

M-Trends

2024 Special Report

How Attackers Leverage AiTM to Overcome MFA

Mandiant has observed an increase in compromises against cloud-based identities configured with multi-factor authentication (MFA). As the adoption of MFA becomes commonplace across organizations, attackers are becoming proficient in methodologies capable of overcoming weaknesses in widely-adopted MFA methods. Most notable is the increasing adoption of web proxy or adversary-in-the-middle (AiTM) phishing pages, which are capable of rendering most MFA implementations ineffective by stealing sensitive login session tokens.

Common MFA Methods

MFA solutions often provide a variety of mechanisms for the management and approval of authentication requests. While mechanisms exist that are resistant to AiTM phishing, they often require additional infrastructure and overhead. However, the most commonly employed MFA mechanisms are the ones that are susceptible to attackers leveraging AiTM phishing.

MFA Type	Description
Push notification	Phone call or mobile application based prompt that only requires a user to accept a phone app push notification or press a key on their mobile device. Push notifications often lack context about the resource being accessed and can enable MFA fatigue attacks, in which users are sent repeated requests until the prompt is approved.
One-time password (OTP) / Time-based one-time password (TOTP)	Code from a SMS or email message, or a time-bound code generated by a mobile application or hardware device that is input along with a username and password during or following authentication. SIM swapping and credential harvesting webforms are common methods of stealing these codes, but they are also susceptible to exposure from seed theft or takeover of an account with access to cloud-synced TOTP codes.
Push notification with number matching verification	A push notification prompt generated on a user's mobile device that can only be accepted upon inputting a code generated by the logon portal. This addresses abuse mechanisms associated with MFA fatigue as well as TOTP code and seed theft.
Certificate-based authentication (CBA)	Authentication requiring X.509 certificate to be installed on devices. Resistant to AiTM phishing attacks.
Hardware keys	Physical devices compatible with the FIDO2 or U2F standard, which use public-key cryptography with supported cloud authentication services. This standard requires the server requesting a key to match the server tied to that key, therefore making it resistant to AiTM phishing attacks.

Credential Harvesting Evolved: Adversary-in-the-Middle

Attackers often leverage credential harvesting forms, or phishing pages, as a means to obtain logon credentials from their targets. These websites, which are designed to resemble popular login portals, can forward to an attacker credentials and MFA codes submitted by the targeted user. During an investigation into a business email compromise, Mandiant observed an attacker operating a credential harvesting form that forwarded credentials and time-based MFA codes to a private Telegram channel. This instant notification of stolen credentials provided the attacker an opportunity to successfully log in prior to the MFA code expiring, granting initial access into the targeted account.

AiTM phishing pages go beyond typical credential harvesting forms, and use infrastructure designed to overcome commonly implemented MFA methods. Unlike traditional credential harvesting forms, AiTM pages behave as a reverse web proxy between the targeted user and the legitimate logon portal. AiTM pages not only intercept credentials and MFA codes, but more critically, the post-authentication session token issued by the logon portal. These tokens can be used by an attacker to bypass security controls that are only evaluated on the initial sign-in.

Compared to traditional credential harvesting forms, the relative complexity of setting up AiTM phishing infrastructure may have kept its adoption by attackers limited in the past. However, in 2023, Mandiant observed a marked increase of AiTM phishing pages in use by attackers. The acceleration of AiTM usage amongst attackers has likely been aided by the availability of phishing-as-a-service offerings in the cybercriminal underground. Such offerings can provide less technically sophisticated attackers access to regularly maintained phishing infrastructure through which they can launch complex campaigns.

Detection and Mitigation

While AiTM phishing represents an evolution of attacker capabilities in the face of stronger controls such as MFA, compromises through AiTM phishing pages and the ensuing use of stolen session tokens provides defenders with detection opportunities. Since AiTM phishing pages are designed to intercept and forward a targeted user's login information to a cloud authentication service, authentication logs will record the IP address associated with this phishing infrastructure as the user's source IP address. The attacker's IP address and associated User-Agent string, which may differ from the initial AiTM logon, will also be recorded when authenticating with a stolen token. Defenders should continue to monitor for anomalies, such as geographically infeasible or unexpected source IP addresses, and logins originating from data centers.

In nearly all of Mandiant's investigations involving compromised cloud accounts, attackers were observed enrolling their own MFA methods shortly upon gaining initial access. Typically, this was done by interacting with a self-service security portal. While this activity isn't exclusive to AiTM attacks and session token theft, it's still worth highlighting as an effective detection opportunity, especially if paired with other logon anomalies. A regular review of new MFA registrations, as well as auditing accounts with multiple MFA methods configured, can reveal events worth further investigation.

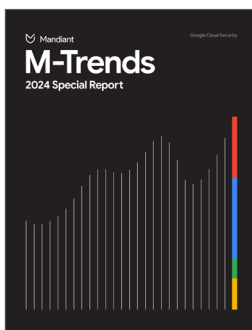
To best defend against AiTM attacks, organizations should pursue a combination of AiTM-resistant MFA methods and access policies. Most cloud authentication services support access policies that can block logons based on organization-defined locations, device management status, or an assessment of risk based on the account's historical logon properties. When implementing these access policies, it is important to understand which can be applied continuously throughout the logon session. Typically, most access policies are only applied at the initial token issuance stage, which will not offer protection against the use of previously stolen tokens.

Detection Opportunity	MITRE ATT&CK	Rule Logic
Okta - Detect AiTM Phishing using FastPass	T1078 T1556	eventType = "auth_via_mfa" AND result=FAILURE AND reason="FastPass declined phishing attempt"
Azure - Change of Authentication Method	T1098 T1556	LoggedByService="Authentication Methods" AND Category="UserManagement" AND OperationName="User registered security info"
M365 - Detects disabling of Multi Factor Authentication	T1556	LogSource = M365 Audit logs AND Operation="*Disable Strong Authentication.*"
Device Registration without MFA	T1078.004	Logsource = Azure sign in logs AND resourceDisplayName = "Device Registration Service" AND status = "Success" AND NOT authenticationRequirement = "multifactorAuthentication"
Attempt to reset Okta MFA factors for user	T1098	Logsource = Okta System events AND action = "user.mfa.factor.reset_all"

Conclusion

As AiTM phishing pages continue to grow in prevalence, many organizations today still rely on security controls that do not offer token theft protection. Furthermore, mitigating token theft and stolen token usage does not presently fit into a single, one-size-fits-all solution. Organizations can better protect against AiTM token theft by implementing phishing-

resistant MFA methods and effective access policies, and reduce the risk of stolen token use with policies that are continuously evaluated during a logon session. If these controls are paired with effective anomaly-based detection methodologies, organizations can greatly reduce the risk of phishing attacks and an attacker's dwell time.



Read the full report: [M-Trends 2024 Special Report](#)