ENGLISH · 18 OCTOBER 2026

Their credentials. Their infrastructure.

User API keys, publisher keys, Steam session JWTs and dated Link Filter checks: inspect the infrastructure behind the Valve enforcement investigation.

Prepared	18 October 2026
Attribution	Agent Milo
Live article	phishdestroy.io/steam_dossier/steam-access
Reading files	PDFs, article JSON and verification

A dated reading edition of the published article. Original evidence, reported claims and editorial interpretation retain the distinctions and limits stated in the text.

READING MAP / 05 SECTIONS

Follow the record.

Article overview	3
Three credentials in the trading system	3
Valve supplies the rails.	18
Same filter. Different treatment.	21
Inspect the evidence.	26
Cited source records	27
Edition, sources & verification	33

The entries are clickable. The PDF bookmarks provide another route through the document. External source links open the referenced publication or retained file.

EVIDENCE FILE 03 / THE INFRASTRUCTURE RECORD OWNERSHIP, GAMBLING & PLATFORM CONTROL10 OCT 2026 • WORKING PAPER
STEAM ACCESS

Their credentials. *Their infrastructure.*

The external service still needs the system Valve controls.

INVESTIGATION BY **AGENT MILO**
User API keys, publisher keys and Steam session JWTs serve different purposes. This file follows the documented credential paths, the infrastructure beneath them and the dated Link Filter responses. Version-pinned code audits remain attached as separate evidence files.

Inspect the three credentials ↓Open the code audit ↗
FOLLOW THE ACCESS RECORD

1. 01 / ISSUE**A Steam credential.**
   Account identity, issuer-defined context and expiry.
2. 02 / USE**A service receives access.**
   Documented collection and renewal paths, pinned to their versions.
3. 03 / ENFORCE**A route can be examined.**
   Saved requests, filter responses and the operator's declared host.

Original 11 October edition · complete text →Preserved original wording, alongside the current sections →

01
TOKENS & PERMISSIONS

Three credentials in the trading system

THREE CREDENTIALS / THREE ACCOUNT CONTEXTS

User key. Publisher key. Session JWT.

Compare who receives each credential, what it accesses and how it enters the skin-trading system.

PHISHDESTROY / THE CONVENIENT CONFUSION

Congratulations. The player is now the integration.

Automation is forbidden in the Subscriber Agreement. Meanwhile, an outside trading business teaches the player to supply the credentials its automated workflow needs. Whose automation is this—and whose account carries the consequences? [E09] §4.C

FOR THE DEVELOPER

Applications. Permissions. IP restrictions.

A publisher needs an API to operate its game. Valve documents application associations, permission groups and optional calling-IP restrictions, and tells publishers to keep their keys on secure servers. A recognizable security model. [E16]

FOR THE PLAYER

Copy this. Hand it over. Repeat.

Why must a person selling a skin become a credential courier? In April 2024, CSGORoll told sellers to obtain a token from their Steam session. In June, it announced an extension to collect, refresh and send that token to its servers. Very convenient—for the business receiving access. [E04] [E05]

What does the player gain: a game feature, or another account credential to hand to an outside operator? The dossier's history of stolen inventories makes that a security question, not a terminology exercise. When one access route changes, the commercial system finds another route through the customer's session. Read the original key-security investigation ↗

CSGORoll's own blog words: the P2P announcement presents the platform as the anti-scam enforcement layer — it bans scammers and gamblers, it says. In the same document it explains why Valve cannot ban the mechanism, because every trade belongs to a player's account. Banning the bots, on this architecture, means banning the players. The operator's security blog and the impossibility argument are the same sentence. [E04]

THE PDF / BOARDING-PASS LOGIC
A boarding pass can be a PDF.
So every PDF is a boarding pass?

JWT describes the token's format. "WebAPI" is the label used in this workflow. Neither answers the question of whose account authorizes the request. A reassuring name does not turn a player's session credential into a publisher's controlled integration.

The format is JWT. The account is the player's. The outside operator receives the credential. Valve's answer should explain the access and the protection—not invite the user to admire the vocabulary. [E17] [E05] SIH's token-return handler: read the actual code ↗

Three columns · swipe horizontally to compare on a smaller screen →

User API Key, Publisher API Key and Session JWT compared using the same seven fields

