El Buró Federal de Investigación de Estados Unidos (FBI) emitió una advertencia el martes, indicando que individuos vinculados a Corea del Norte podrían intentar convertir en efectivo criptomonedas robadas por un valor superior a los 40 millones de dólares.

La agencia encargada de hacer cumplir la ley atribuyó la actividad en la cadena de bloques a un adversario conocido por el gobierno estadounidense como TraderTraitor, que también responde al nombre de Jade Sleet.

Una investigación realizada por el FBI reveló que este grupo había transferido alrededor de 1,580 bitcoins obtenidos de diversos robos de criptomonedas durante las últimas 24 horas, y actualmente se dice que retiene esos fondos en seis billeteras distintas.

Es de conocimiento público que Corea del Norte suele confundir los límites entre la ciberguerra, el espionaje y delitos financieros. TraderTraitor, en particular, ha sido vinculado a una serie de ataques dirigidos contra cadenas de bloques y casas de cambio de criptomonedas con el propósito de saquear activos digitales y generar ingresos ilícitos para la nación, que se encuentra bajo sanciones internacionales.

Entre los ataques perpetrados se incluyen el robo de 60 millones de dólares en moneda virtual de Alphapo el 22 de junio de 2023; el robo de 37 millones de dólares en moneda virtual de CoinsPaid el 22 de junio de 2023; y el robo de 100 millones de dólares en moneda virtual de Atomic Wallet el 2 de junio de 2023, así como ataques dirigidos contra la Ronin Network de Sky Mavis y el Harmony Horizon Bridge el año pasado.

Este grupo de amenazas guarda similitudes con otro grupo norcoreano conocido como APT38 (también identificado como BlueNoroff o Stardust Chollima), que a su vez forma parte de la amplia constelación de Lazarus. El mes pasado, Mandiant, propiedad de Google, también relacionó a TraderTraitor con UNC4899, un equipo de piratas informáticos que se atribuye el hackeo de JumpCloud a finales de junio de 2023.

De acuerdo con los datos recopilados por TRM Labs, una firma especializada en inteligencia de cadenas de bloques, se estima que los hackers norcoreanos han sustraído más de 2,000

millones de dólares en criptomonedas desde 2018 en el contexto de aproximadamente 30 ataques, con un monto de 200 millones de dólares robados solo en 2023.

El FBI emitió un llamado a las entidades del sector privado para que examinen los datos en la cadena de bloques relacionados con estas direcciones y estén alertas para prevenir transacciones directas o indirectas con las mismas.