Alerta de seguridad	24ICSOAuth-102022
Clase de alerta	Campaña Phishing
Tipo de Incidente	Phishing OAuth
Fecha de lanzamiento	24 de octubre de 2022
Última revisión	24 de octubre de 2022

Notificación

El presente reporte es producto del análisis de múltiples fuentes, terceras partes afectadas o de investigación propia del equipo de respuesta a incidentes del instituto de ciberseguridad (CSIRT).

Este tipo de alerta no genera o tiene una afectación sobre servicios o ambientes productivos, tampoco involucra un compromiso de la seguridad de la infraestructura interna o externa, es una metodología de fraude conocida como Phishing

Resumen

Se han identificado **campañas de phishing** empleando el protocolo **de autenticación abierta (OAuth)**, en el que los atacantes envían correos electrónicos con un enlace de consentimiento malicioso para que una aplicación de terceros acceda a la cuenta de un usuario y **realice acciones** en nombre del usuario **sin exponer ninguna contraseña**. Esta es relacionada a una vulnerabilidad de configuración.

Microsoft 365

Ilustración 1 – Logotipo ilustrativo de Microsoft

Contenido

Análisis

Para autorizar estas aplicaciones de productividad, la plataforma de identidad de Microsoft implementa protocolos estándar de la industria, como OAuth 2.0. Las aplicaciones OAuth obtienen permiso al mostrar un cuadro de diálogo "**Permisos solicitados**" muestra qué permisos solicita el tercero.

Lo mostramos en la siguiente captura de pantalla.

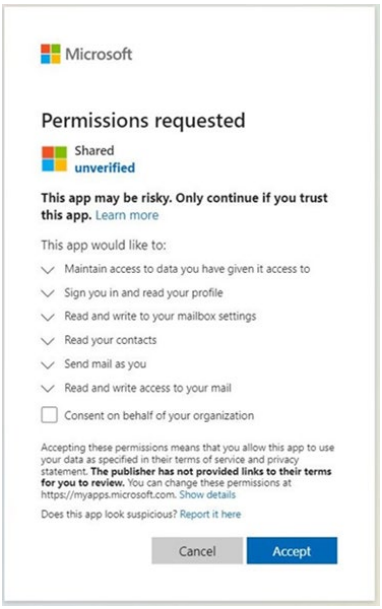

Ilustración 2- Cuadro de diálogo que solicita el consentimiento del usuario para los permisos solicitados por la aplicación OAuth

Pasos realizados

1. Se solicita el consentimiento del usuario para las aplicaciones dirigidas mediante el envío de enlaces de consentimiento a los objetivos en correos electrónicos de phishing y mensajes de chat.
2. Una vez que el objetivo hace clic en el enlace y autoriza la aplicación, el atacante obtiene tokens de acceso con los alcances solicitados y tokens de actualización para la persistencia y exfiltración de los datos del objetivo.
3. Si el usuario también tiene una función de administrador en el inquilino, el riesgo se duplica, ya que el atacante puede realizar todas las acciones a través de la aplicación en el contexto de un usuario elevado.

