Según la información proporcionada por Microsoft, hackers procedentes de China han logrado acceder a las cuentas de correo electrónico de alrededor de 25 organizaciones, incluyendo entidades gubernamentales.

Estos ataques han sido vinculados a un grupo de amenazas conocido como Storm-0558, el cual se cree que es una banda de ciberespionaje especializada en hackear redes de correo electrónico para obtener información confidencial. La compañía de software no ha especificado las ubicaciones exactas de las organizaciones gubernamentales afectadas.

El 16 de junio de 2023, Microsoft comenzó a investigar estos ataques tras recibir quejas de usuarios sobre un comportamiento extraño en los correos electrónicos de Office 365. Durante la investigación, se descubrió que a partir del 15 de mayo de 2023, los actores de amenazas pertenecientes al grupo Storm-0558 lograron acceder a las cuentas de clientes que posiblemente estaban relacionadas con alrededor de 25 entidades, incluyendo los Departamentos de Estado y Comercio de Estados Unidos.

Sin embargo, Microsoft no especificó qué empresas, instituciones gubernamentales o países se vieron afectados por estos incidentes de seguridad en el correo electrónico. La embajada china en Londres calificó al gobierno de Estados Unidos como *«el mayor imperio de hacking del mundo y un ladrón cibernético global»*, además de tildar estas afirmaciones como *«desinformación».* A pesar de los hechos o el contexto, China niega constantemente su participación en operaciones de hacking.

Adam Hodge, portavoz del Consejo de Seguridad Nacional de la Casa Blanca, mencionó que una brecha en la seguridad en la nube de Microsoft *«afectó sistemas no clasificados»*, pero no proporcionó más detalles al respecto.

> Hodge continuó diciendo: *«Los funcionarios se pusieron en contacto inmediatamente con Microsoft para identificar el origen y la vulnerabilidad en su servicio en la nube».*

Los hackers lograron robar 25 correos electrónicos

Según Microsoft, alrededor de 25 cuentas de correo electrónico, incluyendo aquellas pertenecientes a agencias gubernamentales y cuentas de usuarios vinculadas a estas instituciones, fueron comprometidas por el grupo cibernético Storm-0558. Microsoft utiliza el término *«Storm»* para identificar y monitorear redes de hackers que son nuevas, están en crecimiento o se encuentran en desarrollo. No se han revelado los nombres de las agencias gubernamentales que fueron objetivo de Storm-0558.

De acuerdo con el análisis de Microsoft, el grupo de hackers Storm-0558, al que la compañía describe como un adversario *«con amplios recursos»,* utilizó Outlook Web Access en Exchange Online (OWA) y Outlook.com para acceder a las cuentas de usuario mediante la falsificación de tokens de autenticación. A través de una clave de firma de Microsoft obtenida, los hackers lograron falsificar estos tokens para acceder a OWA y Outlook.com. Posteriormente, aprovecharon una vulnerabilidad de validación de tokens para hacerse pasar por usuarios de Azure AD y acceder a cuentas de correo electrónico corporativas.

El comportamiento malicioso de Storm-0558 pasó desapercibido durante aproximadamente un mes antes de que los usuarios informaran a la compañía sobre actividades inusuales en sus correos electrónicos, según lo indicado por Microsoft.