

01/10/26

Un detenido en España en una operación internacional contra el grupo de ransomware KillSec

Resumen

El dispositivo se enmarca en una operación internacional, coordinada por Europol y Eurojust y con la participación del FBI, que ha finalizado con un total de tres detenidos y ocho entradas y registros en España, Grecia, Reino Unido y Rumanía

En España se ha practicado una detención a un menor de edad, y dos entradas y registros en la provincia de Alicante

La investigación española ha sido desarrollada por la Guardia Civil y los Mossos d'Esquadra en un Equipo Conjunto de Investigación

La operación internacional, coordinada con Europol y Eurojust, se dirige contra KillSec y su infraestructura criminal

Contenido

La Guardia Civil, a través del Departamento de Cibercrimen de la Unidad Central Operativa (UCO), y los Mossos d'Esquadra de la DIC han detenido en Alicante a un menor de edad de nacionalidad rumana, por su presunta participación en el grupo de ransomware KillSec. En la actuación se han practicado dos entradas y registros, en un domicilio y en una oficina de un establecimiento hotelero de la provincia de Alicante. Además, una mujer ha quedado como investigada por su presunta relación con los hechos.

En los registros se ha intervenido material informático, teléfonos móviles, carteras de criptoactivos y servicios de anonimización y cifraje de información relacionados con la presunta actividad delictiva del entramado. En un primer análisis, los investigadores han podido evidenciar transacciones correspondientes a pagos en forma de rescate por parte de algunas víctimas.

La investigación de la Guardia Civil, denominada Operación ROTOMA, se inició en 2025 a partir de la colaboración policial con el FBI de San Juan de Puerto Rico, orientada a identificar a personas relacionadas con KillSec que pudieran residir en España. Los investigadores de la UCO partiendo únicamente de una imagen de perfil, lograron identificar a uno de los administradores del grupo criminal que residía en la provincia de Alicante.

Por parte de Mossos d'Esquadra, el caso comenzó a partir de un ciberataque, presuntamente del grupo KILLSEC, contra una entidad catalana a principios de 2025. Según la investigación, los atacantes habrían accedido a los sistemas de la empresa, sustraído información sensible e intentado extorsionarla. Ante estos hechos, los especialistas de cibercrimen de la DIC de los Mossos d'Esquadra abrieron una investigación para esclarecer la autoría de la intrusión, la filtración de datos y el posterior intento de extorsión. Los daños ocasionados por este ciberataque ascenderían a cerca de un millón de euros.

La constitución de un Equipo Conjunto de Investigación entre ambos cuerpos permitió coordinar las pesquisas, identificar al sospechoso residente en España, ubicar su residencia y determinar tanto su presunto rol como principal administrador del grupo como su posible participación en el ataque cometido en Cataluña.

En las actuaciones en España se ha contado con el apoyo de especialistas de Europol y agentes de Bélgica, Alemania y Estados Unidos.

Una actuación internacional contra KillSec

La actuación española se integra en la operación internacional KillSwitch, desarrollada contra el grupo KillSec y coordinada con Europol y Eurojust. En la investigación han participado autoridades de Bélgica, Finlandia, Alemania, Grecia, Rumanía, España, Suiza, Reino Unido y Estados Unidos, con apoyo de las empresas de ciberseguridad Bitdefender y Group-IB.

Este grupo habría realizado más 1.000 ciberataques en todo el mundo, de los cuales unos 500 habrían tenido éxito con más de 280 víctimas, algunas habrían abonado rescates de alrededor de 500.000 euros en criptomonedas.

La actuación desarrollada ayer, permitió que las autoridades policiales y judiciales tomaron el control de la infraestructura de este grupo, incluyendo su página de filtraciones. Así mismo se han asegurado al menos 110 terabytes de datos. Durante la investigación también se pusieron bajo control policial cinco servidores centrales, se intervinieron dominios utilizados por el grupo y se actuó sobre evidencias, activos y posibles beneficios delictivos, incluidas criptomonedas.

Cómo actuaba el grupo

KillSec, activo aproximadamente desde 2024, accedía a sistemas de organizaciones mediante la explotación de vulnerabilidades y de puntos de acceso deficientemente protegidos, especialmente en entornos de almacenamiento en la nube. Sus integrantes copiaban información interna sensible y la trasladaban a infraestructura bajo su control.

Las víctimas eran identificadas en un sitio de filtraciones de la internet oscura y recibían amenazas de publicación de los datos sustraídos si no pagaban el rescate exigido. Cuando la víctima no pagaba, los archivos podían ponerse a disposición para su descarga gratuita. Los investigadores atribuyen a los sospechosos distintos cometidos, entre ellos los de administrador, desarrollador, negociador y afiliado.

Actuación contra servidores y activos criminales

La actuación coordinada se ha dirigido tanto contra las personas que presuntamente integraban KillSec contra los sistemas que utilizaban para llevar a cabo sus actividades. Las autoridades han practicado ocho registros domiciliarios en España, Grecia, Reino Unido y Rumanía, han efectuado tres detenciones y han intervenido pruebas y activos.

Durante la investigación, cinco servidores centrales han quedado bajo el control policial, incluyendo infraestructuras utilizadas presuntamente para gestionar las actividades del grupo y almacenar los datos sustraídos a las víctimas.

Las autoridades también han asumido el control de diversos dominios operados por KILLSEC y han redirigido los visitantes a un aviso oficial de intervención policial.

Los investigadores continúan examinando los dispositivos y los datos intervenidos, a la vez que rastrean los beneficios derivados de la actividad criminal del grupo, incluidos los activos en criptomonedas. Las pruebas obtenidas podrían permitir identificar nuevas víctimas, nuevos ataques y otras personas implicadas.

Qué es el ransomware

El ransomware es un tipo de malware o código malicioso que bloquea equipos o impide el acceso a la información, normalmente mediante su cifrado, y exige un rescate para recuperar los datos o evitar su destrucción o difusión. En modalidades de doble extorsión, los autores no solo bloquean la información, sino que también la sustraen y amenazan con publicarla para aumentar la presión sobre la víctima.

Este tipo de amenaza puede aprovechar vulnerabilidades o accesos mal protegidos y también propagarse mediante técnicas de ingeniería social, como enlaces o archivos adjuntos maliciosos. Su impacto puede comprometer información sensible y afectar a la continuidad de la actividad de las organizaciones.

Coordinación y continuidad de la investigación

La Joint Cybercrime Action Taskforce (J-CAT) ha coordinado a nivel policial las actuaciones con el apoyo del Centro Europeo contra la Ciberdelincuencia de Europol.

A nivel Judicial las investigaciones han sido coordinadas por Eurojust. Estas actuaciones han permitido asestar un importante golpe a uno de los grupos de Ciberdelincuencia organizado más activos.

Dado el volumen de información incautada, se continúan analizando los dispositivos y los datos intervenidos, rastreando los posibles beneficios delictivos e investigando a otros integrantes del grupo criminal, por lo que no se descartan nuevas actuaciones.