El reciente ataque dirigido contra la infraestructura de correo electrónico de Microsoft, llevado a cabo por un actor estatal chino conocido como Storm-0558, se afirma que tiene una amplitud mayor de lo inicialmente considerado.

De acuerdo con la compañía de seguridad en la nube Wiz, la clave de firma inactiva de la cuenta de Microsoft (MSA) utilizada para falsificar tokens de Azure Active Directory (Azure AD o AAD) con el fin de obtener acceso ilegal a Outlook Web Access (OWA) y Outlook.com, también podría haber permitido al adversario generar tokens de acceso falsos para diferentes tipos de aplicaciones de Azure AD.

Esto incluiría todas las aplicaciones que admiten la autenticación de cuentas personales, como OneDrive, SharePoint y Teams; las aplicaciones de clientes que soportan la función *«Iniciar sesión con Microsoft»,* y aplicaciones multiinquilino en ciertas condiciones.

> *«Todo en el mundo de Microsoft depende de los tokens de autenticación de Azure Active Directory para el acceso. Un atacante con una clave de firma de AAD es el atacante más poderoso que puedas imaginar, ya que puede acceder a casi cualquier aplicación, como si fuera cualquier usuario. Esto es como tener un superpoder de 'cambio de forma'»,* expresó Ami Luttwak, director de tecnología y co-fundador de Wiz.

Microsoft, la semana pasada, reveló que la técnica de falsificación de tokens fue explotada por Storm-0558 para extraer datos no clasificados de los buzones de correo de las víctimas, pero los detalles precisos de la campaña de ciberespionaje aún no se conocen del todo.

El fabricante de Windows indicó que todavía está investigando cómo el adversario logró obtener la clave de firma de la cuenta de Microsoft (MSA). Sin embargo, no está claro si la clave funcionaba como una especie de llave maestra para desbloquear el acceso a los datos pertenecientes a casi veinte organizaciones.

El análisis realizado por Wiz cubre algunas de las lagunas, ya que la compañía descubrió que

«todas las aplicaciones de cuentas personales de Azure v2.0 dependen de una lista de 8 claves públicas, y todas las aplicaciones multiinquilino de Azure v2.0 que tienen habilitada la cuenta de Microsoft dependen de una lista de 7 claves públicas».

Se encontró además que Microsoft sustituyó una de las claves públicas enumeradas (identificación de huella digital: «d4b4cccda9228624656bff33d8110955779632aa«) que había estado presente desde al menos 2016, en algún momento entre el 27 de junio de 2023 y el 5 de julio de 2023, aproximadamente durante el mismo período en que la empresa afirmó haber revocado la clave MSA.

> *«Esto nos llevó a creer que aunque la clave privada comprometida adquirida por Storm-0558 fue diseñada para el inquilino MSA de Microsoft en Azure, también tenía la capacidad de firmar tokens OpenID v2.0 para múltiples tipos de aplicaciones de Azure Active Directory»,* informó Wiz.

> *«Storm-0558 aparentemente logró obtener acceso a una de las diversas claves destinadas a firmar y verificar los tokens de acceso de AAD. La clave comprometida tenía la autoridad para firmar cualquier token de acceso OpenID v2.0 para cuentas personales y aplicaciones de AAD de audiencia mixta (multiinquilino o cuenta personal)».*

Esto implicaba efectivamente que la vulnerabilidad teóricamente podría permitir que actores maliciosos falsificaran tokens de acceso para su uso en cualquier aplicación que dependa de la plataforma de identidad de Azure.

Aún peor, la clave privada adquirida podría haber sido utilizada para falsificar tokens para

autenticarse como cualquier usuario en una aplicación afectada que confiara en certificados de audiencia mixta y cuentas personales de Microsoft OpenID v2.0.

> *«Las claves de firma del proveedor de identidad son probablemente los secretos más poderosos en el mundo moderno. Con las claves del proveedor de identidad, uno puede obtener acceso inmediato a todo, a cualquier buzón de correo electrónico, servicio de archivos o cuenta en la nube»*, expresó Shir Tamari, investigador de seguridad de Wiz.

Actualización

Microsoft compartió la siguiente declaración con The Hacker News:

> *Muchas de las afirmaciones realizadas en este blog son especulativas y no se basan en evidencia. Recomendamos que los clientes revisen nuestros blogs, especialmente nuestro blog de Inteligencia de Amenazas de Microsoft, para obtener más información sobre este incidente e investiguen sus propios entornos utilizando los Indicadores de Compromiso (IOC) que hemos hecho públicos. También hemos ampliado recientemente la disponibilidad de registro de seguridad, haciéndolo gratuito para más clientes por defecto, para ayudar a las empresas a gestionar un panorama de amenazas cada vez más complejo.*