01STEAM ACCOUNT HOLDERUser API KeyA key registered to a user's account.E16 · User-key documentation ↗	02GAME DEVELOPER / PUBLISHERPublisher API KeyA key managed by a Steamworks publisher.E16 · Publisher-key documentation ↗	03LOGGED-IN STEAM SESSIONSession JWTThe browser's `webapi_token`.E04 · CSGORoll's token instructions ↗
WHO GETS IT **A Steam account holder.** This is the personal user-key route. [E16]	WHO GETS IT **A Steamworks publisher.** An administrator creates the key for a publisher group. [E16]	WHO GETS IT **A logged-in Steam user's browser.** The token comes from that active session. [E04]
WHERE IT COMES FROM **Account-key registration.**steamcommunity.com/dev/apikey ↗The registration associates a domain with the account's key.	WHERE IT COMES FROM **Steamworks group administration.**Steamworks → Users & Permissions → Manage Groups ↗The administrator chooses applications and key permissions.	WHERE IT COMES FROM **The browser's session configuration.**steamcommunity.com/pointssummary/ajaxgetasyncconfig ↗CSGORoll's instructions identify the field `webapi_token`.
WHAT IT GIVES ACCESS TO **Account data and user-key methods.** The trade-record reference includes `GetTradeHistory`, `GetTradeOffers` and `GetTradeOffer`. [E44]	WHAT IT GIVES ACCESS TO **Publisher and game-server operations.** Examples include player-ticket verification, purchases and inventory services, within the key's permissions. [E16] [E45]	WHAT IT GIVES ACCESS TO **Authenticated access in the user's session context.** CSGORoll documents using it to monitor the seller's trades. [E04]
PERMISSIONS & IP CONTROLS **The Steam user's account context.** Access is determined by which methods accept that key. The historical security record examines broad account access and its abuse. Read the key-security record ↗	PERMISSIONS & IP CONTROLS **App associations and permission groups.** A publisher key can also be restricted to selected calling IP addresses. [E16]	PERMISSIONS & IP CONTROLS **Subject, audience and session claims.** The supplied JWT includes `sub`, `aud: web:community` and IP-related fields. Steam applies the access rules. [E17]
LIFETIME & RENEWAL **A registered, persistent credential.** The historical investigation follows continued access after registration; Valve controls whether the key remains accepted. Registration and lifecycle evidence ↗	LIFETIME & RENEWAL **Managed through the publisher group.** Group configuration, permissions and Valve's access controls govern its use. [E16]	LIFETIME & RENEWAL **Temporary session credential.** Roll's April 2024 instructions require daily replacement. The token carries an expiry time; the current code audit separately identifies the available renewal paths. [E04]
HOW IT REACHES A SERVER **A key in an API request.** Valve supports a request parameter or the `x-webapi-key` header. [E16]	HOW IT REACHES A SERVER **A request from a secure publisher server.** The publisher host, `partner.steam-api.com`, requires a publisher key and HTTPS. [E43]	HOW IT REACHES A SERVER **A token handed to the outside platform.** Roll's June 2024 announcement describes automatic collection, renewal and upload. Its current version 1.2 instead provides a token-copy popup for manual submission. [E05]

01STEAM ACCOUNT HOLDERUser API KeyA key registered to a user's account.E16 · User-key documentation ↗	02GAME DEVELOPER / PUBLISHERPublisher API KeyA key managed by a Steamworks publisher.E16 · Publisher-key documentation ↗	03LOGGED-IN STEAM SESSIONSession JWTThe browser's `webapi_token`.E04 · CSGORoll's token instructions ↗
ROLE IN THIS INVESTIGATION **The historical account-access route.** The dossier follows key registration, consent attribution and trade substitution. Registration and consent exhibits ↗	ROLE IN THIS INVESTIGATION **The game-publisher integration route.** This is the developer-side context people often mean when they say "Steam API." [E23] [E45]	ROLE IN THIS INVESTIGATION **The seller-session route documented by CSGORoll.** Monitoring the Steam exchange feeds the operator's decision to credit or release its own coins. [E04] [E07]

CSGOROLL'S
DOCUMENTED ROUTE
Column 03: the seller's Steam session.
The user supplies the token. The platform monitors the trade and controls the coin settlement.

THE STANDARDS LAG / PUBLIC, DATED, UNANSWERED

The standards were public. The dates are the record.

Steam ships on the App Store and Google Play, sells through the major card processors, and consumes third-party APIs like any other large platform. Each of those relationships carries a published, dated security requirement that Valve must satisfy to keep operating. Nothing in this table is a private standard, an internal memo or a trade secret — every entry is a public document with a publication date. Set those dates against the dates on which Steam's own Web API acquired the same protections. [E13]

Published external security requirements set against the Steam Web API's own dates

The published standard	The date it took effect	The Steam Web API on the same question
Scoped authorisation	OAuth 2.0 — RFC 6749, October 2012. Section 3.3 defines scope so a client receives only the access it asks for. It has been the default of every major platform API since.	**Granular scopes arrived on 16 January 2026.** Before that, a single Steam Web API key carried full read and write over the account's trades regardless of why it was issued — thirteen years and three months after the specification that defines the control.

The published standard	The date it took effect	The Steam Web API on the same question
A second factor on privileged access	PCI DSS 3.2, requirement 8.3 — mandatory from 1 February 2018 for all non-console administrative and all remote access to the cardholder data environment. Apple then required two-factor authentication of every Developer Program account holder from 27 February 2019: “developers with the Account Holder role in a developer program will need to enable two-factor authentication to sign in.”	**A second factor was required to create an API key from 4 December 2023.** Until then a stolen session cookie was enough — no prompt on the account holder’s phone, no notification afterwards. Four years and nine months after Apple made Valve itself use a second factor merely to sign in to a developer portal.
Credential lifecycle and revocation	Twitch requires of every third-party application: “Your app must validate the OAuth token when it starts and on an hourly basis thereafter” — and retired its legacy v5 API outright on a published schedule, 28 February 2022.	**No published key-lifecycle record.** The 2023 change protected the creation endpoint; no Valve statement located with it addresses keys already registered, and no changelog accompanied the change at all. Whether pre-fix keys were invalidated cannot be established from public data.

The benchmark, from the parent dossier’s token comparison: a GitHub fine-grained token can be restricted to a single repository, read-only, with a mandatory thirty-day expiry, and it logs IP, user agent and timestamp on every call. The Steam Web API key was a single 32-character string carrying full trade authority — read, cancel, decline — never expiring, with no IP binding and no user-visible audit trail. Valve’s own developers manage open-source software on GitHub daily inside the first model; the monolithic key was what 130 million Steam players were issued. [E13]

2012 → 2026
Thirteen years and three months.
That is the interval between RFC 6749 defining scoped authorisation and the Steam Web API acquiring granular scopes on 16 January 2026. No key-lifecycle record has ever been published.

