INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-25 13:42 UTC

Kali365 Phishing-as-a-Service Platform Abuses OAuth Device Code Flow to Hijack Microsoft 365 Accounts

THREAT CAMPAIGN | **HIGH** | CVSS 8.1

SCC Item ID	SCC-CAM-2026-0363
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	8.1
Affected Products	Microsoft 365 accounts (all plans); OAuth device code authentication flow
Published	2026-05-25
Discovery Source	Gemini

Executive Summary

Security researchers have documented Kali365, a commercial Phishing-as-a-Service platform that exploits Microsoft's OAuth device code authentication flow to hijack Microsoft 365 accounts. Attackers trick users into authorizing access on a legitimate Microsoft login page, generating a persistent session token that bypasses multi-factor authentication entirely. Any organization relying on Microsoft 365 for email, file storage, or collaboration is at risk of account takeover, data exfiltration, and business email compromise without credential theft.

Technical Analysis

Threat actors are deploying phishing-as-a-service platforms that exploit Microsoft's OAuth 2.0 device authorization grant flow (RFC 8628) as an account takeover vector against Microsoft 365. In a device code phishing attack, the threat actor initiates an OAuth device authorization request, obtains a user_code and device_code, then social-engineers the target into visiting the legitimate Microsoft device login page (login.microsoftonline.com/common/oauth2/deviceauth) and entering the attacker-supplied code. Because the victim authenticates on a genuine Microsoft domain, MFA challenges are satisfied by the victim and the resulting access token and refresh token are returned to the attacker's polling client. The attacker retains a long-lived refresh token granting persistent access to Microsoft 365 services, Exchange Online, SharePoint, OneDrive, Teams, without possessing the victim's credentials or requiring any further MFA interaction. These platforms lower the technical barrier for this technique, enabling large-scale campaigns. Relevant CWEs: CWE-287 (Improper Authentication), CWE-384 (Session Fixation), CWE-1390 (Weak Authentication). MITRE ATT&CK:

T1566 (Phishing), T1528 (Steal Application Access Token), T1078 (Valid Accounts), T1621 (Multi-Factor Authentication Bypass), T1550.001 (Use Alternate Authentication Material: Application Access Token). No CVE applies; this exploits a legitimate OAuth feature, not a software vulnerability. No vendor patch exists, mitigation requires policy and detection controls.

