no autorizadas, también se destacan por aprovechar marcos de automatización legítimos como Easyclick y Auto.js para realizar clics y gestos, lo que lo convierte en el segundo malware de Android después de PixPirate en incorporar dichos IDE de flujo de trabajo.

Pero las campañas de ingeniería social también han ido más allá del phishing y el smishing en las redes sociales al establecer páginas de destino convincentes que imitan los servicios criptográficos populares con el objetivo de transferir Ethereum y NFT de las billeteras hackeadas.

Esto, según Recorded Future, se logra mediante la inyección de una secuencia de comandos

de drenaje criptgráfico en la página de phishing que atrae a las víctimas para que conecten sus billeteras con ofertas lucrativas para acuñar tokens no fungibles (NFT).

Estas páginas de phishing listas para usar se venden en los foros de la red oscura como parte de lo que se ha llamado; un esquema de phishing como servicio (PhaaS), *que permite a otros hackers alquilar dichos paquetes y ejecutar rápidamente operaciones maliciosas a escala.*

> *«Los drenadores de criptomonedas son scripts maliciosos que funcionan como e-skimmers y se implementan con técnicas de phishing para robar los criptoactivos de las víctimas»,* dijo la compañía en un informe la semana pasada.

> *«El uso de servicios legítimos en las páginas de phishing de drenaje criptográfico puede aumentar la probabilidad de que la página de phishing pase la prueba de fuego de la estafa de un usuario inteligente. Una vez que las billeteras criptográficas se han visto comprometidas, no existen salvaguardas para evitar la transferencia ilícita de los activos a las billeteras de los atacantes».*

Los ataques se producen en un momento en que los grupos criminales han robado un récord de 3800 millones de dólares en criptomonedas en 2022, y gran parte del aumento se atribuye a los equipos de hacking patrocinados por el estado de Corea del Norte.