IMPORTANT CYBERSECURITY NEWS: TEAMFILTRATION PENTESTING TOOL WEAPONIZED TO HIJACK MICROSOFT TEAMS, OUTLOOK, AND OTHER ACCOUNTS

Vairav Cyber Security News Report

Date: June 27, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A global account takeover campaign, dubbed **UNK_SneakyStrike**, has exploited the publicly available TeamFiltration pentesting framework to target over **80,000 Microsoft Entra ID** (formerly Azure AD) accounts across approximately **100 cloud tenants**. Attackers used automated password-spraying and user-enumeration via the Microsoft Teams API, gaining **access to native apps like OneDrive, Outlook, and Teams**. This misuse of a legitimate red-team tool underscores the blurred line between offensive security tooling and real-world threats.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: UNK_SneakyStrike has been leveraging TeamFiltration since December 2024, with aggressive account takeover attempts and multiple compromises. TeamFiltration was released by TrustedSec in early 2021 and on GitHub in August 2022, is designed for cloud penetration testing, offering enumeration, credential spraying, data exfiltration, and creating persistence via OneDrive.

Identification: Proofpoint identified a rare, hardcoded Microsoft Teams user-agent string in authentication logs, and suspicious use of OAuth client IDs to retrieve “family refresh tokens”. Detection stemmed from analyzing GitHub’s TeamFiltration defaults and correlating behavior with live traffic

Threat Actor: The campaign is attributed to a cybercriminal group indicated by the name UNK_SneakyStrike. There are no definitive ties to known APT groups.

Affected Entities/Industries:

- Cloud tenants of 100 global organizations with 80,000+ user accounts affected.
- Organizations in the U.S. (42%), Ireland (11%), and UK (8%).

Potential Impact:

- Account takeover allows offensive operators to access Teams, OneDrive, Outlook, potentially leading to sensitive data exfiltration and persistent backdoors.
- Compromised accounts with elevated privileges could manipulate policies, disable MFA, or clear logs—posing severe operational and reputational risks

Exploitation Methods:

- User enumeration via Microsoft Teams API using a "sacrificial" Office 365 Business Basic account.
- Password spraying across many accounts to stay under detection thresholds.
- Data exfiltration and backdoor deployment via OneDrive, replacing legitimate files to maintain persistence.
- Rotation of AWS IPs across regions to evade network-based detection.

RELATED THREAT INTELLIGENCE & IOCs

Malicious IPs

- 44.220.31[.]157
- 44.206.7[.]122
- 3.255.18[.]223
- 44.206.7[.]134
- 44.212.180[.]197
- 3.238.215[.]143
- 44.210.66[.]100
- 3.216.140[.]96
- 44.210.64[.]196
- 44.218.97[.]232

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Block or flag logins using the distinctive outdated Teams user-agent string.
- Monitor and restrict logins from AWS IP ranges, especially bursty multi-region patterns.
- Review OTP/token issuance logs for family refresh token activity using unusual client IDs.

Security Best Practices

- Enforce strong password policies and rate-limiting for token and sign-in attempts.
- Mandate MFA for all users, covering both human and service accounts.
- Implement conditional access policies in Entra ID limiting risky logins.
- Regularly audit and disable inactive or service accounts, applying least privilege.

For Advanced Security Teams

- Use UEBA to detect burst-based login spikes against multiple accounts.
- Track OAuth app consent and token issuance, especially linked to known suspicious OAuth IDs.
- Analyze OneDrive and SharePoint activity for unexpected file replacements or uploads.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://cybersecuritynews.com/hackers-leverage-teamfiltration-pentesting-framework/
- https://www.proofpoint.com/us/blog/threat-insight/attackers-unleash-teamfiltration-account-takeover-campaign

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