BLACKSWAN CYBERSECURITY

THREAT ADVISORY

Identity-target Threat Identification and Mitigation

(Bypassing MFA via Session Token Theft)

May 2026

Severity: High
Threat Actors: Cybercriminals, ransomware groups, nation-state actors, and initial access brokers using tools like Evilginx, infostealers, and custom proxies.

Executive Summary

Session token theft (also known as session hijacking, cookie theft, or pass-the-cookie attacks) is a post-authentication technique that allows attackers to bypass MFA entirely. After a legitimate user completes password + MFA, the application issues a session token (often stored as a cookie or OAuth token). Attackers who steal this token can impersonate the user without re-authenticating.

This attack defeats standard MFA because the token serves as proof that authentication (including the second factor) has already occurred. It is commonly combined with **Adversary-in-the-Middle (AiTM)** phishing or malware. Incidents have been observed across Microsoft 365, SaaS applications, and other web services, enabling Business Email Compromise (BEC), data theft, and lateral movement.

How the Attack Works

1. **Credential Phishing or Initial Compromise**: User is phished (often via AiTM proxy like Evilginx), or malware infects the device (infostealer).
2. **Successful Authentication**: Victim enters credentials and completes MFA on a legitimate-looking site or compromised device.
3. **Token Capture**: The attacker captures the resulting session cookie/token (e.g., via proxy interception, browser storage extraction, or malware scraping cookies/DPAPI-protected data).
4. **Impersonation**: Attacker imports the token into their own browser/session (e.g., using cookie editor extensions). The application trusts the token as valid, and grants access without triggering MFA again.

Key Characteristics:

- Tokens act as **bearer credentials** (possession equals access).
- No new MFA prompt for the attacker.
- Works against many cloud/SaaS platforms, including those with "phishing-resistant" MFA if the token is stolen post-auth.
- Tokens can enable persistence until expiration or revocation.

Common vectors include AiTM phishing kits, info-stealers (often sold on dark web markets), XSS vulnerabilities, or network sniffing on unsecured connections.

THREAT ADVISORY

Identity-target Threat Identification and Mitigation

(Bypassing MFA via Session Token Theft)

May 2026

Indicators of Compromise (IOCs)

- Logins from unusual IPs, devices, or geographies shortly after legitimate sessions.
- Concurrent sessions from different locations/devices.
- Anomalous behavior post-login (e.g., inbox rules created, data exfiltration, privilege changes) with no corresponding MFA events.
- Unusual User-Agent strings or browser fingerprints.
- Alerts from endpoint detection on cookie scraping or DPAPI access.

Impact

- Full account takeover without credential knowledge.
- Bypass of Conditional Access policies tied only to initial login.
- Lateral movement in SSO environments.
- Potential for long-lived access via refresh tokens.

Remediation and Mitigation (Defense-in-Depth)

No single control fully eliminates the risk, but layered defenses significantly reduce it.

Immediate Response (If Compromised)

- Revoke all active sessions/tokens for the affected user.
- Force password reset and re-enrollment of MFA factors.
- Review and reset any changes (e.g., email forwarding rules, app consents).
- Investigate the device for malware and isolate it.

Technical Mitigations

- **Short Token Lifetimes & Rotation**: Issue short-lived access tokens (minutes to hours) with secure refresh token rotation. Revoke previous tokens on refresh or logout.
- **Token Binding / Device-Bound Credentials**: Cryptographically bind tokens to specific devices or client certificates so stolen tokens fail on attacker infrastructure. (e.g., Microsoft token protection in Conditional Access).
- **Secure Cookie Configuration**:
  - Set Secure, HttpOnly, and SameSite=Strict/Lax flags.
  - Use HTTPS everywhere + HSTS.
- **Phishing-Resistant MFA**: Prioritize FIDO2/WebAuthn security keys, passkeys, or platform authenticators (Windows Hello, etc.). These resist AiTM better than push/TOTP.
- **Conditional Access / Risk-Based Policies** (especially in Microsoft Entra ID/Azure AD):
  - Require compliant/managed devices.
  - Block or challenge risky sign-ins (impossible travel, new locations, anomalous tokens).
  - Enforce Continuous Access Evaluation (CAE) for real-time token invalidation on risk signals.

  - Require re-authentication for sensitive actions.
- **Session Monitoring & Anomaly Detection**:
  - Detect concurrent sessions, token reuse across IPs, or behavioral deviations.
  - Use Identity Threat Detection and Response (ITDR) tools.
- **Endpoint Protection**: Prevent infostealers with EDR/XDR, application control, and browser hardening.
- **Least Privilege & Just-in-Time Access**: Limit blast radius.

Operational & User Controls
- Educate users: Avoid clicking suspicious links, use password managers, log out of sessions, and report anomalies.
- Disable persistent browser sessions where possible.
- Regularly review MFA enrollments and session policies.
- Block legacy authentication protocols that bypass MFA.

Development/Architecture Best Practices
- Avoid storing sensitive tokens in local/session storage (use HttpOnly cookies where possible).
- Implement proper OAuth/OIDC security (PKCE, sender-constrained tokens, etc.).
- Monitor for OAuth token abuse.

Conclusion and Recommendations
Session token theft highlights that **MFA is necessary but not sufficient**. Organizations should shift toward zero-trust principles: continuous verification, device binding, and behavioral analytics. Prioritize phishing-resistant authentication and robust session management.

Action Items:
1. Audit current token/session policies and Conditional Access rules.
2. Pilot FIDO2/passkeys for high-privilege users.
3. Enable token protection and CAE where supported.
4. Test detection playbooks for anomalous sessions.

Monitor vendor updates (Microsoft, Okta, etc.) for new token-binding features. This threat evolves rapidly with AiTM tools and stealer ecosystems.

For tailored implementation advice, consult Blackswan and/or your security team.

Stay vigilant - tokens are the new keys.

Contact Blackswan Cybersecurity at 855-BLK-SWAN or
Contact@BlackswanCybersecurity.com

BLACKSWAN CYBERSECURITY

THREAT ADVISORY

Identity-target Threat Identification and Mitigation

(Bypassing MFA via Session Token Theft)

May 2026