Hackers patrocinados por el estado afiliados a Corea del Norte, han estado detrás de una serie de ataques cibernéticos a los intercambios de criptomonedas en los últimos tres años, según nuevas revelaciones.

Al atribuir el ataque con probabilidad *«media-alta»* a Lazarous Group (también conocido como APT38 o Hidden Cobra), los investigadores de la compañía israelí de seguridad ClearSky, dijeron que la campaña, denominada como CryptoCore, tenía como objetivo plataformas de intercambio en Israel, Japón, Europa y Estados Unidos, lo que resultó en el robo de criptomonedas por millones de dólares.

Los hallazgos son la consecuencia de juntar los artefactos de una serie de informes aislados pero similares detallados por F-Secure, CERT JPCERT/CC japonés y NTT Security durante los últimos meses.

Desde que aparecieron en escena en 2009, los hackers de Hidden Cobra utilizaron sus capacidades cibernéticas ofensivas para realizar espionaje y robos de criptomonedas contra empresas e infraestructura crítica.

El objetivo de los atacantes se alinea con los intereses económicos y geopolíticos de Corea del Norte, que están motivados principalmente por la ganancia financiera como un medio para eludir las sanciones internacionales.

En los últimos años, Lazarous Group ha ampliado más sus ataques para apuntar a las industrias de defensa y aeroespacial.

CryptoCore, también llamado CryptoMimic, Dangerous Password, CageyChameleon y Leery Turtle, no se diferencia de otras operaciones de Lazarous Group en que se centra principalmente en el robo de carteras de criptomonedas.

Según las investigaciones, la campaña comenzó en 2018 y el modus operandi implica aprovechar el spear-phishing como una ruta de instrusión para apoderarse de la cuenta del administrador de contraseñas de la víctima, usándola para saquear las claves de la billetera y

transferir las criptomonedas a una billetera del atacante.

El grupo ha robado aproximadamente 200 millones de dólares, según un informe de ClearSky publicado en junio de 2020, que vinculaba a CryptoCore con cinco víctimas ubicadas en Estados Unidos, Japón y Medio Oriente. Al conectar los puntos, las últimas investigaciones muestran que las operaciones se han extendido más de lo que se había documentado antes, al tiempo que evolucionan simultáneamente varias partes de su vector de ataque.

Una comparación de los indicadores de compromiso (IoC) de las cuatro divulgaciones públicas no solo encontró suficientes superposiciones de comportamiento y a nivel de código, sino que también ha planteado la posibilidad de que cada uno de los informes aborde distintos aspectos de lo que parece ser un ataque a gran escala.

Además, ClearSky dijo que reafirmó la atribución al comparar el malware implementado en la campaña CryptoCore con otras campañas de Lazarous Group y encontró fuertes similitudes.

> *«Este grupo ha pirateado con éxito numerosas empresas y organizaciones de todo el mundo durante muchos años. Hasta hace poco, no se sabía que este grupo atacara objetivos israelíes»,* dijeron los investigadores de ClearSky.