Autoridades ucranianas anunciaron este miércoles el arresto de la banda de ransomware Clop, agregando que interrumpieron la infraestructura utilizada en los ataques dirigidos a víctimas en todo el mundo desde al menos 2019.

Como parte de una operación conjunta entre la Policía Nacional de Ucrania y las autoridades de la República de Corea y Estados Unidos, seis personas fueron acusadas de ejecutar un esquema de doble extorsión en el que las víctimas que se niegan a pagar un rescate fueron amenazadas con la filtración de información financiera delicada, datos personales o datos de clientes robados antes de cifrar los archivos.

Los ataques de ransomware ascienden a 500 millones de dólares en daños monetarios, dijo la Policía Nacional, y agregó que *«la policía ha logrado cerrar la infraestructura desde la que se propaga el virus y bloquear los canales para legalizar las criptomonedas adquiridas de forma criminal».*

Al parecer, los agentes del orden realizaron 21 registros en la capital de Ucrania y la región de Kiev, incluidas las casas de los acusados y sus automóviles, lo que resultó en la incautación de equipos informáticos, automóviles y 5 millones de jrivnias (184,679 dólares).

Los presuntos delincuentes enfrentan hasta 8 años de prisión por cargos de interferencia no autorizada en el trabajo de computadoras, sistemas automatizados, redes de computadoras o redes de telecomunicaciones. Sin embargo, no está claro si las personas arrestadas son afiliadas o desarrolladores centrales de la operación de ransomware.

Desde que apareció en escena en 2019, el actor de amenazas Clop se ha relacionado con una serie de ataques de alto perfil como el de Accellion, Qualys, Software AG IT, ExecuPharm, Indiabulls, así como con varias universidades como la Universidad de Maastricht, Facultad de Medicina de la Universidad de Stanford, Universidad de Maryland y Universidad de California.

El desarrollo se produce cuando otro grupo de ransomware con el nombre de Avaddon cerró sus operaciones y entregó las claves de descifrado asociadas con 2934 víctimas a Bleeping Computer la semana pasada, probablemente en respuesta a un mayor escrutinio por parte

de las fuerzas del orden y los gobiernos de todo el mundo luego de una serie de ataques contra infraestructura crítica.