SOPHOS MDR THREAT CASE

Better Together: Sophos MDR and Microsoft Break the AiTM Chain

ORGANIZATION

Industry	Construction & Engineering
Size	1,000 Employees
Region	Berlin, Germany

SOLUTION

Sophos MDR Complete

Adversary activity

The attacker sends a phishing campaign using a legitimate hosting platform that bypasses the firm's existing email defenses. Several employees interact with the message, but one user ultimately reaches an attacker-controlled **spoofed Microsoft 365 login page** and enters their credentials. With these, the attacker logs in from two known threat actor-controlled IP addresses, accesses the mailbox, and creates inbox rules to divert email replies.

Threat detection

7:26 UTC Sophos MDR is alerted to sign-ins from **malicious IP addresses.**

7:27 UTC A Sophos MDR detection rule designed to analyze **Microsoft Graph Security telemetry** identifies an Adversary in the Middle (AiTM) user compromise.

7:28 UTC Multiple correlated detections fire on malicious sign-ins, risky sign-in after link click, and **inbox rule creation.**

Investigation

7:55 — 8:24 UTC Sophos MDR triages the case and investigates these detections, leveraging Microsoft Graph Security telemetry to reveal **one cohesive attack chain:**

Phishing campaign → Legitimate host site harboring a malicious login page → Compromised user credentials → Account access from malicious, out-of-region IP addresses → Inbox rule creation

Response

8:24 — 10:00 UTC This customer chose Sophos MDR's **"Collaborate" response mode**, so we contact them to guide them through full remediation in **under two hours.** The phishing email is removed, attacker sessions are revoked, user credentials are reset, and Microsoft 365 response actions are enabled. We then advise strengthening defenses with MFA, geolocation-based Conditional Access, and expand M365 response automation.

Learn more at sophos.com/MDR