Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°167	Fecha: 16-07-2023
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	El error de Microsoft permitió a los hackers violar más de dos docenas de organizaciones a través de tokens de Azure AD falsificados		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

Microsoft anunció que un error en su código fuente permitió a un actor malicioso conocido como Storm-0558 falsificar tokens de Azure Active Directoy (Azure AD) utilizando una clave de firma de consumidor de cuenta (MSA).

Storm-0558, pudo violar la seguridad de 24 organizaciones, incluyendo entidades gubernamentales y cuentas de consumidores, para acceder de manera no autorizada a servicios como OWA y Outlook.

El origen de la adquisición de la clave de firma MSA por parte de Storm-0558 aún está bajo investigación.

2. DETALLES:

Queda por aclarar si el problema de la validación de tokens fuera explotado como una "vulnerabilidad de día cero" o si Microsoft sabia del problema antes de que fuera objeto del ataque.

Aún se sigue investigando el método que pudo haber empleado el actor malicioso para obtener la llave.

A pesar que fue solucionado el problema de validación de la clave creada solo para cuentas MSA, este error de validación ocasionó que esta clave fuera de confianza para firmar tokens de Azure AD.

Aunque China ha negado las acusaciones, se sospecha que Storm-0558, conocido en internet como un actor de amenazas ubicado en China, tenga relación con los ataques ya que es conocida su dedicación en realizar actividades cibernéticas maliciosas que son consistentes con el espionaje. Suele incluir entre sus objetivos principales a órganos de gobierno, diplomáticos, económicos y legislativos de Estados Unidos y Europa, entorno relacionado con intereses geopolíticos de Taiwán y uigures, así como compañías de medios, grupos de expertos y proveedores de equipos y servicios de telecomunicaciones.

Se sabe que Storm-0558 ha estado activo desde agosto de 2021, orquestando la recolección de credenciales, campañas de phishing y ataques de tokens OAuth dirigidos a cuentas de Microsoft para perseguir sus objetivos. Microsoft describe a Storm-0558 como experto con buenos recursos y con una comprensión aguda de varias técnicas y aplicaciones de autenticación.

En principio el acceso a las redes del objetivo se hace a través del phishing y la explotación de fallas de seguridad en aplicaciones públicas, lo que facilita el despliegue del shell web China Chopper para el acceso de puerta trasera y una herramienta llamada Cigril para facilitar el robo de credenciales.

Luego, Storm-0558 emplea scripts de Python (Fig. 1) PowerShell y (Fig. 2) para extraer datos de correo electrónico como archivos adjuntos, información de carpetas y conversaciones completas mediante llamadas a la API de Outlook Web Access (OWA).

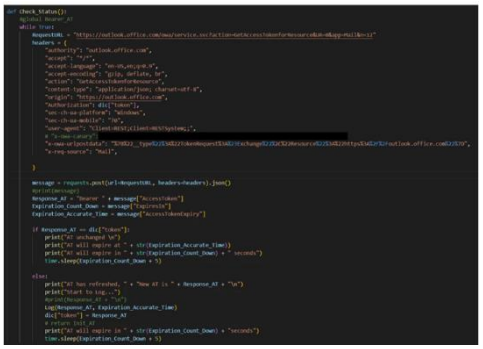

Figura 1. Fragmento de código Python de la funcionalidad de actualización de token utilizada por el actor de amenazas.

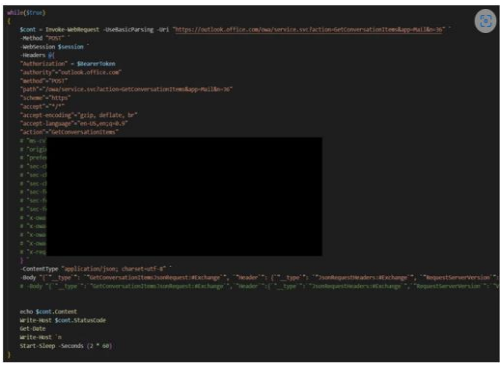

Figura 2. Fragmento de código de PowerShell de la llamada de la API de REST de OWA a GetConversationItems.

Desde la campaña del 16 de junio de 2023, Microsoft identificó la causa raíz, empezó un seguimiento de la campaña, interrumpió actividades maliciosas, fortaleció el entorno, notificó a cada cliente afectado y coordinó con múltiples entidades gubernamentales. Afirma que mitigó el problema a partir del 26 de junio de 2023.

La revelación de este incidente también ha llevado a críticas hacia Microsoft, como lo dicho por el senador estadounidense Ron Wyden "Cobrar a la gente por las características premium necesarias para no ser hackeado es como vender un automóvil y luego cobrar extra por cinturones de seguridad y bolsas de aire". Además, el Comité de Inteligencia y Seguridad del Parlamento (ISC) del Reino Unido ha publicado un informe destacando la capacidad que tiene China para penetrar en los sistemas de TI del gobierno extranjero y del sector privado de otros países.

Microsoft evitó dar alguna recomendación al respecto luego de haber mitigado esta actividad en nombre de sus clientes de los servicios que acceden a Exchange Online y Outlook.com.

3. RECOMENDACIONES:

- Conocer la procedencia de un correo electrónico si te llevan varios correos electrónicos al día, preferible trasladarlo a una carpeta de SPAM.
- Deshabilitar la carga de imágenes de forma automática.
- Procurar no abrir el correo electrónico y menos si contienen la extensión.exe.
- Borrar el historial de la caché de tu navegador de manera periódica y evitar marcar la opción de guardar contraseñas.
- Utilizar diferentes contraseñas para las cuentas de correo electrónico a las que tienes acceso, y modificar las contraseñas con cierta frecuencia (04 - 06 meses).
- Evitar abrir correos con ofertas, regalos o falsas promociones del tipo: "Te ha tocado un viaje a Nueva York con todos los gastos pagados".
- Pasar el cursor del ratón sobre los enlaces del email antes de abrirlos, para que pueda comprobar si la dirección URL es correcta.

Fuente de Información:	• hxxps://thehackernews.com/2023/07/microsoft-bug-allowed-hackers-to-breach.html • hxxps://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/