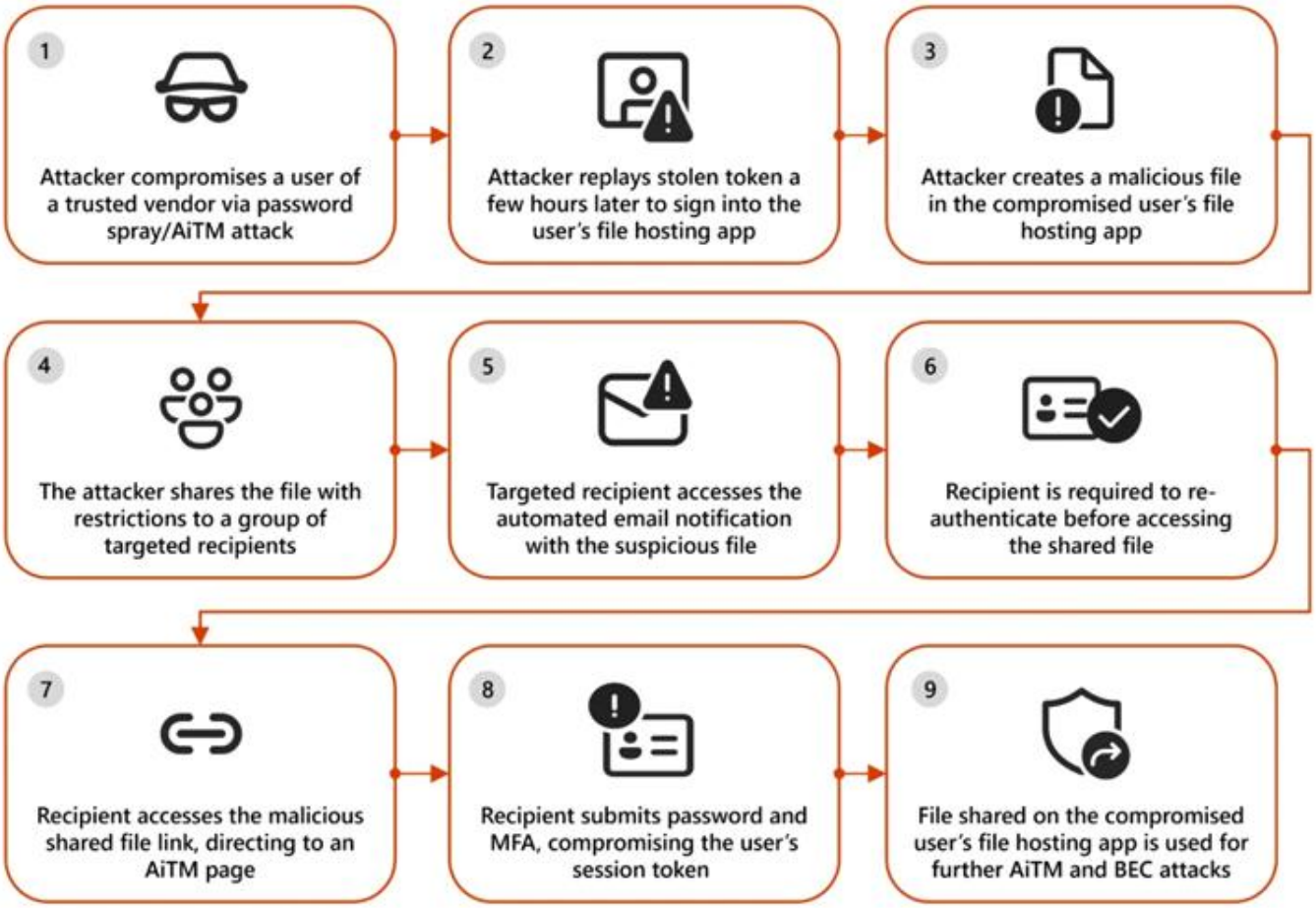
Microsoft está alertando sobre campañas de ciberataques que explotan servicios legítimos de almacenamiento de archivos, como SharePoint, OneDrive y Dropbox, muy utilizados en entornos empresariales como una táctica para evadir defensas.

El objetivo principal de estas campañas es diverso y amplio, permitiendo que los actores maliciosos comprometan identidades y dispositivos, así como realicen ataques de compromiso de correo electrónico empresarial (BEC), lo que en última instancia conlleva fraude financiero, exfiltración de datos y movimiento lateral a otros dispositivos.

La utilización de servicios de internet legítimos (LIS) se ha convertido en un vector de riesgo cada vez más común adoptado por los adversarios para integrarse con el tráfico legítimo de la red de una manera que frecuentemente elude las defensas de seguridad tradicionales y complica los esfuerzos de atribución.

Este enfoque también se conoce como vivir de sitios confiables (LOTS), ya que aprovecha la confianza y familiaridad con estos servicios para sortear las regulaciones de seguridad del correo electrónico y distribuir malware.

Microsoft ha indicado que ha estado observando una nueva tendencia en las campañas de phishing que utilizan servicios legítimos de almacenamiento de archivos desde mediados de abril de 2024, que involucran archivos con acceso restringido y limitaciones de solo visualización.



Tales ataques generalmente comienzan con el compromiso de un usuario dentro de un proveedor de confianza, aprovechando este acceso para subir archivos y cargas maliciosas en el servicio de almacenamiento de archivos, los cuales posteriormente se compartirán con una entidad objetivo.

