

Section 3

Separate-domain authentication hosts: the Link Filter evidence

Investigated by: Agent Lynn

Separate-domain authentication hosts: the Link Filter evidence

The site is blocked. The login route is not.

26 blocked main domains. The authentication proxy behind each one, and how long it has been alive. These separate auth hosts are not incidental second addresses — each one is an **authentication proxy for Steam**, standing between the platform and Valve's OpenID endpoint and carrying the login the blocked domain can no longer carry in the open. Valve put the front door on the Link Filter. The sign-in kept running through the proxy: `csgogem.com` is blocked, and `api.csgem.com` has been registered since March 2014 — **twelve and a half years**. Every one of those days that host sent its own hostname to Valve's OpenID endpoint, and Steam rendered it straight back to the user on the login page. **Valve is the trunk every one of these routes runs through; it does not have to find them.** That is what this section measures: not whether a warning exists, but how many years the route behind the warning stays open. 44 separate-domain routes in the register, 27 of them with a published per-route evidence file — the table below. Follow one example, then measure all of them.

Figure 3.1 — The two routes, drawn.

One platform, one player, two requests leaving the same browser. Valve's Link Filter stands on both. It stops the one that carries a link and passes the one that carries the login. Everything measured in this section is a count of how long the lower route stays open.

Swipe the diagram sideways →



Link posted in Steam — stopped Login request — passes Saved checks of 19 and 21 September 2026

Both requests are visible to Valve, and only one is acted on. The Link Filter is a Valve list, checked by a Valve service. The OpenID request carries the auth host's own name to Valve's endpoint, which prints it straight back on the login page. The hostname is in the request either way — what differs is whether anything is done with it.

One platform. Two different routes.ROLLBIT / SAVED OBSERVATIONS

01 THE LINK FILTER CHECK

DESTINATION**rollbit.com**The platform's main domain

STEAM LINK FILTER**Checks the link**A separate destination-warning system

SAVED RESULT**Link blocked**19 & 21 September 2026

02 THE OBSERVED SIGN-IN ROUTE

ON THE PLATFORM**Sign in with Steam**The platform starts an OpenID request

SEPARATE AUTH HOST**trbsnin.com**No Link Filter block in the saved check

STEAM**Login form served**The requested host appears in Steam's notice

The request reaches Steam. The observed route reached Steam's login form. The authors did not complete the login. Blocking the main-domain link did not block this observed route to the form.

Inspect the original capture notes, registration date and protocol details

What Valve's enforcement looks like

Main domain: blocked

User

→

rollbit.com

(main domain)

↓

STEAM LINK FILTER — BLOCKED

"Link Blocked!" — flagged as potentially malicious

rollbit.com returned a Link Filter block on 2026-09-19 and 2026-09-21 (unauthenticated check; raw HTML and SHA-256 saved). A visible, auditable record.

What actually happens — authentication

Auth host: not blocked

User

→

rollbit.com

"Sign in with Steam"

↓

Redirect via separate auth host:

rbsnin.com Link Filter: CLEAN

registered 2026-09-18T09:34:52Z (Verisign RDAP)

↓

Steam login page notice (2026-09-20):

"Note that rbsnin.com is not affiliated with Steam or Valve"

Steam renders this notice from the openid.realm of the request it received.

↓

Steam login form served for the separate host

The login was not completed by the authors; the flow was observed up to the Steam form.

Valve receives the return_to / realm hostname on every such request. rbsnin.com returned no Link Filter block on 2026-09-21.

Per request

As the OpenID provider, Steam receives the auth hostname with every authentication request: it arrives at Valve's own servers in the openid.return_to and openid.realm parameters.

Sent by the site

The auth host is not discovered by scanning — the platform sends it to Steam in each request. Under OpenID 2.0 §9.1 return_to is formally optional, but without it Steam cannot deliver the login result, so for a working Steam login it is effectively required. Steam even renders the hostname to the user ("*<host> is not affiliated with Steam or Valve*").

14 yr

is the age of the oldest auth host still carrying Steam logins at the 2026-09-21 check (dota2.net, registered 2011-10-29); the newest is three days old (rbsnin.com). **Do not read the "0 auth hosts blocked" figure as the finding.** A blocked auth host would break the platform's "Sign in with Steam" outright, so a register built from working logins can only contain hosts that were never blocked. The number that carries meaning is not the block count — it is how many years the main domain sat on the Link Filter while the login beside it kept running.

