SOPHOS MDR THREAT CASE

Credential stuffing attack with Sophos Firewall and Sophos Endpoint

ORGANIZATION

Industry Financial services
Size Commercial
Region USA

SOLUTION

Sophos MDR
Sophos Firewall

Adversary activity

The attack begins with the adversary **logging in** via the organization's Sophos Firewall VPN using **credentials stolen** from a different system — they wait two weeks before continuing.

02:50 UTC The attacker pivots to an **endpoint** protected by Sophos MDR, from the VPN.

04:47 UTC The attacker executes a script on the endpoint that **runs discovery commands** and changes multiple passwords.

Threat detection

04:54 UTC A **detection is generated** in Sophos MDR due to WMIC (Windows management instrumentation command-line) remotely calling an executable from a suspicious directory for ransomware staging.

A case is **created and assigned** to a Sophos MDR analyst for investigation.

Investigation

06:26 UTC Following the investigation, the Sophos MDR analyst **confirms** the malicious activity and **communicates** their findings to the customer.

An active incident is initiated, and the Sophos MDR analyst executes **response actions** on the customer's behalf to neutralize the threat.

Response

Case closed 08:39 UTC The MDR analyst uses the Sophos **Active Threat Response** feature, creating 'threat indicators' on the Sophos Firewall to block malicious IP addresses.

The analyst also **removes malicious binaries** from the endpoint and recommends resetting user credentials and upgrading the VPN gateway.

Learn more at sophos.com/MDR