LITORALPRESS

Fecha: 02-02-2026
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: **Reporte de Entel Digital alerta alza de ransomware, filtración de datos y ciberespionaje en 2025**

Pág. : 20
Cm2: 610,4

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

En Chile casi se triplicaron las víctimas por datos filtrados, en un escenario marcado por amenazas más silenciosas, persistentes y sofisticadas.

Reporte de Entel Digital alerta alza de ransomware, filtración de datos y ciberespionaje en 2025

POR MARCO ZECCHETTO

La seguridad informática en Latinoamérica y el mundo enfrenta un cambio relevante, marcado por nuevas formas de ataque silenciosas, el avance del *ransomware* (secuestro de datos), el aumento en las filtraciones de datos, y la expansión de grupos organizados de ciberespionaje.

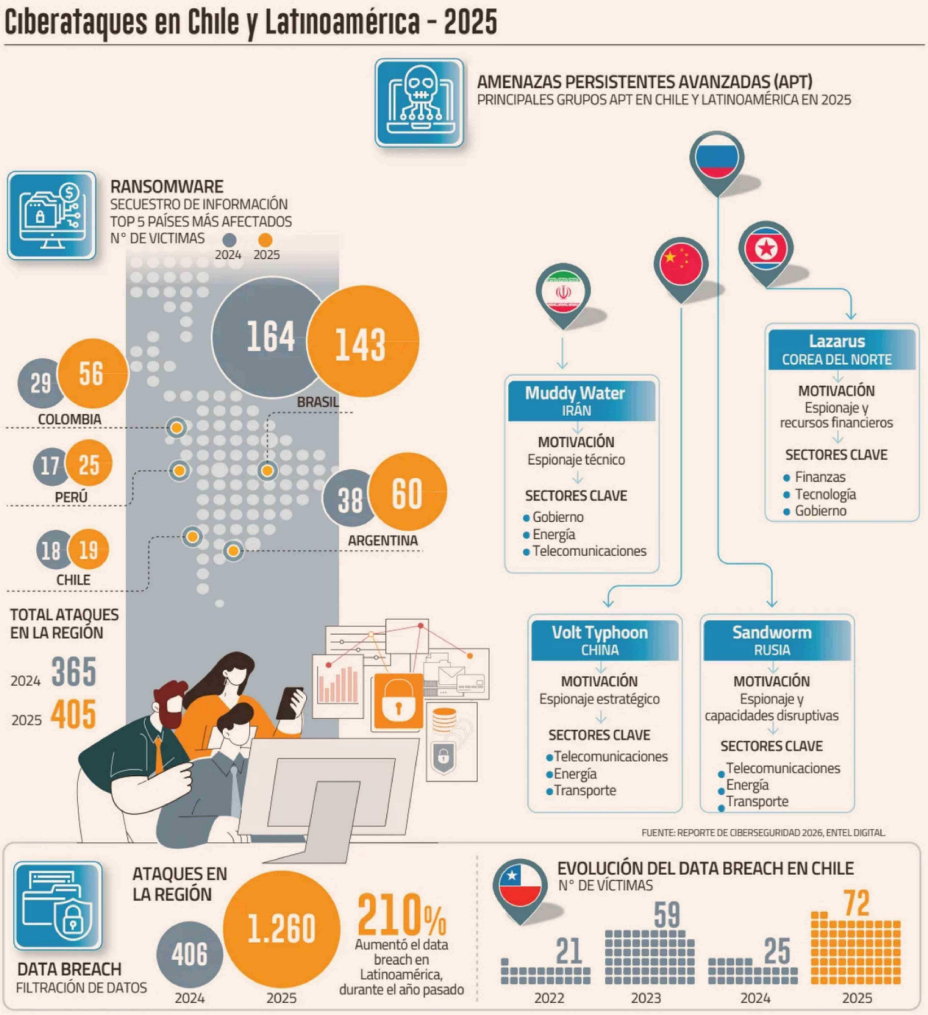
A ello se suma una mayor sofisticación de los atacantes, el uso de inteligencia artificial (IA) y una ampliación de las superficies de ataque, especialmente en entornos digitales críticos. Así lo señaló el Reporte de Ciberseguridad 2026, elaborado por el Centro de Ciberinteligencia (CCI) de Entel Digital.

