SOPHOS MDR THREAT CASE

Suspicious Microsoft Azure Command Line Interface (CLI) activity

SOPHOS

ORGANIZATION

Industry Government
Size 1,300 employees
Region Spain

SOLUTION

Sophos MDR
+ Microsoft 365 Mgmt. Activity integration
+ Microsoft 365 Graph security integration

Adversary activity

09:06 UTC The attacker attempts to access the customer's cloud environment using the Microsoft **Azure Command Line Interface** (CLI).

Threat detection

09:06 UTC A case is **automatically created** based on **suspicious activity detected** where the user agent is set to 'node-fetch' with the application 'Microsoft Azure CLI'. This has been observed in previous campaigns and is an indicator of compromise.

Sophos automation is used to deliver the fastest response possible, using event data ingested through the **M365 Management Activity integration**.

Investigation

09:07 UTC The **high-fidelity detection** determines that the login activity is **anomalous** compared to normal user activity. By leveraging Sophos automation, this case does not require a Sophos MDR analyst to conduct an investigation prior to escalating to the customer.

Response

09:07 UTC Sophos MDR **immediately informs the customer** of the findings, including the user and location, and recommends the customer revokes session tokens, resets user credentials, reviews and applies MFA, and reviews conditional access policies.

10:33 UTC Customer responds and confirms that the activity was **not expected** and **implements the recommendations** provided.

Learn more at sophos.com/MDR

SOPHOS