17/08/24

Detenido en España el líder de una importante red internacional de ciberdelincuencia

Resumen

Ha sido arrestado en la localidad malagueña de Estepona acusado de ser el creador y administrador de Ransom Cartel y de la creación y distribución de otros ransomware como CryptXXX o Cryptowall

El operativo fue dirigido por la Guardia Civil y participaron también agentes del Servicio Secreto y el FBI de Estados Unidos y la NCA de Reino Unido

Contenido

La Guardia Civil, en el marco de una operación internacional denominada ‘operación Seacatch’, ha detenido al líder de una red internacional de ransomware y malvertising. En la operación han formado parte tanto la National Crime Agency (Reino Unido) como el Servicio Secreto de Estados Unidos, la oficina del FBI de Kansas City (EEUU), el Servicio de Seguridad de Ucrania, la Policia Judiciaria de Portugal y la Oficina Central contra el Cibercrimen de Polonia.

La explotación de la operación se realizó de forma coordinada con detenciones y registros en España, Ucrania, Portugal y Alemania, en los que se obtuvo información sobre la organización criminal investigada. Además, Reino Unido trabajó con la policía de Singapur para localizar la infraestructura utilizada por Ransom Cartel.

La actuación en España permitió la detención de un hombre de 38 años en la ciudad malagueña de Estepona acusado de ser el creador y administrador de Ransom Cartel y de la creación y distribución de ransomware como CryptXXX o Cryptowall, entre otros. Sus lazos con el cibercrimen son conocidos al menos desde 2013, siendo un actor relevante en diferentes foros con nombres como “J.P. Morgan”, “xxx” y “lansky”.

También ha sido acusado de la difusión de Angler Exploit Kit y de millones de estafas derivadas de su uso mediante la instalación de malware en los dispositivos de las víctimas o redirección a páginas fraudulentas. Entre los malwares que más rédito proporcionó a la organización se encuentra Reveton, uno de los primeros en hacerse popular que bloquea el ordenador de la víctima y muestra una notificación que aparenta ser de un cuerpo policial. La organización pudo llegar a obtener así unos ingresos anuales de alrededor de 34 millones de dólares.

Hay una segunda persona investigada, también un hombre de 38 años, relacionado con la explotación del Angler Exploit Kit.

Este grupo criminal fue pionero en cuanto a la explotación de los modelos de “ransomware como servicio” y exploit kits. Fue así como se facilitó el crecimiento del cibercrimen haciéndolo accesible a personas sin conocimientos técnicos avanzados.

La investigación necesitó también una importante coordinación a nivel judicial, siendo recibidas en España comisiones rogatorias internacionales desde Estados Unidos y Reino Unido, con un papel clave de la Magistrada de Enlace española antes las autoridades de Estados Unidos.

Imágenes