Un cibercriminal ruso buscado por Estados Unidos por su implicación en las operaciones de ransomware LockBit y Hive ha sido detenido por las autoridades en Rusia.

De acuerdo con un informe publicado por el medio ruso RIA Novosti, Mikhail Pavlovich Matveev enfrenta acusaciones de haber desarrollado un programa malicioso que cifraba archivos y exigía el pago de un rescate para obtener la clave de descifrado.

“El investigador ha reunido pruebas suficientes, y el caso penal, con la acusación formal firmada por el fiscal, ha sido remitido al Tribunal del Distrito Central de Kaliningrado para su evaluación y resolución”, informó el Ministerio del Interior de Rusia en un comunicado.

Matveev ha sido acusado bajo la Parte 1 del Artículo 273 del Código Penal de la Federación Rusa, que penaliza la creación, distribución y uso de software diseñado para causar *«destrucción, bloqueo, modificación o copia de información almacenada en sistemas informáticos».*

El gobierno estadounidense lo procesó en mayo de 2023, acusándolo de ejecutar ataques de ransomware que afectaron a *«miles de víctimas»* tanto en Estados Unidos como en otros países. Matveev también opera bajo seudónimos como Wazawaka, m1x, Boriselcin, Uhodiransomwar y Orange.

El propio Matveev ha admitido públicamente sus actividades ilegales, alegando que las autoridades locales las toleran mientras mantenga su lealtad a Rusia. Ha sido sancionado por el Departamento del Tesoro de los Estados Unidos, que también ofreció una recompensa de hasta 10 millones de dólares por información que facilitara su captura o enjuiciamiento.

Un informe reciente de la firma suiza de ciberseguridad PRODAFT indicó que Matveev lidera un equipo de seis especialistas en pruebas de penetración para llevar a cabo los ataques de ransomware.

Además de colaborar con grupos como Conti, LockBit, Hive, Trigona y NoEscape, Matveev ocupó un puesto de liderazgo en la organización de ransomware Babuk hasta principios de

2022. También se sospecha que mantiene vínculos estrechos con el grupo criminal ruso conocido como Evil Corp.

Esta detención ocurre poco después de que cuatro integrantes de la disuelta operación de ransomware REvil fueran condenados a varios años de prisión en Rusia tras ser declarados culpables de piratería informática y lavado de dinero.