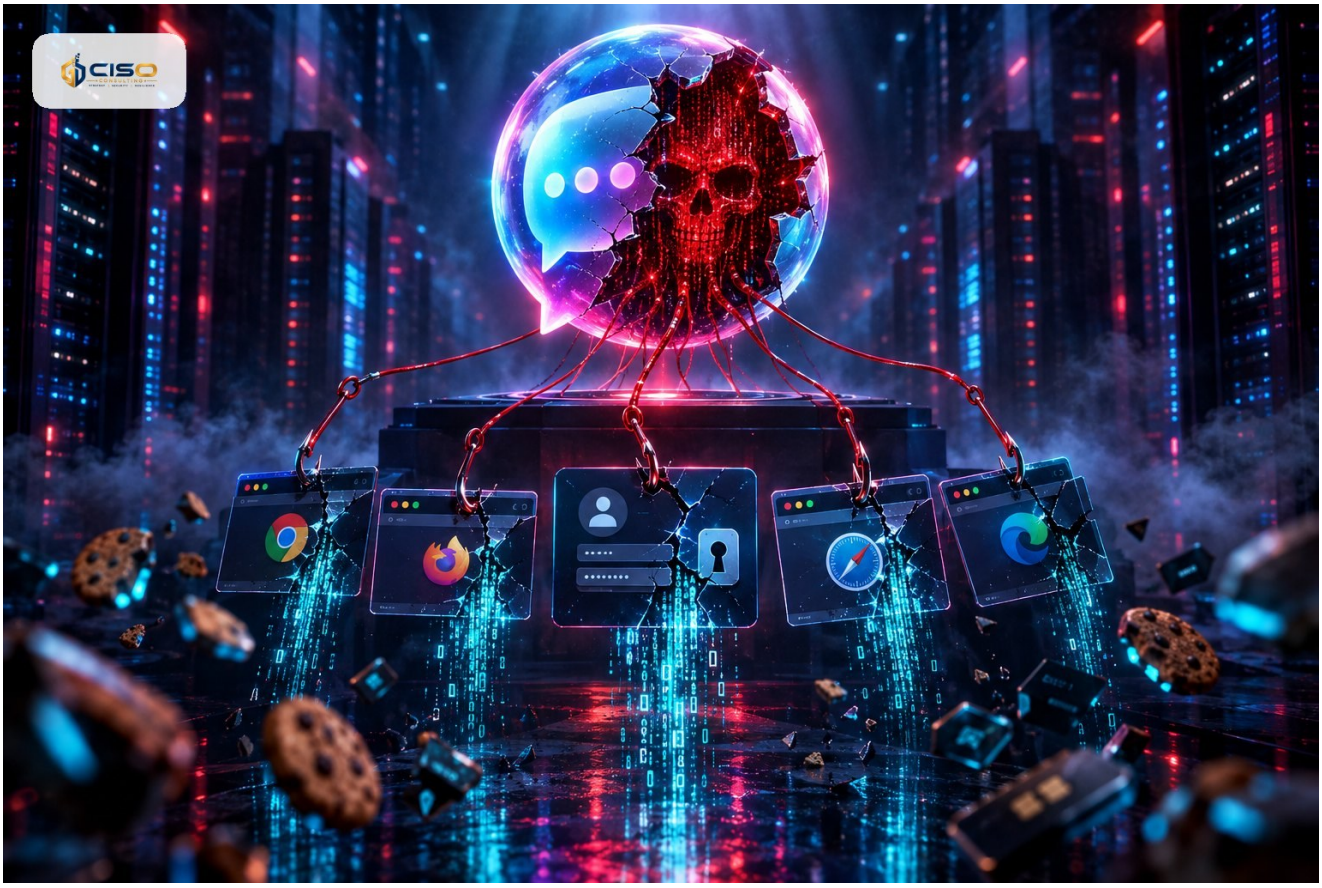
Fake AI tool campaigns target business accounts and browser sessions



ANY.RUN linked 1,258 public sandbox analyses to campaigns impersonating popular AI products to spread malware and take over business accounts. The activity ran from April to October 2026.

- Attackers impersonate popular AI products to distribute malware.
- The goals include stealing browser sessions and compromising business accounts.
- ANY.RUN tied 1,258 public sandbox analyses to these campaigns between April and October 2026.
- US businesses made up 16% of country-attributed targets.
- The campaigns add operational pressure on MSSPs that serve affected clients.

What was reported

The Hacker News reports that attackers are posing as well-known AI products in order to deliver malware, steal browser sessions and compromise business accounts. ANY.RUN, a malware analysis provider, connected 1,258 public sandbox analyses to fake AI campaigns observed between April and October 2026.

US companies accounted for 16% of the targets that could be attributed to a country. The report notes that these campaigns also raise operational pressure on managed security service providers (MSSPs) that support such businesses.

Why it matters in the Kingdom

The source concerns US companies and does not describe activity in Saudi Arabia. Even so, the technique is not tied to one geography: staff in any organisation may look for AI tools and download or sign in to a lookalike. Stolen browser sessions can give an attacker access to business accounts without needing a password, which makes early detection important.

The source excerpt does not give details of the malware families, the lure domains or the detection methods, so we do not speculate on them here.

Practical stance

Treat unapproved AI tools as a risk to manage rather than only a policy matter. Give staff a clear, approved route to the AI tools they need, and make sure your security monitoring, whether in-house or provided by an MSSP, can spot suspicious downloads and unusual account sign-ins early.

What to do now

1. Publish a list of approved AI tools and the official sources to obtain them.
2. Remind staff not to install AI software or browser extensions from unverified links or ads.
3. Review how long browser and cloud sessions stay valid, and enforce multi-factor authentication on business accounts.
4. Ask your MSSP or SOC how it would detect a fake AI download or a hijacked session.
5. Prepare a response step to revoke sessions and reset credentials when an account is suspected to be compromised.