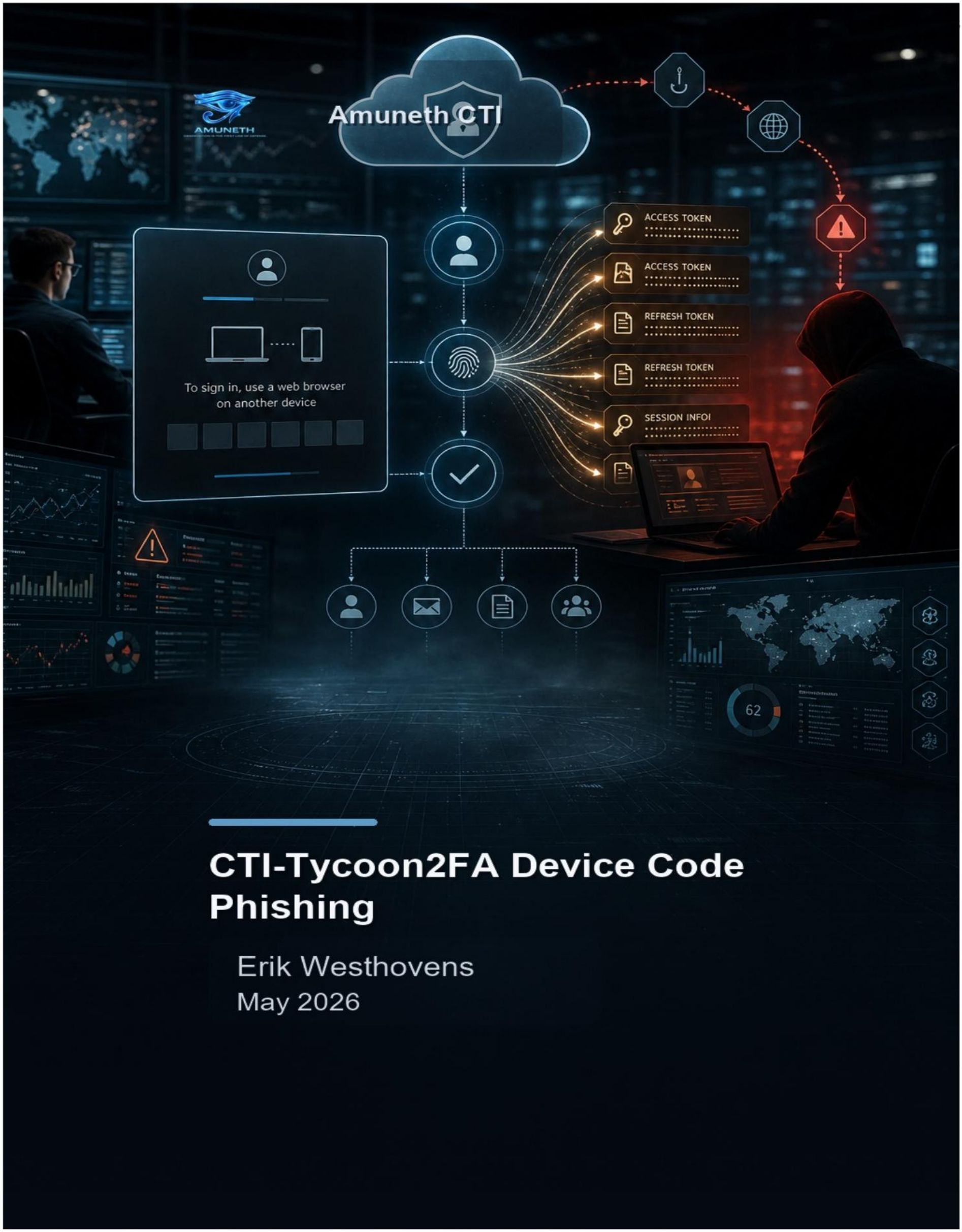

CTI-Tycoon2FA Device Code Phishing

Erik Westhovens

May 2026

REPORT HEADER

Cyber Threat Intelligence Report

Subject: How OAuth device-code phishing bypasses traditional MFA and abuses Microsoft 365 tokens

