SOPHOS MDR THREAT CASE

BEC threat actor stopped in 84 seconds

SOPHOS

PARTNER
Sophos MSP
IT Services Provider
South Carolina, US

ORGANIZATION
Industry Business services
Size 100-150 employees
Region New York, US

SOLUTION
Sophos MDR

Adversary activity

19:03:38 UTC The attacker uses the **FlowerStorm AiTM** (Adversary in the Middle) phishing kit to gain control of a user's account at a consulting firm.

19:05:43 UTC Once inside, the attacker authenticates from multiple session IDs, source IPs, and creates an inbox rule that diverts emails from a supplier into an archival folder and marks them as "read," setting the stage for a **wire transfer fraud.**

Threat detection

19:17:28 UTC Sophos MDR identifies the attack through a **purpose-built detection** for the FlowerStorm AiTM phishing kit, combined with behavioral signals across identity and email activity. Sophos detections catch abnormal session behavior (the multiple session IDs and source IPs tied to a single account) and the creation of this subtle mailbox rule, revealing **a full BEC attempt**.

Investigation

19:17:37 UTC **AI speed —** Sophos' AI analysis **correlates activity** across identity and email layers, confirming this attack within seconds. Sophos MDR contains the threat immediately, thanks to this automatic triage.
Human judgment — From there, **human analysts** validate the attacker's intent by confirming the inbox rule was created specifically for a known supplier — a strong indicator that the attacker was preparing for wire fraud.

Response

19:18:52 UTC **AI speed —** Sophos MDR immediately contains the attack through automated response actions. **Within 84 seconds** of detection, the user sign-in is blocked and all active sessions are revoked.

19:50:16 UTC **Human judgment —** Sophos MDR analysts identify the exact inbox rule and **remove it**. This agentic response with human judgment **stops the attack** in seconds while ensuring nothing is left behind.

Learn more at sophos.com/MDR

SOPHOS