LITORALPRESS

Fecha: 28-01-2026
Medio: El Mercurio
Supl. : El Mercurio - Chile Tecnológico
Tipo: Noticia general
Título: Estudio identifica fallas en la protección de comunicaciones vía satélite

Pág. : 4
Cm2: 758,8

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

CIFRADO DE EXTREMO A EXTREMO Y UNA GESTIÓN MODERNA DE CLAVES EVITA RIESGOS:

Estudio identifica fallas en la protección de comunicaciones vía satélite

En Chile, los enlaces GEO se utilizan en defensa y soberanía, infraestructura crítica y grandes empresas. Expertos consultados explican que la entrada en vigencia de la Ley Marco y la creación de la Agencia Nacional de Ciberseguridad establecen un marco que mejora las exigencias.

RICHARD GARCÍA

Una serie de vulnerabilidades en las comunicaciones vía satélites geoestacionarios (GEO) se expusieron recientemente en la Annual Computer Security Applications Conference (ACSAC), en Honolulu, Hawái, una de las principales conferencias en seguridad informática.

La investigación, desarrollada por equipos de la Universidad de Maryland y de California, documentó la existencia de enlaces que transmiten información y que pueden ser interceptados con equipamiento comercial de bajo costo. El análisis se concentró en satélites GEO (aquellos que permanecen fijos respecto de la superficie terrestre) y no en constelaciones de órbita baja, más conocidos como LEO.

Los autores descubrieron que al apuntar una antena comercial al cielo y analizar el espectro es posible observar tráfico que incluye llamadas, mensajes y comunicaciones internas de empresas y organismos estatales. El punto crítico, apuntaron los expertos, no es la posibilidad de captar una señal satelital —algo técnicamente posible desde hace décadas—, sino que parte de ese tráfico de datos viaje sin estar cifrado o protegido, permitiendo que la información sea interceptada.

Para obtener estos resultados construyeron un escáner universal de satélites GEO utilizando equipamiento comercial estándar, capaz de barrer el cielo en busca de satélites visibles, identificar los transpondedores disponibles (canales satelitales) en cada uno y decodificar con precisión paquetes IP desde cada transpondedor.

El monitoreo se prolongó durante siete meses en forma ininterrumpida, tiempo durante el cual los investigadores pudieron recabar datos desde 411 transpondedores. Durante ese tiempo pudieron obtener información desde el sector industrial, organismos gubernamentales e infraestructura crítica.

Un portavoz de T-Mobile reconoció al medio estadounidense CNET que una fracción acotada de sitios estuvo expuesta, y afirmó que se implementaron medidas correctivas, incluyendo cifrado de señalización a nivel nacional. Otros proveedores (que no fueron identificados por los investigadores) indicaron haber advertido durante meses a operadores satelitales sobre los riesgos de transmitir datos sin protección.

HYPD PHOTOS

¿QUÉ PASA EN CHILE?

El especialista chileno Álvaro Melo, gerente de ciberseguridad en ITQ Chile, aseguró que cuando existen transmisiones sin cifrar, la interceptación no solo es posible, sino que hacerlo es sencillo y económico. "Investigaciones recientes han demostrado que con un kit de televisión satelital estándar (antena parabólica y un sintonizador digital USB o SDR) se pueden capturar señales de satélites en órbita geoestacionaria. El problema radica en que los satélites GEO funcionan como espejos que rebotan la señal sobre un área geográfica inmensa, denominada huella satelital. Cualquier persona dentro de esa huella puede escuchar el tráfico. Y si ese tráfico no está cifrado, se pueden extraer correos, bases de datos e incluso conversaciones de voz en tiempo real", advierte.

El experto explica que, en Chile, los enlaces GEO se utilizan intensamente en tres ámbitos: defensa y soberanía (bases antárticas, patrulleras y puestos remotos), infraestructura crítica (sistemas Scada para control remoto de válvulas, sensores y redes eléctricas), y grandes empresas y comercio que los emplean como respaldo cuando falla la red terrestre.

Para Marcelo Mendoza, profesor de Ciencia de la Computación de la Pontificia Universidad Católica de Chile, "toda comunicación se puede interceptar. El factor crítico está en si esa información se puede decodificar o no, y eso depende de los protocolos de seguridad utilizados". Y agrega que "la comunicación de Defensa en Chile usa canales seguros, por lo que nuestra información estratégica no está en riesgo". En cuanto a comunicaciones corporativas del sector privado, existen distintas formas de compartir esta información, por lo que tienen diferentes niveles de seguridad.

