La Oficina Federal de Investigaciones (FBI) de Estados Unidos confirmó este lune que los hackers de Corea del Norte fueron responsables del robo de 100 millones de dólares en criptomonedas del Harmony Horizon Bridge en junio de 2022.

La agencia de aplicación de la ley atribuyó el ataque a Lazarus Group y APT38, el último de los cuales es un grupo de amenazas patrocinado por el estado de Corea del Norte que se especializa en operaciones cibernética financieras.

El FBI afirmó además que la intrusión de Harmony aprovechó una campaña de ataque denominada TradeTraitor que fue revelada por la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) en abril de 2022.

El modus operandi implicaba usar trucos de ingeniería social para engañar a los empleados de las empresas de criptomonedas para que descargaran aplicaciones no autorizadas como parte de un esfuerzo de contrataión aparentemente benigno.

> *«El viernes 13 de enero de 2023, los ciberactores norcoreanos usaron RAILGUN, un protocolo de privacidad, con el fin de lavar más de 60 millones de dólares en Ethereum (ETH) robados durante el atraco de junio de 2022. Una parte de este ethereum robado se envió posteriormente a varios proveedores de servicios de activos virtuales y se convirtió en bitcoin (BTC)»,* dijo el FBI.

Una parte de los fondos robados se congeló en coordinación con los proveedores de servicios de activos virtuales, mientras que se dice que el bitcoin restante se transfirió a 11 billeteras distintas controladas por los hackers.

Cabe mencionar que el movimiento de fondos relacionado con el hackeo de Harmony One fue descubierto por primera vez la semana pasada por un investigador de blockchain que usa el alias en línea ZachXBT. Según el fundador de Binance, Changpeng Zhao, se recuperaron 124 BTC (aproximadamente 2.84 millones de dólares) después de que se bloquearon las transferencias.

También se frustró un intento posterior de transferir los fondos a otra plataforma llamada Huobi, dijo Zhao en un tuit compartido el 16 de enero de 2023.

La plataforma de seguimiento criptográfico y antilavado de dinero MistTrack, en su propio análisis, reveló que las ganancias robadas se trasladaron de la cadena de bloques de Bitcoin a las redes de Avalanche, Ethereum y Tron a través de una ruta de cadena cruzada elegida para ofuscar el rastro.

Los robos de criptomonedas son una parte de una actividad cibernética maliciosa organizada por el organismo de inteligencia de Corea del Norte, la Oficina General de Reconocimiento, para generar ingresos sustanciales para la nación afectada por las sanciones mediante el robo de dinero de las instituciones financieras (FASTCash y BeagleBoyz).

El desarrollo también se produce en medio de una serie de ataques de ransomware dirigidos a DNV, el Ministerio de Obras Públicas y Transporte (MOPT) de Costa Rica, la Universidad de Duisburg-Essen y Yum! Brands en las últimas semanas.

Los datos recopiladores por la compañía de análisis de blockchain Chainalysis, muestran que los atacantes extorsionaron al menos 465.8 millones de dólares de las víctimas en 2022, por debajo de un máximo de 765 millones y 766 millones de dólares en 2020 y 2021, respectivamente.

> *«Sin embargo, eso no significa que los ataques hayan disminuido. En cambio, creemos que gran parte de la disminución se debe a que las organizaciones víctimas se niegan cada vez más a pagar a los atacantes de ransomware»,* dice un informe de la semana pasada.