Kali365 Uses Microsoft Device Codes to Bypass MFA

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

The Federal Bureau of Investigation (FBI) is warning organizations about Kali365, a new phishing service that targets Microsoft 365 users.

Instead of stealing passwords, Kali365 convinces users to approve a login request through Microsoft's device code authentication process. Once approved, a threat actor can gain access to Outlook, Teams, OneDrive, and other Microsoft 365 services using stolen OAuth tokens, often without triggering additional MFA prompts.

Overview

The Federal Bureau of Investigation (FBI) recently released an advisory regarding Kali365, a Phishing-as-a-Service (PhaaS) platform that gives threat actors an easy way to gain access to Microsoft 365 accounts. The service was first observed in April 2026 and is being sold through Telegram.

The attack begins with a phishing email that appears to come from a trusted cloud or document-sharing service. The email instructs the user to visit a legitimate Microsoft verification page and enter a device code. Because the website is real, many users may not realize anything is wrong.

When the code is entered, the user unknowingly approves access for the threat actor's device. The threat actor can then capture OAuth access and refresh tokens associated with the account. Those tokens can be used to access Microsoft 365 resources such as Outlook, Teams, OneDrive, and SharePoint.

Unlike traditional phishing attacks, Kali365 does not need to steal a user's password. The threat actor is using valid authentication tokens issued by Microsoft after the user approves the request. According to the FBI, the service includes phishing templates, AI-generated content, and management tools that help threat actors launch and monitor phishing campaigns.

Aspire Protects

- Review Microsoft Entra ID sign-in logs for device code authentication activity.
- Restrict or disable device code authentication where business operations permit.
- Identify legitimate uses of device code authentication before implementing restrictions.

- Investigate unfamiliar Microsoft 365 sessions and sign-in activity.
- Educate users to be cautious of unexpected requests to enter device codes.
- Encourage users to report suspicious login requests immediately.

TTPs to Watch

Initial Access

- Phishing [T1566] – The threat actor may send phishing emails that direct users to complete a device code authentication request.

Credential Access

- Steal Application Access Token [T1528] – The threat actor may capture OAuth access and refresh tokens after the victim authorizes access.

Persistence

- Valid Accounts: Cloud Accounts [T1078.004] – The threat actor may use stolen OAuth tokens associated with a Microsoft 365 cloud account to maintain access to Outlook, Teams, OneDrive, and other services.

Behavioral IoCs

Security teams should watch for:

- Unexpected device code authentication events
- New or unfamiliar OAuth application authorizations
- Sign-ins from unusual locations
- Unrecognized devices associated with Microsoft 365 accounts
- Suspicious access to Outlook, Teams, OneDrive, or SharePoint

There are no known technical IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Any organization/industry using Microsoft 365 may be affected, including:

- Education
- Energy
- Finance

- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire 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

Internet Crime Complaint Center (IC3) | Kali365 Phishing-as-a-Service Kit Hijacks Microsoft 365 Access Tokens