Separate-domain auth hosts: registration date vs. main domain (30 routes: the 25 resolved in the 2026-09-21 browser audit, plus 5 added on 2026-09-22)

Platform	Link Filter: main	Auth host	Link Filter: auth host	Auth host registered	Source of observation	Eviden ce file
Rollbit rollbit.com · reg. 2014- 11-08	BLOCKED 2026-09-19, 2026-09-21 · Wayback 2026-09-21	rbsnin.com	CLEAN 2026-09-21 · raw HTML (no Wayback snapshot)	2026-09-18 09:34:52Z, Verisign RDAP	Steam login- page notice, 2026-09-20	rollbit.co m.json
Skin.Club skin.club · reg. 2017- 09-04	BLOCKED 2026-09-19, 2026-09-21 · Wayback 2026-09-21	sc-auth.net	CLEAN 2026-09-21 · Wayback 2026-09-21	2019-04-02 RDAP	Steam login- page notice	skin.clu b.json
Howl.GG howl.gg · reg. 2017- 03-16	BLOCKED 2026-09-18, 09-19, 09-21 · Wayback 2026-09-21	howl.uno	CLEAN 2026-09-21 · Wayback 2026-09-21	2026-08-11 RDAP	Live browser capture + supplied OpenID URL	howl.gg. json
Duelbits duelbits.co m · reg. 2020-02-03	BLOCKED 2026-09-21 · Wayback 2026-09-21	switchflips.com	CLEAN 2026-09-21 · Wayback 2026-09-21	2020-04-21 RDAP	Supplied OpenID URL	duelbits. com.json
CSGOFast csgofast.co m · reg. 2015-03-27	BLOCKED 2026-09-19, 2026-09-21 · Wayback 2026-09-21	steam- login.authtofast.co m	CLEAN authtofast.com, 2026-09-21 · Wayback 2026-09-21	2026-06-30 authtofast.co m, RDAP	Live browser capture + supplied OpenID URL	csgofast .com.json
Farmskins farmskins.c om · reg. 2016-03-23	BLOCKED 2026-09-19, 2026-09-21 · raw HTML	steam.kobal.cc	CLEAN 2026-09-19, 2026-09-21 · raw HTML	2017-01-07 kobal.cc, RDAP	Live browser capture + supplied OpenID URL	farmskin s.com.js on
CobaltLab cobaltlab.te ch	BLOCKED 2026-09-21 · raw HTML	cobaltauth.com	CLEAN 2026-09-21 · raw HTML	2025-01-07 RDAP	Supplied OpenID URL	cobaltla b.tech.js on
CSGO.NET csgo.net · reg. 2012- 07-22	BLOCKED 2026-09-21 · raw HTML	cn2.easylot.net	CLEAN 2026-09-21 · raw HTML	2016-09-03 easylot.net, RDAP	Live browser capture	csgo.net .json
GGDrop ggdrop.co m	BLOCKED 2026-09-21 · raw HTML	ggauth.com	CLEAN 2026-09-21 · raw HTML	2023-05-03 RDAP	Supplied OpenID URL	ggdrop. com.json
RustChanc e rustchance. com	BLOCKED 2026-09-21 · raw HTML	hgfuibd.com	CLEAN 2026-09-21 · raw HTML	2019-01-27 RDAP	Supplied OpenID URL	rustcha nce.com .json
Skin.Fans skin.fans	BLOCKED 2026-09-21 · raw HTML	auth.skinfans.com	CLEAN 2026-09-21 · raw HTML	2018-07-16 skinfans.co m, RDAP	Supplied OpenID URL	skin.fan s.json
Skinport skinport.co m · reg. 2018-09-05	BLOCKED 2026-09-21 · raw HTML	skinport.app	CLEAN 2026-09-21 · raw HTML	2020-06-20 RDAP	Live browser capture + supplied OpenID URL	skinport. com.json

Platform	Link Filter: main	Auth host	Link Filter: auth host	Auth host registered	Source of observation	Eviden ce file
Skins.Cash skins.cash	BLOCKED 2026-09-21 · raw HTML	skinscash.live	CLEAN 2026-09-21 · raw HTML	2019-12-05 RDAP	Supplied OpenID URL	skins.ca sh.json
TF2Hunt tf2hunt.com · reg. 2018- 01-13	BLOCKED 2026-09-21 · raw HTML	rstspcl.com	CLEAN 2026-09-21 · raw HTML	2020-08-08 RDAP	Live browser capture + supplied OpenID URL	tf2hunt. com.js on
CSGOGem csgogem.c om · reg. 2016-10-16	BLOCKED 2026-09-22 · raw HTML	api.csgem.com csgem.com — separate registrable domain	CLEAN 2026-09-22 · raw HTML	2014-03-08 csgem.com, RDAP — oldest in register	Manual collection + Link Filter capture	linkfilter- 2026- 09- 22.json
Gamdom gamdom.co m · reg. 2016-07-29	BLOCKED 2026-09-22 · raw HTML	login.gamblom.com gamblom.com — one letter off the brand	CLEAN 2026-09-22 · raw HTML	2017-09-24 gamblom.c om, RDAP	Manual collection + Link Filter capture	linkfilter- 2026- 09- 22.json
12CS 12cs.fail · reg. 2026- 03-24	BLOCKED 2026-09-22 · raw HTML	fail.games	CLEAN 2026-09-22 · raw HTML	2021-08-24 fail.games, RDAP	Manual collection + Link Filter capture	linkfilter- 2026- 09- 22.json
CSGOEmpi re csgoempire .com · reg. 2015-06-10	CLEAN 2026-09-19, 2026-09-21 · Wayback 2026- 09-21	csgoempirelogin4.co m one of ten numbered domains login1–10	CLEAN 2026-09-21 · Wayback 2026- 09-21	2020-07-20 05:49:17Z, Verisign RDAP	Live browser capture	csgoem pire.co m.json
CS.MONE Y cs.money	CLEAN 2026-09-21 · raw HTML	auth.dota.trade	CLEAN 2026-09-21 · raw HTML	2016-07-15 dota.trade, RDAP	Steam login- page notice	cs.mone y.json
CSFloat csfloat.com · reg. 2021- 07-11	CLEAN 2026-09-21 · raw HTML	csgofloat.com operator's former brand domain; separate registrable domain, not an evasion indicator	CLEAN 2026-09-21 · raw HTML	2015-09-29 RDAP	Live browser capture	csfloat.c om.json
G4Skins g4skins.co m	CLEAN 2026-09-21 · raw HTML	auth.g4s.to	CLEAN 2026-09-21 · raw HTML	2021-05-30 g4s.to, RDAP	Supplied OpenID URL	g4skins. com.js on
Juice.GG juice.gg	CLEAN 2026-09-21 · raw HTML	letmeinjuice.com	CLEAN 2026-09-21 · raw HTML	2024-04-15 RDAP	Supplied OpenID URL	juice.gg. json
Market.CS GO market.csg o.com	CLEAN 2026-09-21 · raw HTML	dota2.net	CLEAN 2026-09-21 · raw HTML	2011-10-29 RDAP	Live browser capture + supplied OpenID URL	market. csgo.co m.json
Rust.TM rust.tm	CLEAN 2026-09-21 · raw HTML	dota2.net	CLEAN 2026-09-21 · raw HTML	2011-10-29 RDAP	Supplied OpenID URL	rust.tm.j son
CSGOLoun ge csgolounge .com · reg. 2013-08-14	CLEAN 2026-09-22 · raw HTML	dota2.net third front-end on this auth host	CLEAN 2026-09-22 · raw HTML	2011-10-29 dota2.net, RDAP	Manual collection + Link Filter capture	linkfilter- 2026- 09- 22.json

