SOPHOS MDR THREAT CASE

MDR vs. BEC
A Sophos Managed Service Provider Win

SOPHOS

PARTNER
Sophos MSP
Incident Response Provider
California, US

ORGANIZATION
Industry Construction
Size 1-50 Employees
Region Florida, United States

SOLUTION
Sophos MDR Essentials

Adversary activity

The attacker uses the phishing kit **Wikikit/Sneaky2FA**, an Adversary in the Middle (AiTM) attack that dupes a victim into entering their credentials into a highly realistic Microsoft Office 365 **spoofed login page**. This fake login page allows the threat actor to steal the username, password, and authentication elements like 2FA codes and session tokens to gain access to the victim's account.

Threat detection

21:17 UTC The customer is supported by a **Sophos Managed Service Provider (MSP)** partner with Incident Response capabilities. The MSP uses Sophos MDR with "Authorize" mode enabled, allowing Sophos to act on their behalf.

Sophos MDR is alerted to this suspicious login activity by a proprietary Sophos WikiKit/Sneaky2FA **detection rule**.

Investigation

Further **telemetry and threat intelligence** confirm the attacker is using a valid session token — a clear indicator of an AiTM attack. Sophos MDR analysts find the attacker staging a more severe Business Email Compromise (BEC) attack, attempting to create new mailbox rules for further control.

This behavior **elevates the alert** instantly.

Response

21:19 UTC After just **95 seconds**, Sophos MDR blocks sign-ins and revokes every active session, cutting off the threat actor's access entirely. Sophos MDR provides the MSP with **full remediation steps** (credential resets, MFA re-enrollment, sign-in checks, and mailbox audits) for their customer. Together, Sophos MDR and the MSP prevent escalation, business interruption, and any need for an insurance claim.

Learn more at sophos.com/MDR

SOPHOS