Un grupo de ciberdelincuentes vinculado a la República Popular Democrática de Corea (RPDC) ha estado atacando a empresas relacionadas con criptomonedas utilizando un malware de varias etapas que puede infectar dispositivos con macOS de Apple.

La compañía de ciberseguridad SentinelOne, que ha bautizado la campaña como *Hidden Risk* (Riesgo Oculto), la atribuye con alta certeza al grupo BlueNoroff, conocido anteriormente por emplear familias de malware como RustBucket, KANDYKORN, ObjCShellz, RustDoor (también conocido como Thiefbucket) y TodoSwift.

> Según los investigadores Raffaele Sabato, Phil Stokes y Tom Hegel en un informe, la actividad *«emplea correos electrónicos que difunden noticias falsas sobre tendencias de criptomonedas para infectar objetivos a través de una aplicación maliciosa disfrazada de archivo PDF».*
>
> *«Es probable que la campaña haya comenzado ya en julio de 2024 y utiliza señuelos en formato de correo electrónico y PDF con titulares falsos o historias sobre temas relacionados con criptomonedas».*

Según un aviso emitido por el Buró Federal de Investigaciones (FBI) de Estados Unidos en septiembre de 2024, estas campañas forman parte de ataques de ingeniería social «*altamente personalizados y difíciles de detectar*», orientados a empleados en los sectores de finanzas descentralizadas (DeFi) y criptomonedas.

Los ataques suelen presentarse como oportunidades laborales falsas o supuestas inversiones corporativas, en los que los atacantes mantienen contacto prolongado con las víctimas para ganar su confianza antes de introducir el malware.

SentinelOne reportó que, en octubre de 2024, detectó un intento de phishing dirigido a una empresa del sector de criptomonedas, en el que se entregó una aplicación tipo «dropper» que imitaba un archivo PDF bajo el nombre «*Hidden Risk Behind New Surge of Bitcoin*

Price.app» alojado en delphidigital[.]org.

La aplicación, desarrollada en el lenguaje de programación Swift, fue firmada y notariada el 19 de octubre de 2024 con el ID de desarrollador de Apple *«Avantis Regtech Private Limited (2S8XHJ7948)»*. Sin embargo, Apple revocó la firma posteriormente.

Al ejecutarse, la aplicación descarga y muestra un archivo PDF señuelo desde Google Drive, mientras de manera encubierta recupera y ejecuta un ejecutable de segunda etapa desde un servidor remoto. Este ejecutable Mach-O x86-64, basado en C++, actúa como una puerta trasera para ejecutar comandos de forma remota.

El backdoor también incorpora un mecanismo de persistencia novedoso que explota el archivo de configuración *zshenv*, marcando la primera vez que esta técnica es utilizada en ataques reales por autores de malware.

> *«Este método tiene especial relevancia en las versiones modernas de macOS, ya que Apple introdujo notificaciones para avisar al usuario cuando se instala un método de persistencia en segundo plano, particularmente con LaunchAgents y LaunchDaemons, a partir de macOS 13 Ventura»*, explicaron los investigadores.
>
> *«No obstante, el abuso del archivo zshenv no genera tales notificaciones en las versiones actuales de macOS».*

Además, se ha observado que el grupo de amenazas emplea el registrador de dominios Namecheap para establecer una infraestructura en torno a temas de criptomonedas, Web3 e inversiones, buscando así una apariencia de legitimidad. Entre los proveedores de hosting más utilizados están Quickpacket, Routerhosting y Hostwinds.

Cabe destacar que la cadena de ataques presenta cierta similitud con una campaña previa que fue señalada por Kandji en agosto de 2024, en la cual también se usó una aplicación

dropper para macOS llamada *«Risk factors for Bitcoin's price decline are emerging(2024).app»* para desplegar TodoSwift.

No está claro qué motivó a los atacantes a cambiar sus tácticas o si esto responde a la cobertura mediática. *«Los actores norcoreanos son reconocidos por su creatividad, adaptabilidad y por estar al tanto de los informes sobre sus actividades, por lo que es posible que simplemente estemos viendo métodos exitosos diferentes surgidos de su programa de ciberofensiva»,* comentó Stokes.

Un aspecto preocupante de la campaña es la capacidad de BlueNoroff para adquirir o secuestrar cuentas válidas de desarrollador de Apple y utilizarlas para que su malware sea notarizado por Apple.

«Durante los últimos 12 meses, los actores de ciberseguridad norcoreanos han lanzado una serie de campañas contra industrias relacionadas con criptomonedas, muchas de las cuales implicaron una preparación extensa de los objetivos a través de redes sociales», dijeron los investigadores.

«La campaña *Hidden Risk* se desvía de esta estrategia al adoptar un enfoque más tradicional y crudo de phishing por correo electrónico. A pesar de la simplicidad del método de infección inicial, son evidentes otros rasgos distintivos de campañas anteriores apoyadas por la RPDC».

Este desarrollo ocurre en un momento en que otros hackers norcoreanos también están realizando campañas para buscar empleo en empresas occidentales y entregar malware utilizando bases de código y herramientas de videoconferencia comprometidas, bajo el pretexto de un desafío de contratación o una tarea de prueba.

Dos conjuntos de intrusión, denominados Wagemole (también conocido como UNC5267) y Contagious Interview, han sido atribuidos a un grupo de amenazas identificado como Famous Chollima (también conocido como CL-STA-0240 y Tenacious Pungsan).

ESET, que ha denominado a la campaña Contagious Interview como DeceptiveDevelopment, la ha clasificado como un nuevo subgrupo del Grupo Lazarus, enfocado en atacar a desarrolladores freelance de todo el mundo con el objetivo de robar criptomonedas.

> *«Las campañas Contagious Interview y Wagemole destacan las tácticas en evolución de los actores de amenazas norcoreanos, quienes continúan robando datos, consiguen trabajos remotos en países occidentales y evaden sanciones financieras»,* explicó Seongsu Park, investigador de Zscaler ThreatLabz, a principios de esta semana.
>
> *«Con técnicas avanzadas de ofuscación, compatibilidad multiplataforma y robo de datos generalizado, estas campañas representan una amenaza creciente tanto para empresas como para personas individuales».*