El siguiente diagrama muestra cómo es el funcionamiento de este ataque

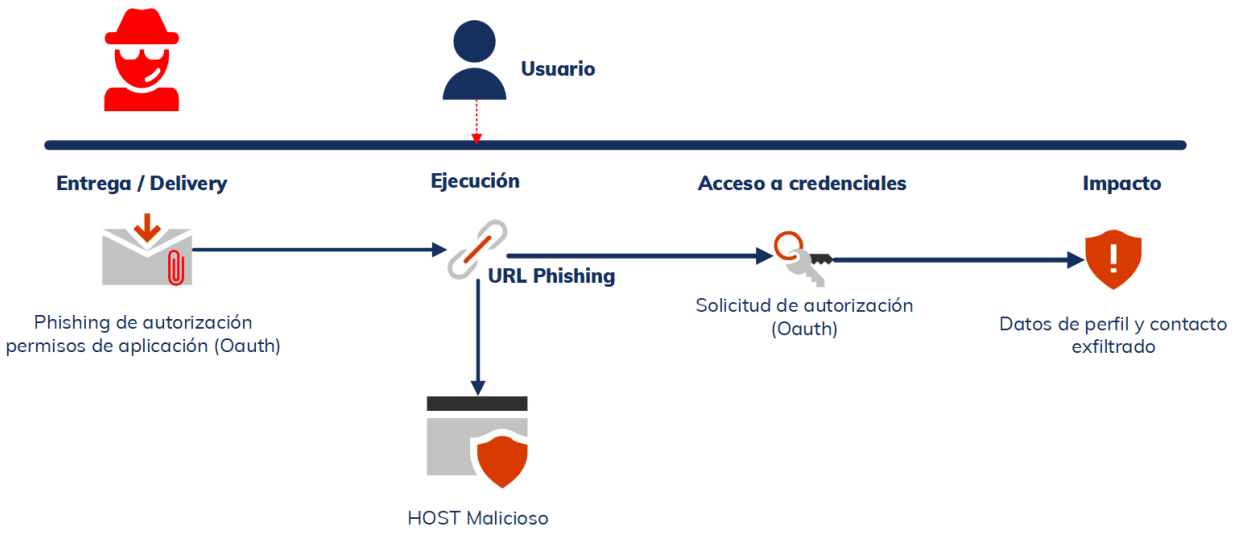

Ilustración 3 - Flujo de ataque de phishing de consentimiento de OAuth

Fases de Kill Chain:

- Registro de aplicaciones maliciosas
- Creación de aplicaciones MultiTenant maliciosas en el Tenant propiedad del atacante.
- Aprovechar un Administrador de Tenant ya comprometido para comprometer las aplicaciones existentes con permisos de alto privilegio.
- Registro de nuevas aplicaciones en un Administrador de Tenant comprometido.

Creación de la APP maliciosa

La fase inicial de un ataque de phishing de consentimiento de OAuth comienza con la creación de una aplicación de OAuth en Azure AD u otros proveedores de identidad. Los atacantes tienen varias opciones para configurar aplicaciones maliciosas, detallamos enseguida:

- **Estas aplicaciones** funcionan como una **identidad de usuario** a la que se le pueden asignar permisos.
- **Estos permisos** permiten que la aplicación **acceda a una API** a través de llamadas REST en lugar de la interacción del usuario.
- **Los atacantes** eligen los permisos para las aplicaciones maliciosas en función de sus objetivos, esos permisos suelen ser **privilegios elevados**, como offline.access, MailboxSettings.ReadWrite y files.readwrite.All.
- Esto permitirá **establecer un acceso** persistente a los datos del usuario y manipular la configuración del buzón del usuario, como agregar reglas a la bandeja de entrada y automatizar la exfiltración de datos de correo electrónico.
- Algunos permisos con privilegios elevados como **MailboxSettings.ReadWrite y files.readwrite.All** requieren el consentimiento del administrador antes de que la aplicación pueda acceder a los recursos. Por lo tanto, los atacantes intentan comprometer las cuentas de administrador para obtener estos permisos para sus aplicaciones maliciosas.

Ilustración 4 - Ataque de phishing de consentimiento de OAuth con exfiltración de datos de correo electrónico

Correo phishing y otorgamiento de consentimiento del usuario

La siguiente fase del ataque consiste en enviar enlaces de phishing de consentimiento a los objetivos a través de correos electrónicos o mensajes de chat utilizando tácticas comunes de ingeniería social.

Ilustración 5 - Ejemplo de correo electrónico con un enlace de consentimiento para ver un documento compartido

Al hacer clic en el enlace, podemos observar que nos redirige al siguiente enlace:

Ilustración 6 - Un ejemplo de estructura del enlace para redirección de consentimiento

Al hacer clic en el enlace de consentimiento, al usuario objetivo se le presenta una ventana de solicitud de consentimiento que muestra el nombre de la aplicación, el logotipo y los datos del usuario a los que la aplicación del atacante solicita acceso.

Los atacantes tienden a usar nombres y logotipos conocidos para hacerse pasar por una aplicación comercial legítima y engañar al objetivo para que otorgue su consentimiento a la aplicación.

Impactos generados a la organización

Exfiltración de datos y movimiento lateral

Una vez que la víctima otorga el consentimiento a la aplicación, el atacante obtiene tokens de acceso que se pueden usar para filtrar los datos del usuario, así como tokens de actualización para el acceso persistente a los datos del usuario.

Luego, el atacante usa el token de acceso con los ámbitos de permiso solicitados en la concesión de consentimiento para filtrar los datos del usuario a través de API, como MS Graph API. Esta API permite que las aplicaciones OAuth en Azure AD accedan a la gran cantidad de datos en M365 de forma programática.

