El grupo Lazarus, vinculado a Corea del Norte, ha sido identificado como responsable de una nueva campaña de ciberataques llamada *«Operation 99».* Esta operación tiene como objetivo a desarrolladores de software que buscan trabajos freelance en los sectores de Web3 y criptomonedas, utilizando malware como herramienta principal.

«La campaña comienza con supuestos reclutadores falsos que se presentan en plataformas como LinkedIn, atrayendo a los desarrolladores con evaluaciones de proyectos y revisiones de código», señaló Ryan Sherstobitoff, vicepresidente senior de Investigación e Inteligencia de Amenazas en SecurityScorecard, en un informe publicado recientemente.

> *«Cuando la víctima cae en la trampa, se le solicita clonar un repositorio de GitLab aparentemente inofensivo, pero que contiene código malicioso. Este código establece conexiones con servidores de comando y control (C2), permitiendo la instalación de malware en el sistema de la víctima.»*

Las víctimas de esta operación han sido detectadas en varias partes del mundo, con una mayor concentración en Italia. También se han reportado casos en países como Argentina, Brasil, Egipto, Francia, Alemania, India, Indonesia, México, Pakistán, Filipinas, Reino Unido y Estados Unidos.

Según la empresa de ciberseguridad, la campaña, descubierta el 9 de enero de 2025, utiliza tácticas relacionadas con ofertas de empleo, similares a las empleadas en ataques anteriores del grupo Lazarus, como la operación «Dream Job» (también conocida como NukeSped). Sin embargo, en esta ocasión se enfoca en desarrolladores relacionados con Web3 y criptomonedas.

La característica distintiva de la Operación 99 es su estrategia para captar la atención de los desarrolladores a través de proyectos de codificación, todo como parte de un esquema de reclutamiento falso. Esto incluye la creación de perfiles engañosos en LinkedIn para redirigir a las víctimas a repositorios peligrosos en GitLab.

El propósito de estos ataques es desplegar herramientas diseñadas para robar datos, incluyendo código fuente, información confidencial, claves de carteras de criptomonedas y otros elementos sensibles dentro de los entornos de desarrollo.

Entre los componentes maliciosos utilizados se encuentran Main5346 y su variante Main99, que funcionan como descargadores para tres cargas adicionales:

1. Payload99/73 (y su variante Payload5346): Recopilan información del sistema, como archivos y contenido del portapapeles, finalizan procesos de navegadores web, ejecutan comandos arbitrarios y establecen conexiones persistentes con los servidores C2.
2. Brow99/73: Extraen datos de navegadores web para facilitar el robo de credenciales.
3. MCLIP: Supervisan y extraen en tiempo real la actividad del teclado y del portapapeles.

> *«Al comprometer las cuentas de los desarrolladores, los atacantes no solo obtienen acceso a propiedad intelectual, sino también a carteras de criptomonedas, lo que les permite realizar robos financieros directos. El robo de claves privadas y datos sensibles podría generar pérdidas millonarias en activos digitales, fortaleciendo los objetivos financieros del grupo Lazarus»,* explicó la empresa.

El diseño del malware es modular, adaptable y compatible con sistemas operativos como Windows, macOS y Linux, lo que subraya la sofisticación y la capacidad de evolución constante de las amenazas cibernéticas impulsadas por estados nación.

> *«Para Corea del Norte, el hacking es una fuente crucial de ingresos. El grupo Lazarus ha utilizado repetidamente las criptomonedas robadas para financiar las metas del régimen, acumulando grandes cantidades de dinero. Con el crecimiento acelerado de las industrias de Web3 y criptomonedas, la Operación 99 apunta directamente a estos sectores en auge»,* afirmó Sherstobitoff.