Masterhacks – Diversos gobiernos creen que el régimen de Kim Jong-un es sospechoso de una gran cantidad de ataques informáticos que tienen como finalidad recolectar bitcoins, revelando así un interés en la criptomoneda como vía para eludir su aislamiento económico y poder financiarse.

Expertos en seguridad informática y servicios de inteligencia de distintos países sospechan que Corea del Norte estuvo detrás de algunos ciberataques mundiales en los últimos años, incluido el virus WannaCry que afectó a sistemas de muchos países. Ahora, advierten sobre un malware parecido que amenaza a las monedas digitales.

Corea del Norte se interesó por el bitcoin en 2012, mucho antes de que su valor se elevara a niveles récord, según explicó el analista de ciberseguridad Simon Choi a EFE.

> Ese país *«ha creado desde entonces sus propias minas (sistemas informáticos para generar bitcoins) y casas de intercambio, y ha desarrollado varios programas malignos relacionados con el bitcoin e intentado hackear servicios internacionales de compraventa de criptomonedas»,* dijo Choi.
>
> *«Creemos que Corea del Norte ya se ha hecho con una cantidad significativa de bitcoins, aunque es imposible saber cuántos»,* agregó el experto.

Las últimas víctimas fueron cuatro casas de cambio surcoreanas de criptomonedas, las cuales sufrieron ataques entre abril y julio, y el rastro apunta a los mismos *«actores norcoreanos»* como sospechosos del hackeo masivo de bancos internacionales en 2016, según señaló un informe reciente de la compañía FireEye.

> *«Podríamos estar presenciando una segunda ola de esta campaña: actores con apoyo estatal que buscan robar bitcoins y otras divisas virtuales con vistas a eludir las sanciones y obtener monedas convertibles para financiar al régimen»,* señala el informe.

Los hackers utilizaron técnicas de *«spearphishing»,* por medio de correos electrónicos destinados a empleados de las casas de cambio.

Por otro lado, Kaspersky Lab señaló los *«vínculos directos»* entre Corea del Norte y el grupo hacker Lazarus, responsable de ataques como el que sufrió el Banco Central de Bangladesh en 2016, considerado como uno de los mayores robos informáticos de la historia, con un motín de 81 millones de dólares.

Ese mismo grupo de hackers es sospechoso de la propagación de WannaCry, virus que secuestró información de empresas e instituciones de más de 150 países el pasado mes de mayo.

Los hackers responsables del ataque pedían rescates en bitcoins para que las víctimas pudieran recuperar su información. El malware incluía partes del código idénticas al de ataques anteriores relacionados con Pyongyang.

Lazarus también se relaciona con el ataque que sufrió Sony Pictures a finales de 2014, luego del estreno de la película «The Interview», una comedia sobre el asesinato del líder Kim Jong-un.

En las investigaciones sobre WannaCry, los expertos encontraron direcciones IP de «comando y control» del software pertenecientes a organismos estatales norcoreanos, pero algunos analistas afirmaron que se podría tratar de una distracción de los creadores del virus para ocultar su rastro.

> *«Es muy difícil saber a ciencia cierta quién está detrás de todos estos ataques», dijo Choi, afirmando también que atribuir los ataques a Pyongyang «es sólo una conjetura, aunque basada en una enorme cantidad de datos y compartida por muchas organizaciones e investigadores".*

Según las estimaciones del analista, el monto total que Corea del Norte supuestamente pudo

haber obtenido por medio de los ataquesa cibernéticos desde 2011, es de cerca de 97 millones de dólares.