SOPHOS MDR THREAT CASE

Inside a Teams tech support scam with a hidden RAT

SOPHOS

PARTNER
Sophos MSP
Technology solutions provider
Illinois, US

ORGANIZATION
Industry Legal
Size 25-50 employees
Region Illinois, US

SOLUTION
Sophos MDR

Adversary activity

20:55 UTC The attacker impersonates an internal "IT Support" user in Microsoft Teams, exploiting **default Teams settings** with external access enabled.

21:08 UTC The attacker carries out a convincing vishing support call with a legitimate user to gain desktop access and install a **remote access Trojan (RAT)** during their live call.

Threat detection

21:17 UTC These attacks are notoriously difficult to detect, as they rely on legitimate Teams activity rather than malware or links. Sophos MDR automatically identifies the scam through deep **Microsoft audit log integration** and proprietary analysis, correlating display names against trusted domains. External users posing as "IT Support" from untrusted sources are immediately flagged.

Investigation

Human-led Sophos MDR investigation uncovers a 16-minute call where the attacker installs a stealthy **Java RAT disguised as "Chrome,"** delivered from a completely different organization's compromised SharePoint instance.

This multi-capacity malware can abuse cloud services for command-and-control, reconnaissance, and can map a path **toward Active Directory escalation**.

Response

21:59 UTC Operating in Authorize mode, Sophos MDR takes action on behalf of the MSP and customer, blocking the fake "IT Support" account and **revoking all active sessions**. Upon further investigation, Sophos MDR eradicates the RAT, removes persistence, and isolates the host. We then guide the **MSP and customer** through targeted remediation with credential resets, device rebuilds, and Microsoft Teams policy hardening.

Learn more at sophos.com/MDR

SOPHOS