

México, vulnerable ante robo de datos; se ofertan en plataformas y foros de ciberdelincuentes

Traficantes de bases de datos que operan en sitios clandestinos como Injection Inferno, BreachForums y Forum leaks venden catálogos de información de millones de personas desde los mil hasta los más de 100,000 pesos, según su interés y el postor

Mario Camarillo Cortés
nacional@cronica.com.mx

Con ofertas que van de los mil a los más de 100,000 pesos, traficantes de bases de datos extraídos ilegalmente de sistemas informáticos, dispositivos móviles y redes de corporativos, presentan todos los días al mejor postor catálogos con datos privados de comerciantes, clientes de tiendas departamentales, instituciones financieras, aeropuertos, centros de espectáculos, entretenimiento y de sistemas de gestión de información de grupos corporativos y de dependencias del gobierno, sin que exista aún un programa que blinde en su totalidad la vulnerabilidad de información sensible y en muchos casos clasificada como de seguridad nacional

Piratas informáticos y plataformas de cibercriminales como Injection Inferno, BreachForums y Forum leaks, entre otros, venden a través de plataformas privadas o en foros de Telegram, datos de millones de clientes y usuarios de redes empresariales no solo en México sino del extranjero, lo que concierte a este delito en un cáncer digital difícil de erradicar.

Un foro que fue desmantelado en marzo de este 2026 es LeakBase, que contaba con unos 142,000 usuarios registrados y se dedicaba a la compra, venta e intercambio de bases de datos filtradas. Fue desarticulada tras un operativo de agencias de inteligencia internacionales coordinada por Europol en 14 países y derivó en detenciones, entre ellas la de su administrador en Rusia.

Reportes de Interpol, Ameripol (Comunidad de policías de América), de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) y de la OEA que colaboran con dependencias en México como la Unidad de Inteligencia Financiera y el Gabinete de Seguridad, refieren que todos los días está latente el robo de bases de datos con datos de millones de personas a través de programas maliciosos de Malware que utilizan software diseñados para infiltrarse, espiar y tomar el control de sistemas informáticos con nombres, teléfonos, correos electrónicos, datos bancarios y documentos de identidad que se ofertan y circulan en grupos de traficantes de datos en plataformas como Telegram, en foros de ciberdelincuentes o en la Dark Web, donde opera el mercado negro para la venta de información de empresas y gobiernos.

En septiembre pasado, la Secretaría Anticorrupción y Buen Gobierno informó que derivado de investigaciones contra la ciberdelincuencia, se identificó la circulación y venta de 13 millones de registros de ciudadanos mexicanos en la plataforma de Telegram, donde se exponía información privada y sensibles de ciudadanos y que presuntamente fueron sustraídos de Call centers.

Las secretarías de Hacienda y la de Anticorrupción resaltan que algunos de los puntos de filtración para la venta de bancos de datos se desarrolla en varios estados del país a través de la venta informal de chip de telefonía celular, toda vez que al no contar con vigilancia oficial tienen a su merced de manera fraudulenta, registros con datos de terceros como credenciales de Elector, CURP o datos biométricos de potenciales clientes quienes entregan sus datos para contar con una línea de celular, por lo que al no haber una responsabilidad directa en el resguardo de datos personales, la han llegado a ofrecer a delincuentes que la utilizan para delitos como extorsión o robo de identidad.

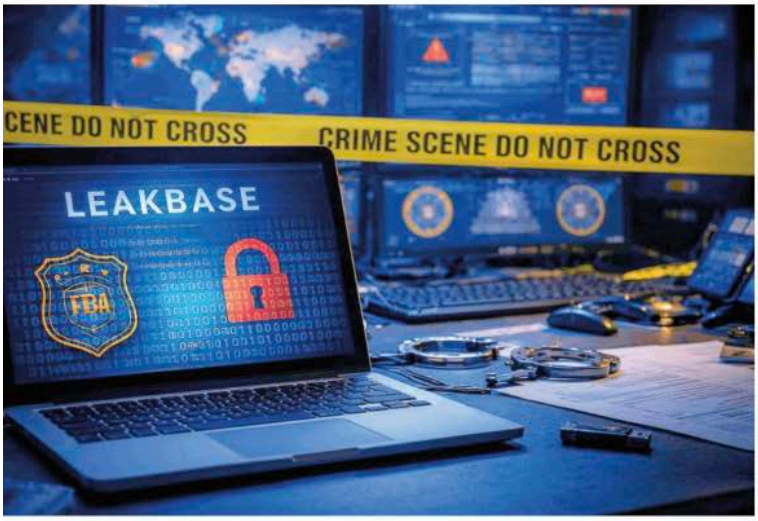
La Interpol y la UNODC coinciden en que las principales plataformas utilizadas en el mercado negro en México y en varios países de América Latina incluyen foros de ciberdelincuencia en la Dark Web, como BreachForums y motores de inteligencia de amenazas o repositorios de filtraciones.

