Google session hijacking campaign uses calendar invites and live proxies



A phishing campaign active since mid-August 2026 steals live Google sessions from corporate users, with links designed to pass the usual reputation checks. Material Security researchers report taking down hundreds of attacker domains.

- The campaign has been running since mid-August 2026 and targets corporate users' live Google sessions.
- Links reportedly pass the checks defenders normally use to judge them, and this was deliberate.
- The title points to calendar invites and live proxies as the delivery and capture methods.
- Material Security's Threat Research team found it and has taken down hundreds of attacker domains under Operation CloudFire.

What was reported

Since mid-August 2026, a phishing operation has been taking over live Google sessions belonging to corporate users. According to The Hacker News, the links used in the campaign came back clean on every check defenders typically rely on to judge a link, and the operator built it that way deliberately.

The Threat Research team at Material Security identified the campaign. It has since taken down hundreds of attacker domains in an effort it calls Operation CloudFire. The report's headline refers to calendar invites and live proxies, which suggests the lure arrives as a calendar item and the session is captured through a proxy in real time. The excerpt available to us does not give further technical detail.

Why it matters

When a session is stolen, the attacker inherits an already authenticated account. Controls that focus on the password or on link reputation alone may not catch this. Organisations that rely on a clean reputation verdict as a sign of safety should treat that signal as one input among several.

Because the source excerpt is brief, we do not know which users were targeted, how many were affected, or what the attackers did after gaining access. We recommend reading the full report and Material Security's own findings before drawing conclusions.

Practical stance

The response is a review of existing controls rather than an emergency. Focus on how quickly your teams can detect and end an unexpected session, and on whether staff know to question unsolicited calendar invites.

What to do now

1. Review how quickly your team can detect and revoke an active Google session for a suspected account compromise.
2. Brief staff to treat unsolicited calendar invites with links as potential phishing, even if the sender looks familiar.
3. Do not treat a clean link-reputation result as proof of safety; add behavioural and sign-in monitoring for Google Workspace accounts.
4. Check whether your phishing-response playbook covers stolen sessions, not only stolen passwords.
5. Read the full Material Security report and apply any published indicators to your monitoring.