El documento alertó que durante 2025 se perfilaron 138 grupos de ciberactores a nivel global, un 20% más que los 115 identificados en 2024. Esto incluye desde organizaciones de *ransomware* -como Qilin y Akira- hasta grupos de amenazas persistentes avanzadas (APT), varios de ellos vinculados a Estados como China y Rusia, orientados al ciberespionaje y a ataques contra gobiernos e infraestructuras críticas.

En esa línea, el director del CCI de Entel Digital, Eduardo Bouillet, explicó que el *ransomware* "sigue y seguirá siendo" una de las principales amenazas a nivel global y regional, aunque advirtió que hoy converge con otros actores y técnicas de robo de información que "no levantan sospechas inmediatas" y elevan el nivel de riesgo.

También apuntó al rol de la IA como un "amplificador" de las capacidades ofensivas, permitiendo campañas más automatizadas, hiperpersonalizadas y difíciles de detectar.

En Latinoamérica, se registraron 405 ataques de *ransomware* durante 2025, un 11% más que en 2024.



Por países, Brasil se mantuvo como el más afectado, con 143 ataques, seguido por Argentina (60), Colombia (56), Perú (25) y Chile (19). Nuestro país mejoró su posición regional, tras haber ocupado el cuarto lugar en 2024.

Bouillet indicó que este comportamiento responde, en parte, a la consolidación del *ransomware* como industria criminal, con modelos de negocio estructurados y tácticas de doble y triple extorsión, donde los atacantes no solo cifran información, sino que además roban datos y presionan a las víctimas con su eventual filtración.

Según el reporte, este fenómeno se ha visto reforzado por los *brokers* de acceso inicial, intermediarios ilícitos que comercializan accesos no autorizados y facilitan el ingreso de grupos criminales a redes y sistemas en las organizaciones.

Filtración de datos y espionaje

Uno de los hallazgos más relevantes del reporte fue la fuerte alza de las filtraciones de datos en la región. Durante el año pasado, este tipo de ataques en Latinoamérica aumentaron un 210%, y en Chile las víctimas casi se triplicaron, pasando de 25 casos en 2024 a 72 en 2025.

Bouillet explicó que esto se debió a la ingesta de datos desde nuevas fuentes y también a la venta ilegal de accesos a través de *infostealers*, programas maliciosos (*malware*) que "utilizan las malas prácticas de los usuarios" para robar credenciales y comercializarlas.

Por otro lado, el documento advirtió sobre la presencia de grupos APT en la región, como Volt Typhoon (China), Sandworm (Rusia) y Lazarus (Corea del Norte), cuyo modus operandi está orientado al espionaje a través de accesos "ocultos" y persistentes en redes estratégicas durante largos períodos, con el objetivo de recopilar información sensible y prepararse para efectuar interrupciones futuras a infraestructuras críticas.

El reporte indicó que estos actores también son capaces de aprovechar las vulnerabilidades en redes físicas conectadas a internet, como sistemas de control industrial, y su foco en Chile son los sectores de banca, Gobierno, salud, servicios tecnológicos y telecomunicaciones.

Ante esto, el informe destacó la necesidad de que los Operadores de Importancia Vital -servicios esenciales críticos para el funcionamiento del país- bajo la Ley Marco de Ciberseguridad "maduren sus capacidades en gobernanza, arquitectura, operación y ciberdefensa industrial".

Entre los riesgos emergentes para infraestructuras críticas en 2026 y 2027, el reporte destacó el uso de IA para la identificación automática de vulnerabilidades en redes industriales; *malware* para borrar configuraciones industriales; la explotación de la nube e interfaces de programación de aplicaciones (API); amenazas de interferencia en servicios satelitales; y el aumento de organizaciones "semi estatales" que operan como "mercenarios digitales", combinando espionaje y monetización.