Los operadores asociados con el subgrupo BlueNoroff de Lazarus, fueron vinculados a una serie de ataques cibernéticos dirigidos a pequeñas y medianas empresas en todo el mundo, con el objetivo de robar sus fondos de criptomonedas, siendo esta otra operación motivada financieramente por el grupo patrocinado por el estado de Corea del Norte.

La compañía rusa de seguridad cibernética Kaspersky, que está rastreando las intrusiones bajo el nombre de «SnatchCrypto», dijo que la campaña se lleva a cabo desde 2017 y agregó que los ataques están dirigidos a nuevas empresas del sector FinTech ubicadas en China, Hong Kong, India, Polonia, Rusia, Singapur, Eslovenia, República Checa, Emiratos Árabes Unidos, Estados Unidos, Ucrania y Vietnam.

> *«Los atacantes han estado abusando sutilmente de la confianza de los empleados que trabajan en las empresas objetivo al enviarles una puerta trasera de Windows con todas las funciones de vigilancia, disfrazada como un contrato u otro archivo comercial. Para eventualmente vaciar la billetera criptográfica de la víctima, el actor ha desarrollado recursos extensos y peligrosos: infraestructura compleja, exploits e implantes de malware»*, dijeron los investigadores.

BlueNoroff y Lazarus, son conocidos por implementar un arsenal diverso de malware para un ataque múltiple contra las empresas para obtener fondos de forma ilícita, incluso confiar en una combinación de tácticas de phishing avanzadas y malware sofisticado, para las sanciones del régimen de Corea del Norte y generar ingresos para sus programas de armas.

En todo caso, estas ciberofensivas están dando sus frutos a lo grande. Según un nuevo informe publicado por la compañía de análisis de cadenas de bloques Chainalysis, el grupo Lazarus se ha relacionado con siete ataques a plataformas de criptomonedas que extrajeron casi 400 millones de dólares en activos digitales solo en 2021, frente a los 300 millones de dólares en 2020.

> *«Estos ataques se dirigieron principalmente a empresas de inversión y bolsas*

> *centralizadas, para desviar fondos de las billeteras «calientes» conectadas a Internet de estas organizaciones a direcciones controladas por la RPDC. Una vez que Corea del Norte obtuvo la custodia de los fondos, comenzaron un cuidadoso proceso de lavado para encubrir y retirar dinero a través de mezcladores para ocultar el rastreo»,* dijeron los investigadores.

La actividad maliciosa documentada que involucra al actor del estado-nación ha tomado la forma de atracos habilitados cibernéticamente contra instituciones financieras extranjeras, en particular los ataques a la red bancaria SWIFT en 2015-2016, con campañas recientes que resultaron en el despliegue de una backdoor denominada AppleJeus, que se hace pasar por una plataforma de comercio de criptomonedas para saquear y transferir dinero a sus cuentas.

Los ataques de SnatchCrypto no son diferentes en el sentido de que inventan elaborados esquemas de ingeniería social para ganarse la confianza de sus objetivos haciéndose pasar por firmas legítimas de capital riesgo, solo para usar como cebo a las víctimas para que abran documentos con malware que recuperan una carga útil diseñada para ejecutar un ejecutable malicioso recibido a través de un canal encriptado desde un servidor remoto.

Un método alternativo utilizado para desencadenar la cadena de infección es el uso de archivos de acceso directo de Windows (.lnk) para obtener el malware de la siguiente etapa, un script de Visual Basic, que luego actúa como punto de partida para ejecutar una serie de cargas intermedias antes de instalar una puerta trasera con todas las funciones que viene con capacidades *«enriquecidas»* para realizar capturas de pantalla, registrar pulsaciones de teclas, robar datos del navegador Chrome y ejecutar comandos arbitrarios.

Sin embargo, el objetivo final de los ataques es monitorear las transacciones financieras de los usuarios comprometidos y robar criptomonedas. Si un objetivo potencial usa una

extensión de Chrome como Metamask para administrar billeteras criptográficas, el adversario se mueve sigilosamente para reemplazar localmente el componente principal de la extensión con una versión falsa que alerta a los operadores cada vez que se inicia una transferencia grande a otra cuenta.

Para desviar los fondos, se realiza una inyección de código malicioso para interceptar y modificar los detalles de la transacción a pedido.

> *«Los atacantes modifican no solo la dirección de la billetera del destinatario, sino que también llevan la cantidad de moneda al límite, esencialmente vaciando la cuenta en un solo movimiento»,* explicaron los investigadores.

> *«Las criptomonedas son un sector muy objetivo cuando se trata de ciberdelincuencia debido a la naturaleza descentralizada de las monedas y al hecho de que, a diferencia de las tarjetas de crédito o las transferencias bancarias, la transacción se realiza rápidamente y es imposible revertirla»,* dijo Erick Kron, defensor de la conciencia de seguridad en KnowBe4.

> *«Los estados-nación, especialmente aquellos bajo aranceles estrictos u otras restricciones financieras, pueden beneficiarse enormemente al robar y manipular criptomonedas. Muchas veces, una billetera de criptomonedas puede contener múltiples tipos de criptomonedas, lo que las convierte en un* objetivo muy atractivo», dijo Kron.