Capturado venezolano en España líder de hackers más activos del mundo

La Policía Nacional ha detenido en Alicante al líder del aparato financiero de uno de los grupos hacktivistas más importantes del mundo, los ‘Kelvin Security’, con más de 300 ataques de alto nivel a sus espaldas contra sectores estratégicos de más de 90 países en los últimos tres años.

Los objetivos principales del grupo, según informa la Policía Nacional, son las infraestructuras críticas y las instituciones gubernamentales. Además de España, sus objetivos incluyen países como Estados Unidos, Alemania, Italia, Argentina, Chile y Japón.

Se dedican a explotar vulnerabilidades de entidades estratégicas para, una vez producida la intrusión, obtener credenciales de acceso y extraer información confidencial que posteriormente venden, a través de foros criminales de la dark web, una parte de Internet que permite que los usuarios oculten su identidad y ubicación de cara a otras personas y a los agentes de la ley.

Al arrestado, un ciudadano venezolano, se le imputan los delitos de pertenencia a organización criminal, revelación de secretos, daños informáticos y blanqueo de capitales. Se le considera el principal responsable del blanqueo del dinero obtenido por las actividades criminales del grupo hacktivista y operaba principalmente a través del intercambio de criptomonedas.

Este sábado por la mañana se puso a disposición del titular del Juzgado de Instrucción número 7 de Alicante, que ha decretado su ingreso en prisión.

La investigación comenzó hace dos años, cuando los agentes tuvieron conocimiento de sofisticados ciberataques sufridos en los sistemas informáticos de los Ayuntamientos de Getafe (Madrid) y Camas (Sevilla). Más tarde, lo fueron el Ayuntamiento de La Haba (Badajoz) y el Gobierno de Castilla-La Mancha.

Los expertos en ciberinvestigación detectaron que los ataques informáticos se reivindicaban por el grupo ‘Kelvin Security’, a través de foros cibercriminales clandestinos a los que se accede a través de la dark web en los que se vendían datos confidenciales exfiltrados, que eran valiosos para personas vinculadas a terceros países presentes en estos foros.

Los agentes comprobaron que el grupo aprovechaba vulnerabilidades en páginas web, software y en servicios de almacenamiento de información de instituciones y entidades pertenecientes a sectores estratégicos de todo el mundo para realizar una extracción masiva de información sensible de datos internos, clientes, trabajadores y usuarios.

Co información de 800 noticias