

Forum:[Hack Forums](#)

Thread: [\[Stealer\] Gmail/Youtube keeps logging me out when I use cookies to log in](#)

•CHESTER• - June 5, 2025, 6:11 am

So I have been testing out PureLogs as I have always been curious about info stealers. I setup two VPS, one as the server and one as the client. I logged into a bunch of stuff on the client like gmail, amazon, ebay, reddit, and some random websites.

The stealer works as intended and I am able to view the cookies and other information on the server. Then I instantiated an instance of Chrome with those cookies using playwright. Then I am able to log in to all websites as the client including amazon, ebay, reddit, and so forth. But not Google owned services like gmail and youtube.

When I launch the browser with the cookies, it logs in for half a second, then instantly logs out.

Why is this happening? And how to I counteract it?

UPDATE: When I export cookies from my browser using the extension EditThisCookie, I am able to session hijack my gmail session. But when I use the cookies extracted by Pure Logs, I am unable to session hijack my gmail session.

DramaKing - June 5, 2025, 8:25 am

Maybe Gmail doesn't recognize the device, but that wouldn't explain why a browser extension works.

coocochi - July 24, 2025, 12:15 am

Interesting post, have you been able to figure out why this is happening?, and is it even possible to access a gmail account using cookies?

brainfreeze752 - August 14, 2025, 4:10 pm

unfortunately it won't work for gmail. i know this from my experience with cookie stealers that use reverse proxy to hijack session cookies. Gmail currently have a lot of security layers that detect MITM attacks and cancel the sessions associated with them. one of these security features involve mapping the cookie to the browser. once you use the cookie on a different browser they will cancel the cookie therefore logging you out.

if you want to access a gmail account your best bet is a live panel. The con about a live panel is that it requires you to be active when the user is logging in so that you can bypass 2FA.

MEDUSA LIVE PANEL CAN BYPASS ALL OF GMAILS 2FA methods and it allows you to design a ENDING PAGE that relates to the lure in the campaign so the users won't get suspicious and change the password.

if you want persistent access incase the use decide to change the password you can create a filter to auto delete incoming emails from gmail and create a passkey for the account

Maur0 - August 15, 2025, 8:57 am

@brainfreeze752 is right, the only way to get gmail accounts is by a HVNC, currently cookies login is not possible for gmail and youtube. Maybe with evilginx but cookies no.

Maur0 - August 15, 2025, 2:59 pm

(Aug 15, 2025 02:28 PM)SIM-2267354 Wrote: [\[CITE\]](#) is it possible on wallets?
wallets what? you mean the seed stealing? if its so, yes, its possible, but for that you would need special stealers for that, not a normal stealer on hackforums

infectedstub - August 16, 2025, 8:30 am

Google began deploying a feature called Device Bound Session Credentials (DBSC) in mid-2025. This binds session cookies to the original device where they were issued, making them unusable if stolen and used on a different machine.

The Verge. With DBSC, even if you successfully steals and uses the session cookies via Playwright Chrome, Google will detect the device mismatch and immediately invalidate the session—resulting in the immediate logout behavior you described.

SOURCE : <https://www.theverge.com/news/715117/google-workspace-dbsc-cookie-stealing-attack>

HerrWinston - August 17, 2025, 2:23 am

(Aug 15, 2025 02:59 PM)Maur0 Wrote: [\[CITE\]](#) wallets what? you mean the seed stealing? if its so, yes, its possible, but for that you would need special stealers for that, not a normal stealer on hackforums

i might be wrong but arent there a few seed stealer and Drainer on here? I dont think your that wrong looking around here

DramaKing - August 21, 2025, 8:40 pm

(Aug 16, 2025 08:30 AM)infectedstub Wrote: [\[CITE\]](#) Google began deploying a feature called Device Bound Session Credentials (DBSC) in mid-2025. This binds session cookies to the original device where they were issued, making them unusable if stolen and used on a different machine.

The Verge. With DBSC, even if you successfully steals and uses the session cookies via Playwright Chrome, Google will detect the device mismatch and immediately invalidate the session—resulting in the immediate logout behavior you described.

SOURCE : <https://www.theverge.com/news/715117/google-workspace-dbsc-cookie-stealing-attack>
Shouldn't be able to decrypt the cookies once DBSC is fully implemented.