IMPORTANT CYBERSECURITY NEWS: RUSSIAN HACKERS EXPLOIT MICROSOFT DEVICE CODE AUTHENTICATION IN TARGETED ATTACKS AGAINST M365 ACCOUNTS

Vairav Cyber Security News Report

Date: 2025-02-17

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

Thirbam Sadak 148
Baluwatar, Kathmandu

EXECUTIVE SUMMARY

A recent cybersecurity incident has emerged involving Russian threat actors exploiting Microsoft's Device Code Authentication to compromise Microsoft 365 (M365) accounts. Attackers are conducting sophisticated phishing campaigns, impersonating officials from entities such as the U.S. Department of State and the Ukrainian Ministry of Defence, to deceive users into granting access to their accounts. This method allows attackers to bypass traditional multi-factor authentication (MFA) mechanisms, posing significant risks to targeted organizations.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: The attackers employ Device Code Authentication phishing, a technique that leverages Microsoft's legitimate device code authentication flow. By sending phishing emails or messages that prompt users to enter a device code on a legitimate Microsoft page, attackers capture authentication tokens, granting them unauthorized access to M365 accounts.

Identification: Cybersecurity firm Volexity observed these campaigns starting in mid-January 2025. Microsoft's Threat Intelligence Center also reported similar activities, noting the exploitation of device code authentication in phishing attacks.

Threat Actor: The campaigns have been attributed to Russian nation-state actors, specifically groups such as Storm-237, CozyLarch (APT29) and others tracked as UTA0304 and UTA0307. These groups are known for conducting espionage activities aligned with Russian interests.

Affected Entities/Industries: The attacks have primarily targeted organizations across various sectors, including government agencies, non-governmental organizations (NGOs), information technology services, defense, telecommunications, health, higher education, and energy sectors. Geographically, victims span regions such as Europe, North America, Africa, and the Middle East.

Potential Impact: Compromised accounts can lead to unauthorized data access, including sensitive communications and intellectual property. Attackers may leverage this access for espionage, data exfiltration, and establishing persistent footholds within networks, potentially leading to further exploitation or operational disruptions.

Exploitation Methods: Attackers initiate contact through messaging platforms like WhatsApp, Signal, or Microsoft Teams, posing as trusted individuals to build rapport. They then send phishing messages containing device codes, prompting users to authenticate on legitimate Microsoft pages. Once the code is entered, attackers capture the resulting authentication tokens, granting them access to the user's M365 account without needing passwords.

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- **Disable Device Code Authentication**: If not required, consider disabling device code authentication to prevent its exploitation.
- **Revoke Suspicious Tokens:** Immediately revoke any authentication tokens associated with suspicious activities to prevent unauthorized access.

Security Best Practices

- **Enhance User Awareness:** Educate users about the risks of phishing attacks, especially those involving device code prompts, and encourage them to verify unsolicited authentication requests.
- **Implement Conditional Access Policies:** Configure policies to restrict device code authentication to trusted devices or networks only.

For Advanced Security Teams

- **Monitor Authentication Logs:** Continuously monitor and analyze authentication logs for anomalies, such as unexpected device code authentications or access from unfamiliar locations.
- **Deploy Advanced Threat Protection:** Utilize advanced security solutions capable of detecting and responding to sophisticated phishing attempts and unauthorized token usage.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://www.volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication/
- https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/#Update-February-14
- https://www.bleepingcomputer.com/news/security/microsoft-hackers-steal-emails-in-device-code-phishing-attacks/
- https://thehackernews.com/2025/02/microsoft-russian-linked-hackers-using.html

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com