El gigante estadounidense de telecomunicaciones T-Mobile detectó intentos de intrusión en la red por parte de un proveedor de telefonía fija

La empresa de telecomunicaciones estadounidense T-Mobile reveló que recientemente identificó intentos de actores malintencionados de infiltrarse en sus sistemas en las últimas semanas. Sin embargo, destacó que no se comprometió información sensible.

Según Jeff Simon, director de seguridad de T-Mobile, estos intentos de intrusión *«provienen de la red de un proveedor de servicios de línea fija conectado a la nuestra»*. Además, señaló: *«No hemos visto intentos previos similares».*

La compañía aseguró que sus medidas de seguridad lograron evitar que los atacantes afectaran sus servicios o accedieran a datos de clientes. Como respuesta, T-Mobile cortó la conexión con la red del proveedor involucrado, cuyo nombre no fue revelado. Aunque no señaló a ningún actor o grupo específico detrás del ataque, confirmó que compartió la información con las autoridades estadounidenses.

En una entrevista con Bloomberg, Simon explicó que los atacantes ejecutaron comandos de descubrimiento en los enrutadores para mapear la estructura de la red. Sin embargo, la empresa logró contener el ataque antes de que los intrusos pudieran avanzar lateralmente por el sistema. T-Mobile es la primera organización en hacer pública esta brecha de seguridad.

Este incidente ocurre poco después de informes sobre un grupo de ciberespionaje vinculado a China, conocido como Salt Typhoon (también llamado Earth Estries, FamousSparrow, GhostEmperor o UNC2286), que habría atacado a varias empresas de telecomunicaciones estadounidenses, como AT&T, Verizon y Lumen Technologies, en una operación de recolección de inteligencia.

> *«En resumen, nuestras defensas funcionaron como estaba previsto: desde nuestro diseño de red en capas hasta un monitoreo sólido, alianzas con expertos en ciberseguridad externos y una respuesta rápida. Esto evitó que los atacantes avanzaran y, lo más importante, que accedieran a información sensible de nuestros clientes. Otros proveedores podrían estar enfrentando escenarios diferentes»,*

> afirmó Simon.