Entre los traficantes de bases de datos identificados también por autoridades en México y que usan plataformas que aparecen y desaparecen según su interés, lo encabezan Injection Inferno, BreachForums y Forum leaks. Injection Inferno es un hacker que ve oportunidades para robar información sensible de empresas, bancos o dependencias de gobiernos.

Este traficante cibernético que aparece y desaparece de plataformas y foros clandestinos de internet ha acaparado la atención en México desde febrero de 2025, cuando puso a la venta al mejor postor en la dark web lo que denominó "La base de datos más grande de México", comprendida por un archivo de 701 GB con información sensible que incluía registros electorales, bancarios, fiscales, telefónicos, laborales, educativos, de salud e incluso propiedad privada.

Este hacker tiene presencia no solo en México sino en toda América Latina, y se detectó su presencia cuando en mayo de 2024 creó un canal de Telegram donde comercializaba bases de datos filtradas de empresas e instituciones de la región, centrando sus operaciones en México, Argentina, Perú, Chile y Brasil, destaca un estudio de la agencia de ciberseguridad Secure Soft Corporation.

Otro de los foros clandestinos identificados en México es Forum leaks, cuya plataforma de acceso https://bf.st/Forum-Official, da entrada a consultar las propuestas de venta de bases de datos de personas y empresas.



BreachForums, anteriormente conocida como RaidForums es otra plataforma de la Dark Web donde traficantes de datos publican y subastan bases de archivos de corporativos e instituciones y a lo que se puede acceder a través de la página https://web.archive.org/web/20220130172025/https://raidforums.com/misc.php?action=help&hid=24.

En México, de acuerdo con información de la secretaría de Hacienda y Crédito Público (SHCP), a través de la Unidad de Inteligencia Financiera (UIF) y brigadas de ciberinteligencia, han identificado y sancionado redes operativas mediante el rastreo de acciones atípicas y cuentas bancarias ligadas a extorsión y fraude cibernético. Sin embargo, la investigación directa que se lleva a cabo sobre la comercialización ilegal de bases de datos suele enfocarse en desmantelar las redes de llamadas fraudulentas, a través de los Call centers o congelamiento de sus flujos financieros, más no en la clasificación pública de estos hackers.

Agencias especializadas en ciberseguridad aseguran que la sobreoferta de datos ha abaratado estos paquetes y facilita que pasen de unas manos a otras, donde incluso se han detectado archivos con miles de datos de usuarios que se ofertan hasta en mil pesos. En México, de acuerdo con instituciones que integran el Gabinete de Seguridad, la plataforma más recurrente y accesible donde se ofertan bases de datos es Telegram, por medio de canales privados y grupos de compraventa clandestinos.

TAFICANTES INTERNACIONALES

A nivel internacional y donde no se descarta que estén circulando bases de datos extraídos en México destacan XSS, un foro ruso de ciberdelincuencia más seguido, le siguen Exploit.in, foro de ciberdelincuencia ruso que funciona como un punto de encuentro y mercado negro digital para hackers.

En la misma lista aparecen la estadounidense BreachForums; RAMP (Ransomware Anonymous Market Place) de origen ruso; LeakBase, sin origen definido y que fue desmantelado en marzo de 2026; DarkForums, sin país de origen definido; BHF (Black Hat Forum), de origen ruso; Altenen, sin origen definido y asociado a discusiones relacionadas con el fraude; Dread, opera sin sitio exclusivo como centro comunitario de la Dark Web y Niflheim, identificada como una plataforma de los Nueve Mundos de la cosmología nórdica.

En este mismo punto, Interpol y Naciones Unidas destacan que las naciones con mayor número de casos en robo y venta de datos corporativos y de clientes de empresas y comercios lo encabeza Estados Unidos, al ser el mercado más grande del mundo para la industria de los data brokers (agentes o corredores de datos).

En América Latina el líder en este delito es Brasil, seguido por México, Argentina, Colombia, Chile y Perú, naciones que concentran la mayor parte del tráfico de comercio electrónico y de actividad digital en la región, lo que los convierte en blanco fácil tanto de campañas de marketing agresivas como de filtraciones y venta clandestina de bases de datos.

En el caso de naciones de Asia y Europa del Este, los países que destacan por la presencia de traficantes de datos lo encabeza India, Sudáfrica, Rusia, España y Francia, entre otros.

