Boletín de alerta

Boletín Nro.: 48
Fecha de publicación: 07/05/2026
Tema: Alerta 2026-48 Bypass de políticas de acceso condicional en Microsoft Entra ID mediante Device Code Phishing
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Los ataques observados afectan a implementaciones de autenticación de **Microsoft Entra ID** (anteriormente Azure AD) que tengan **habilitado el flujo de autenticación *Device Code Flow* u OAuth Device Authorization Grant.**

Productos y servicios impactados potencialmente:

- **Microsoft Entra ID / Azure AD**
- **Microsoft 365**
- **Microsoft Teams**
- **Microsoft Graph API**
- **Aplicaciones OAuth integradas con Device Code Flow**
- **Aplicaciones que utilizan autenticación "Other clients" en Conditional Access**

Descripción

Recientemente, Microsoft Threat Intelligence reveló una **campaña activa** atribuida al grupo de amenazas **Storm-2372**, actor alineado presuntamente con intereses rusos, que está explotando el flujo de autenticación *Device Code Flow* de Microsoft Entra ID **para evadir controles de autenticación multifactor (MFA)** y políticas de acceso condicional. Esta técnica afecta directamente entornos Microsoft 365 y Azure AD/Entra ID, permitiendo a los atacantes secuestrar sesiones autenticadas y obtener acceso persistente a cuentas corporativas.

El ataque no aprovecha una falla de software tradicional, sino un abuso del mecanismo OAuth 2.0 diseñado para dispositivos con capacidades limitadas de entrada, como Smart TVs, dispositivos IoT o terminales sin navegador completo. Los atacantes generan un código legítimo de autenticación desde infraestructura real de Microsoft y posteriormente engañan a las víctimas mediante correos spear phishing o mensajes por Signal, WhatsApp o Microsoft Teams para que ingresen dicho código en el portal oficial microsoft.com/devicelogin. Una vez que la víctima autentica exitosamente y completa MFA, el atacante recibe automáticamente un token OAuth válido que le permite acceder a la cuenta sin necesidad de robar

credenciales ni contraseñas.

Uno de los aspectos más preocupantes es que este método puede eludir múltiples mecanismos defensivos tradicionales. Debido a que la autenticación ocurre contra infraestructura legítima de Microsoft y el usuario realmente completa MFA, muchas soluciones antiphishing, filtros de reputación URL y controles de seguridad basados en robo de credenciales no detectan la actividad maliciosa. Además, si las políticas de Conditional Access no contemplan explícitamente el tráfico asociado a “Other clients” o Device Code Authentication, los atacantes pueden autenticarse desde sesiones consideradas confiables y heredar el nivel de confianza ya existente del usuario comprometido.

Tras obtener acceso inicial, los actores de amenaza han sido observados realizando enumeración mediante Microsoft Graph API, robo de correos electrónicos, persistencia mediante refresh tokens, movimiento lateral y acceso continuo a recursos corporativos. Microsoft confirmó que las campañas activas han afectado sectores gubernamentales, defensa, telecomunicaciones, salud, educación, energía y empresas tecnológicas en múltiples regiones del mundo desde agosto de 2024.

Solución:

Microsoft recomienda bloquear completamente el uso de Device Code Flow cuando no sea estrictamente necesario dentro del entorno corporativo. Esto puede realizarse mediante políticas de Conditional Access en Microsoft Entra ID, restringiendo específicamente autenticaciones provenientes de “Other clients” o flujos de autenticación heredados.

- Limitar acceso a dispositivos administrados y ubicaciones confiables.
- Implementar autenticación continua y controles de riesgo por identidad.
- Monitorear eventos OAuth anómalos, microsoft.com/devicelogin, Graph API sospechoso y generación inusual de tokens.
- Usar Microsoft Sentinel y Defender for Cloud Apps para detectar Device Code Phishing.
- Ante sospecha, revocar refresh tokens y sesiones (revokeSignInSessions) y forzar reautenticación.
- Revisar consentimientos OAuth recientes y capacitar a usuarios sobre esta técnica basada en ingeniería social y dominios legítimos de Microsoft.

Guía oficial de Microsoft:

- **Storm-2372 Conducts Device Code Phishing Campaign**

Información adicional:

- **https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/**
- **https://www.volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication**
- **https://www.sentrium.co.uk/labs/blocking-device-code-flow-in-microsoft-entra-id**