COOKIE-BITE ATTACK BYPASSES MFA TO HIJACK CLOUD SESSIONS VIA BROWSER COOKIES

Vairav Cyber Security Campaign Report

Date: April 23, 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 newly discovered attack technique, dubbed “Cookie-Bite”, allows cybercriminals to bypass multi-factor authentication (MFA) by stealing authentication cookies, granting persistent and unauthorized access to cloud platforms like Microsoft 365 and Azure Portal. Revealed by Varonis Threat Labs, the attack exploits browser session cookies specifically ESTSAUTH and ESTSAUTHPERSISTENT used in Azure Entra ID (formerly Azure AD), effectively rendering traditional MFA protections insufficient.

By hijacking these session tokens, attackers can impersonate users, bypass conditional access policies (CAPs), and maintain long-term access, even after password resets or session revocations. This technique underscores the evolving threat landscape where identity and access tokens become key targets in cloud-centric environments.

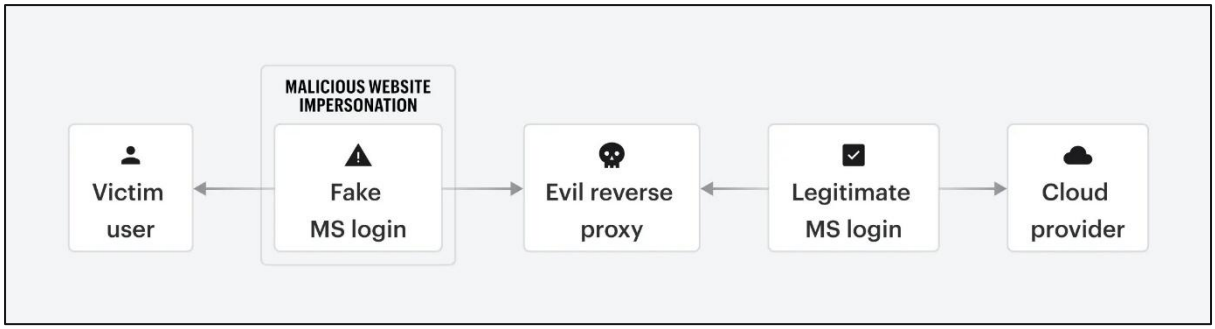

Figure 1: AiTM attack process

INCIDENT ANALYSIS

The Cookie-Bite attack capitalizes on the value of session cookies used to authenticate users in cloud services. Once stolen, these tokens can be injected into an attacker’s browser to bypass login credentials and MFA challenges, granting direct access to enterprise systems. The persistent nature of the attack ensures continued access by extracting fresh cookies during every login attempt.

Attackers use multiple methods to steal these tokens, including:

- Adversary-in-the-Middle (AiTM) attacks via reverse proxy tools.
- Memory dumping of browser processes.
- Malicious Chrome extensions crafted to extract authentication cookies silently.
- Decrypting local cookie storage within browsers.

Researchers demonstrated in their proof-of-concept that attackers can develop malicious Chrome extensions capable of covertly harvesting authentication cookies as users sign into Microsoft's login portal. Once captured, these cookies are sent to servers controlled by the attacker and can be injected into the attacker's browser, granting instant unauthorized access to the victim's cloud session.

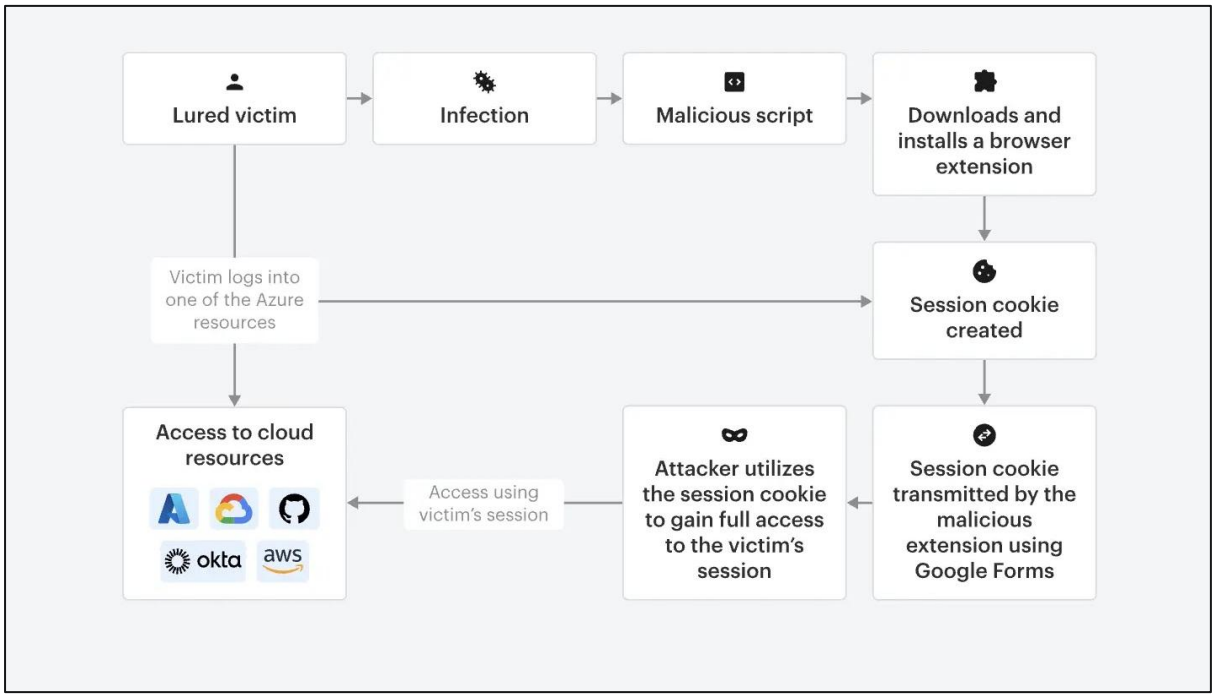

Figure 2: PoC

Attackers mimic legitimate access patterns by collecting host information, IP addresses, browser fingerprints, and operating system details, successfully bypassing Conditional Access Policies (CAPs) and risk-based sign-in protections. With this access, they can interact with powerful tools like Microsoft Graph Explorer to enumerate users, access mailboxes, and escalate privileges across the cloud environment.

The Cookie-Bite technique demonstrates the critical importance of protecting authentication cookies and challenges the sufficiency of passwords and MFA alone. As attackers shift toward session hijacking and identity impersonation, organizations must adopt identity-aware, behavior-driven defenses that go beyond traditional security controls to protect their cloud infrastructure.

RECOMMENDED ACTIONS

- **Monitor Anomalous Sign-ins:** Continuously analyze user behavior and login patterns to detect deviations that could indicate cookie reuse or impersonation attempts.
- **Leverage Microsoft Risk-Based Protections:** Enable Microsoft's risk detection signals to evaluate the risk level during sign-in events and trigger additional authentication when anomalies are detected.
- **Tightening Conditional Access Controls:** Implement strict Conditional Access Policies (CAPs) to only allow login from compliant, managed devices, minimizing exposure to hijacked session tokens.
- **Enforce Browser Extension Controls:** Use Chrome enterprise policies to whitelist approved browser extensions, blocking unauthorized or malicious add-ons from extracting session data.
- **Adopt Token Binding Protections:** Deploy token protection mechanisms (such as Microsoft's Continuous Access Evaluation) to bind tokens to the device and prevent their reuse from another environment.
- **Session Management Best Practices:** Regularly revoke and rotate session tokens and enforce short token lifetimes to reduce the effectiveness window for stolen cookies

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