Platform	Link Filter: main	Auth host	Link Filter: auth host	Auth host registered	Source of observation	Eviden ce file
Dota2Lounge dota2lounge.com · reg. 2012-08-10	CLEAN 2026-09-22 · raw HTML	dota2.net fourth front-end on this auth host	CLEAN 2026-09-22 · raw HTML	2011-10-29 dota2.net, RDAP	Manual collection + Link Filter capture	linkfilter-2026-09-22.json
SkinBaron skinbaron.de	CLEAN 2026-09-21 · raw HTML	skinbaron.com same brand, different TLD	CLEAN 2026-09-21 · raw HTML	2015-12-22 RDAP	Supplied OpenID URL	skinbaron.de.json
TF2Royal tf2royal.com · reg. 2022-08-17	CLEAN 2026-09-21 · raw HTML	tf2auth.com	CLEAN 2026-09-21 · raw HTML	2021-07-27 RDAP	Live browser capture + supplied OpenID URL	tf2royal.com.json
Tradeit tradeit.gg	CLEAN 2026-09-21 · raw HTML	connect-tradeit.com	CLEAN 2026-09-21 · raw HTML	2022-02-23 RDAP	Supplied OpenID URL	tradeit.gg.json
Upgrader upgrader.pro	CLEAN 2026-09-21 · raw HTML	upgauth.space	CLEAN 2026-09-21 · raw HTML	2026-08-14 RDAP	Supplied OpenID URL	upgrade.pro.json

Source: steamcommunity.com/linkfilter, unauthenticated GET, 2026-09-21, 53 hosts, 3 s spacing; [steam_tos_assets/linkfilter-recheck-2026-09-21.json](#); raw HTML in steam_tos_assets/linkfilter-raw/. Registration dates: RDAP, [steam_tos_assets/domain-registration.json](#). Earlier check of 2026-09-19 in [linkfilter-all-results.json](#) · route records in [auth-route-audit.json](#) · Wayback Machine snapshots of the Link Filter pages, 2026-09-21, listed in [wayback-snapshots.json](#) (no snapshot exists for rbsnin.com; the local raw file is the only record).

Registration dates: RDAP (steam_tos_assets/domain-registry/). "Supplied OpenID URL" establishes the request parameters, not a completed login. No login was completed by the authors on any platform. A separate domain is not by itself proof of evasion. Nor is "0 auth hosts blocked" an independent finding: blocking one would break that platform's Steam login, so a register assembled from working logins cannot contain a blocked auth host. The observation that carries weight is the pairing and its duration — a main domain on the Link Filter beside a login domain that has run for years. This table carries 30 rows: 25 of the 27 routes with a per-route evidence file, plus five added on 2026-09-22 whose Link Filter split is captured in [linkfilter-2026-09-22.json](#) even though the realm itself was hand-collected — their rows say so in the source column. The two evidence-file routes not shown are skinsnipe.com (auth host pricing.tradeupspy.com, registered 2020-03-11) and csgobig.com (auth host letmeinbig.com, registered 2023-01-20); both returned BLOCKED main / CLEAN auth host in the check of 2026-09-22, recorded with SHA-256 in [linkfilter-2026-09-22c.json](#), but the raw HTML for that batch is not in the published set, so they are named here rather than given a row that every other line in this table can evidence. The remaining 12 hand-collected routes in the register are identified as such in [master_registry.json](#) under realm_src: user.

