SOPHOS MDR THREAT CASE

Threat hunt uncovers AI-lured crypto wallet theft

SOPHOS

ORGANIZATION

Industry MSP
Size 25 Employees
Region Ohio, US

SOLUTION

Sophos MDR

Adversary activity

A threat actor **poisons ChatGPT** results with a malicious link designed to intercept a common cryptocurrency workflow: connecting a hardware wallet through a browser-based wallet. A user working from a personal device in a BYOD environment follows the AI-surfaced link and completes what appears to be a legitimate authentication step, unwittingly **providing wallet credentials**. The adversary steals cryptocurrency.

Threat hunting

This activity occurred in a personal browser over legitimate cloud services, leaving no malware, blocked connection, **nor clear security alert**. When customers need clarity, Sophos Threat Hunters analyze historical endpoint and integrated telemetry to uncover patterns that blend into **everyday activity**. Guided by human expertise and AI analysis, the team reconstructs what happened, confirms malicious activity, and explains the full attack path.

Investigation

Sophos MDR analysis of browser history reveals the **full attack path**, from a ChatGPT search to interaction with a spoofed wallet setup flow that captured credentials and enabled theft. By correlating timestamps and browser activity, Sophos MDR confirms the attacker duped a user during a crypto setup process, with **no evidence of broader compromise** or lateral impact.

Response

Sophos MDR focuses on preventing any further misuse of the crypto accounts by advising a credential and MFA reset of the affected wallets and terminating active sessions, ensuring the attacker **cannot regain access**.

Sophos MDR also recommends treating AI responses as unverified sources and reinforcing this risk through security awareness training.

Learn more at sophos.com/MDR

SOPHOS