The standards table in the parent dossier ↗The GitHub / Steam token comparison ↗
START WITH THE TERMS

An API is an interface. Access comes from a credential.

The phrase “Steam API” covers more than integration inside a game. Steam publishes both native game interfaces and HTTP services used by websites and account-based tools. Its own key documentation explicitly separates user keys from publisher keys. [E16] [E34]

Steamworks SDK
Libraries and interfaces a developer integrates into a game: achievements, friends, leaderboards and other Steam features. [E23]

Steam Web API
HTTP endpoints that software calls for data or operations. The method determines the authentication it requires. [E43]

API key / session token
The credential presented with a request. User keys, publisher keys and browser-session tokens belong to different account contexts.

JWT
A format that carries claims inside a token. It belongs to the credential layer.

Verification is a platform function.

02 APR 2024

Steam restricts inventory visibility

Valve's release notes introduce ten days of invisibility for purchased and traded Counter-Strike items when other users inspect an inventory. [E28]

10 APR 2024

Monitoring through a user's token

After Steam's API changes interrupted the previous P2P workflow, CSGORoll introduced a replacement: the seller supplies a token from their own logged-in Steam session. [E04]

25 JUN 2024

The extension supplies the server

The extension workflow automatically collects, refreshes and sends the WebAPI token to CSGORoll's servers. The user's credential becomes part of the platform's verification infrastructure. [E05]

01 OCT 2024

The method changes. Control stays.

The later workflow adds inventory monitoring, user confirmation and platform-run disputes for token-free trades. The operator still decides how delivery is recognised and settlement proceeds. [E06]

HOW THE CONTROL WORKS

Identity. Monitoring. Settlement.

Identity
Steam OpenID identifies the account used to sign in to the outside service. [E08]

Monitoring
The documented WebAPI token supplies authenticated access for trade checks. JWT is a format for carrying claims; the receiving service determines the access it accepts. [E05] [E11]

Settlement
The operator links the recognised trade to its own coin ledger and release rules. [E07]

The mechanism connects the user's Steam activity to an accounting decision controlled by the platform.

EXHIBIT B / THE DECODED FIELDS

Read the credential behind the label.

The supplied excerpt declares `typ: JWT` and `alg: EdDSA`. Its claims name a Steam account, the `web:community` audience and timestamps. "WebAPI token" is the field name; JWT identifies the token format. [E17] [E11]

In June 2024, CSGORoll made the destination explicit: its extension "transmits your WebAPI token to our servers". [E05]

The endpoint's character: `ajaxgetasyncconfig` is undocumented and internal. Without a session it returns an empty shell — `{"success":1,"data":[]}` — with one, it hands the browser a signed JWT. Valve built it so Steam's own site could call its own API; it was never built for a casino's servers. No published contract, no scope negotiation, no revocation path for the third-party use documented here. And the session token travels as an `Authorization: Bearer` header, not in a URL — after the 2024 change it is the credential the trade methods accept. The credential changed; the third party watching your trades did not. [E04] [E17]

Inspect the redacted field record ↗
SUPPLIED DECODED EXCERPTIDENTIFIERS REDACTED

typ / alg
JWT / EdDSA

sub
Steam account identifier

aud
["web:community"]

iat · nbf · exp
Issued · valid from · expires

jti
Token identifier

ip_subject
ip_confirmer
IP-related claims
Values redacted

Field transcription from the investigation notes. No live credential is reproduced.

EVERY FIELD IN THE SUPPLIED EXCERPT

Identity, time and issuer-defined context.

How to read the supplied JWT without confusing a field with a permission

Field	Meaning in this record	Role in the access decision
`typ`	JWT: the declared token type.	Identifies the format being parsed.
`alg`	EdDSA: the declared signing algorithm. [E25]	The signing layer protects integrity.
`iss`	Issuer identifier.	Who issued the claims.
`sub`	Subject: the Steam account identifier in the supplied notes.	Which account the token concerns.
`aud`	Intended recipient; the excerpt contains `web:community`.	Audience validation, alongside the endpoint's authorisation rules.
`iat`	Issue time.	When the token was created.
`nbf`	Earliest acceptance time.	The token is not valid before this time.
`exp`	Expiry time.	The token must cease to be accepted at expiry.
`jti`	Token identifier.	Identifies this token instance.
`oat`, `rt_exp`	Additional timestamps listed in the supplied Steam payload.	Issuer-defined session metadata. Their exact processing is part of Steam's implementation.
`ip_subject`, `ip_confirmer`	IP-related fields, with addresses redacted.	Issuer-defined network context; enforcement depends on the receiving service.

Standard claim definitions: RFC 7519, §4.1. Additional claim names: §4.3. The field values and names come from the supplied, redacted excerpt. [E11] [E17]

SIGNED JWT / THREE PARTSANNOTATED STRUCTURE

A compact signed JWT joins three base64url-encoded parts with dots. Select a part to see what it contributes. [E24]

```
{
  "typ": "JWT",
  "alg": "EdDSA"
}
```

What kind of object is this?

