Internet Crime Complaint Center (IC3)

Published: 2026-05-21 · Archived: 2026-08-06 02:01:09 UTC

The Federal Bureau of Investigation (FBI) is issuing this Public Service Announcement (PSA) to warn the public about an emerging Phishing[1]-as-a-Service[2] (PhaaS) platform called Kali365, first seen in April 2026. Kali365 has primarily been distributed via Telegram, enabling cyber threat actors to obtain Microsoft 365 access tokens and bypass multi-factor authentication[3] (MFA) protocols without intercepting the user's credentials.

Through the Kali365 platform subscription, cyber threat actors can capture "OAuth" tokens and gain persistent access to targeted individuals/entities' Microsoft 365 environments. Kali365 lowers the barrier of entry, providing less-technical attackers access to AI-generated phishing lures, automated campaign templates, real-time targeted individual/entity tracking dashboards, and OAuth token capture capabilities.

How the Scam Works

1. **Lure**: An attacker sends a phishing email impersonating trusted cloud productivity and document-sharing services. This phishing email contains a device code with instructions to visit a legitimate Microsoft verification page and enter the code.
2. **Authorization**: The targeted individuals/entities navigate to the real Microsoft page and pastes in the device code, unknowingly authorizing the attacker's device to access their account.
3. **Token Theft**: The attacker captures OAuth access and refresh tokens, granting them access to the targeted individuals/entities' Microsoft 365 account.
4. **Persistence**: The attacker can now access Microsoft 365 services such as Outlook, Teams, and OneDrive without needing a password or completing any additional MFA challenges.

Tips to Protect Yourself

Restricting device code flow to limit or block device authentication codes can help prevent or limit this style of attack.

- Create a conditional access policy to block device code flow for all users, with limited exceptions for required business processes.
- Audit existing device code flow usage to identify legitimate dependencies before creating a conditional access policy.
- Block authentication transfer policies to prevent users from transferring authentication from computers to mobile devices.
- If you cannot completely restrict device code flow usage, exclude emergency access accounts to prevent lockouts.

Report It

If you or someone you know has been impacted by the Kali365 Phishing kit, file a complaint with the Internet Crime Complaint Center (IC3) at www.ic3.gov. Be sure to include any available information, such as:

- Any phishing emails (email header, body)
- Suspicious logins (time, IP address, location)
- Any unauthorized devices or active sessions added to the account

Please see the Cybersecurity & Infrastructure Security Agency's (CISA) Phishing Guidance: Stopping the Attack Cycle at Phase One, which provides best practices and mitigations to protect against phishing techniques.

Source: https://www.ic3.gov/PSA/2026/PSA260521