

M365 credential stuffing stopped in 63 seconds

**PARTNER**

Sophos MSP
IT Services Provider
Arizona, US

**ORGANIZATION**

Industry Education
Size 11,000 employees
Region New Mexico, US

**SOLUTION**

Sophos MDR
Sophos Mobile

**Adversary activity**

19:10:17 UTC The attacker attempts to access a **Microsoft 365 account** at a major public school system using **credential stuffing**, an identity-based attack that automatically tests credentials stolen in previous data breaches.

They successfully **establish a session** from an anomalous IP address, gaining the same level of access as a legitimate user.

**Threat detection**

20:04:56 UTC Sophos MDR identifies the Microsoft 365 session is associated with a **known application identifier** previously linked to credential-stuffing campaigns.

By correlating multiple signals of unauthorized access, the detection separates a likely account takeover from routine authentication behavior and immediately **initiates the response** process.

63 seconds**Automated response**

20:05:59 UTC With sufficient confidence to **act without manual review** in this case, the system automatically responds to the detection in just **63 seconds**.

Sophos MDR blocks the user's sign-in and revokes active sessions, **disrupting the attack** before the adversary can establish persistence or expand access.

**Human judgment**

22:01:41 UTC With the immediate threat **already contained**, Sophos MDR experts review the incident, validate the findings, and work directly with the customer and technology partner to **complete remediation**.

The team provides guidance on credential resets, identity hardening, and access controls, helping **reduce the likelihood** of future credential-based attacks.

Sophos ITDR can help uncover exposed credentials that may be leveraged in these types of attacks.

Learn more at sophos.com/MDR