The header declares the JWT type and EdDSA signature algorithm. These are the header values recorded in the supplied excerpt. The algorithm belongs to the signing layer. [E17] [E25]

TYPE + SIGNING METHOD


```
{
  "sub": "[SteamID redacted]",
  "aud": ["web:community"],
  "iss": "[issuer value omitted]",
  "iat": "[issued timestamp]",
  "nbf": "[valid-from timestamp]",
  "exp": "[expiry timestamp]",
  "oat": "[additional timestamp]",
  "rt_exp": "[additional timestamp]",
  "jti": "[token ID omitted]",
  "ip_subject": "[redacted]",
  "ip_confirmer": "[redacted]"
}
```


Whose session context travels with it?

`sub` identifies the subject; `aud` identifies intended recipients. The standard timestamps record issuance, earliest acceptance and expiry. Steam's additional fields carry issuer-specific session context. [E11]

The field-by-field table above separates standard JWT claims from Steam's additional session metadata. All supplied field names are also preserved in the downloadable excerpt.

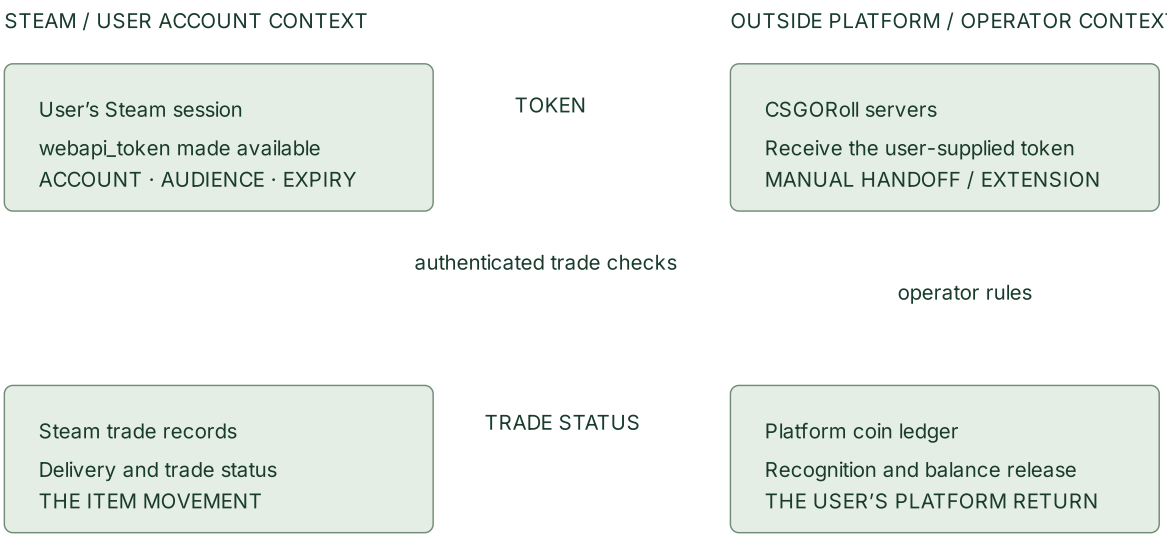
IDENTITY + AUDIENCE + TIME
ENCODED HEADER + PAYLOAD**Signature integrity**

Readable claims, verifiable integrity.

A signature covers the encoded header and payload. Verification checks that signed input with the appropriate key. Base64url encoding makes those first two parts readable; encryption is a separate mechanism. [E24]

This exhibit presents the supplied fields. The signature is represented structurally because the notes contain no complete signed token.

DECODING → CONTENT / VERIFICATION → INTEGRITY
FOLLOW THE ACCESS / CONTROL MODEL



Swipe the diagram to inspect both sides.

01 / SESSION CONTEXT

The credential starts in the user’s Steam session.

Its account identifier, audience and timestamps travel in the token. CSGORoll’s documented seller workflow obtains this credential from the logged-in browser.

E04 · Read the documented workflow ↗ [E17 · Supplied fields]
EXPIRY / RENEWAL / CONTINUED MONITORING

A short-lived token can support an ongoing commercial connection.

Roll’s April 2024 instructions require daily replacement. Its June 2024 announcement describes background collection, refresh and upload. The currently distributed Roll package uses a manual-copy popup; Empire’s separately audited extension implements session renewal. These are different implementations of the same dependency: the platform needs continuing information from the user’s Steam account to settle its own ledger. [E04] [E05]

CODE AUDIT / 10 OCTOBER 2026

Follow the session credential into the extension.

The current CSGORoll-linked package and SIH 2.11.12 were inspected for token extraction, renewal triggers, server transmission and trade-control paths. The appendix pins each finding to a version, file and hash, and separates the 2024 workflow from the currently distributed code.

Read the extension code audit ↗

▼ **Before the session-token workflow: the user-key registration problem+**

The Steam Dossier’s historical API-key case traces a credential registered through a compromised authenticated browser session. The consent action was not a person’s deliberate grant: the account holder never saw the key-registration page, and a script executed the headless POST that submitted the registration fields with the stolen session cookie — machine-

injected consent. Steam Support nonetheless attributes the key to the account holder. Valve holds the registration and request records; publish who performed the consent action behind the key it attributed. Inspect the consent and registration record ↗

The documented trade-substitution pattern then follows monitoring, cancellation and a replacement offer, with the user's confirmation attached to the substituted transaction. A persistent account credential and an active session become parts of the same abuse chain. Follow the documented substitution sequence ↗

Valve's public Web API documentation describes website developers and account-key registration. Its API Terms are dated July 2010. This history belongs to user-account access and web services, alongside the separate Steamworks game-integration pathway. [E33] [E34]