Audience: SOC, Incident Response, Threat Hunting, Identity Security, Security Leadership

Date: May 2026

Author: Erik Westhovens

Management Summary

Tycoon2FA is evolving from a classic adversary-in-the-middle phishing kit into a delivery framework for OAuth device-code phishing. The central risk is that the victim does not merely surrender a password or MFA response, but authorizes tokens for an attacker-controlled device through a legitimate Microsoft authentication flow.

This attack matters because the visible login page can be genuine. The user is sent to Microsoft's legitimate device-login page, enters a code, and completes MFA normally. To the user, the process appears trustworthy, while Microsoft issues access and refresh tokens to the actor operating the phishing campaign.

The operational impact is concentrated around Microsoft 365 and Entra ID. A valid token can provide access to Exchange Online, Microsoft Graph, OneDrive for Business, and other cloud data within the user's permissions. Password rotation alone is not sufficient when active sessions, refresh tokens, device registrations, or OAuth consents remain valid.

For defenders, the priority shifts from phishing awareness alone to identity telemetry, token control, Conditional Access for authentication flows, device registration governance, Graph API monitoring, and rapid session revocation during incident response.

Key Takeaways

- Device-code phishing abuses a legitimate OAuth flow and does not need to show a fake Microsoft login page.
- MFA is not technically broken; the user authorizes a valid attacker session.
- Detection should focus on device-code flow events, token activity, new device registrations, suspicious Graph API activity, and abnormal sign-in patterns.
- Microsoft recommends getting as close as possible to a full block on device code flow and allowing only well-documented exceptions.

Chapter 1

1. Threat Overview

Tycoon2FA shows how phishing is shifting from credential theft to identity session compromise.

Tycoon2FA is a phishing-as-a-service kit previously known for adversary-in-the-middle login flows that intercepted credentials, MFA responses, and session cookies. In March 2026, Microsoft described how Tycoon2FA impersonated trusted brands at scale and enabled continued access unless active sessions and tokens were explicitly revoked.

The recent development is that the same operational layer is now being used for OAuth device-code phishing. eSentire analyzed a late-April 2026 campaign in which a Trustifi click-tracking URL in a lure email ultimately led to Microsoft's legitimate device-login flow. The victim entered an actor-generated code and authorized tokens for the actor-controlled device.

For organizations, this represents a clear escalation in identity risk. The attack is less dependent on a convincing fake login page and more dependent on abusing genuine authentication processes. As a result, the familiar user guidance to check whether the login page is real is no longer sufficient as a standalone defense.

Assessment

- The attack uses legitimate Microsoft authentication as part of the social-engineering chain.
- The primary objective is token and session access, not only the password.
- MFA remains important, but ordinary MFA may not prevent this flow when the user approves the transaction.

Chapter 2

2. Actor and Campaign Profile

Tycoon2FA is most relevant as a reusable commercial kit, not only as a single actor label.

Tycoon2FA should be treated as enabling infrastructure for multiple operators. The value of the kit lies in lowering the barrier for phishing campaigns that attempt to bypass MFA and session security. Microsoft and partners disrupted Tycoon2FA infrastructure in March 2026, but eSentire later reported continued activity and reuse of Tycoon2FA fingerprints.

eSentire linked the device-code variant to known Tycoon2FA characteristics, including Check Domain architecture, encryption layers, anti-debugging, and HTML wrapping patterns. This suggests that the lure changed, while the underlying framework remained largely recognizable.

Attribution should therefore remain cautious. The defensive focus is not the operator name, but the repeatable attack chain: lure delivery, redirect and filtering, device-code authorization, token abuse, and cloud data access.

Attribution Notes

- Treat Tycoon2FA as a PhaaS capability that can be used by different operators.
- Post-takedown activity shows that disruption does not automatically end the tradecraft.
- Detect the technique and token outcomes, not only known domains.