> *«Los archivos enviados a través de correos de phishing están configurados para ser accesibles solo para el destinatario designado. Esto requiere que el destinatario inicie sesión en el servicio de almacenamiento de archivos, ya sea Dropbox, OneDrive o SharePoint, o que vuelva a autenticar ingresando su dirección de correo electrónico junto con una contraseña de un solo uso (OTP) recibida a través de un*

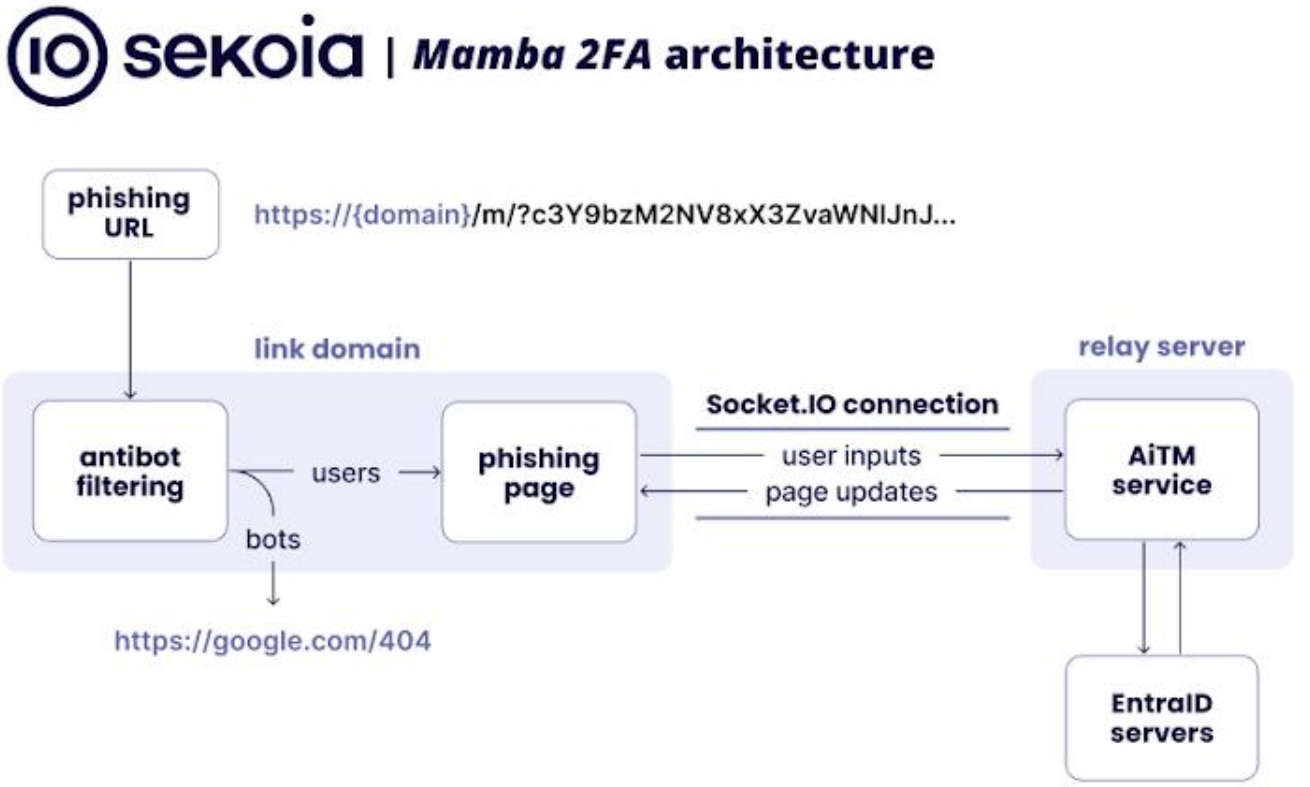
> *servicio de notificaciones»,* afirmó.

Además, los archivos compartidos en el marco de los ataques de phishing están configurados en modo «solo visualización», lo que impide que se descarguen y que se detecten las URL incrustadas dentro del archivo.

Cuando un destinatario intenta acceder al archivo compartido, se le solicita verificar su identidad proporcionando su dirección de correo electrónico y una contraseña de un solo uso enviada a su cuenta de correo electrónico.

Una vez que se autoriza exitosamente, al objetivo se le indica que haga clic en otro enlace para ver el contenido real. Sin embargo, al hacerlo, es redirigido a una página de phishing adversaria en el medio (AitM) que roba su contraseña y tokens de autenticación de dos factores (2FA).

Esto no solo permite a los actores maliciosos tomar el control de la cuenta, sino que también la utilizan para llevar a cabo otras estafas, incluidos ataques BEC y fraude financiero.



> *«Si bien estas campañas son genéricas y oportunistas en su esencia, emplean técnicas sofisticadas para realizar ingeniería social, evadir la detección y ampliar el alcance de los actores maliciosos a otras cuentas e inquilinos»,* indicó el equipo de Inteligencia de Amenazas de Microsoft.

Este desarrollo se produce mientras Sekoia presentó un nuevo kit de phishing AitM llamado Mamba 2FA, que se comercializa como phishing como servicio (PhaaS) a otros actores maliciosos para realizar campañas de phishing por correo electrónico que distribuyen archivos adjuntos HTML que simulan las páginas de inicio de sesión de Microsoft 365.

El kit, que se ofrece bajo un modelo de suscripción por $250 al mes, es compatible con Microsoft Entra ID, AD FS, proveedores de SSO de terceros y cuentas de consumidores.

Mamba 2FA ha estado en uso activo desde noviembre de 2023.

> *«Gestiona las verificaciones de dos pasos para métodos de MFA no resistentes al phishing, como códigos de un solo uso y notificaciones de aplicaciones. Las credenciales y cookies robadas se envían inmediatamente al atacante a través de un bot de Telegram»,* declaró la compañía francesa de ciberseguridad.