The issuance record: Valve's user-key page issued a 32-character hex key to any logged-in account in a single click — no terms confirmed, no verification, no email notification. A day-old account with nothing in it qualified. [E16] [E34]

The key had no expiry, no scopes and no IP binding: all-or-nothing account access, passed as a bare `?key=` parameter in the URL — logged by proxies, cached by servers, preserved in links. "Endless session" is not a metaphor; it was the documented property of the credential. With that key a site could call `GetPlayerSummaries`, `GetOwnedGames` and the full `IEconService` trade set — reading the account's economy with the owner's eyes. For years this was the standard deposit path of every skin site. [E44]

The silent fix: until 4 December 2023, a stolen session cookie alone could register that full-privilege key — no password, no Steam Guard prompt, no notification to the person whose account it was. On that date Valve began requiring mobile confirmation for key registration, closing the cookie-only route — without a changelog, detected by users rather than announced, about seven years after Valve's 2016 statement and roughly six after the scam panels the archive preserves. And Valve has published nothing about the keys minted before the fix: no statement located with the change addresses keys already registered, and whether pre-fix keys were invalidated cannot be established from public data. The key itself was built never to expire — the zombie-key reservoir, credentials minted from stolen cookies, invisible to their owners, absent from any record a data subject could inspect. The question every refund refusal turns on — is a key created on this account years ago still live? — is one only Valve can answer, and it has not. [E13] Read the vulnerability profile and the fix record ↗

The 2024 closure: Valve closed the key-protected trade methods — and the credential economy did not shrink, it migrated. Within days CSGORoll was instructing sellers to paste a live session token instead. Valve closed one door and the commercial system walked through the user's own session. [E04]

Read the historical registration and trade-method exhibits ↗

THE HIJACK WALKTHROUGH / RECONSTRUCTION OF THE PRE-2023 PATTERN

The victim never visits the key page.

The parent dossier's interactive hijack simulation, promoted into this record. Before 2023, the stolen Steam session could register a persistent Web API key. That key let the attacker monitor and cancel the victim's pending offer; the attacker's clone account then sent the replacement. The victim's mobile confirmation completed the substituted trade. The entry is ordinary phishing: a compromised friend account sends the link, the victim enters credentials and a Steam Guard code into a lookalike portal, and the phishing server captures the active `steamLoginSecure` session cookie. The second factor has been used, not bypassed — two-factor authentication protects the moment of login, not what the resulting session can do afterwards. The timings below are illustrative, not live measurements of the current platform; the sequence is the record. [E13]

PHASE B / SILENT KEY REGISTRATION

The key is registered by a script.

```
POST steamcommunity.com/dev/ajaxregisterkey
Cookie: steamLoginSecure=<stolen session>
Body: agreeToTerms=agreed&domain=localhost
```

The victim never saw the key-registration page. A script holding the stolen cookie executes the headless POST — and because a script has no real domain to give, it sends `localhost`, the value later found on the hijacked account. Valve returns a full-privilege master key. Pre-2023 this required no password, no Steam Guard approval and no notification, and the key came with no scope limit: a session cookie converted into a durable credential.

PHASE C / THE TRADE SWAP

The legitimate trade is cancelled and cloned.

The script polls `IEconService/GetTradeOffers`. The moment the victim initiates a legitimate trade, the script cancels it — sub-second, no prompt to the account holder — and a clone bot sends an identical offer carrying the same name and avatar, dressed with the recipient's real profile data from `ISteamUser/GetPlayerSummaries`. Steam sees valid API calls carrying a valid key issued to that account. Every call is correctly authenticated.

THE EXPLOIT COMPLETED

The confirmation is genuine. The offer is not.

Expecting the mobile prompt for their original trade, the victim approves the replacement. The confirmation is authentic — made by the account holder, on a registered device — but the offer it confirms is not the one the user initiated. That is the record Steam Support reads when the complaint arrives, and the reason the archived complaints were closed as user error.

Four documented endpoints do the whole job — none of them is a flaw

Endpoint	Role in the sequence	What it contributes
`IEconService/GetTradeOffers`	Polls the account	Monitors the account's trade offers — the details of newly created, pending or modified offers, including offer IDs and the recipient's profile. [E44]
`IEconService/CancelTradeOffer`	Voids the real trade	Programmatically invalidates the legitimate offer before the account holder completes the mobile confirmation.
`ISteamUser/GetPlayerSummaries`	Dresses the clone	Returns the legitimate recipient's profile name and avatar URL, so a prepared clone account can be dressed to match.
`dev/ajaxregisterkey`	Mints the credential	Historically, any active `steamLoginSecure` cookie session could register a key — no Steam Guard confirmation on the mobile device, no notification to the account holder. [E34]

The consent checkbox was never clicked by a human. Under GDPR Article 7 and Article 4(11), consent must be a freely given, specific, informed and unambiguous indication of the data subject's wishes — a headless POST carrying a stolen cookie is none of those things. It is a forged signature on a transfer of liability. The dossier's position is that a terms-acceptance field submitted by a hostile script, with no page shown to the account holder, cannot meet that definition; whether it does is for the supervisory authority. [E13]

FOUR ENDPOINTS
NONE IS A FLAW

A stolen session could mint durable account access.