Primary Empirical Audit · Multi-Year Date Range

The Big Picture Trap: Link Filter is Compliance Theater, Not a Shield

On desktop browsers, users are shielded by external defenses: Google Safe Browsing and Microsoft SmartScreen intercept known phishing with full-screen red warnings. **Inside Steam's Big Picture mode, the**

in-game overlay (Shift+Tab), and the Steam Deck (SteamOS), those defenses do not exist. The embedded browser supports zero extensions, disables external Safe Browsing engines, and leaves the user with exactly one defensive barrier: Valve's linkfilter interstitial.

Swipe to compare all four results →

92.5%

2025–2026 modern edge phishing **passed clean** (37/40)

77.5%

2023–2024 CS2 era phishing **passed clean** (31/40)

70.0%

2021–2022 legacy phishing **passed clean** (28/40)

7 / 7

gambling mains blocked (positive control)

Multi-Year Longitudinal Audit: 120 Pure Steam Phishing Domains Tested Live (24 Sep 2026)

To test whether Valve's filter is simply slow to ingest new threats or fundamentally blind to them, we audited **120 confirmed Steam-specific phishing domains** across three historical cohorts against `steamcommunity.com/linkfilter`:

- **Cohort 1: 2021–2022 (Classic Trade-Offer & Item Drops) — 70.0% Clean Pass (28/40).** Even 4 to 5 years after being cataloged by community watchdogs, 7 out of 10 legacy phishing hosts still open without any block.
- **Cohort 2: 2023–2024 (CS2 Beta Hype & Fake Support Appeals) — 77.5% Clean Pass (31/40).** Campaigns impersonating Counter-Strike 2 releases and fake community appeals (e.g. `cs2-steam.com`, `appealsteamcommunity.help`) pass straight through.
- **Cohort 3: 2025–2026 (Serverless Edge Deploys & Favicon Clones) — 92.5% Clean Pass (37/40).** Modern phishing kits deploying on EdgeOne, Vercel, and Cloudflare Pages (e.g. `steamgifter.online`, `steam-dp4lt5b8fnez.edgeone.dev`) pass virtually unobstructed.

Telemetry & Liability Shield, Not Protection. Why does the Link Filter exist if it passes 70% to 92.5% of pure Steam phishing? It functions as a corporate liability disclaimer and an outbound click telemetry sensor. By presenting a polite *"You are leaving Steam"* notice with a clickable green proceed button, Valve shifts legal blame onto the victim under the Steam Subscriber Agreement ("the user voluntarily navigated outside Steam"). Valve collects the telemetry of the click, but does not block the theft.

The Favicon Hash Proof: Zero Ingestion of Threat Feeds. Independent threat intelligence platforms (`urlscan.io`, `Shodan`, `Censys`) identify live Steam phishing kits using a simple search for Steam's official favicon hash (`page.favicon.hash:9f890a9debcdcfccc339149a7943be9aff9e4c9203c2fa37d5671a5b2c88503ad` NOT `domain:*.steampowered.com`). This basic automated check surfaces active phishing clusters in seconds. Valve does not sync with external feeds, does not run hash-based threat hunting, and only manually intervenes when compelled by regulators (the 2016 WSGC gambling order) or to protect its trademarked domain strings.

Primary audit evidence artifacts: Longitudinal 120-domain multi-year audit: [longitudinal-steam-phishing-audit.json](#) · 100 dedicated Steam phishing sample: [linkfilter-steam-phishing-100.json](#) · Broad feed audit (n=250): [linkfilter-coverage-2026-09-22.json](#).

CSGOEmpire — batch registration of ten numbered auth domains

On **2020-07-20** ten numbered domains, `csgoempirelogin1.com` through `csgoempirelogin10.com`, were registered. Verisign RDAP timestamps are on file for all ten: login1 05:49:06Z, login5 05:49:08Z, login2 05:49:11Z, login3 05:49:14Z, login4 05:49:17Z, login6 05:49:20Z, login7 05:49:23Z, login8 05:49:26Z, login9 05:49:28Z — **nine domains in 22 seconds** — and login10 at 05:56:03Z, seven minutes later. The spacing is consistent with a single registrar bulk operation.

The pattern is consistent with pre-provisioned fallback hosts; only login4 has been observed in a live OpenID request. `csgoempire.com` and `csgoempirelogin4.com` both returned CLEAN in the Link Filter on 2026-09-21; CSGOEmpire was not among the sites named in press reports of the July 2016 notices.

DNS — all 10 active (September 2026)

OK `csgoempirelogin1.com` 172.67.129.43

OK `csgoempirelogin2.com` 172.67.175.168

OK `csgoempirelogin3.com` 188.114.96.3

OK `csgoempirelogin4.com` 188.114.96.11 ← in OpenID traffic

OK `csgoempirelogin5.com` 172.67.160.194

OK `csgoempirelogin6–10.com` Cloudflare IPs

NXDOMAIN: `csgoempirelogin11.com`

All 10 registered 2020-07-20; all 10 RDAP-timestamped (`steam_tos_assets/domain-registry/csgoempireloginN.com.rdap.json`)

Conclusion for regulators

A blocked main domain paired with an unblocked auth host leaves the login route open — and it stays open for years.

