September 2025
Adversary-in-the-Middle (AitM) Attacks Evolve to Bypass MFA at Scale

AT A GLANCE

- **Top Targeted Industries:** Threat actors are using Adversary-in-the-Middle (AitM) attacks to target industries rich with sensitive data and access, including Insurance (75%), Consulting (40%), and Construction (32%).
- **MFA No Longer a Silver Bullet:** AitM phishing campaigns are specifically designed to bypass multi-factor authentication by stealing web session cookies and tokens in real-time, making traditional MFA methods less effective on their own.
- **Phishing is the Foot in the Door:** Over 63% of AitM attacks begin with a phishing email, demonstrating that social engineering remains the primary initial access vector for these sophisticated campaigns.
- **Key Threat Actor:** Financially motivated groups like Storm-1167 are prominent, using advanced AitM phishing kits to automate the theft of credentials and session tokens.

OVERVIEW

Cyber threat intelligence reveals a significant rise in the frequency and sophistication of Adversary-in-the-Middle (AitM) attacks. Unlike traditional phishing that simply harvests credentials, AitM campaigns use reverse-proxy infrastructure to intercept the entire authentication process, including MFA challenges and session cookies. This allows attackers to hijack active sessions, granting them the same access as the legitimate user without needing to crack passwords or continuously phish for credentials.

Analysis of security alerts shows a clear pattern of industry targeting. In 2024, the **Insurance** sector was disproportionately affected, with 75% of organizations in this vertical impacted by AitM attacks. Other heavily targeted sectors include **Consulting (40%)**, **Construction (32%)**, **Manufacturing (31%)**, and **Business Services (31%)**. This focus indicates a strategic effort by threat actors to compromise organizations that hold valuable customer data, intellectual property, and privileged access to other networks.

These attacks are becoming both more common and more advanced. Threat actors are leveraging AitM phishing kits that dynamically create pixel-perfect replicas of legitimate login pages, making them nearly impossible for users to spot. Once a user enters their credentials, the AitM infrastructure captures the session cookie, effectively bypassing MFA and giving the attacker persistent access until the session expires or is revoked.

This report contains valuable insights and recommendations for defending against modern AitM attacks for navigating the evolving cyber landscape. To unlock the full content, reach out to your customer success manager or email us at info@criticalstart.com.
