La empresa de telecomunicaciones T-Mobile confirmó el viernes que fue víctima de una brecha de seguridad en marzo, después de que el grupo LAPSUS$ lograra acceder a sus redes informáticas.

El reconocimiento se produjo luego de que el periodista de investigación Brian Krebs, compartiera chats internos pertenecientes a los miembros principales del grupo que indicaban que LAPSUS$ violó la seguridad de la empresa varias veces en marzo, antes del arresto de sus siete miembros.

T-Mobile dijo en un comunicado que el incidente ocurrió *«hace varias semanas, con el mal actor utilizando credenciales robadas para acceder a los sistemas internos. No tenemos evidencia que el intruso haya podido obtener algo de valor».*

Las credenciales de VPN para el acceso inicial se obtuvieron de sitios web ilícitos como Russian Market, con el objetivo de obtener el control de las cuentas de los empleados de T-Mobile y, en última instancia, permitir que el actor de amenazas lleve a cabo ataques de intercambio de SIM a voluntad.

Además de obtener acceso a una herramienta interna de administración de cuentas de clientes llamada Atlas, los chats muestran que LAPSUS$ había violado las cuentas de Slack y Bitcuket de T-Mobile, utilizando esta última para descargar más de 30,000 repositorios de código fuente.

LAPSUS$, en poco tiempo desde que surgió el panorama de amenazas, ganó notoriedad por sus violaciones de Impresa, NVIDIA, Samsung, Vodafone, Ubisoft, Microsoft, Okta y Globant.

A inicios de abril, la Policía de la Ciudad de Londres reveló que había acusado a dos de los siete adolescentes, uno de 16 y otro de 17, que fueron arrestados el mes pasado por sus supuestas conexiones con el grupo LAPSUS$.