No server exploit was required. The stolen session registered the key; the key supplied monitoring and cancellation; the clone account supplied the replacement offer. Steam accepted the credentials at each step. The defect was the authority granted without an effective check on who was exercising it. [E13]

Step through the hijack simulation in the parent dossier ↗

FIRST ABUSE / NOTIFICATION / FIX / REAPPEARANCE

The abuse mechanisms returned more than once. Publish the trail per mechanism.

The API-key registration route was restricted and reappeared through session tokens. Session theft was answered and returned through extensions reading the same cookies. For each mechanism, the record request aimed at Valve is the same trail: first abuse, first user notification, fix date, reappearance — and the losses carried in between. [E04] [E05]

THE DOCUMENTED CONNECTION

1. 01**Steam session**

The seller is logged in.

2. 02**Token handoff**
   The platform receives the session token.
3. 03**Trade monitoring**
   Delivery is checked through the documented workflow.
4. 04**Platform balance**
   Recognition and coin release follow the operator's rules.

PUBLIC VISIBILITY / ITEM LINEAGE

The original-ID tracking route was removed.

The former `IEconItems_730/GetPlayerItems` endpoint exposed an item's original identifier, which could be matched across inventory changes. Its closure in 2017 removed that public identifier from the tracking route. The engineering history describes the replacement approach using float, seed and paint properties. That matching method does not restore the original-ID record. [E48]

The consequence for this investigation is control over evidence: the user is asked to explain where an item went while the authoritative transfer records remain inside Steam. The dossier follows the loss of public tracing and what it means for a victim seeking a remedy.

Read the item-lineage and evidence-access record ↗
IDENTITY / CREDENTIAL / ECONOMIC RESULT

Follow what each step gives the platform.

Three different operations in one user journey

Step	What moves through the system	What the operator obtains
Steam OpenID	Steam returns an authenticated SteamID to the service's login flow; the request declares the service's return address.	An authenticated Steam identity for the site's user record. [E34]
Session-token handoff	The seller's browser-session token is copied or collected by the extension.	The credential used in the documented trade-monitoring workflow. [E05]
Settlement decision	A Steam transfer is recognised under the platform's verification rules.	The basis for crediting, withholding or releasing its own coin balance. [E07]

The intermediary has moved into the account-access and accounting layers. Direct item delivery leaves that control in place.

▼ **The concrete interfaces: account data, trade records and publisher servers+**

The Web API is organised as host → interface → method → version. A method is an operation; its required credential determines the account context accepted for that operation. The reference documentation therefore has to be read at both levels. [E43]

Concrete technical examples behind the terminology

Reference	What it describes	Why it matters here
`api.steampowered.com`	HTTP services organised into named methods, with public and authenticated operations.	A website or server can make these calls; the interface extends beyond code running inside a game.
`IEconService`	Trade history and offer records, including `GetTradeHistory`, `GetTradeOffers` and `GetTradeOffer`.	These methods document a user authentication key: a concrete account-access role outside game-client integration. [E44]
`ISteamUserAuth/AuthenticateUserTicket` on `partner.steam-api.com`	Publisher-side verification of a user's authentication ticket.	The application's identity and the publisher's credential are explicit parts of the request. [E45]
`partner.steam-api.com`	A separate HTTPS host for secure publisher servers; every request requires a publisher key.	Valve documents its availability, firewall setup and access requirements separately from the public host. [E43]

The publisher contour is engineered like a real API boundary: a key required on every request, 403 and a hard IP rate-limit without it, a host outside the shared Akamai cache, HTTPS only, documented CIDR ranges for firewalls — and publisher access scoped to the partner's own AppIDs: leaderboards, micro-transactions, workshop moderation and finance calls through `ISteamMicroTxn`, `ISteamLeaderboards`, `IPublishedFileService` and `IPartnerFinancialsService`. Everything the user-key page lacked in 2010–2024 exists one layer up — for publishers. [E43] [E16]

Publisher-key documentation adds group administration, application associations, method permission groups and optional IP allowlists. CSGORoll's documented token handoff instead starts with the seller's Steam Community session. That is the access relationship the investigation follows. [E16] [E04]

Original Web API overview ↗ JWT format reference ↗

NEW / EMPIRE, ROLL & FAST

Trade tracking. Session access.

Empire's login-cookie extraction and inactive session-renewal tab; Roll's two extension identities; Fast's current SIH installation and permission flow. The code is pinned to downloaded packages and public frontend files.

Open the new investigation ↗

▼ **Read the original 11 October wording**

Preserved verbatim from the supplied 11 October 2026 edition. “Today” and “currently” refer to that edition; its original estimates and formulations remain available alongside the dated text above.

The parent dossier’s interactive hijack simulation, promoted into this record. Before 2023, a Web API key registered on an account could read its inventory, cancel a pending trade offer and create a new one — and no trade-confirmation screen was shown to the account holder for any of those actions. The entry is ordinary phishing: a compromised friend account sends the link, the victim enters credentials and a Steam Guard code into a lookalike portal, and the phishing server captures the active steamLoginSecure session cookie. The second factor has been used, not bypassed — two-factor authentication protects the moment of login, not what the resulting session can do afterwards. The timings below are illustrative, not live measurements of the current platform; the sequence is the record. [E13]

Returns the legitimate recipient’s profile name, avatar URL and level, so a prepared clone account can be dressed to match.

The only thing the attacker had to steal was the key. None of the four endpoints needed exploiting — a valid key calls them and Steam answers. Every call is correctly authenticated; the defect is what the key was allowed to do. [E13]

Open this passage in the complete original edition →

02
THE INFRASTRUCTURE BELOW THE PLATFORM

Valve supplies the rails.

