Microsoft anunció el viernes que un error de validación en su código fuente permitió que se falsificaran tokens de Azure Active Directory (Azure AD) por parte de un actor malicioso conocido como Storm-0558, quien utilizó una clave de firma de cuenta de Microsoft (MSA) para infiltrarse en dos docenas de organizaciones.

> *«Storm-0558 adquirió una clave de firma de cuenta de Microsoft inactiva y la utilizó para crear tokens de autenticación falsos de Azure AD empresariales y MSA de consumidor, con el fin de acceder a OWA y Outlook.com. La forma en que el actor obtuvo la clave está siendo investigada actualmente»*, afirmó el gigante tecnológico en un análisis más profundo de la campaña.

> *«Aunque la clave estaba destinada únicamente para cuentas de MSA, un problema de validación permitió que esta clave se considerara válida para firmar tokens de Azure AD. Este problema ha sido corregido».*

No está claro de inmediato si el problema de validación del token fue aprovechado como una *«vulnerabilidad de día cero»* o si Microsoft ya era consciente del problema antes de que se produjera el abuso.

Los ataques se dirigieron aproximadamente a 25 organizaciones, incluyendo entidades gubernamentales y cuentas de consumidores asociadas, con el objetivo de obtener acceso no autorizado a correos electrónicos y extraer datos de buzones. No se informa que ningún otro entorno haya sido afectado.

La compañía recibió información sobre el incidente después de que el Departamento de Estado de Estados Unidos detectara una actividad de correo electrónico anormal relacionada con el acceso a datos de Exchange Online. Se sospecha que Storm-0558 es un actor de amenazas con sede en China que realiza actividades cibernéticas maliciosas consistentes con el espionaje, aunque China ha negado las acusaciones.

Los principales objetivos del grupo de hackers incluyen organismos gubernamentales diplomáticos, económicos y legislativos de Estados Unidos y Europa, así como personas relacionadas con los intereses geopolíticos de Taiwán y los uigures. También han atacado a empresas de medios, grupos de expertos y proveedores de equipos y servicios de telecomunicaciones.

Se cree que han estado activos desde al menos agosto de 2021, llevando a cabo acciones de recolección de credenciales, campañas de phishing y ataques de tokens OAuth dirigidos a cuentas de Microsoft para alcanzar sus objetivos.

*«Storm-0558 opera con un alto nivel de conocimiento técnico y seguridad operativa»,* declaró Microsoft, describiéndolo como una entidad técnicamente hábil, bien financiada y con un profundo entendimiento de diversas técnicas de autenticación y aplicaciones.

> *«Los actores tienen pleno conocimiento del entorno del objetivo, las políticas de registro, los requisitos de autenticación y los procedimientos y políticas.»*

El acceso inicial a las redes objetivo se logra a través de técnicas de phishing y la explotación de vulnerabilidades de seguridad en aplicaciones de cara al público, lo que resulta en la implementación de la shell web China Chopper para obtener acceso no autorizado y una herramienta llamada Cigril para facilitar el robo de credenciales.

Storm-0558 también utiliza scripts de PowerShell y Python para extraer datos de correo electrónico, como archivos adjuntos, información de carpetas y conversaciones completas, utilizando llamadas a la API de Outlook Web Access (OWA).

Microsoft declaró que desde el descubrimiento de la campaña el 16 de junio de 2023, ha *«identificado la causa raíz, establecido un seguimiento continuo de la campaña, interrumpido las actividades maliciosas, fortalecido el entorno, notificado a todos los clientes afectados y coordinado con múltiples entidades gubernamentales»*. Además, destacó que se han aplicado medidas para solucionar el problema *«en nombre de los clientes»* a partir del 26 de

junio de 2023.

Aunque aún no está claro el alcance exacto de la brecha, este es el ejemplo más reciente de un actor de amenazas con base en China que lleva a cabo ataques cibernéticos con el objetivo de obtener información confidencial y logra una operación de inteligencia sigilosa sin llamar la atención durante al menos un mes antes de ser descubierta en junio de 2023.

Esta revelación se produce en medio de críticas hacia Microsoft por su manejo del hackeo y por restringir las capacidades forenses detrás de barreras adicionales de licencias, lo que impide a los clientes acceder a registros de auditoría detallados que podrían haber ayudado a analizar el incidente.

> *«Es como vender un automóvil y cobrar extra por las características de seguridad esenciales, como los cinturones de seguridad y los airbags»*, fue citado el senador estadounidense Ron Wyden.

Este acontecimiento también coincide con la publicación de un informe detallado sobre China por parte del Comité de Inteligencia y Seguridad del Parlamento del Reino Unido (ISC), en el cual se menciona la *«altamente efectiva capacidad de ciberespionaje»* del país y su capacidad para infiltrarse en sistemas informáticos de diversos gobiernos extranjeros y empresas del sector privado.