Chapter 3

3. Initial Access and Delivery

The delivery chain uses reputation, redirects, and anti-analysis controls to move the victim toward the real device-login flow.

The campaign described by eSentire began with a lure email themed as a forwarded vendor invoice reminder. The initial click passed through a Trustifi click-tracking URL. eSentire stated that it had no evidence of a Trustifi vulnerability; the actor abused the reputation and redirect functionality of a legitimate service.

The victim was then redirected to a Cloudflare Workers subdomain where the in-browser delivery chain used several layers. The page included encrypted payloads, anti-debug controls, headless and proxy detection, and ASN-based filtering against cloud providers, security vendors, sandboxes, and analysis platforms.

These layers matter for SOC teams because simple sandboxing or URL preview may not expose the full malicious flow. The live payload may be shown only to targets that pass the filtering logic, while researchers or security tools may see a blank page, redirect, or expired content.

Delivery Indicators

- Legitimate click tracking and cloud hosting can create reputation laundering.
- Anti-analysis makes static URL assessment less reliable.
- Suspicious device-code instructions in email, Teams, SharePoint, or invoice-themed lures should be prioritized.

Chapter 4

4. Device-Code Phishing Mechanics

The attack centers on making the user authorize a code that was requested by the actor.

Device code authentication is intended for devices with limited input capabilities. A device requests a code; the user enters that code on another device through a legitimate login page; the original client then receives tokens. In a phishing context, the actor requests the code and tricks the victim into entering it.

Microsoft explains that an actor can receive access and refresh tokens through this process and then access accounts and data within the user's permissions. In the Storm-2372 campaign, Microsoft observed Microsoft Graph use for mailbox searches and email collection.

The critical point is that MFA can be completed correctly in this flow. The user confirms the login but does not understand that the authorization applies to an actor-controlled session. This means many traditional trust signals - genuine login page, valid TLS, successful MFA - may appear reassuring while the attack succeeds.

Attack Logic

- The user enters the code on a genuine Microsoft page.
- The attacker receives tokens through the client that initiated the device-code flow.
- MFA bypass in this case is primarily trust abuse, not a cryptographic break.

Chapter 5

5. Token Abuse and Microsoft 365 Impact

A successful token opens access to cloud data and may remain useful beyond the phishing moment itself.

Tycoon2FA device-code campaigns target session and token material. eSentire reported that the observed variant impersonated Microsoft Authentication Broker, with Exchange Online, Microsoft Graph, and OneDrive for Business as relevant Microsoft 365 surfaces.

With valid tokens, an actor can search mailboxes, access files, make Graph API calls, and send internal phishing from the compromised account. Microsoft observed device-code phishing actors searching mailboxes for terms such as username, password, admin, credentials, and secret.

The impact can grow when the actor uses a refresh token for additional token requests or device registration. Microsoft described that Storm-2372's use of the Microsoft Authentication Broker client ID could help register an actor-controlled device and obtain broader resource access.

Business Impact

- Password reset without token revocation is insufficient.
- Review inbox rules, forwarding, OAuth consents, device registrations, and Graph API activity.
- Compromised accounts may be used for lateral phishing inside the same organization.

Chapter 6

6. Defensive Risk Assessment

The highest exposure sits with organizations that allow device code flow without clear use cases.

Organizations with broad Microsoft 365 adoption, extensive external collaboration, BYOD usage, permissive Conditional Access, and limited Entra ID monitoring face elevated risk. The attack does not need to leave endpoint malware behind, which can make EDR-centered response late or incomplete.

The threat is especially relevant for users with access to sensitive mailboxes, finance workflows, SharePoint sites, OneDrive data, executive communications, HR data, supplier information, and customer records. A single successful authorization may be enough to collect confidential cloud data.

