06/03/26

Operación internacional contra el foro de datos robados LeakBase

Resumen

Se trataba de uno de los principales foros de compraventa de datos personales procedentes, en gran medida, de bases datos de grandes compañías y de equipos domésticos infectados con diferentes tipos de malware, que eran empleados para fraudes, suplantaciones y ciberataques

En España se ha llevado a cabo una detención y dos registros en las provincias de A Coruña y Bizkaia en los que se ha intervenido numeroso material informático y documentación

Acumulaba más de 142.000 usuarios y funcionaba como mercado de bases de datos filtradas y credenciales robadas

Contenido

La Guardia Civil junto con Policía Nacional han participado en una operación internacional coordinada por Europol en 14 países contra el foro de datos robados conocido como LeakBase.

Se trataba de uno de los principales foros de compraventa de datos personales procedentes, en gran medida, de bases datos de grandes compañías y de equipos domésticos infectados con diferentes tipos de malware, que eran empleados para fraudes, suplantaciones y ciberataques, que contaba con más de 142.000 usuarios.

En España se ha llevado a cabo una detención y dos registros en las provincias de A Coruña y Bizkaia en los que se ha intervenido numeroso material informático y documentación.

Accesible desde la *clearweb* y activo desde 2021 contaba con contenido predominantemente en inglés, combinando elementos de un foro al uso, con elementos propios de un mercado, en el que se permitía la compra, venta e intercambio de datos personales.

Este foro aglutinaba gran cantidad de información, incluyendo pares de credenciales (correo electrónico y contraseña) que eran posteriormente utilizados para la comisión de nuevos hechos delictivos, como el robo de cuentas, fraudes o accesos ilícitos a sistemas informáticos.

La plataforma facilitaba la compraventa de contraseñas y datos personales para ser utilizados en fraudes, suplantaciones de identidad y ciberataques. Contaba con más de 142.000 usuarios registrados y operaba como un mercado clandestino de bases de datos filtradas y credenciales sustraídas.

El foro se había consolidado como un centro clave en el ecosistema del cibercrimen, especializado en el comercio de bases de datos filtradas y los llamados “stealer logs”, archivos de credenciales robadas mediante un programa malicioso de robo. LeakBase mantenía un amplio repositorio, en constante actualización, de bases de datos comprometidas, que abarcaban desde filtraciones antiguas hasta información recientemente vulnerada.

Operaba mediante un sistema interno que favorecía la generación de confianza entre los miembros y sostenía una activa comunidad clandestina. Entre sus normas internas destacaba la prohibición expresa de vender o publicar datos relacionados con Rusia.

En diciembre de 2025, LeakBase contaba con más de 142.000 usuarios registrados, cerca de 32.000 publicaciones y más de 215.000 mensajes privados, cifras que evidencian su dimensión y proyección internacional.

Entre los días 3 y 4 de marzo se llevaron a cabo actuaciones coordinadas en múltiples jurisdicciones que permitieron desarticular la operativa del foro y actuar contra sus usuarios más activos. Entre los países participantes se encontraban autoridades de Australia, Estados Unidos, Canadá, Bélgica, Alemania, Grecia, Kosovo, Malasia, Países Bajos, Polonia, Portugal, Rumanía, España y Reino Unido.

En la fase operativa, las autoridades realizaron actuaciones coordinadas en múltiples jurisdicciones, que incluyeron detenciones, registros domiciliarios e intervenciones directas conocidas como “knock-and-talk”. A nivel mundial se llevaron a cabo cerca de 100 operaciones y medidas dirigidas contra 37 de los usuarios más activos de la plataforma.

Una vez identificada la infraestructura del foro se analizó la actividad de sus usuarios cruzando la información con investigaciones en Europa y otros continentes. Los datos sensibles se compartieron de manera segura a través de la organización, lo que permitió a los investigadores vincular sospechosos, víctimas y pruebas digitales a nivel internacional.

En la sede de Europol en La Haya, se llevó a cabo un operativo de análisis de datos que reunió a especialistas para examinar rápidamente la información incautada e identificar los objetivos de mayor relevancia. Además, se estableció un Puesto de Mando Conjunto, que permitió a los países participantes compartir actualizaciones del operativo en tiempo real.

En España se identificaron dos usuarios con avanzados conocimientos técnicos que, presuntamente implicados en la investigación, habían implementado complejos sistemas de anonimización y desarrollado técnicas avanzadas para ocultar su huella digital y dificultar su localización.

Una vez identificados se llevó a cabo el arresto de uno de ellos, permaneciendo el segundo pendiente de localización y detención, y el registro de sus domicilios en las provincias de A Coruña y Bizkaia, donde los agentes intervinieron numeroso material informático y documentación.

Como parte de la investigación, las autoridades incautaron la base de datos del foro, lo que permitió la desanonimización de numerosos usuarios que creían operar de manera anónima. Los agentes continúan rastreando activamente las huellas digitales para identificar a más infractores y establecer sus identidades en el mundo real.

Esta operación también sirve como recordatorio de que, cuando se produce una filtración de datos, la información robada no desaparece automáticamente, sino que puede reaparecer en plataformas ilegales, donde podría ser utilizada para estafas, suplantaciones de identidad o intentos de acceso no autorizado a cuentas. Proteger los datos personales sigue siendo esencial. Emplear contraseñas fuertes y únicas, junto con la activación de la autenticación multifactor, ayuda a reducir significativamente los riesgos si la información se ve comprometida.