Two central authorities.
Different parts of the same exchange.

Valve governs the Steam account and item infrastructure. The outside operator governs its own ledger and access rules. Moving the item directly between users leaves both dependencies in place.

Steam’s agreement confines Wallet funds to its ecosystem and makes their use subject to Valve’s rules. The outside operator adds another controlled balance and another set of conditions around the same item economy. [E09]

13 JUL**2016**VALVE / PUBLIC STATEMENT

The mechanism was already named.

Valve identified Steam authentication and automated account activity in skin gambling, said it had no business relationships with those sites, and stated that using those services to operate a gambling business was prohibited.

E08 · Read Valve's statement ↗
S / D
CONTINUE THE INFRASTRUCTURE INVESTIGATION

Their rules. Their system.

The Steam Dossier examines the written rules, observed routes and enforcement record.

↗
USERS, DEVELOPERS AND THE RIGHT TO DECIDE

Documentation does not give the community control.

Valve's API terms reserve the ability to change the service or end access, including access for a particular application. Developers can build an integration and users can participate in it, but both remain dependent on decisions made by Valve. A public interface, a discussion board or a wiki does not transfer authority over those decisions to its readers. [E33]

That is the communication and accountability problem: the people affected need an attributable rule, change record and reasoned remedy, while the power to accept a credential, move an item or restore access stays with the platform.

Inspect our captured support, developer and wiki records ↗
THREE POSITIONS / ONE ITEM ECONOMY

The right being defended runs through the system being restricted.

13 JUL 2016

The real-money boundary

> "Steam does not have a system for turning in-game items into real world currency."

> "We have no business relationships with any of these sites. We have never received any revenue from them. And Steam does not have a system for turning in-game items into real world currency."

The full statement is the quote to test: ten years later, every clause is testable against the fee record, the sponsorship record and the $1 million sale. [E08] [E38]

> "Using the OpenID API and making the same web calls as Steam users to run a gambling business is not allowed by our API nor our user agreements."

In 2026 the same web calls are made with a session token pasted by the user — and the calls are the user's own. Valve wrote the rule in a form its own architecture evades. [E04]

Erik Johnson / Valve's original statement ↗

THE RULEBOOK

The commercial-use boundary

Steam's rules reserve commercial permissions and explicitly list gambling under prohibited commercial activity. The participant's account supplies the access through which an outside service can operate.

Steam Online Conduct ↗

11 MAR 2026

The transferability defence

Valve presents continued transfers as a consumer right. The same transfers let items leave one account for another while an outside platform handles the cash or coin side of the exchange.

Valve's public response ↗

Reading these positions together reveals the selective boundary. The system's public description can stop at Steam's Wallet, while its items travel through cash-priced outside markets. The right invoked for the collector is also the infrastructure used by the commercial service. The investigation follows the whole route across that boundary.

2016 / 2026
ONE SYSTEM
Both cannot be the company's understanding of its own system.
2016 — "Steam does not have a system for turning in-game items into real world currency."
2026 — transferability is a right Valve refuses to remove, while the complaint records a $1 million sale. [E08] [E14] [E38]

Subscriber Agreement analysis ↗Clauses against recorded platforms ↗The market above Steam's ceiling ↓
OCT**2016**VALVE / WSGC RESPONSE

Forty notices. Account-level enforcement.

Valve told the Washington State Gambling Commission it had sent cease-and-desist notices to more than forty sites and disabled associated Steam accounts, while defending Steam trading and OpenID. The response is the direct anchor for the closing demand below: publish when access was disabled, what returned and under whose control.

E19 · Valve's October 2016 response ↗
The July 2016 notices set a ten-day deadline. Our dossier follows that demand through the October response and into a route register where 26 main-domain warnings coexist with separate authentication hosts. The register counts 44 separate auth-host domains carrying Steam logins for third-party platforms beside those 26 blocked main domains — each a domain registered apart from the platform's main address; the split is systematic, not incidental. [E13]

The oldest recorded split route reaches back to a March 2014 host registration. The register preserves those dated checkpoints and identifies the mechanism Valve's enforcement should have interrupted. Publish when access was disabled, what returned and under whose control.

Open letter and Washington record ↗July 2016 notices and dated history ↗The route register ↗

03
THE VISIBLE ENFORCEMENT LAYER

Same filter. Different treatment.

20 URLS CHECKED
We submitted the addresses in this investigation to Steam's own Link Filter. CSGORoll, CSGOEmpire and Hellcase received an ordinary external-link notice with a continue link. The exact `www.csgoroll.com` variant also supplied a continue link. Sixteen other supplied addresses received a hard block. The difference is visible in Valve's response. [E18]

▼ **Steam's browser, Big Picture and the destination warning+**
Valve's original Big Picture presentation includes a built-in web browser. DARKNAVY's June 2024 technical research describes Steam's `steamwebhelper` as a Chromium Embedded Framework application rendering Store, Community and Friends content. [E46] [E47]

The browser surface and the Link Filter perform different jobs: one renders the page; the other controls Steam's warning and onward link. The investigation follows that visible destination decision. For the supplied gambling addresses below, the wrapper either blocks the route or supplies a continue link. The wider dossier examines the client, overlay and Big Picture context.

The Link Filter's character is a man-in-the-middle layer on every link Steam users exchange: Steam intercepts the destination, renders its own warning page, and decides whether to hand the user onward. The same interception Valve once needed bots for, repackaged as a "safety" feature whose block list Valve controls.

