SOPHOS MDR THREAT CASE

Backup Server Compromise Thwarted

SOPHOS

ORGANIZATION

Industry Environmental Consulting
Size 250-300 Employees
Region Alberta, Canada

SOLUTION

Sophos MDR Complete
Sophos Firewall

Adversary activity

The attacker begins an SSL VPN session on the customer's Sophos Firewall, then accesses a Veeam backup server, both via legacy accounts with previously compromised credentials and from an out-of-region IP address.

The attacker attempts to create a new user account with administrative privileges on the Veeam Backup Service.

Threat detection

Case opened 10:11 UTC Sophos MDR flags this suspicious **combination of commands** on the Veeam backup server and a case is automatically created.

10:20 UTC The case is triaged and escalated to **High Severity.** The customer has Sophos MDR's **"Authorize"** response mode enabled, allowing Sophos to act immediately on their behalf.

Investigation

10:28 UTC A Sophos MDR analyst isolates the Veeam backup server and discovers the **VPN session** on the customer's Sophos Firewall.

10:38 UTC Sophos MDR terminates the VPN session and **disables** the attacker's account.

10:40 UTC Sophos MDR contacts the customer and elevates the case to **Critical**, initiating **Incident Response**.

Response

Case closed 11:00 UTC The customer confirms the accounts were from a **decommissioned** IT provider. Sophos MDR provides remediation guidance and confirms completion with the customer, including resetting credentials, disabling legacy accounts, blocking attacker IP addresses, deploying MFA, and upgrading the Veeam Backup Service to the latest secure version.

Learn more at sophos.com/MDR

SOPHOS