EnCyb

Severity: High

Advisory Type: Security

# Weak Cookie Encryption in Microsoft Teams

Advisory Report

TLP: AMBER

## SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

## EXECUTIVE SUMMARY

A new BOF (Beacon Object File) tool exploits weak cookie encryption in Microsoft Teams to steal user tokens and chats. It abuses MS Teams' reliance on the user's DPAPI key instead of stronger browser protections. This enables stealthy account impersonation without admin access.

- Active Region: Global
- Affected Sector: General
- Affected Product: Microsoft Teams (Weak Cookie Encryption in Microsoft Teams)
- Severity: High
- Published Date: November 3, 2025

## TECHNICAL DETAILS

Stealthy in-process BOF attack commonly referenced as teams-cookies-bof that duplicates Teams/WebView2 cookie handles, decrypts DPAPI-protected cookies, and steals tokens to read/send chats and access Microsoft Graph.

- **Target:** Local token/cookie theft via in-process handle duplication and process injection (BOF/DLL or COM hijack) enables credential misuse and impersonation.
- **Root Cause:** Teams protects cookies with the current user's DPAPI master key (user-level protection) rather than a SYSTEM-level service like modern Chromium browsers, plus the WebView2 process keeps a locked cookies file that can be read via duplicated handles from inside a process.
- **Prerequisite for Exploitation:** The attacker must achieve code execution in the targeted user's session (examples: a C2 implant/Beacon, BOF loaded into Beacon, a malicious script, or in-process injection). Local admin or tenant admin privileges are not required; access to the user profile and ability to invoke DPAPI (CryptUnprotectData) from the same user context is sufficient. Techniques such as DLL/COM hijacking or reflective loading are feasible delivery/implant options but are not strictly required for every variant.

## IMPACT

- Attackers can send messages as the victim, enabling targeted phishing and fraud.
- Attackers can read chat histories and attachments to steal sensitive business information.
- Stolen tokens permit Microsoft Graph calls to access mail, OneDrive, SharePoint and expand compromise across the tenant.
- Access and refresh tokens can be abused repeatedly until revoked, allowing long-lived stealthy access.
- In-process handle duplication and token reuse avoid file-copy artifacts and common file-based

## RECOMMENDATIONS

- Immediately invalidate all Teams and Microsoft 365 session tokens if compromise is suspected; enforce MFA reauthentication.
- Limit user-level execution of BOFs, scripts, and unsigned binaries using application allowlisting or endpoint protection policies.
- Apply the latest Microsoft updates and restrict DLL/COM hijacking by enforcing secure installation paths and signed modules.
- Reduce user permissions, disable unnecessary local admin rights, and isolate Teams processes through sandboxing or EDR controls.
- Educate employees about phishing and unusual Teams behaviour; encourage prompt reporting of suspicious login or message activity.

## REFERENCES

- https://cybersecuritynews.com/bof-tool-exploits-microsoft-teams/
- https://gbhackers.com/new-bof-tool-bypasses-microsoft-teams-cookie-encryption/

# SECURE, SCALE, SUCCEED WITH CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com

www.encyb.com