Microsoft Entra Accounts Targeted Through Device Code Phishing and Vishing

TL;DR

Threat actors, including Russia-linked Storm-2372, are abusing Microsoft Entra's OAuth device code flow to hijack enterprise accounts. Victims are tricked into entering attacker-generated codes on Microsoft's real login page.

Once completed, attackers receive valid access and refresh tokens that can outlive password resets and provide persistent access to Microsoft 365 and connected SaaS apps.

Overview

Attackers are abusing a legitimate Microsoft authentication feature known as the OAuth 2.0 device authorization flow. It was designed for devices like smart TVs and printers that can't easily handle full logins. Instead of typing credentials on the device, users enter a short code on another screen to finish signing in. Threat actors are now generating those codes themselves and convincing employees to enter them at `microsoft[.]com/devicelogin`. The login happens on Microsoft's legitimate site, and the user completes MFA as part of the normal process.

Once the user enters the code and signs in, Microsoft issues authentication tokens tied to the attacker's device session. That includes an access token and a refresh token. The attacker polls the session and retrieves them.

Microsoft has attributed multiple campaigns to Storm-2372. Other state-aligned clusters and financially motivated threat actors have adopted the technique. Activity has increased through late 2025 and into 2026, with open-source phishing kits lowering the barrier to entry.

How the Attack Is Delivered

Attackers generate `a device_code and user_code` using a legitimate OAuth client ID.

Delivery methods include:

- Phishing emails that instruct victims to enter a code to access a document, voicemail, or meeting
- Voice calls where the attacker poses as IT support and walks the employee through the process

In more advanced cases, threat actors have leveraged the Microsoft Authentication Broker flow to register attacker-controlled devices in **Entra ID**. That can result in a Primary Refresh Token (PRT), which provides deeper persistence across services.

With valid tokens, attackers can access:

- Exchange Online
- SharePoint and OneDrive
- Microsoft Teams
- SaaS applications federated through Entra SSO

Password resets alone do not immediately revoke issued refresh tokens. If tokens are not revoked, access can persist. There is no patch for this activity because it does not involve a software flaw. Threat actors are abusing a legitimate Microsoft Entra authentication feature, not exploiting a vulnerability. Mitigation requires configuration changes, such as disabling device code flow if it is not needed or restricting it through Conditional Access policies, rather than installing a security update.

Aspire Protects

- Disable device code authentication if your organization does not require it:
- Update-MgPolicyAuthorizationPolicy -AllowedToUseDeviceCodeFlow $false
- Restrict Conditional Access policies. Limit it to specific users, approved applications, and trusted network locations.
- Review Entra sign-in logs for device code authentication events. Look for unusual geographic patterns or unfamiliar OAuth applications.
- Audit and revoke suspicious OAuth app consents.
- If compromise is suspected, revoke refresh tokens and terminate active sessions immediately. A password reset alone is not enough.
- Educate employees that they should never enter a device login code unless they personally initiated the authentication request.

TTPs to Watch

Initial Access

- Phishing (T1566) – The attacker delivers device codes through phishing emails or voice-based social engineering and convinces the victim to complete authentication.

Credential Access

- Steal Application Access Token (T1528) – The attacker retrieves OAuth access and refresh tokens generated during the device authorization flow.

Defense Evasion

- Use Alternate Authentication Material: Application Access Token (T1550.001) – The attacker authenticates using stolen tokens instead of credentials, bypassing MFA prompts.

Persistence

- Account Manipulation: Device Registration (T1098.005) – In advanced variants, the attacker registers a rogue device in Entra ID to maintain ongoing access.

Behavioral IoCs

- Device code authentication events in Entra sign-in logs
- Unexpected OAuth app consents
- New device registrations tied to user accounts
- Logins from unusual geographic locations following device code flows

Targeted Industries

Recent campaigns have targeted:

- Government
- Defense
- Financial Services
- Technology
- Manufacturing
- Higher Education
- Transportation

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security

professionals to identify and respond to threats across a broader attack surface.

- Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.

- Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

OAuth 2.0 device authorization grant - Microsoft identity platform | Microsoft Learn

RFC 8628 - OAuth 2.0 Device Authorization Grant

A collection of client IDs that can be used to authenticate a user, and their associated application name that shows up in Azure Sign-In logs. · GitHub

Uncovering the Sophisticated Phishing Campaign Bypassing M365 MFA