Adicional, como parte de las actividades de exfiltración se realizan diversas tareas entre las que se encuentran:

- Busca en las carpetas de correo electrónico y los mensajes del usuario
- Crear reglas de mensajes para reenviar correos electrónicos a cuentas de correo electrónico de atacantes externos
- Envían correos electrónicos a potenciales víctimas suplantando la identidad del usuario comprometido y eliminan correos electrónicos para ocultar sus huellas.
- Según los alcances de la aplicación, el atacante también puede acceder a las cargas de trabajo de OneDrive y SharePoint para obtener datos de usuario.

Malas noticias

En este caso, restablecer las credenciales del usuario no revoca el acceso de la aplicación a los datos del usuario, ya que la aplicación utiliza tokens de acceso que no realizan la autenticación, sino que autorizan a la aplicación a acceder a los datos con el supuesto consentimiento del usuario.

Habilitar la autenticación multifactor (MFA) tampoco evitará este ataque. Para remediar este riesgo, es necesario revocar en el arrendatario el consentimiento otorgado a la solicitud.

Acciones recomendadas

1.- Bloquear el "**consentimiento del usuario**" para prohibir que los usuarios den su consentimiento a las aplicaciones que solicitan permisos con privilegios elevados dentro de Azure AD.

Para esto tendrías que seguir los siguientes pasos:

- Inicie sesión en Azure Portal (http://portal.azure.com/) como administrador global.
- En el apartado de "**Administrar**" seleccionamos la opción de "**Aplicaciones empresariales**".
- En el apartado de "seguridad" seleccionamos la opción de "**Consentimiento y permisos**".
- Selecciona la opción que más se adapte a tu organización.

Ilustración 7 - Opciones de consentimiento del usuario para Azure AD

2.- Verificar los buzones que usan el reenvío automático de correo electrónico y validar con los propietarios de la cuenta si este es el comportamiento esperado. Considera desactivar el reenvío automático de correo electrónico en Office 365 y Exchange Server.

3.- Verificar la configuración de filtrado de correo electrónico de Office 365 para asegurarse de bloquear los correos electrónicos falsificados, el spam y los correos electrónicos con malware.

4.- Active las políticas de archivos adjuntos seguros para verificar los archivos adjuntos al correo electrónico entrante.

5.- Active las políticas de enlaces seguros para verificar la redirección a sitios web maliciosos en correo electrónico entrante.

6.- Educar a los usuarios finales sobre las tácticas de phishing de consentimiento como parte de la formación de concienciación sobre seguridad o phishing. La capacitación debe incluir la verificación de errores ortográficos y gramaticales en los correos electrónicos de phishing o en la pantalla de consentimiento de la aplicación, así como nombres de aplicaciones, logotipos y direcciones URL de dominio falsificados que parezcan originarse en aplicaciones o empresas legítimas.

7.- Instruya a su organización sobre cómo funcionan los marcos de permisos y consentimiento.

Técnicas MITRE ATT&CK observadas

Esta amenaza utiliza técnicas de atacante documentadas en el marco MITRE ATT&CK.

Acceso inicial

- T1566.002 Spearphishing Link | URL en enlaces de correo electrónico a la página de phishing
- T1566.003 Spearphishing via Service | Uso de aplicaciones de terceros
- T1199 Trusted Relationship | Aproveche la relación o el destinatario de confianza con Microsoft 365

Acceso a Credenciales

- T1528 Steal Application Access Token | Enviar token de acceso de usuario al atacante.
- T1114.002 Email Collection: Remote Email Collection | Enviar token de usuario e información personal confidencial al atacante.
- T1114.003 Email Collection: Email Forwarding Rule | Aplicaciones que crean reglas de mensajes para reenviar correos electrónicos a las identificaciones de correo electrónico del atacante.

Evasión de defensa

- T1036 Masquerading | Aplicaciones que se hacen pasar por aplicaciones legítimas con homoglifos, errores tipográficos en cuclillas y suplantación del logotipo de la marca
- T1564 Hide Artifacts: Email Hiding Rules | Aplicaciones que crean reglas de mensajes para ocultar o eliminar correos electrónicos en la bandeja de entrada del objetivo

Alerta de seguridad OAuth Microsoft 365

¿Te podemos ayudar?
contacto@iciberseguridad.io

Síguenos **en nuestras redes sociales**

ICS Instituto de Ciberseguridad

Recuerda, «Prevención antes que reacción»

@iciberseguridad @institutoCSIO +52 81 2587 2530 +52 81 2672 1298 csirt@iciberseguridad.io