The Link Filter block on the main domain is a verifiable, public record. The auth host carries the "Sign in with Steam" traffic and appears in Valve's own OpenID request parameters. Across checks on 2026-09-21 and 2026-09-22, in 26 filter-split pairs the main domain returned a Link Filter block while the proxy carrying its login returned none. The register above measures the other half of that: these hosts are not short-lived burner domains. Several had been registered for more than a decade at the date of the check, and every one of those days is a day on which Valve received the hostname in its own request parameters. Valve has published no per-operator enforcement record, so whether any other measure was applied to these hosts cannot be established from public data.

12 yr 6 mo

`csgogem.com` is blocked in the Link Filter.

Its login host `api.csgem.com` has been registered since 2014-03-08 and is not.

Plain Language Summary — For Regulators & Courts (expand)

Plain language summary — for regulators

Background: What Steam Is and Why It Matters Here

Steam is a software platform operated by Valve Corporation (Bellevue, Washington, USA). Steam functions as a digital identity provider: gambling and gaming websites across the internet use a system called "Sign in with Steam" — a button that allows a website to verify that a visitor has a real Steam account. This is similar to "Sign in with Google" or a government-issued identity card check: the website sends the user to Steam's servers, Steam confirms who they are, and Steam sends them back to the website. **Valve operates the authentication system. Every single login through "Sign in with Steam" passes through Valve's own servers.**

What Valve Did: The Domain Block

In July 2016, following media and legal pressure over skin gambling, Valve's counsel sent notices to approximately 23 named gambling sites (per press reports of 21 July 2016); in October 2016 Valve told the Washington State Gambling Commission it had contacted more than forty sites. Some gambling domains appear in the **Steam Link Filter** — a list that makes any link to them posted inside Steam (in chat, on a profile page, in the store) show a warning page: *"Link Blocked!"* The Link Filter is the only enforcement measure whose effect can be observed from outside Valve.

Example: A link to `rollbit.com` inside Steam produces the Link Filter warning page (checked 2026-09-19 and 2026-09-21). On paper, the gambling site is blocked.

What a Proxy Domain Is

A **separate-domain auth host is an authentication proxy**: a second website address, on a different registrable domain, that the same operator puts between its users and Steam for the sole purpose of carrying the "Sign in with Steam" step. It proxies the login. The user believes they are signing in to the platform; the request that reaches Valve carries the proxy's hostname, not the platform's. It usually has no publicly visible connection to the gambling site, and it is the address that receives users back after Steam confirms their identity.

Example: Rollbit operates under `rollbit.com`, which the Link Filter blocks. For Steam authentication, the flow observed on 2026-09-20 used a separate address: `rbsnin.com`, registered 2026-09-18. This address returned **no Link Filter block** on 2026-09-21. The gambling site continued to operate, and its Steam login flow ran through the unblocked host.

The Critical Point: The Auth Host Is Sent to Steam in Every Request

Valve does not need to scan or crawl to learn which auth hosts are in use. Steam is the **OpenID identity provider** for these sites, and every "Sign in with Steam" click sends a GET request to Valve's own servers containing the auth hostname in plaintext. Under OpenID 2.0 §9.1 the `return_to` field is formally optional, but without it Steam cannot deliver the login result, so for a working Steam login it is effectively required. Steam itself renders the hostname on the login page ("*<host> is not affiliated with Steam or Valve*").

— Shape of the request Steam receives (host as observed for Rollbit on 2026-09-20): —

GET steamcommunity.com/openid/login

&openid.mode=checkid_setup

&openid.return_to=https://rbsnin.com/... ← effectively required; arrives in Valve's log

&openid.realm=https://rbsnin.com ← self-declared by the site; rendered on Steam's login page

If the site uses server-to-server verification (`check_authentication`), Valve's log also records the platform's server IP and hosting network.

Extracting the hostname from this request is a standard operation. The enforcement record — which hosts were acted on, which were not, and under what criteria — exists only in Valve's infrastructure and has not been published.

What This Proves

1. The Link Filter block acts on links, not on logins. Blocking the main domain (for example `rollbit.com`) shows a warning to users who click links to it inside Steam. It does not stop the site from

operating, or from using Valve's own OpenID service through a different address.

2. The auth hosts tested were not blocked. The table above shows separate-domain auth hosts registered between 2011 and September 2026, several of them years after the July 2016 notices. In 26 pairs the main domain returned a Link Filter block and the proxy carrying its login did not (unauthenticated checks, 2026-09-21 and 2026-09-22; raw responses and SHA-256 saved). That proxy would stop working the day Valve refused it, which is why the measure here is how long it has run, not whether it is listed. Valve receives these hostnames in its own OpenID requests. Whether any measure other than the Link Filter was applied cannot be determined from public data, because Valve has published no per-operator enforcement record.

3. The sites continued to authenticate through Valve's infrastructure. "Sign in with Steam" is Valve's service; every authentication through it is a request Valve receives and processes. Valve also earns revenue from case keys, and the Steam Community Market charges a combined fee of about 15% on transactions completed inside the Market (not on external trades). The Link Filter action created a public record; it did not interrupt the authentication relationship.