Action Checklist

1. Step 1: Containment, Restrict or disable the OAuth device code flow in Microsoft Entra ID (formerly Azure AD) for all users who do not require it for device onboarding. Navigate to Entra ID > Authentication Methods > Device Code Flow and block via Conditional Access policy targeting 'Device Code' as an authentication flow. Per NIST AC-17 (Remote Access) and CIS 6.3, enforce MFA and restrict non-interactive authentication paths for externally-exposed applications. Review and revoke any OAuth tokens granted in the last 90 days that originated from unfamiliar device locations using Microsoft Entra sign-in logs.
2. Step 2: Detection, Query Microsoft Entra ID sign-in logs for authentication method 'Device Code' (AuthenticationDetails field: 'Device Code' or SignInEventType: 'deviceCodeFlow'). Alert on device code authentications originating from locations, ASNs, or device states inconsistent with normal user behavior. In Microsoft Sentinel or your SIEM, correlate AU-2 (Event Logging) and AU-6 (Audit Record Review) controls: look for token issuances followed by access to Exchange, SharePoint, or Teams from a different IP than the authentication event. Hunt for refresh token usage (GrantType: 'refresh_token') from IPs with no prior authentication history for that account. IOC patterns: anomalous OAuth app consent grants, access from Tor/VPN exit nodes, bulk email forwarding rules created post-authentication.
3. Step 3: Eradication, There is no patch; this is a protocol-level technique. Disable device code flow via Conditional Access policy in Entra ID where not operationally required (Microsoft documentation: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview). Revoke all active refresh tokens for confirmed or suspected compromised accounts using Microsoft Graph API (Revoke-MgUserRefreshToken in Microsoft.Graph.Users.Actions PowerShell module) or the Entra ID portal. Implement a Conditional Access policy requiring compliant or Hybrid Azure AD-joined devices for all M365 access, blocking token replay from unauthorized devices per NIST AC-3 (Access Enforcement) and D3-CRO (Credential Rotation).
4. Step 4: Recovery, After token revocation, require re-authentication for all affected accounts. Audit mailbox rules, forwarding addresses, and OAuth application consent grants created during the suspected compromise window. Validate that no persistent access remains via delegated permissions or admin consent grants to unknown third-party apps. Monitor re-authenticated accounts for 30 days for anomalous access patterns per NIST SI-4 (System Monitoring) and AU-6 (Audit Record Review). Confirm Conditional Access policies blocking device code flow are enforced in report mode first, then switch to block mode after validating no legitimate device onboarding is disrupted.
5. Step 5: Post-Incident, This campaign exposes gaps in three control areas: (1) NIST IA-2 (Identification and Authentication), MFA alone does not protect against token-based session hijacking; evaluate phishing-resistant MFA (FIDO2/passkeys) per CISA guidance on phishing-resistant MFA. (2) NIST AC-6 (Least Privilege) and CIS 5.4, review which accounts have access to high-value M365 workloads and apply scoped permissions. (3) AU-12 (Audit Record Generation) and CIS 8.2 (Collect Audit Logs), confirm that Entra ID sign-in logs and unified audit logs are retained for a minimum of 90 days (180 days recommended) and are ingested into your SIEM. Conduct a tabletop exercise simulating OAuth token theft to validate your detection-to-revocation runbook.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to legal, privacy counsel, and senior leadership if Entra ID Unified Audit Log or MailItemsAccessed records confirm attacker access to mailboxes containing PII, PHI, financial data, or attorney-client privileged communications, or if any Global Administrator or privileged role account shows a deviceCode authentication event, as both conditions may trigger mandatory breach notification obligations under HIPAA, GDPR, or applicable state breach notification law.
Recovery Notes	After token revocation and mailbox rule cleanup, re-authenticate all affected accounts through a device-compliant session and verify via 'Get-MgUserOauth2PermissionGrant' that no attacker-registered OAuth apps retain delegated permissions — token revocation alone does not remove delegated permission grants, which can survive as an independent re-entry vector. Monitor re-authenticated accounts via the Unified Audit Log for a minimum of 30 days, specifically watching for recurrence of deviceCode authentication events, new inbox rule creation, and any MailItemsAccessed volume spikes that would indicate a second operator session using a previously unknown token. Validate that Conditional Access policy blocking device code flow is confirmed in 'block' mode (not report-only) for all non-device-onboarding user populations before closing the incident.
Forensic Artifacts	Entra ID Interactive and Non-Interactive Sign-In Logs filtered on AuthenticationProtocol = 'deviceCode': captures the exact moment each Kali365 phishing lure succeeded, including the user UPN, source IP/ASN, device ID (absent for unauthorized devices), and OAuth access token issuance timestamp — the foundational artifact for establishing the initial compromise timeline. | Microsoft 365 Unified Audit Log — MailItemsAccessed operation: records every OAuth client that accessed mailbox content post-token-issuance, with client_id, IP, and item count, directly evidencing Kali365 operator data access and enabling quantification of potential PII/PHI exposure for breach notification purposes. | Microsoft 365 Unified Audit Log — New-InboxRule and Set-Mailbox operations: captures attacker-created email forwarding rules and ForwardingSmtpAddress changes planted during the compromise window to establish mail persistence independent of the OAuth session — these survive token revocation and are a critical eradication verification artifact. | Entra ID Audit Logs — 'Consent to application' and 'Add delegated permission grant' operations: records every OAuth application that received user or admin consent during the attack window, including the client_id, permission scope (e.g., Mail.Read, Files.ReadWrite), and consenting user — directly identifies attacker-registered apps used by Kali365 for persistent access. | SharePoint and OneDrive Unified Audit Log — AnonymousLinkCreated, SharingSet, and FileDownloaded operations: captures bulk file access and external sharing link creation by the OAuth-authenticated attacker session, providing evidence of data exfiltration scope tied specifically to the compromised M365 file storage workloads targeted in Kali365 campaigns.

