Los usuarios de criptomonedas son el objetivo de una campaña activa de ingeniería social que utiliza falsas empresas emergentes para engañarlos y hacer que descarguen malware capaz de robar activos digitales, tanto en sistemas Windows como macOS.

> *«Estas operaciones maliciosas se hacen pasar por compañías de inteligencia artificial, videojuegos y Web3, utilizando cuentas falsas en redes sociales y documentación de proyectos alojada en plataformas legítimas como Notion y GitHub»*, explicó la investigadora Tara Gould de Darktrace en un informe.

Esta elaborada estafa en redes sociales lleva activa un tiempo, y una versión anterior, en diciembre de 2024, utilizó plataformas falsas de videollamadas para engañar a las víctimas con la excusa de discutir oportunidades de inversión, luego de contactarlas por apps de mensajería como Telegram.

Los usuarios que descargaban el supuesto software de reuniones eran infectados de forma sigilosa con malware tipo stealer como Realst. Esta campaña fue nombrada *Meeten* por la empresa Cado Security (adquirida por Darktrace a principios de este año), en referencia a uno de los servicios de videoconferencias falsos utilizados.

Dicho esto, hay indicios de que esta actividad podría estar ocurriendo desde al menos marzo de 2024, cuando el equipo de Jamf Threat Labs descubrió un dominio llamado *meethub[.]gg* utilizado para distribuir el malware Realst.

Los hallazgos más recientes de Darktrace indican que esta campaña no solo continúa siendo una amenaza activa, sino que ahora abarca una mayor variedad de temáticas, como inteligencia artificial, videojuegos, Web3 y redes sociales.

Además, se ha observado que los atacantes aprovechan cuentas comprometidas en X (antes Twitter), tanto de empresas como de empleados —principalmente aquellas verificadas— para acercarse a sus objetivos y dar una apariencia legítima a sus falsas organizaciones.

> *«Utilizan sitios frecuentemente empleados por compañías de software como X, Medium, GitHub y Notion»,* señaló Gould. *«Cada empresa falsa cuenta con un sitio web profesional que incluye empleados, blogs de productos, documentos técnicos y hojas de ruta.»*

Una de estas compañías ficticias es Eternal Decay (@metaversedecay), que afirma ser un juego basado en blockchain, y ha compartido imágenes legítimas alteradas digitalmente en X para aparentar que participa en conferencias. El objetivo es construir una presencia en línea creíble que aumente la posibilidad de que las víctimas se infecten.

Algunas de las otras empresas falsas identificadas son las siguientes:

- BeeSync (X cuentas: @BeeSyncAI, @AIBeeSync)
- Buzzu (X cuentas: @BuzzuApp, @AI_Buzzu, @AppBuzzu, @BuzzuApp)
- Cloudsign (cuenta X: @cloudsignapp)
- Dexis (cuenta X: @DexisApp)
- KlastAI (cuenta X: Enlaces a la cuenta X de Pollens AI)
- Lunelior
- NexLoop (cuenta X: @nexloopspace)
- NexoraCore
- NexVoo (cuenta X: @Nexvoospace)
- Pollens AI (X cuentas: @pollensapp, @Pollens_app)
- Slax (X cuentas: @SlaxApp, @Slax_app, @slaxproject)
- Solune (X cuenta: @soluneapp)
- Swox (X cuentas: @SwoxApp, @Swox_AI, @swox_app, @App_Swox, @AppSwox, @SwoxProject, @ProjectSwox)
- Wasper (X cuentas: @wasperAI, @WasperSpace)
- YondaAI (cuenta X: @yondaspace)

El ataque comienza cuando una de estas cuentas controladas por los atacantes contacta a una víctima a través de X, Telegram o Discord, invitándola a probar su software a cambio de

un pago en criptomonedas.

Si la víctima acepta participar, es redirigida a un sitio web ficticio, donde se le pide ingresar un código de registro proporcionado por el supuesto empleado, para así descargar una aplicación en formato Electron para Windows o una imagen de disco (DMG) para macOS, dependiendo del sistema operativo.

En equipos Windows, al ejecutar la aplicación maliciosa, la víctima ve una pantalla de verificación de Cloudflare, mientras en segundo plano se analiza el sistema y se descarga un instalador MSI que se ejecuta de forma oculta. Aunque no se conoce con certeza el contenido del malware, se sospecha que se trata de un ladrón de información.

En macOS, por otro lado, la descarga lleva a la instalación del conocido malware Atomic macOS Stealer (AMOS), diseñado para robar documentos, datos de navegadores web y monederos de criptomonedas, y enviar esta información a servidores externos.

El archivo DMG también contiene un script que configura persistencia en el sistema mediante un *Launch Agent*, asegurando que la app se ejecute automáticamente al iniciar sesión. Además, descarga y lanza un binario en Objective-C/Swift que registra el uso de la aplicación y los tiempos de interacción del usuario, los cuales son transmitidos a un servidor remoto.

Darktrace también señaló que esta campaña comparte tácticas similares con las empleadas por un grupo de tráfico conocido como Crazy Evil, que engaña a las víctimas para que instalen malware como StealC, AMOS y Angel Drainer.

> *«Si bien no está claro si estas campañas [...] pueden atribuirse a Crazy Evil o a alguno de sus subgrupos, las técnicas utilizadas son similares»*, dijo Gould. *«Esta campaña demuestra el esfuerzo que hacen los actores de amenazas para hacer que estas empresas falsas parezcan legítimas, con el fin de robar criptomonedas, además del uso de nuevas variantes de malware diseñadas para evadir detección.»*