Hackers hijacked legitimate Chrome extensions to try to steal data

A cyberattack campaign inserted malicious code into multiple Chrome browser extensions as far back as mid-December, *Reuters* reported yesterday. The code appeared designed to steal browser cookies and authentication sessions, targeting "specific social media advertising and AI platforms," according to a blog post from Cyberhaven, one of the companies that was targeted.

Cyberhaven blames a phishing email for the attack, writing in a separate technical analysis post that the code appeared to specifically target Facebook Ads accounts. According to *Reuters, s*ecurity researcher Jaime Blasco believes the attack was "just random" and not targeting Cyberhaven specifically. He posted on X that he'd found VPN and AI extensions that contained the same malicious code that was inserted into Cyberhaven.

Cyberhaven says hackers pushed an update (version 24.10.4) of its Cyberhaven data loss prevention extension containing the malicious code on Christmas Eve at 8:32PM ET. Cyberhaven says it discovered the code on December 25th at 6:54PM ET and removed it within an hour, but that the code was active until December 25th at 9:50PM ET. The company says it released a clean version in its 24.10.5 update.

Cyberhaven's recommendations for companies that may be affected include that they check their logs for suspicious activity and revoke or rotate any passwords not using the FIDO2 multifactor authentication standard. Prior to publishing

its posts, the company notified customers via an email that *TechCrunch* reported Friday morning.

https://www.theverge.com/2024/12/28/24330758/chrome-extension-cyberhaven-hijack-phishing-cyberattack-facebook-ads-authentication-theft