

EvilTokens threat hunt stops session theft in seconds



PARTNER

Sophos MSP
IT Services Provider
New Jersey, US



ORGANIZATION

Industry Business services
Size 100-200 employees
Region California, US



SOLUTION

Sophos MDR
Sophos Endpoint
Sophos Email



Adversary activity

An attacker deploys an **EvilTokens** phishing campaign against a healthcare staffing organization. A user interacts with the phishing lure where their session token is captured through a **legitimate authentication flow**.

EvilTokens steals authenticated Microsoft 365 session tokens, allowing attackers to inherit **entire sessions**. Existing controls mitigate some of the potential access, but the attacker still poses a **major risk**.



Threat detection

21:13:21 UTC Sophos MDR's **Threat Hunting AI agent** continuously hunts for hidden threats using the latest intelligence from Sophos X-Ops.

During a global EvilTokens hunt, Sophos MDR identifies the user account that interacted with the malicious phishing lure. The finding is **automatically escalated**, initiating response actions before the compromised session can be leveraged by the attacker.

116 seconds



Automated response

21:15:17 UTC Sophos MDR rapidly correlates the known **token-theft phishing activity** and the exposed Microsoft 365 session to validate the threat.

Using Sophos' direct **Microsoft response integrations**, the system automatically blocks the user's sign-in and revokes the active session. The time from the threat hunt discovery to containment takes just **116 seconds**.



Human judgment

Automation handles speed and scale, Sophos MDR experts **own the outcome**. The team reviews findings and works with the customer and partner on clear remediation steps.

Building on this organization's controls, Sophos MDR validates the response, recommends a credential reset, and stages additional Conditional Access controls designed to further **reduce the risk** of future session-token theft attacks.

Learn more at sophos.com/MDR