Per-Action IR Details

Step 1: Containment — Restrict or disable the OAuth device code flow in Microsoft Entra ID (formerly Azure AD) for all users who do not require it for device onboarding. Navigate to Entra ID > Authentication Methods > Device Code Flow and block via Conditional Access policy targeting 'Device Code' as an authentication flow. Per NIST AC-17 (Remote Access) and CIS 6.3, enforce MFA and restrict non-interactive authentication paths for externally-exposed applications. Review and revoke any OAuth tokens granted in the last 90 days that originated from unfamiliar device locations using Microsoft Entra sign-in logs.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-17 (Remote Access), NIST AC-3 (Access Enforcement), NIST AC-7 (Unsuccessful Logon Attempts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For teams without Entra ID P1/P2 licensing required for Conditional Access: use PowerShell to enumerate and revoke active refresh tokens for all users via 'Get-MgUser | ForEach-Object { Revoke-MgUserSignInSession -UserId $_.Id }' (Microsoft Graph PowerShell SDK, free). Export sign-in logs manually from Entra ID portal (free tier retains 7 days) and parse for 'deviceCode' in the AuthenticationMethod column using a simple PowerShell CSV filter: 'Import-Csv signinlogs.csv | Where-Object { $_.AuthenticationMethod -eq "Device Code" }'. Prioritize token revocation for admin and high-privilege accounts first.

Evidence: Before revoking tokens, export and preserve the full Entra ID Sign-In Logs (portal: Entra ID > Monitoring > Sign-in logs) filtered on AuthenticationProtocol = 'deviceCode' for the prior 90 days — this captures the exact user, timestamp, IP, ASN, device ID (or absence thereof), and token issuance event tied to each Kali365-style phishing lure. Also capture the Entra ID Audit Logs showing any OAuth app consent grants (Operation: 'Consent to application') created during the same window, as Kali365 operators may have registered persistent delegated permissions. Preserve these exports to immutable storage before any revocation action destroys the evidentiary chain.

Step 2: Detection — Query Microsoft Entra ID sign-in logs for authentication method 'Device Code' (AuthenticationDetails field: 'Device Code' or SignInEventType: 'deviceCodeFlow'). Alert on device code authentications originating from locations, ASNs, or device states inconsistent with normal user behavior. In Microsoft Sentinel or your SIEM, correlate AU-2 (Event Logging) and AU-6 (Audit Record Review) controls: look for token issuances followed by access to Exchange, SharePoint, or Teams from a different IP than the authentication event. Hunt for refresh token usage (GrantType: 'refresh_token') from IPs with no prior authentication history for that account. IOC patterns: anomalous OAuth app consent grants, access from Tor/VPN exit nodes, bulk email forwarding rules created post-authentication.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without Sentinel, use the Microsoft 365 Unified Audit Log (free, retained 90 days for E3+) queried via PowerShell: 'Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-90) -EndDate (Get-Date) -Operations "UserLoggedIn" | Where-Object { $_.AuditData -like "*deviceCode*" }'. For refresh token abuse detection, query: 'Search-UnifiedAuditLog -Operations "MailboxLogin" | Where-Object { $_.ClientIP -ne $previousAuthIP }' — pipe output to CSV for manual IP comparison. Use the free Sigma rule 'azure_ad_device_code_phishing.yml' (available in SigmaHQ GitHub repository) converted to a KQL query if you have any log forwarding capability. Flag any New-InboxRule or Set-Mailbox operations in the UAL that follow within 60 minutes of a deviceCode authentication event.

Evidence: Capture Microsoft 365 Unified Audit Log entries for MailItemsAccessed, New-InboxRule, Set-Mailbox (ForwardingSmtpAddress), and FileAccessed operations in Exchange, SharePoint, and OneDrive occurring within 24 hours after each identified deviceCode token issuance — this is the lateral movement and data access trail specific to post-authentication Kali365 activity. Collect Entra ID Non-Interactive Sign-In Logs separately (these are suppressed in the standard sign-in log view) as refresh token re-use by Kali365 operators appears here, not in the interactive log. Document the full OAuth token chain: authorization code issuance time, access token issuance, and first refresh token use, including the client_id of the application that received the grant.