COMPRADORES

Instituciones del Gabinete de Seguridad, a través del Centro Nacional de Respuesta a Incidentes Cibernéticos, refieren que grupos delictivos son los principales clientes que buscan y compran estos lotes de información para montar campañas de correo masivo o mensajes SMS personalizados (smishing). Una vez con este catálogo masivo son puestos en exhibición en foros clandestinos se manejan ofertas a manera de subasta sin importar los postores.

En esta lista se suman empresas informales de telemarketing o Call center, despachos de cobranzas y vendedores de servicios de dudosa procedencia. Asimismo, grupos del crimen organizado también figuran entre los principales compradores de estas bases de datos que las adquieren los registros para mapear el patrimonio de potenciales víctimas de ciertos sectores de la población para planear asaltos o secuestros.

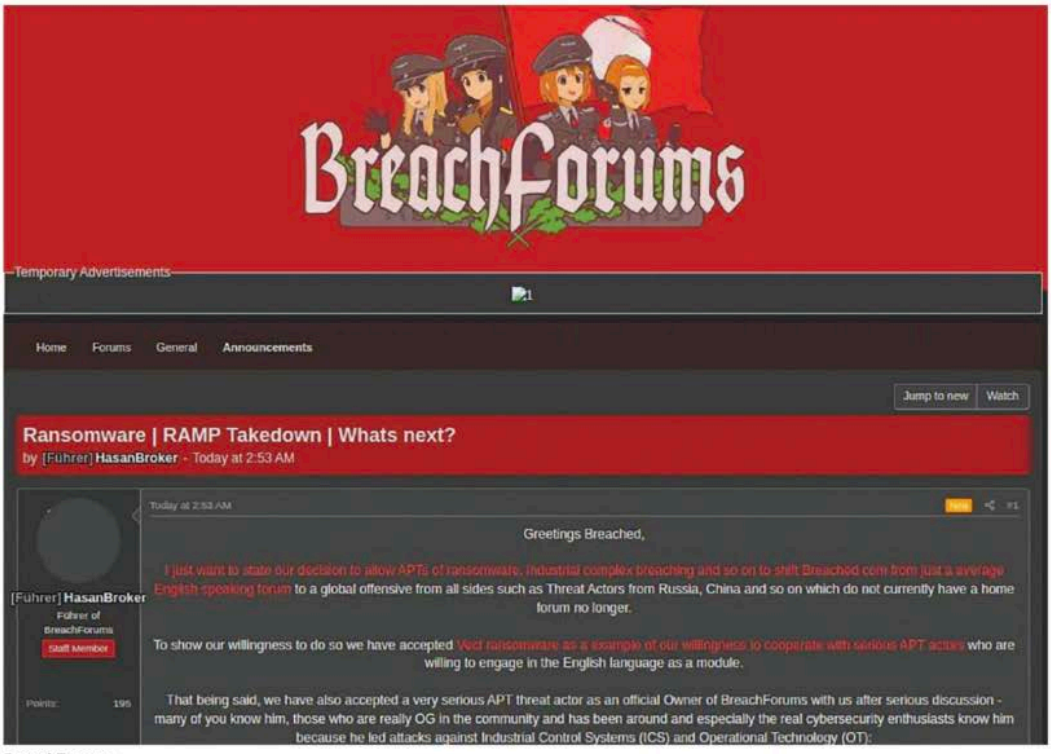
Reportes de la empresa especializada en ciberseguridad TecnetOne, revela que piratas informáticos han echado mano de un Shadow#reactor, una operación sofisticada diseñada para desplegar Remcos RAT o virus troyanos de acceso remoto que permite a los atacantes tomar el control total de los sistemas infectados.

El estudio esta agencia revela que al menos 118 dependencias del Gobierno Federal presentan condiciones de vulnerabilidad ene sus tres niveles, lo que las coloca dentro una amenaza sistémica, capaz de afectar a instituciones en todo su sistema.

SIN GARANTÍAS

Aunque el marco jurídico mexicano es sólido, las leyes por sí mismas son herramientas preventivas, sancionatorias y regulatorias contra el delito de robo y venta de datos personales, pero no constituyen una barrera técnica impenetrable contra hackeos, filtraciones o corrupción interna, por lo que en términos estrictos, no existe una garantía absoluta del 100% de que las leyes de protección de datos personales impidan que la información digital o física llegue al mercado negro en México.

En México está vigente la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), medida que obliga a las empresas y negocios privados para recabar, almacenar y proteger la información de sus clientes, al contar con medidas de seguridad administrativas, técnicas y físicas. Sin embargo, y pese a que existen sanciones con multas y cárcel, el robo masivo de información sigue vigente•



BreachForums