SOPHOS MDR THREAT CASE

From behavioral detection to full credential containment

SOPHOS

PARTNER
Sophos MSP
Managed IT solutions provider
Saskatchewan, CA

ORGANIZATION
Industry Energy sector
Size >25 employees
Region Alberta, CA

SOLUTION
Sophos MDR

Adversary activity

The threat actor gains initial access by logging into the organization's VPN using a **compromised account without MFA.**

Once inside, the attacker uses multiple tools to **dump LSASS memory** to harvest full credentials and authentication tickets for lateral movement.

Threat detection

5:37 UTC Sophos MDR detects the behavior for **LSASS credential access** on a domain-joined endpoint.

This detection fires based on credential-dumping behavior rather than a known malware signature, allowing Sophos MDR to quickly identify a hands-on-keyboard attacker using **legitimate tools.**

Investigation

5:56 UTC Sophos MDR analysts discover several credential harvesting tools and expand the scope of the investigation. Our team confirms lateral movement across multiple hosts using stolen credentials and Cloudflare tunnels over RDP.

Correlating this **endpoint, identity, and network data** identifies the root cause as a compromised VPN account without MFA.

Response

Operating in "collaborate" response mode with the customer's MSP, Sophos MDR delivers rapid, approval-based containment to stop hands-on-keyboard activity. Abused tools are blocked globally a single Sophos Central policy change.

Sophos MDR then guides **VPN hardening, MFA enforcement** via Entra ID SSO, and **domain-wide credential resets.**

Learn more at sophos.com/MDR

SOPHOS