Barracuda reported more than 7 million device-code phishing attacks in four weeks in April 2026 and observed other attackers combining the approach with Tycoon2FA capabilities. This points to rapid commercialization and makes it likely that device-code phishing will be adopted by more phishing kits.

Risk Drivers

- Risk is high when device code flow is available to all users by default.
- The attack is harder to recognize because legitimate Microsoft URLs may be used.
- Leadership should treat this as an identity control gap, not only an awareness problem.

Chapter 7

7. Detection and Threat Hunting

Hunting must combine identity, token, device registration, and Microsoft Graph activity.

The primary hunt hypothesis is: a user completed a device-code flow that does not match a known business use case, followed by token or Graph API activity from unfamiliar infrastructure. Combine Entra sign-in logs, audit logs, Defender XDR, Cloud App Security, Exchange audit, and endpoint or context data.

Microsoft recommends monitoring for device-code phishing attempts, risky sign-ins, anomalous token activity, close-in-time device registrations, and refresh token revocation during suspected compromise. Defender XDR or Sentinel queries should not look only for failed sign-ins, but also for successful device-code flow events.

Practical signals include sign-ins using the device code authentication protocol, user-agent patterns such as command-line clients or Node.js libraries during operator polling, sudden Graph Mail.Read or Files.Read-like activity, mailbox searches for credential terms, new inbox rules, forwarding, impossible travel, and new device registrations shortly after a suspicious login.

Hunt Leads

- Search for successful device-code flow events, not only blocked attempts.
- Correlation across Entra ID, Exchange, Graph, and Defender is required.
- A clean endpoint does not mean the account is clean.

Chapter 8

8. Response and Containment

Containment must include tokens, sessions, devices, and OAuth consents.

When device-code phishing is suspected, the account should be temporarily blocked or placed under heightened control. Refresh tokens and active sessions should then be revoked, the password reset, MFA methods reviewed, and MFA registration repeated where necessary.

Next, check whether actor-controlled devices were registered, whether new OAuth app consents exist, whether inbox rules or forwarding were added, and whether Graph API or Exchange Online was used for bulk search or exfiltration. Separate account takeover, data access, and potential lateral phishing during scoping.

User communication should be concrete: do not enter codes at microsoft.com/devicelogin unless the request matches a known business action that you initiated yourself. A real Microsoft page can still be part of an attack when the code was supplied by someone else.

Containment Checklist

- Revoke sessions and refresh tokens immediately when compromise is suspected.
- Investigate device registrations and OAuth consents alongside mailbox activity.
- Search for internally forwarded phishing from the compromised account.

Chapter 9

9. Recommendations and Outlook

The most effective measures are restricting device code flow and strengthening identity assurance.

Microsoft recommends getting as close as possible to a full block on device code flow. Start with report-only Conditional Access to inventory legitimate usage, then allow only well-documented exceptions for legacy tooling or specific secured use cases.

Strengthen MFA with phishing-resistant methods such as FIDO2 security keys, passkeys, or Windows Hello for Business. Combine this with Conditional Access for compliant devices, sign-in risk, location, client app, authentication flows, and privileged users. Restrict who can register devices and review break-glass exclusions periodically.

The outlook is that device-code phishing will be integrated into more phishing kits. Tycoon2FA shows that the same PhaaS operators can adapt their framework from credential relay to token authorization. Organizations without mature identity telemetry and token response will remain exposed to this shift.

Recommended Actions

- Block device code flow unless there is a demonstrable business use case.
- Make token revocation and OAuth consent review standard parts of account compromise response.
- Train users specifically on device-code requests, QR codes, and login prompts they did not initiate.

SOC Reference

Detection and Response Matrix

Use this matrix as a starting point for SOC hunting and incident response around device-code phishing in Microsoft 365 and Entra ID.

How to use this reference

- First validate whether device code flow is legitimately used in the organization.
- Prioritize successful events with unknown location, unknown device, abnormal user-agent, or follow-on Graph activity.
- Treat token activity as compromise evidence even when MFA succeeded.

