DIARIO FINANCIERO®

Fecha: 27/02/2026 Audiencia: 40.297 Sección: CIENCIA Y TECNOLOGIA
Vpe: $5.857.619 Tirada: 13.432 Frecuencia: 0
Vpe pág: $8.127.680 Difusión: 13.432
Vpe portada: $21.104.600 Ocupación: 72,07%

Las organizaciones cibercriminales que están espiando a Chile y Latinoamérica

POR LAURA FLORES

■ Grupos vinculados a China, Rusia y Corea del Norte concentraron operaciones de ciberespionaje en sectores estratégicos como telecomunicaciones, energía y banca en la región.

El ciberataque de la organización criminal Salt Typhoon, vinculada a China, operó por más de un año sin ser detectado hasta 2024 y afectó a más de 80 redes telefónicas a nivel global, informó The New York Times el 4 de septiembre de 2025. Entre ellas, grandes compañías estadounidenses de telecomunicaciones como AT&T y Verizon.

A raíz de estos incidentes, el 19 de junio de 2025 la entidad gubernamental *Canadian Centre for Cybersecurity* (Centro Canadiense para la Ciberseguridad, en español) publicó un informe en su sitio web en el que señaló que las empresas de telecomunicaciones son el principal objetivo de la organización global de ciberespionaje de actores chinos, aunque no descartó que también se dirijan a otros sectores.

Este escenario enciende las alertas sobre el uso de las capacidades cibernéticas chinas en Latinoamérica y en Chile.

Según el investigador de seguridad informática de ESET, Mario Micucci, en 2023 comenzaron a detectarse campañas de ciberespionaje de grupos chinos, como Volt Typhoon, Nylon Typhoon, Mustang Panda y APT41.

En su mayoría se trata de grupos APT (Amenaza Persistente Avanzada), organizaciones criminales estructuradas, muchas veces respaldadas por actores estatales o grandes grupos criminales, que buscan acceder a redes informáticas y sistemas críticos, manteniendo una presencia continua en el tiempo, utilizando métodos de *malware* -programa o código- diseñado para infiltrarse, dañar, espiar o tomar el control de sistemas.

Micucci dijo que los APT que operan en Latinoamérica "son variados", y destacó la presencia de organizaciones de Corea del Norte, como Lazarus, y de China, como Famous Sparrow o Evasive Panda, "cuyos objetivos son gobiernos y grandes empresas".

El ejecutivo advirtió que estos ataques pueden comprometer la seguridad nacional e internacional de la región, ya que se dirigen a "las infraestructuras críticas de los Estados, como, por ejemplo, empresas hidroeléctricas o en defensa".

Según la sexta edición del Reporte de Ciberseguridad 2026 de Entel Digital, los actores más relevantes en materia de ciberespionaje y con un accionar de alto riesgo en Latinoamérica son Volt Typhoon (China), Sandworm (Rusia) y Lazarus (Corea del Norte), y sus principales blancos de ataque son los sectores de energía, transporte, gobierno, finanzas, banca y telecomunicaciones. Sus motivaciones apuntan al espionaje estratégico, capacidades disruptivas y recursos financieros.

El director del Centro de Ciberinteligencia de Entel Digital, Eduardo Bouillet, afirmó que en la región "lo dominante sigue siendo el cibercrimen con motivación económica, con *ransomware* (secuestro de datos) y filtraciones de datos, con grupos como LockBit, Akira, Qilin, SafePay y RansomHub", pero la presencia directa o indirecta de actores APT "ya es parte del mapa de operación" y dijo que estos grupos están "orientados a telecomunicaciones e infraestructura crítica".

> "En Chile y Perú buscan acceso profundo y persistente sobre operadores críticos y dependencias tecnológicas".

Explicó que los grupos APT tienen motivaciones geopolíticas y de inteligencia, con ataques e infiltraciones a "gobiernos, defensa, telecomunicaciones, energía, transporte y servicios esenciales, incluyendo el acceso por las cadenas de suministro", es decir, a través de los servicios de nube, proveedores de software y otros tipos de prestadores de servicios a organizaciones.

También comentó que el reporte de Entel Digital apunta a que "en Chile y Perú buscan acceso profundo y persistente sobre operadores críticos y dependencias tecnológicas", con objetivos geopolíticos y económicos.

Chile: riesgo "plausible"

Bouillet explicó que el riesgo de ciberespionaje en Chile "es plausible", ya que "buscan acceso persistente y preposicionamiento en infraestructura crítica y cadena de suministro". Además, advirtió que "los accesos pueden ser indirectos, explotando dependencias en telecomunicaciones y servicios de *cloud*".

Detalló que estas APT pueden ocurrir en Chile a partir del accionar de terceros, proveedores o tecnología expuesta, más que por un ataque frontal.

En tanto, el analista político y profesor de la Universidad de Valparaíso, Guillermo Holzmann, se refirió a la falta de desarrollo en materia de ciberseguridad en Chile: "Se habla mucho de ciberseguridad, pero hay muchas empresas- e incluso desde el propio Estado- que están bastante atrasadas al respecto".

Holzmann agregó "que las oportunidades para poder ingresar a los sistemas son altas" y que un eventual ataque podría afectar la seguridad nacional e internacional.

"En el caso de Chile, claramente, es importante poder ingresar a ver todos los proyectos o todas las cosas, y eso interesa tanto a Estados Unidos, a países europeos y a China (...) Y la instalación de *malware* o de cualquier tipo de software para poder sacar la información sin que se note, existe, o sea, dada la posición que tiene el país, es sin lugar a duda, de mucho interés", comentó.

La IA como acelerador de riesgo en 2026

Bouillet de Entel Digital también abordó el uso de la inteligencia artificial (IA) en la región y señaló que "lo que viene es la IA acelerando el ataque", con métodos más creíbles, como *phishing* (robo de identidad) masivos, automatización de etapas con IA agéntica y ataques más rápidos en la cadena de suministro de proveedores.

Estos avances, explicó, "reducen tiempos de intrusión y aumentan la precisión táctica, especialmente contra usuarios y proveedores tecnológicos".

Y agregó que en Latinoamérica se verán campañas "mejor diseñadas, más baratas de ejecutar y más difíciles de atribuir" con más velocidad y más escala en los ataques, "por lo que la resiliencia y la preparación dejan de ser opcionales".