Los expertos en ciberseguridad han alertado sobre una campaña activa que está dirigida a jugadores y a inversores en criptomonedas, disfrazándose como proyectos de código abierto alojados en GitHub.

Esta operación, que involucra cientos de repositorios, ha sido bautizada como GitVenom por la empresa Kaspersky.

> *«Entre los proyectos comprometidos se encuentran una herramienta de automatización para gestionar cuentas de Instagram, un bot de Telegram que permite el control remoto de billeteras de Bitcoin y un programa de crack para jugar a Valorant»*, señaló la firma de ciberseguridad con sede en Rusia.
>
> *«Todas estas funciones eran completamente falsas, y los delincuentes detrás de la campaña aprovecharon para robar información personal y financiera, además de modificar direcciones de criptomonedas copiadas en el portapapeles».*

Gracias a esta actividad maliciosa, los atacantes lograron sustraer 5 bitcoins, lo que equivale a aproximadamente 456,600 dólares en el momento en que se reportó el caso. Se estima que esta operación ha estado en marcha durante al menos dos años, ya que algunos de los proyectos fraudulentos fueron publicados en ese período. Los países con más intentos de infección registrados han sido Rusia, Brasil y Turquía.

Los proyectos utilizados en la campaña están desarrollados en múltiples lenguajes de programación, tales como Python, JavaScript, C, C++ y C#. Sin embargo, el lenguaje utilizado es irrelevante, ya que el propósito final siempre es el mismo: ejecutar una carga maliciosa oculta, encargada de descargar otros archivos desde un repositorio de GitHub controlado por los atacantes y ejecutarlos en el sistema de la víctima.

Uno de los componentes más relevantes es un stealer de información basado en Node.js, diseñado para recolectar contraseñas, datos bancarios, credenciales almacenadas,

información de billeteras de criptomonedas y el historial de navegación. Posteriormente, comprime todos estos datos en un archivo .7z y los envía a los ciberdelincuentes mediante Telegram.

Asimismo, dentro de los proyectos falsos alojados en GitHub también se distribuyen herramientas de acceso remoto como AsyncRAT y Quasar RAT, que les permiten a los atacantes tomar el control de los dispositivos infectados. Además, incluyen un malware clipper, cuyo propósito es modificar direcciones de billeteras copiadas en el portapapeles y reemplazarlas con una perteneciente a los atacantes, desviando así los fondos a sus cuentas.

> *«Plataformas como GitHub, utilizadas por millones de desarrolladores en todo el mundo, seguirán siendo un objetivo para los actores maliciosos, quienes emplearán software falso para propagar sus infecciones»,* explicó Georgy Kucherin, investigador de Kaspersky.
>
> *«Por este motivo, es fundamental manejar con precaución cualquier código desarrollado por terceros. Antes de ejecutarlo o incorporarlo en un proyecto propio, es esencial verificar minuciosamente sus acciones».*

Este hallazgo surge en un contexto donde Bitdefender ha revelado una nueva modalidad de estafa, en la que ciberdelincuentes están aprovechando torneos de e-sports como IEM Katowice 2025 y PGL Cluj-Napoca 2025 para atacar a los jugadores de Counter-Strike 2 (CS2) con el objetivo de engañarlos.

> *«A través del secuestro de cuentas de YouTube, los atacantes se hacen pasar por jugadores profesionales como s1mple, NiKo y donk, con el fin de atraer a los seguidores a supuestos sorteos de skins de CS2. Sin embargo, estos engaños terminan en el robo de cuentas de Steam, sustracción de criptomonedas y pérdida de objetos valiosos dentro del juego«,* advirtió la empresa de ciberseguridad

> rumana.