El gobierno de Estados Unidos acusó este lunes a un sospechoso ucraniano, arrestado en Polonia el mes pasado, por implementar el ransomware REvil para apuntar a múltiples empresas y entidades gubernamentales en el país, incluyendo la compañía de software Kaseya.

Según los documentos judiciales no sellados, se alega que Yaroslav Vasinskyi, de 22 años de edad, formó parte de la operación de ransomware al menos desde marzo de 2019 y desplegó alrededor de 2500 ataques contra empresas en todo el mundo.

Vasinskyi, también conocido como Profcomserv, Rabotnik, Rabotnik_New, Yarik45, Yaraslav2468 y Affiliate 22, fue detenido en la frontera polaca el 8 de octubre luego de que se emitiera una orden de arresto internacional a instancias de las autoridades estadounidenses.

En otro hecho importante, el Departamento de Justicia reveló la incautación de 6.1 millones de dólares en supuestos pagos de ransomware recibidos por el ciudadano ruso Yevgeniy Polyanin, quien actualmente está prófugo y ha sido acusado de realizar ataques con el ransomware REvil contra múltiples empresas y entidades gubernamentales en Texas, que se remontan a 16 de agosto de 2019.

Vasinskyi y Polyanin fueron acusados de conspiración para cometer fraude y actividades relacionadas en conexión con computadoras, cargos sustanciales de daños a computadoras protegidas y conspiración para cometer lavado de dinero. Si son declarados culpables de todos los cargos, ambos acusados enfrentan una pena máxima de 115 y 145 años de prisión, respectivamente.

> *«El ransomware puede paralizar una empresa en cuestión de minutos. Estos dos acusados desplegaron algunos de los códigos más virulentos de Internet, creado por REvil, para secuestrar las computadoras de las víctimas. El Departamento profundizará en los rincones más oscuros de Internet y los confines más lejanos del mundo para rastrear a los delincuentes cibernéticos»,* dijo el fiscal federal interino

> Chad E. Meacham.

El último desarrollo se produce en medio de una oleada de actividad policial orquestada por Europol bajo la Operación GoldDust, que resultó en el arresto de otros seis afiliados de ransomware REvil, además de Vasinskyi en Rumania, Kuwait y Corea del Sur. Se cree que la banda de ransomware REvil ha ganado más de 200 millones de dólares desde que inició sus operaciones y cifró globalmente al menos 175 mil computadoras.

Coincidiendo con los arrestos, el gobierno de Estados Unidos también anunció que ofrece una recompensa de hasta 10 millones de dólares por información que lleve a la identificación o ubicación de los líderes claves detrás del ransomware REvil, además de pagar hasta 5 millones de dólares por información que conduzca al arresto o condena de personas, ubicadas en cualquier país, que participen en ataques con el ransomware REvil.

Además, el Departamento del Tesoro de Estados Unidos, impuso sanciones contra Chatex, un intercambio de criptomonedas, por *«facilitar transacciones financieras para los actores de ransomware»,* luego de una designación similar contra el intercambio de criptomonedas ruso SUEX en septiembre de 2021.

> *«El análisis de las transacciones conocidas de Chatex indica que más de la mitad están directamente relacionadas con actividades ilícitas o de alto riesgo, como los mercados de redes oscuras, los intercambios de alto riesgo y el ransomware. Chatex tiene vínculos directos con SUEX OTC, SRO (Suex), utilizando la función de Suex como un intercambio anidado para realizar transacciones»*, dijo el departamento.

Los arrestos y las sanciones son parte de un impulso mayor para luchar contra los ataques de

ransomware, que se han acelerado en frecuencia y escala este año, poniendo en riesgo infraestructura crítica y causando millones en daños, lo que llevó a las autoridades internacionales a responder de forma efectiva a tales intrusiones, al mismo tiempo que contrarresta el abuso de los canales de criptomonedas para lavar los pagos de rescate.