SOPHOS MDR THREAT CASE

Collective immunity: Sophos MDR stops Microsoft phishing campaign targeting multiple customers

SOPHOS

ORGANIZATION

Industry All
Size 1+ employees
Country All

SOLUTION

Sophos MDR

1

Adversary activity

The adversary sends a **phishing email** that results in an employee's account being compromised. The adversary uses the **compromised account** to send phishing emails pretending to be a shared OneNote file from a known supplier with a link to a fake Microsoft login page. These emails are sent to both internal and external recipients.

2

Threat detection

Case created 7:31 UTC

Using telemetry from the customer's Microsoft technologies, Sophos MDR detects **multiple user account compromises** within the customer's Microsoft 365 environment and generates an alert.

3

Investigation and containment

09:54 UTC

Sophos MDR identifies seventeen compromised accounts and escalates the case for urgent response. With the customer's approval, the Sophos MDR analyst disables the affected accounts in Microsoft 365 and Active Directory to **contain the attack**.

4

Collective immunity activation

11:50 UTC

Sophos MDR analysts review the phishing emails sent to external recipients and identify **thirty targeted organizations**, including a second Sophos MDR customer.

Sophos MDR notifies the second customer before they access the phishing link, **preventing further compromise**.

This real-world example demonstrates how rapid detection, effective escalation, and **shared intelligence across Sophos' expansive customer base,** stopped a major phishing campaign in its tracks.

Learn more at sophos.com/MDR

SOPHOS