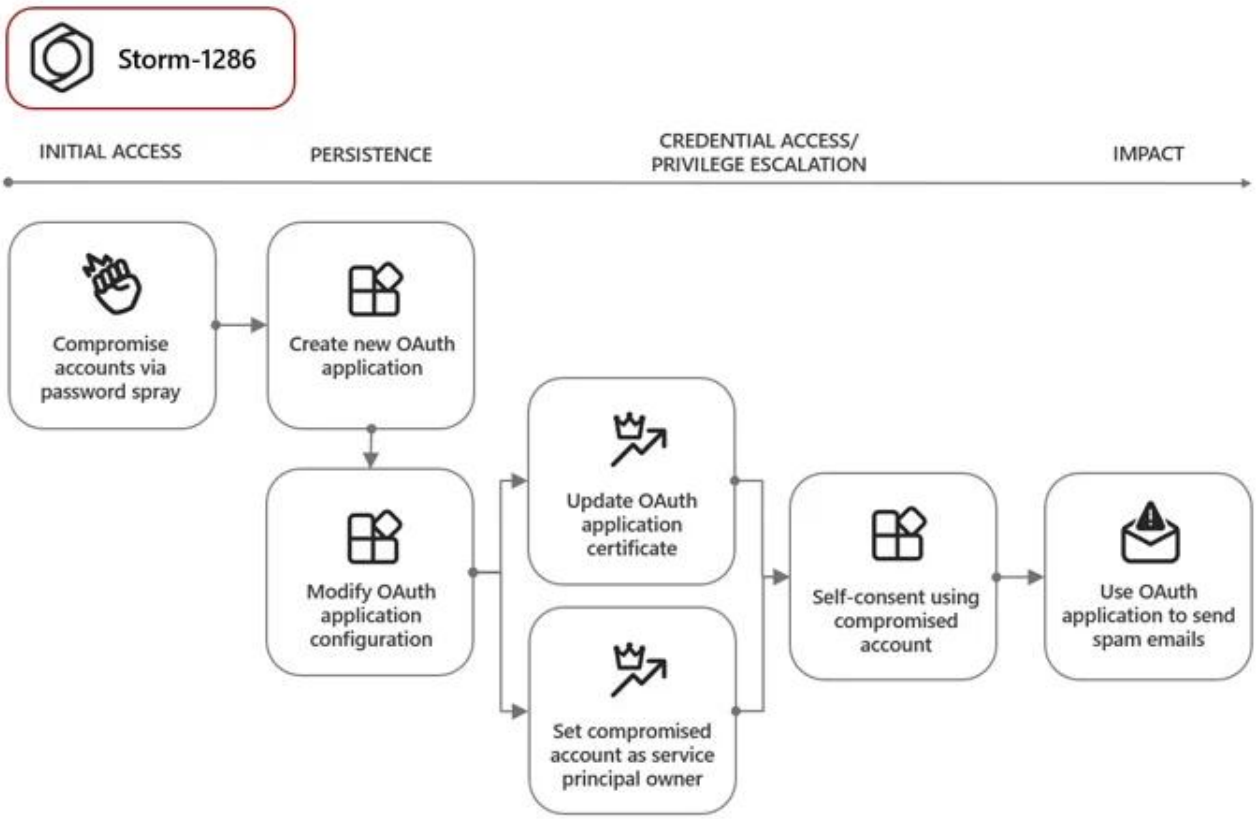
Microsoft ha alertado sobre el uso de aplicaciones OAuth por parte de adversarios como una herramienta automatizada para implementar máquinas virtuales (VM) con el propósito de realizar minería de criptomonedas y llevar a cabo ataques de phishing.

> *«Los actores de amenazas comprometen cuentas de usuario para crear, modificar y otorgar altos privilegios a aplicaciones OAuth que pueden mal utilizar para ocultar actividad maliciosa»,* dijo el equipo de inteligencia de amenazas de Microsoft en un análisis.

> *«El mal uso de OAuth también permite a los actores de amenazas mantener el acceso a aplicaciones incluso si pierden el acceso a la cuenta comprometida inicialmente».*

OAuth, que es la abreviatura de Open Authorization, es un marco de autorización y delegación (en contraposición a la autenticación) que concede a las aplicaciones la capacidad de acceder de manera segura a información de otros sitios web sin revelar contraseñas.

En los ataques detallados por Microsoft, se observa que los actores de amenazas llevan a cabo ataques de phishing o de rociado de contraseñas contra cuentas débilmente protegidas que tienen permisos para crear o modificar aplicaciones OAuth.



Un ejemplo específico es Storm-1283, que utiliza una cuenta de usuario comprometida para crear una aplicación OAuth y desplegar VM para realizar minería de criptomonedas. Además, los atacantes modifican aplicaciones OAuth existentes a las que tiene acceso la cuenta, agregando un conjunto adicional de credenciales para facilitar los mismos objetivos.

En otro caso, un actor no identificado comprometió cuentas de usuario y creó aplicaciones OAuth para mantener la persistencia y lanzar ataques de phishing por correo electrónico. Estos ataques emplean un kit de phishing de adversario en el medio (AiTM) para obtener cookies de sesión de sus objetivos y eludir medidas de autenticación.

> *«En algunos casos, después de la actividad de repetición de cookies de sesión*

> *robadas, el actor aprovechó la cuenta de usuario comprometida para llevar a cabo reconocimiento de fraude financiero BEC abriendo archivos adjuntos de correo electrónico en la Aplicación web de Outlook de Microsoft (OWA) que contienen palabras clave específicas como 'pago' y 'factura'»,* comentó Microsoft.

Otras situaciones detectadas por la empresa después del robo de cookies de sesión incluyen la creación de aplicaciones OAuth para distribuir correos electrónicos de phishing y llevar a cabo actividades masivas de spam. Microsoft está siguiendo esto como Storm-1286.

Para reducir los riesgos asociados con tales ataques, se aconseja que las organizaciones refuercen la autenticación multifactor (MFA), habiliten políticas de acceso condicional y realicen auditorías periódicas de aplicaciones y permisos otorgados.