Step 3: Eradication — There is no patch; this is a protocol-level technique. Disable device code flow via Conditional Access policy in Entra ID where not operationally required (Microsoft documentation: aka.ms/conditionalaccess). Revoke all active refresh tokens for confirmed or suspected compromised accounts using Microsoft Graph API (Revoke-AzureADUserAllRefreshToken) or the Entra ID portal. Implement a Conditional Access policy requiring compliant or Hybrid Azure AD-joined devices for all M365 access,

blocking token replay from unauthorized devices per NIST AC-3 (Access Enforcement) and D3-CRO (Credential Rotation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST IA-2 (Identification and Authentication — Organizational Users), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For teams without Entra ID P1 (required for device compliance Conditional Access): use the free Microsoft Graph PowerShell command 'Invoke-MgInvalidateAllUserRefreshToken -UserId ' for each compromised account to immediately invalidate all issued refresh tokens — this forces re-authentication and terminates any active Kali365 operator session. Audit and remove unauthorized OAuth application consent grants using the free Entra ID portal view (Enterprise Applications > All Applications, filter by 'User consent') and revoke any app with permissions to Mail.Read, Mail.ReadWrite, Files.Read, or Contacts.Read that was not IT-provisioned. Document each revoked app's client_id and grant date for the incident record.

Evidence: Before revoking tokens, preserve a snapshot of all active OAuth delegated permission grants for affected accounts via PowerShell: 'Get-MgUserOauth2PermissionGrant -UserId ' — this records exactly which third-party or attacker-registered apps hold live delegated access, including scope, client_id, and consent timestamp, which is the forensic proof of persistent access established by the Kali365 operator. Also capture 'Get-MgUserAuthenticationMethod -UserId ' to confirm no attacker-registered authentication methods (e.g., additional MFA factors or FIDO2 keys) were added to the account during the compromise window.

Step 4: Recovery — After token revocation, require re-authentication for all affected accounts. Audit mailbox rules, forwarding addresses, and OAuth application consent grants created during the suspected compromise window. Validate that no persistent access remains via delegated permissions or admin consent grants to unknown third-party apps. Monitor re-authenticated accounts for 30 days for anomalous access patterns per NIST SI-4 (System Monitoring) and AU-6 (Audit Record Review). Confirm Conditional Access policies blocking device code flow are enforced in report mode first, then switch to block mode after validating no legitimate device onboarding is disrupted.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AC-2 (Account Management), NIST AU-11 (Audit Record Retention), CIS 6.1 (Establish an Access Granting Process), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without an automated SIEM for 30-day monitoring, establish a weekly manual review cadence using PowerShell: 'Search-UnifiedAuditLog -UserIds -StartDate -EndDate (Get-Date) -Operations "MailboxLogin","FileAccessed","New-InboxRule"' — pipe to CSV and diff against the pre-compromise baseline. Use the free Microsoft 365 Message Trace (Admin Center > Exchange > Mail flow > Message trace) to verify no active forwarding rules are silently redirecting mail post-recovery. Set a calendar reminder to re-run 'Get-MgUserOauth2PermissionGrant' on all affected accounts at days 7, 14, and 30 to catch any re-consented attacker apps.

Evidence: Collect a post-revocation baseline of all inbox rules ('Get-InboxRule -Mailbox ' via Exchange Online PowerShell) and forwarding addresses ('Get-Mailbox | Select ForwardingSmtpAddress, DeliverToMailboxAndForward') immediately after token revocation — compare against any pre-incident snapshots to identify Kali365 operator-planted persistence mechanisms that survive token invalidation. Capture SharePoint and OneDrive sharing link audit events (Unified Audit Log operation: 'SharingSet', 'AnonymousLinkCreated') for the compromise window, as Kali365 post-access activity commonly includes creating persistent external sharing links to exfiltrate data independently of the OAuth session.

Step 5: Post-Incident — This campaign exposes gaps in three control areas: (1) NIST IA-2 (Identification and Authentication) — MFA alone does not protect against token-based session hijacking; evaluate phishing-resistant MFA (FIDO2/passkeys) per CISA guidance on phishing-resistant MFA. (2) NIST AC-6 (Least

Privilege) and CIS 5.4 — review which accounts have access to high-value M365 workloads and apply scoped permissions. (3) AU-12 (Audit Record Generation) and CIS 8.2 (Collect Audit Logs) — confirm that Entra ID sign-in logs and unified audit logs are retained for a minimum of 90 days (180 days recommended) and are ingested into your SIEM. Conduct a tabletop exercise simulating OAuth token theft to validate your detection-to-revocation runbook.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IA-2 (Identification and Authentication — Organizational Users), NIST AC-6 (Least Privilege), NIST AU-12 (Audit Record Generation), NIST AU-11 (Audit Record Retention), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 8.2 (Collect Audit Logs)