El académico explica que la responsabilidad siempre está del lado de la institución usuaria, por cuanto "es la que suscribe protocolos de seguridad y cifrado".

A su juicio, el hallazgo debe ser abordado con prontitud, pero no hay evidencia de que en el caso chileno se trate de una brecha estructural generalizada. "Un gran problema está en que los sistemas de cifrado van a ser menos seguros en el futuro, debido al aumento de las capacidades computacionales que permiten desencriptar el cifrado de los mensajes. Pero es un desafío futuro; en el presente estamos suficientemente protegidos", destaca.

MIRADA INTERNACIONAL

Según Juan Fraire, investigador del equipo Agora del Instituto francés de Investigación en Ciencias y Tecnologías Digitales (Inria, por sus siglas en francés), con base en Lyon, el fenómeno es realista en determinados escenarios, pero no responde a la imagen de *hackers* espaciales, sino a prácticas de seguridad inconsistentes en parte de la infraestructura comercial. "Desde el punto de vista físico, las señales GEO cubren áreas muy amplias, lo que permite su recepción en grandes extensiones geográficas, con antenas y radios definidas por *software* disponible en el mercado. Captar no equivale a acceder al contenido, ya que las comunicaciones militares modernas usan cifrado fuerte. El riesgo aparece cuando enlaces empresariales o de *backhaul* (enlaces que transportan el tráfico desde antenas o zonas remotas hacia el centro de la red) se transmiten sin cifrado o con mecanismos obsoletos", señala.

El especialista sostiene que aun cuando el contenido esté protegido, la observación del tráfico puede revelar información sensible. "Sin acceder al mensaje es posible inferir patrones de actividad, como quién se comunica con quién, en qué momentos y con qué intensidad", asegura.

CONSTELACIONES LEO COMO STARLINK, con cobertura más reducida y dinámica, incorporan cifrado y tecnologías modernas, evitando que las señales sean interceptadas.

> "Investigaciones recientes han demostrado que con un kit de televisión satelital estándar (antena parabólica y un sintonizador digital USB o SDR) se pueden capturar señales de satélites en órbita geoestacionaria".
>
> **ÁLVARO MELO,** gerente de ciberseguridad en ITQ Chile.

A ello se suma la exposición de detalles técnicos como topologías, direcciones IP, esquemas de interconexión que, acumulados en el tiempo, pueden erosionar la seguridad. Desde una perspectiva de soberanía digital, el problema se vuelve más relevante para países que dependen del satélite para conectar regiones aisladas o enfrentar emergencias.

Respecto del estudio estadounidense, Fraire lo interpreta como un síntoma de una brecha estructural en el segmento geoestacionario. "Durante décadas se asumió una seguridad por oscuridad, basada en la complejidad técnica del enlace y en el acceso físico limitado a las señales. La integración creciente con internet, la virtualización de funciones de red y las megaconstelaciones están desmontando esas suposiciones, en el sentido de que las redes satelitales ya no son sistemas aislados, sino componentes activos de la infraestructura digital global", dice. En ese nuevo contexto, la seguridad debe incorporarse desde el diseño de la arquitectura y no como una capa opcional añadida *a posteriori*.

El especialista chileno Álvaro Melo advierte una zona gris en la cadena de responsabilidades: el operador satelital que suele limitarse a proveer capacidad de transporte; el proveedor del enlace que prioriza desempeño, y la responsabilidad final que recae en la institución usuaria. "Es un error técnico asumir que el enlace es privado solo por estar en el espacio. El usuario debe cifrar antes de enviar cualquier dato", afirma. Entre los riesgos potenciales del tráfico sin cifrar menciona, por ejemplo, el espionaje, secuestro de sesiones y la posibilidad de inyección de datos en sistemas de control, escenarios que, aun siendo hipotéticos, justifican controles estrictos.

Según los expertos, las medidas existen y se conocen. Desde el punto de vista técnico, el uso de cifrado de extremo a extremo —incluidos los enlaces de *backhaul* satelital—, junto con una gestión moderna de claves y la separación entre distintos tipos de tráfico, dificulta de manera significativa los intentos de acceso no autorizado. En el caso chileno, la entrada en vigencia de la Ley Marco de Ciberseguridad y la creación de la Agencia Nacional *ad hoc* establecen un marco que, según Melo, debe traducirse en exigencias concretas para infraestructura crítica.

Constelaciones LEO como Starlink, con cobertura más reducida y dinámica, que incorporan cifrado y tecnologías de red más modernas, evitan que las señales sean interceptadas.