Area	Signal	Action
Entra ID	Successful sign-in using device code flow outside known use cases.	Investigate user context, source IP, client app, authentication details, and close-in-time activity.
Tokens	Anomalous token, refresh token reuse, new session after suspicious code entry.	Revoke sessions and refresh tokens, then force re-authentication.
Device	New device registration shortly after suspicious sign-in.	Disable or remove suspicious device, review enrollment permissions and Conditional Access.
Microsoft Graph	Unusual mail search, file access, bulk read, or API calls after token issuance.	Scope data access, preserve logs, and check for exfiltration indicators.
Exchange Online	New inbox rules, forwarding, internal phishing sent from compromised mailbox.	Remove rules, block forwarding, search tenant for follow-on lures.
User report	User entered a code from email, Teams, QR code, invoice, or document lure.	Treat as account compromise until token, device, and OAuth checks are complete.

Matrix entries are intentionally technology-neutral and should be translated into Sentinel, Defender XDR, SIEM, or SOAR content based on available telemetry.

Reference Material

Sources

eSentire TRU - Tycoon 2FA Operators Adopt OAuth Device Code Phishing

https://www.esentire.com/blog/tycoon-2fa-operators-adopt-oauth-device-code-phishing

Published May 12, 2026. Source for the observed Tycoon2FA device-code campaign, delivery chain, Microsoft Authentication Broker impersonation, and technical fingerprints.

Microsoft Security Blog - Inside Tycoon2FA: How a leading AiTM phishing kit operated at scale

https://www.microsoft.com/en-us/security/blog/2026/03/04/inside-tycoon2fa-how-a-leading-aitm-phishing-kit-operated-at-scale/

Published March 4, 2026. Source for Tycoon2FA background, takedown context, session cookie interception, and persistence risk.

Microsoft Security Blog - Storm-2372 conducts device code phishing campaign

https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/

Published February 13, 2025, updated February 14, 2025. Source for device-code phishing mechanics, token abuse, Graph activity, and mitigation guidance.

Microsoft Learn - Block authentication flows with Conditional Access policy

https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-authentication-flows

Microsoft guidance updated April 7, 2026. Source for blocking or restricting device code flow through Conditional Access.

Barracuda - Device code phishing is on the rise with 7 million attacks in four weeks

https://blog.barracuda.com/2026/04/23/threat-spotlight-device-code-phishing

Published April 23, 2026. Source for scale reporting, device-code phishing advantages, and observation that attackers combine the approach with Tycoon2FA capabilities.

Partner Profile

About Amuneth

Amuneth provides intelligence-led security operations designed to help organizations detect, investigate, and contain modern threats across identity, endpoint, network, and cloud environments. Our reporting bridges executive decision-making and operational action by combining threat context, analyst judgment, and practical detection guidance.

For CTI consumers, this final page gives reusable context on the operating model behind the report and clarifies how Amuneth supports ongoing monitoring, escalation, and proactive hunting beyond the specific topic covered in the report.

Security Operations Center

- Continuous monitoring across endpoint, identity, cloud, and network telemetry.
- Triage and escalation workflows that prioritize verified risk over raw alert volume.
- Operational coordination with customer stakeholders during incidents, containment, and follow-up investigation.

Threat Hunting Capabilities

- Hypothesis-driven hunting for identity abuse, stealthy persistence, lateral movement, and data exfiltration patterns.
- Targeted hunts based on current CTI findings, campaign tradecraft, and environment-specific risk signals.
- Cross-source correlation between endpoint, Microsoft 365, Entra ID, firewall, proxy, and cloud telemetry to validate or dismiss emerging attacker behavior.

CTI and Reporting Approach

Amuneth reports are built to support both management and frontline defenders. Each report explains why the development matters, how the threat behaves, where detection opportunities exist, and which defensive actions should be prioritized next.

This standardized format keeps reporting visually consistent while making room for actor-specific findings, malware analysis, campaign tradecraft, and strategic risk interpretation.