Las empresas de inversión de criptomonedas son el objetivo de un grupo de amenazas en desarrollo que utiliza grupos de Telegram para buscar víctimas potenciales.

El Security Threat Intelligence Center (MSTIC) de Microsoft está rastreado la actividad bajo el nombre DEV-0139, y se basa en un informe reciente de Volexity que atribuyó el mismo conjunto de ataques a Lazarus Group de Corea del Norte.

> *«DEV-0139 se unió a los grupos de Telegram usados para facilitar la comunicación entre los clientes VIP y las plataformas de intercambio de criptomonedas, e identificó su objetivo entre los miembros»,* dijo la compañía.

Posteriormente, el atacante se hizo pasar por otra compañía de inversión en criptomonedas e invitó a la víctima a unirse a un grupo de chat distinto de Telegram con el pretexto de pedir comentarios sobre la estructura de tarifas comerciales utilizada por las plataformas de intercambio en todos los niveles VIP.

Cabe mencionar que el programa VIP está diseñado para recompensar a los comerciantes de alto volumen con incentivos y descuentos exclusivos de tarifas comerciales basados en la actividad en los últimos 30 días.

Esta cadena de ataque encaja notablemente con el análisis de Volexity de una campaña de octubre de 2022, en la que el atacante pasó de usar archivos de instalación de MSI a un documento de Microsoft Excel armado que muestra las supuestas tasas de las criptomonedas.

Microsoft describió que el documento contiene datos probablemente precisos para aumentar la probabilidad de éxito de la campaña, lo que sugiere que DEV-0139 está bien versado en el funcionamiento interno de la industria de la criptografía.

El archivo de Excel con malware, por su parte, tiene la tarea de ejecutar una macro maliciosa que se usa para colocar y ejecutar de forma sigilosa una segunda hoja de cálculo de Excel,

que a su vez, incluye una macro que descarga un archivo de imagen PNG alojado en OpenDrive.

Este archivo de imagen contiene tres ejecutables, cada uno de los cuales se usa para lanzar la carga útil de la siguiente etapa, lo que en última instancia allana el camino para una puerta trasera que permite al actor de amenazas acceder remotamente al sistema infectado.

Además, la hoja de cálculo de la estructura de tarifas está protegida con contraseña en un intento por convencer al objetivo de que habilite las macros, iniciando así las acciones maliciosas. Un análisis de metadatos del archivo muestra que fue creado el 14 de octubre de 2022 por un usuario llamado Wolf.

DEV-0139 también se ha relacionado con una secuencia de ataque alternativa en la que se entrega un paquete MSI para una aplicación falsa llamada *«CryptoDashboardV2»* en lugar de un documento de Excel malicioso para implementar el mismo implante.

La puerta trasera permite principalmente el acceso remoto al host recopilando información del sistema de destino y conectándose a un servidor de comando y control (C2) para recibir comandos adicionales.

> *«El mercado de las criptomonedas sigue siendo un campo de interés para los atacantes. Los usuarios objetivo se identifican por medio de canales confiables para aumentar las posibilidades de éxito»,* dijo Microsoft.

En los últimos años, Telegram no solo ha sido testigo de una adopción generalizada en la industria de las criptomonedas, sino que también ha sido cooptado por atacantes que buscan discutir vulnerabilidades de día cero, ofrecer datos robados y comercializar sus servicios a través de la popular plataforma de mensajería.

«Con los usuarios perdiendo la confianza en el anonimato que ofrecen los foros, los mercados ilícitos recurren cada vez más a Telegram», reveló Positive Technologies en un nuevo estudio de 323 canales y grupos públicos de Telegram con más de un millón de suscriptores en total.

> *«La cantidad de ciberataques únicos está en constante crecimiento, y el mercado de los servicios de los ciberdelincuentes se está expandiendo y avanzando hacia las redes sociales y las aplicaciones de mensajería ordinarias, lo que reduce de forma significativa el umbral de entrada para los ciberdelincuentes».*