SOPHOS MDR THREAT CASE

Domain credential abuse remediated in 47 minutes

SOPHOS

PARTNER
Sophos MSP
Technology services provider
Costa Rica, Central America

ORGANIZATION
Industry Legal
Size 50-200 employees
Region Costa Rica, Central America

SOLUTION
Sophos MDR

Adversary activity

An attacker logs in to this customer's environment through a Cisco VPN **without MFA**, most likely **using stolen credentials**.

With initial access confirmed, they pivot to four accounts (two regular users and two admin) and launch brute-force attempts on **two internal Domain Controller servers** to steal additional credentials.

Threat detection

9:54 UTC Sophos MDR detects this high-risk credential-theft behavior on the domain controller servers and automatically classifies the alert to our **Priority Queue**.

9:55 UTC Just **22 seconds later**, an MDR analyst claims the case and begins investigation while the attacker is still active in the environment.

Investigation

Sophos MDR quickly correlates VPN logins, account activity, and internal telemetry to reveal **the root cause**: VPN access via compromised credentials.

We then uncover the abuse of the four accounts and domain controller activity consistent with **large-scale credential theft**. We immediately begin containment while mapping the full scope of the attack.

Response

10:06 UTC - 10:41 UTC Operating in **Collaborative + Authorize Response mode**, Sophos MDR works alongside the MSP and customer. With verbal approval, compromised accounts are disabled, active sessions are terminated, and malicious VPN IPs are blocked. Sophos MDR then guides MFA on the VPN, updates the VPN firmware, updates admin access rules, and resets credentials, providing full remediation in just **47 minutes**.

Learn more at sophos.com/MDR

SOPHOS