TALES FROM THE SOC

AiTM Credential Harvesting Attack Contained in 17 Minutes

Incident Overview

Threat Type: Credential compromise via Adversary-in-the-Middle (**AiTM**) phishing

Time to Containment: 17 Minutes

Attack Characteristics

This incident involved an Adversary-in-the-Middle (AiTM) phishing attack using a malicious proxy-based login page to harvest credentials and hijack user sessions in real time. While no Malware was deployed, by bypassing traditional MFA, the attacker aimed to gain access to internal systems for potential lateral movement and privilege escalation.

Alert Escalation: Low to High Priority

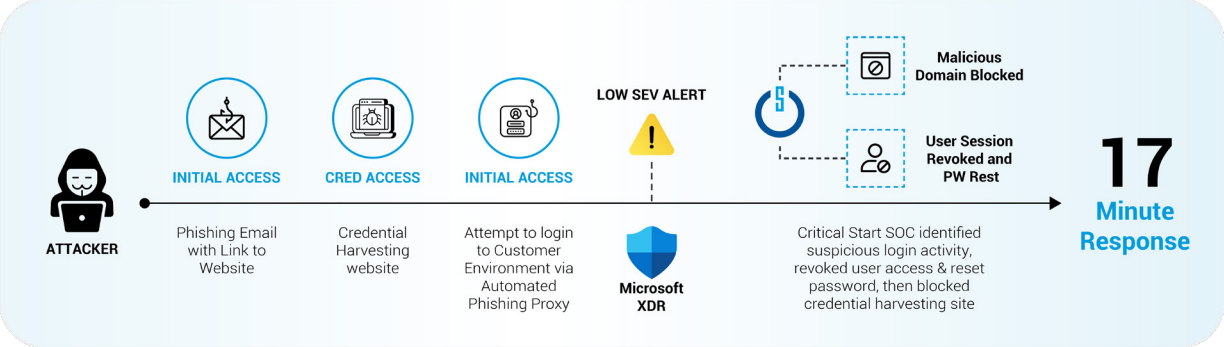
Initial Vendor Severity: Low priority

SOC Escalation: High priority based on telemetry correlation and behavioral indicators

Escalation Rationale: After identifying an Axios user agent commonly indicative of phishing proxies, the SOC escalated this alert as High Severity from the vendor-assigned Low. By correlating the login to a malicious URL and active credential harvesting, the team triggered a coordinated response that prevented the attacker from maintaining undetected access.

Depth of Investigation

The SOC performed a multi-analyst investigation that included analyzing sign-in telemetry, correlating URL clicks to the phishing vector, and conducting a forensic review of the harvesting infrastructure. This layered approach allowed the team to validate the attack scope, block malicious domains, and provide the client with custom detection queries to hunt for similar threats.



Coordinated Cross-Platform Response

Initial Detection: Sign-in event via Axios user agent in Microsoft Defender XDR CORR telemetry

The coordinated, cross-platform response included identifying the malicious sign-in, revoking the user's session tokens, and forcing a password reset to invalidate stolen credentials. Analysts then blocked the phishing domain across the network, delivered a screenshot of the harvesting site for awareness, and held a high-priority call with the client to confirm findings, share IOCs, and provide next steps.

Outcome

The coordinated response successfully contained the credential compromise within 17 minutes, preventing attacker persistence and lateral movement through domain blocking and session expiration. This swift, analyst-driven escalation neutralized the phishing campaign, strengthened the client's defenses and solidified trust through proactive communication and full transparency.