Estados Unidos desmantela una red internacional de «ransomware»

El Departamento de Justicia de Estados Unidos anunció este jueves que desmanteló una red internacional de cibercriminales que hackeaban hospitales, colegios o firmas financieras para pedir rescates, una práctica conocida como «ransomware».

La banda, conocida como Hive, «extorsionó y trató de extorsionar cientos de millones de dólares a víctimas en Estados Unidos y en el resto del mundo», explicó en una rueda de prensa el fiscal general estadounidense, Merrick Garland.

Garland detalló que los criminales escogían como objetivos industrias e infraestructura críticas.

Como ejemplo, el responsable del Departamento de Justicia citó el caso de un hospital del medio oeste que fue atacado durante uno de los picos de la pandemia de covid-19. El ataque impidió al hospital aceptar nuevos pacientes y obligó a los trabajadores a utilizar copias en papel de la información que precisaban.

El ransomware es un tipo de programa informático que bloquea un sistema hasta que se paga una cantidad de dinero. En el caso del grupo Hive, los criminales robaban información sensible de las empresas u organismos que atacaban, tras lo que encriptaban sus sistemas y amenazaban con publicar la información.

El FBI, que logró infiltrarse en el grupo criminal, consiguió hacerse con las claves para desencriptar los sistemas y logró devolver el control de sus ordenadores a muchas víctimas a partir de julio de 2022, lo que previno el robo de 130 millones de dólares.

De momento, no se han anunciado arrestos, pero la página web donde Hive publicaba la información sensible que obtenía en sus golpes fue bloqueada por las autoridades.

En un comunicado, el FBI animó a las víctimas del grupo a que se pongan en contacto con su oficina regional correspondiente para recibir más información.

La operación se desarrolló en conjunto con las autoridades de Alemania y Países Bajos, además de recibir asistencia de parte de numerosas administraciones europeas.

EFE