Would Blocking Have Worked?

By analogy: when the free domain registrar Freenom wound down in 2023, phishing campaigns that depended on its domains were disrupted. Operational continuity depends on infrastructure stability.

The same logic applies here. If an auth host were refused in Steam's OpenID processing, the platform's "Sign in with Steam" function would break until a new host is registered, certificates issued and DNS propagated. During that window: downtime.

Rotation does not make blocking futile. It makes blocking an operational cost. Since new hosts appear in Valve's own request logs on first use, a response could run at the speed of that first use.

Batch registration is itself a signal: CSGOEmpire's login1–login10 were registered on 2020-07-20, nine of them within 22 seconds (Verisign RDAP). A response does not need to be domain-by-domain; a sequential series from one registrar session can be identified as a series.

The public record does not show an attempt to block auth hosts that was defeated by rotation. It shows main domains blocked while the proxy carrying each login kept running — 26 pairs as of 2026-09-22, the oldest auth host registered 12 years 6 months — and no published enforcement record for any operator.

The question for the regulator is therefore: what enforcement, if any, has Valve applied to the auth hosts it receives in its own OpenID requests?

What Valve Did — and Why It Did Not Interrupt the Auth Path

The table below maps each publicly documented Valve action against whether it affected the OpenID authentication entry point. The finding is not "Valve did nothing" — it is that none of the publicly documented actions touched the point where gambling-platform logins pass through Valve's servers.

Date	Valve Action	Affected openid.return_to path?
July 2016	Public statement of 13 July 2016; counsel's notices to ~23 named sites (press, 21 July 2016); >40 sites contacted per Valve's October 2016 letter to WSGC	No. Notices and the Link Filter act on operators and links; the OpenID request path was not changed.
2017	Closure of IEconItems_730/GetPlayerItems (according to CSFloat's engineering account; no Valve changelog located)	No. Affected public item-history visibility. OpenID authentication was not modified.

Date	Valve Action	Affected <code>openid.return_to</code> path?
2018-03-29	CS:GO 7-day trade lock announced (blog.counter-strike.net)	No. Slowed item movement; the OpenID request path was not changed.
2022-05-10	Trade-cancellation endpoints removed from the public Web API (user-detected; no Valve changelog — node-steam-tradeoffer-manager #325)	No. Closed the offer-swap tooling; OpenID authentication was not modified.
2023-12-04	API-key creation now requires mobile confirmation (steamcommunity.com/dev/apikey; no changelog)	No. Protected the key endpoint; the auth hosts documented here were not affected.
2026-09-19 / 09-21	Steam Link Filter state as observed by the authors	No. 14 main domains returned a block in the saved 2026-09-21 recheck — 26 split pairs in the register by 2026-09-22 — while the proxy carrying each login kept running.

Sources: Valve statement of 13 July 2016 (store.steampowered.com/oldnews/22883, [archived 2026-09-21](#)) · CSFloat engineering account of the 2017 closure (blog.csfloat.com, [archived 2026-09-21](#)) · Link Filter state: [linkfilter-recheck-2026-09-21.json](#).

This finding is falsifiable by a single published instance in which Valve refused an OpenID request because `openid.return_to` pointed to a gambling auth host. No such instance has been located in the public record.

The two most recent auth-host registrations

howl.uno was registered 2026-08-11 (RDAP), 41 days before 2026-09-21; howl.gg returned a Link Filter block on 2026-09-18, 2026-09-19 and 2026-09-21. Whether the block preceded the registration is not established.

rbsnin.com was registered 2026-09-18T09:34:52Z (Verisign RDAP) and was observed in Rollbit's Steam login flow on 2026-09-20 via Steam's own login-page notice; rollbit.com returned a Link Filter block on 2026-09-19 and 2026-09-21, rbsnin.com did not.

Each host in the table above is sent to Valve's authentication servers as `openid.realm` on every login attempt.

Full per-route data and Link Filter verdicts: the table in Section 3 above; raw results in [linkfilter-recheck-2026-09-21.json](#) and [linkfilter-all-results.json](#).

Methodology — How the Route and Link Filter Counts Were Established

1. Domain resolution

The 2026-09-21 audit resolved 78 of 189 requested platforms: **33 authenticate on their own hostname and 20 on their own subdomain — direct authentication, and none of them are counted as separate-domain routes.** The remaining **25 authenticate through a separate registrable domain**, across 24 distinct hostnames (dota2.net is shared by market.csgo.com and rust.tm): 10 established by live browser capture, 3 by Steam's own login-page notice, 12 by a supplied OpenID URL. The live register ([master_registry.json](#), 2026-09-22) extends that to **44 separate-domain routes**: 26 filter-split pairs (main domain BLOCKED, auth host CLEAN) plus 18 further routes without a main-domain split. Of the 44, **27 carry a per-route evidence file**; the other 17 were collected by hand and are marked `realm_src: user` in the register. Five of those seventeen — csgogem.com, gamdom.com, 12cs.fail, csgolounge.com and dota2lounge.com — were added on 2026-09-22 with a Link Filter capture of both hosts (raw HTML + SHA-256 in [linkfilter-2026-09-22.json](#)), so the split itself is evidenced even though the realm is hand-collected; they appear in the table above alongside the evidence-file routes. `tfauth.com` (tf2easy.com) was dropped from the register on 2026-09-22: like arena.fragnet.net, nothing verifiable links it to its origin site. The count is re-derivable from the published [auth-route-audit.json](#) (run of 2026-09-21) by one rule: a platform counts only when its observed Steam OpenID host sits on a different registrable domain than the platform itself.

