DIARIO FINANCIERO®

Fecha: 11/03/2026 Audiencia: 40.297 Sección: ECONOMIA
Vpe: $3.770.228 Tirada: 13.432 Frecuencia: 0
Vpe pág: $5.442.800 Difusión: 13.432
Vpe portada: $21.104.600 Ocupación: 69,27%

Google detecta grupo de ciberespionaje ligado al gobierno chino y sospecha que opera en Chile

■ La gigante tecnológica tomó medidas para neutralizar a la entidad llamada UNC2814, activa desde 2017.

POR VALERIA IBARRA

La tercera semana de febrero, pocos días antes de que estallara la polémica por el cable submarino de fibra óptica que China Mobile intentó, infructuosamente, construir entre Concón y Hong Kong, el Google Threat Intelligence Group (GTIG) en conjunto con la filial de ciberseguridad Mandiant -que es parte de Google Cloud- tomó medidas para desmantelar una campaña de espionaje dirigida a organizaciones gubernamentales y de telecomunicaciones en "docenas de países de cuatro continentes".

En un informe difundido una semana después, el 25 de febrero de este año, Google aseguró que "el actor de amenazas, UNC2814, es un presunto grupo de ciberespionaje con nexo con la República Popular China, al que GTIG ha rastreado desde 2017".

Este conjunto de hackers, "prolífico y escurridizo", según la estadounidense, "tiene un largo historial de ataques a gobiernos internacionales y organizaciones globales de telecomunicaciones en África, Asia y América, y había confirmado intrusiones en 42 países cuando se produjo la interrupción". Y entre los países donde hay evidencia o sospecha de ataques está Chile (**ver mapa**).

La subsidiaria local del conglomerado Alphabet Inc. confirmó el reporte y aseguró que es parte del monitoreo continuo que hace la tecnológica a sus instalaciones y servicios.

Como esta alerta coincidió con la denuncia de la Embajada de Estados Unidos en Chile, liderada por Brandon Judd, de que se habían vulnerado las telecomunicaciones en nuestro país y que esta filtración también afectó a una compañía constructora, **DF** consultó a esta delegación diplomática sobre dicho informe.

En la delegación norteamericana señalaron que "como norma, la Embajada no proporciona detalles sobre reuniones que sus diplomáticos sostienen o han sostenido con funcionarios del gobierno, esto es en cuanto a contenido como a fechas". Tampoco se refirieron al reporte.

También se requirió a la embajada de China en Santiago, la que declinó entregar oficialmente una opinión. Sin embargo, fuentes diplomáticas de Beijing en el país dijeron que "hay ciberataques de origen estadounidense por todo el mundo, incluso contra autoridades de países aliados, sin ninguna explicación o declaración del país norteamericano".

Sobre el reporte de Google y el grupo UNC2814, la embajada dijo que "no tenemos la obligación de contestar a acusaciones sin fundamentos o desde un origen sospechoso".

También se le pidió su parecer al saliente subsecretario de Telecomunicaciones, Claudio Araya, quien dijo no conocer el reporte en cuestión.

Cómo actuó y qué buscaba

Según Google, el grupo UNC2814 utilizaba llamadas a la API (interfaz de programación de aplicaciones) para comunicarse con otras aplicaciones de *software* de servicios como aquellas de infraestructura de comando y control "para camuflar su tráfico malicioso como benigno, una táctica común utilizada por los actores de amenazas para mejorar el sigilo de sus intrusiones".

Así, "en lugar de aprovechar una debilidad o fallo de seguridad, los atacantes se basan en productos alojados en la nube para funcionar correctamente y hacer que su tráfico malicioso parezca legítimo", aseguró la compañía liderada por Sundar Pichai.

Para hacer frente a esta disrupción, la tecnológica estadounidense dijo que "se cancelaron todos los proyectos de Google Cloud controlados por el atacante, cortando así su acceso persistente a los entornos comprometidos".

Países con sospecha o confirmación de ser víctimas del grupo de ciberespionaje UNC2814

FUENTE: GOOGLE THREAT INTELLIGENCE GROUP Y MANDIANT

"En lugar de aprovechar una debilidad o fallo de seguridad, los atacantes se basan en productos alojados en la nube para funcionar correctamente y hacer que su tráfico malicioso parezca legítimo", aseguró la gigante tecnológica estadounidense.

También, detalló que "se identificó y desactivó toda la infraestructura UNC2814 conocida", así como la cuenta del grupo atacante. Se tomaron medidas adicionales y Google destacó que pudo repeler la agresión porque la filial de seguridad Mediant había investigado el modus operandi de este grupo.

La gigante tecnológica enfatizó que el grupo chino pudo atacar no por "vulnerabilidad de seguridad en los productos de Google, sino que abusa de la funcionalidad legítima" de las aplicaciones.

"Hasta el 18 de febrero, la investigación de GTIG confirmó que UNC2814 había afectado a 53 víctimas en 42 países de cuatro continentes e identificó infecciones sospechosas en al menos 20 países más", dijo Google.

Según el especialista en ciberseguridad y ciberdefensa, Juan Roa, grupos como UNC2814 buscan infiltrarse en compañías que proveen servicios de telecomunicaciones con el objetivo de capturar y analizar tráficos y obtener información de carácter confidencial para acceder de manera ventajosa a negocios (licitaciones, contratos, etc.) o copiar avances tecnológicos de terceros. A su juicio, rara vez buscan realizar secuestros de datos con fines extorsivos.

Este ejecutivo de seguridad de información y ciberseguridad señala que existen grupos similares en casi todos los países con la capacidad de realizar guerras cibernéticas, como Estados Unidos, Corea del Norte, Israel, Irán, Rusia y China, entre otros.

Otros ataques

De acuerdo a los expertos, estas vulneraciones de seguridad son pan de cada día. Sin ir más lejos, el 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, entre ellas, a compañías estadounidenses como AT&T y Verizon.

La Canadian Centre for Cybersecurity, en un reporte de 2025, señaló que las empresas de telecomunicaciones son el principal objetivo de las entidades de ciberespionaje chino, aunque no descartó que también se dirijan a otros sectores. En su mayoría se trata de grupos APT (Amenaza Persistente Avanzada), que buscan acceder a redes informáticas y sistemas críticos, manteniendo una presencia continua en el tiempo para infiltrarse, dañar, espiar o tomar el control de sistemas.