SOPHOS MDR THREAT CASE

Microsoft 365 credential capture and re-use

SOPHOS

ORGANIZATION

Industry Marketing consultancy
Size 1,200 Employees
Region UK

SOLUTION

Sophos MDR
+ Microsoft 365 Mgmt. Activity integration

Adversary activity

The attacker initially creates a Dropbox account to use for a phishing attack using a compromised supplier's email address.

11:41 UTC The attacker sends a **phishing email** with a malicious PDF attachment to an employee. Multiple email security technologies fail to detect the threat.

12:03 UTC The employee **opens the attachment** and enters their credentials. The malicious PDF file also captures the employee's MFA token.

Threat detection

12:24 UTC A **proprietary Sophos detection rule** identifies successful Microsoft 365 logins for the targeted employee where the user agent string is suspicious, indicating a potential session compromise. A case is automatically created for Sophos MDR to investigate, and an alert is sent to the customer's security team.

Investigation

12:24 UTC The Sophos MDR analyst **investigates login activity** using telemetry from the Microsoft 365 Management Activity integration. Analysing the targeted employee's standard login patterns, Sophos MDR determines that the activity is anomalous.

Response

12:29 UTC The Sophos MDR analyst advises the organization to **reset** the employee's compromised credentials and **terminate active sessions** in Microsoft Entra ID. Sophos also recommends reviewing MFA devices for the affected employee.

13:30 UTC The customer applies the recommended actions and the account is secured.

Learn more at sophos.com/MDR

SOPHOS