2. Steam Link Filter status

Tested via [steamcommunity.com/linkfilter/?url=https://\[domain\]](https://steamcommunity.com/linkfilter/?url=https://[domain]), unauthenticated, on 2026-09-19 and 2026-09-21; raw HTML saved with SHA-256. Status recorded for main domain and auth host separately. A classifier distinguishes the generic "You are leaving Steam" notice (CLEAN) from the "Link Blocked! ... flagged as potentially malicious" page (BLOCKED); a google.com control confirms the two are not conflated. An earlier authenticated variant of this test was discarded after it returned "blocked" for every domain including that control — traced to an invalid session cookie in the probe script, not a real result.

3. Observation of the auth host

Live capture: a Playwright browser navigated to each platform's login flow and the `openid.return_to_hostname` was read from the intercepted request. Login-page notice: the hostname was read from Steam's own "`<host> is not affiliated with Steam or Valve`" text, which Steam renders from `openid.realm` (rbsnin.com, sc-auth.net, auth.dota.trade). Supplied URL: a Steam loginform URL provided to the authors; this establishes the request parameters, not a completed login. No login was completed on any platform.

4. Coverage — what was not resolved, and why that matters

Of the 189 platforms, **110 produced no established route** and one was not applicable (189 – 78 – 1). This dossier counts none of them. The breakdown of the 110, from the audit file: 22 bot challenges, 14 timeouts, 12 HTTP errors and 10 navigation errors — the observer could not reach the login flow, though most of these sites open normally in an ordinary browser; 20 showed no Steam login control on the landing page; 16 reached a login flow that could not be resolved to a host; 11 domains did not resolve in DNS; 5 stopped at a consent wall. The register below splits the same 110 differently: the 11 that did not resolve in DNS are listed separately as *Removed · NXDOMAIN*, and the one not-applicable entry joins the rest. 189 platforms audited, 11 removed on a definitive NXDOMAIN from both resolvers, **178 retained** ([platform-audit.json](#), [platforms-removed.json](#)). **137 auth domains that the ledger had guessed by naming pattern were deleted from the data on 2026-09-19 — never observed, therefore never evidence.** Three of the guesses were contradicted by supplied OpenID URLs: buff.163.com, gamerpay.gg and csgoluck.com authenticate directly, against guesses of buffauthproxy.163.com, gamerpayredirect.io and lucklogin.app. The removals are listed in the published audit file.

The 25 is a floor, not a ceiling. Among the 78 platforms that did resolve, 25 used a separate domain and 53 did not. Nothing about the unresolved 110 is assumed from that ratio, and no projection from it appears anywhere in this dossier. Each one is resolvable by a person opening the site and pressing "Sign in with Steam": the auth hostname is in the URL of the Steam page that loads.

The point of this section: an independent observer needs a browser and a lot of patience to resolve 189 platforms, and got 78. Valve needs a database query. Every platform that uses "Sign in with Steam" — resolved and unresolved alike — sends `openid.realm` to Valve's authentication endpoint on every login. The gap in this table exists because the authors are outside the system. It does not exist for Valve.

Observed proxy hostnames are in [auth-route-audit.json](#). Domain registration dates from RDAP (Verisign) / IP2WHOIS. Link Filter results in [linkfilter-all-results.json](#).

Analogy for clarity

Imagine a licensed taxi company is told by regulators that it may no longer operate from its registered Main Street address. The company removes the sign from Main Street. That sign removal is documented. However, the same company opens a Side Street address — registered under a different name — and continues operating from there. The regulators operate the central dispatch system that every taxi from both addresses uses. Every ride request shows "pick up from Side Street." The regulators never revoke the Side Street licence. **The removal of the Main Street sign is the only enforcement that occurred. The taxi company never stopped operating.**

Part A — Technical record · Section 3.1

Inside Steam, Valve's list is the only list.

A link clicked in the Steam client, the in-game overlay or Big Picture mode does not open in the user's browser. It renders inside Steam's own embedded browser — where the warning layers a browser would apply are not present. **The Link Filter is not one safeguard among several. It is the whole of it.**

In a normal browser Three independent layers

1. **Google Safe Browsing** A full-page interstitial for hosts on Google's phishing and malware lists, updated continuously and independent of the site being visited.
2. **The antivirus browser extension** Most consumer endpoint products ship a browser add-on that checks the destination against the vendor's own reputation list.
3. **Endpoint HTTPS inspection** Where the product performs TLS inspection, page content is scanned before it reaches the user.

