SOPHOS MDR THREAT CASE

Adversary-in-the-Middle (AiTM) attack targeting Microsoft 365

ORGANIZATION

Industry Retail
Size 1K+ stores, 9K+ employees
Region UK and Ireland

SOLUTION

Sophos MDR
+ Microsoft 365 Mgmt. Activity integration

Adversary activity

10:49 UTC The attacker sends a **phishing email** pretending to be a shared OneNote file from a known supplier, containing a link to a fake Microsoft login page.

11:51 UTC The user logs in and the attacker **steals their credentials** and session token.

12:28 UTC The attacker logs into portal.office.com with the user's credentials and **modifies** a Microsoft Teams link in an existing calendar invitation.

Threat detection

12:28 UTC A proprietary **Sophos detection rule** identifies successful logins to 'portal.office.com' for the targeted user where the user agent string is suspicious - indicating a potential **Adversary-in-the-Middle (AiTM)** session compromise. A case is automatically created for Sophos MDR to investigate.

Investigation

Case opened 12:30 UTC The Sophos MDR analyst **reviews Entra ID sign-in logs** for the targeted user (who is office-based in the U.K.) and **identifies successful logins** to 'portal.office.com' from IP addresses geolocated in the USA, the Netherlands, and Germany. The analyst **uncovers** the modification made to the user's calendar invitation by the attacker.

Response

Case closed 14:55 UTC The Sophos MDR analyst advises the organization to **block** the phishing email sender and **reset** the user's compromised credentials. The analyst provides guidance on **terminating** authentication tokens in MS Entra ID and recommends setting up a conditional access policy to **restrict logins** for office-based employees to their specific geolocations.

Learn more at sophos.com/MDR