Compensating: For the tabletop exercise without a dedicated purple team: use the free Microsoft Attack Simulator (included in M365 E3/E5, Defender for Office 365 Plan 2) to launch a simulated OAuth consent phishing campaign targeting your own users, then measure time-to-detection using only the Unified Audit Log and manual PowerShell queries — this directly validates whether your 2-person team can detect and revoke a Kali365-style token grant within an acceptable window. For FIDO2/passkeys evaluation without budget: pilot the free Microsoft Authenticator passkey feature (available to all Entra ID tenants) on admin accounts first, measuring enrollment friction before broader rollout.

Evidence: For lessons-learned documentation, compile the full timeline from earliest deviceCode token issuance (Entra ID sign-in log) through last confirmed attacker access (Unified Audit Log MailboxLogin or FileAccessed) to measure dwell time — this metric directly informs detection rule tuning thresholds for future Kali365 or similar OAuth phishing campaigns. Preserve the client_id values of any attacker-registered or abused OAuth applications as organizational threat intelligence IOCs to block via Conditional Access app restrictions or Defender for Cloud Apps policies going forward.

Detection Guidance

Primary log source: Microsoft Entra ID Sign-In Logs (available in Azure portal and exportable to SIEM). Filter for AuthenticationProtocol = 'deviceCode' or AuthenticationDetail containing 'Device Code Flow'. Correlate sign-in IP with subsequent Microsoft 365 activity IP, divergence is a strong indicator of token replay. In Microsoft Sentinel, use the 'Suspicious application consent' and 'OAuth app with unusual user agent' analytics rules as a baseline. Secondary log source: Microsoft 365 Unified Audit Log, hunt for New-InboxRule events and Set-Mailbox with ForwardingSmtpAddress set within 24 hours of a device code authentication event. Behavioral indicators: (1) User authenticates via device code from an unknown ASN or country; (2) Refresh token used from a different IP/country than initial auth within minutes; (3) Bulk email export or OneDrive download activity immediately post-token issuance; (4) OAuth app consent granted to an application with broad Mail.Read, Files.ReadWrite.All, or Contacts.Read scopes. Apply D3-LAM (Local Account Monitoring) principles: baseline normal OAuth app usage per user and alert on new app consent grants. NIST AU-6 and CIS 8.2 require that these logs be actively reviewed, passive collection without alerting is insufficient for this threat.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`login.microsoftonline.com/common/oauth2/deviceauth`	Legitimate Microsoft device code authentication endpoint abused in Kali365 campaigns — users directed here to enter attacker-supplied codes. Presence of this URL in user-reported phishing lures is a direct indicator.	HIGH

Framework Mappings

MITRE-ATTACK

- **T1566** — Phishing
- **T1528** — Steal Application Access Token
- **T1078** — Valid Accounts
- **T1111** — Multi-Factor Authentication Interception
- **T1550.001** — Application Access Token

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566	Phishing	Initial-Access
T1528	Steal Application Access Token	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1111	Multi-Factor Authentication Interception	Credential-Access
T1550.001	Application Access Token	Defense-Evasion

Sources

Source	URL	Tier
What happens if there's an unusual sign-in to your account	https://support.microsoft.com/en-us/account-billing/what-happens-if...	T1
9 out of 10 Enterprises Have Vulnerabilities in their Microsoft 365 ...	https://www.coreview.com/news/enterprises-vulnerabilities-microsoft...	T3
How to recover a hacked or compromised Microsoft account	https://support.microsoft.com/en-us/accounts-billing/manage/how-to-...	T1
Microsoft Office 365 Breach : r/cybersecurity - Reddit	https://www.reddit.com/r/cybersecurity/comments/1oj8nnw/microsoft_o...	T3
A Timeline of Microsoft Data Breaches and Vulnerabilities - Virtru	https://www.virtru.com/blog/industry-updates/microsoft-data-breache...	T3

Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-05-25 13:42 UTC by TJS Security Command Center