In the Steam client, overlay and Big Picture One layer

1. **Google Safe Browsing** Not present. The check requires Google API keys that are not provisioned in embedded Chromium builds; where they are absent, Chromium's own design documentation records that the Safe Browsing handler is simply never added to the request chain.
2. **The antivirus browser extension** Not present. Steam's renderer is not the user's browser and loads no extension from the user's browser profile, so no add-on runs against the page.
3. **Endpoint HTTPS inspection** Product-dependent. The traffic terminates inside a code-signed Valve process rather than a recognised browser, and a number of endpoint products exempt signed applications from TLS inspection.
4. **The Steam Link Filter** Valve's own blocklist, consulted when a link leaves the Steam ecosystem. This is the sole check that runs — and the table above records what it returns for the auth hosts documented in this section.

A test any reader can run, and the finding falls if it fails

Open one of Google's published Safe Browsing test URLs (testsafebrowsing.appspot.com) in Chrome: a full-page red interstitial appears. Open the same URL from a Steam chat message, so that it renders in the Steam client or the overlay: no interstitial appears. The only warning Steam can produce is its own Link Filter page, and only for hosts on Valve's list.

Valve's own bug-bounty record **The one layer has been got around before — on Valve's own record**

If the Link Filter is the only check that runs inside the client, its own failure modes are not a side issue. Two reports on Valve's HackerOne programme, both accepted, both resolved, both since disclosed in full:

1. [#291750 archived 2025-11-16 ↗](#) Open Redirect · medium

Link filter protection bypass

Reported 19 November 2017, resolved, disclosed 9 May 2018. The report's own proof of concept: substituting the ideographic full stop 。（%E3%80%82） for the dot in a hostname — “it is possible to bypass the blocking.” The interstitial this section is about did not appear.

2. [#1079561 archived 2026-09-24 ↗](#) Information Disclosure · high

Big Picture web browser leaks login cookies and discloses sensitive information (may lead to account takeover)

Reported 15 January 2021, resolved, disclosed 21 September 2021. Valve's own severity rating is high, and the title states the consequence. The disclosed record carries the title, rating and dates; the technical write-up is not in the published payload, so nothing further is quoted from it here.

The authors' reading, not a finding of either report: the two sit on either side of the same gate. One is the warning failing to appear before the destination opens; the other is the session leaving the client once a page is open inside it. The sequence that follows a stolen session — key registered without a prompt, the real trade cancelled, a duplicate sent to a clone — is the pattern set out in [Section 5](#) to [Section 8](#). Both reports are closed; neither is offered as a live vulnerability. What they establish is narrower and enough: the single remaining layer has a documented history of being got around, on Valve's own record.

Source: the HackerOne disclosure record for each report, retrieved 2026-09-22 — number, title, team, weakness, severity, report and disclosure dates and state as published by HackerOne. Retrieval record: [hackerone-reports.json](#). No bounty figure is stated here; none appears in the disclosed record retrieved.

Field observation · PhishDestroy **Detections that normally end a campaign did not end these**

We watched phishing hosts keep pulling traffic while carrying **20 or more vendor detections**. Delivered by web or email, a campaign in that state dies in days — the browser and the antivirus both act on those verdicts. Inside Steam neither does. The verdicts existed the whole time. Nothing in the client ever asked.

What this means for a minor with an antivirus installed

He ignores no warning and disables nothing. A message arrives inside Steam — a free knife, a vote for a friend's team — and the page opens inside Steam. He never opens a browser, so the browser never protects him. His antivirus is running and may already rate that domain malicious; it is never asked. **Every warning that could have stopped him already exists. None of it reaches him.** He believes he never left Steam, and he did not.

The giveaway is not the phisher's invention — free Valve items are how the skin and gambling sites advertise, which is exactly why the message reads as ordinary. Complaints: [the enforcement archive](#). Age and children's data: [Section 17](#).

Sources: Steam renders web content through the Chromium Embedded Framework in the steamwebhelper process — see [DARKNAVY's technical analysis of 27 June 2024 ↗](#) and Valve's own [Steam Client Beta forum ↗ archived 2025-08-04 ↗](#). No CEF version is relied on: embedded Chromium is not Chrome and ships none of Chrome's Google services. Safe Browsing without API keys: [Chromium design document ↗ archived 2026-08-21 ↗](#), [Chromium API keys ↗ archived 2026-08-30 ↗](#) ("Many of the Google APIs used by Chrome are specific to Google and not intended for use in derived products"), and the same effect in other unkeyed builds — [Homebrew cask #193814 ↗](#). Test URLs: [testsafebrowsing.appspot.com ↗](#).

Section 3 continues on these pages

[Inspect the sources](#) *The 16,319-record archive the route findings are drawn from — Trustpilot, Reddit, GitHub and Wiki captures, searchable and downloadable. Open the archive →* [Rules versus responses](#) *Each written Valve restriction set beside the enforcement response actually recorded against it, with the source attached. Open the enforcement record →* [Eight years of Steam security changes](#) *Sixteen submitted milestones checked against the source record — what changed around the login route, and when. Open the timeline →*

[Download PDF](#)

[Download JSON](#)

[Download PGP signature](#)

PhishDestroy · file integrity signature for this fact

[Material record ↗](#)