Read the embedded-browser and authentication-route investigation ↗

CSGOROLL.COM / SAVED RESPONSE

"Notice: You are leaving Steam."

"Continue to external site"
The returned page includes an onward link.

Open this Steam check ↗

SKINPORT.COM / SAVED RESPONSE

"Link Blocked!"

NO CONTINUE LINK

The returned page withholds the onward link.

Open this Steam check ↗

CAPTURED 10 OCT 2026 · 19:02–19:03 UTC / WWW CHECK 20:27 UTC
Public HTTPS responses, without a signed-in Steam session.

Saved Steam Link Filter responses for the supplied addresses

Address submitted	Observed response	Continue link	Original URL
csgoroll.com ↗	Continue link present	Yes	Steam response ↗
www.csgoroll.com ↗	Continue link present	Yes	Steam response ↗
csgoempire.com ↗	Continue link present	Yes	Steam response ↗
hellcase.com ↗	Continue link present	Yes	Steam response ↗
csgostrong.com ↗	Link Blocked	No	Steam response ↗
csgo500.com ↗	Link Blocked	No	Steam response ↗
csgocosmos.com ↗	Link Blocked	No	Steam response ↗
csgocasino.net ↗	Link Blocked	No	Steam response ↗
csgo2x.com ↗	Link Blocked	No	Steam response ↗
csgohouse.com ↗	Link Blocked	No	Steam response ↗
csgoatse.com ↗	Link Blocked	No	Steam response ↗
csgocash.com ↗	Link Blocked	No	Steam response ↗
csgobig.com ↗	Link Blocked	No	Steam response ↗
csgomassive.com ↗	Link Blocked	No	Steam response ↗
skins2.com ↗	Link Blocked	No	Steam response ↗
csgopot.com ↗	Link Blocked	No	Steam response ↗
csgowild.com ↗	Link Blocked	No	Steam response ↗
skinport.com ↗	Link Blocked	No	Steam response ↗
gamdom.com ↗	Link Blocked	No	Steam response ↗
csgofast.hk ↗Supplied test address	Link Blocked	No	Steam response ↗

Showing all 20 recorded responses.

All 20 returned HTTP 200. The classification above comes from the page heading and the presence or absence of an actual continue anchor. Links open the current Steam response; the downloadable record preserves the dated observations.

Download the checks and timestamps ↗
THE ENFORCEMENT QUESTION
The filter can withhold a destination link. For these three sites it supplied one.
What rule explains that dividing line?

26
THE WIDER ROUTE REGISTER

A blocked homepage. An available login route.

The Steam Dossier's September register follows 26 filter-split pairs from the main domain to a separate Steam authentication host.

↗
THE ADDRESS-STRING TEST

What does the filter react to?

We also submitted the `csgofast` name in five literal forms. Steam blocked the bare host, the .com and .hk forms, and a subdomain under example.com. The same text in the query-string example received an ordinary notice. [E36]

The filter's own character is undocumented: Steam has never documented how the Link Filter decides. It appeared around 2016, without announcement, and its block list is not published. The only way to test the enforcement layer Valve actually ships is to submit addresses and record the answers — which is what this register does.

Five literal address inputs and saved Steam responses

Literal target submitted	Saved result
https://csgofast ↗	Link Blocked
https://csgofast.com ↗	Link Blocked
https://csgofast.hk ↗	Link Blocked
https://example.com/?name=csgofast ↗	Continue link present
https://csgofast.example.com ↗	Link Blocked

10 October 2026 · 19:09–19:10 UTC. The displayed links preserve the exact literal requests used for this comparison.

Download this five-input check ↗
THE PHISHING AUDIT / 120 DOMAINS · 24 SEPTEMBER 2026

The filter reads the gambling list fluently. It has never ingested a phishing feed.

The parent dossier submitted 120 confirmed Steam-specific phishing domains to Valve's own Link Filter in three historical cohorts, tested live on 24 September 2026. On the desktop, external defenses such as Google Safe Browsing and Microsoft SmartScreen intercept known phishing with full-screen warnings; inside Steam's embedded browser — Big Picture, the in-game overlay, the Steam Deck — those defenses do not exist, and the Link Filter is the one barrier left. [E13] [E46] [E47]

Targeted Steam sample: the 120 hosts in these three cohorts were selected for Steam phishing through favicon searches and checks for copied Steam sign-in or home-page interfaces. This deliberate selection is separate from the mixed public-list checks below.

120 confirmed Steam-phishing domains, three cohorts, one filter

Cohort	What was submitted	Passed clean
2021–2022 legacy phishing	Classic trade-offer and item-drop campaigns. Even 4 to 5 years after being cataloged by community watchdogs, seven in ten of these hosts still open with no block.	**70.0%** (28/40)
2023–2024 CS2-era phishing	Campaigns impersonating Counter-Strike 2 releases and fake community appeals — `cs2-steam.com`, `appealsteamcommunity.help` — pass straight through.	**77.5%** (31/40)
2025–2026 edge phishing	Serverless edge deploys and favicon clones on EdgeOne, Vercel and Cloudflare Pages — `steamgifter.online` and its kin — pass virtually unobstructed.	**92.5%** (37/40)
Gambling mains positive control	The control every phishing audit needs: the filter's own category.	**7 / 7 blocked**

Additional public-list checks · 6 October 2026

1,088,753 distinct hosts

Additional analysis of public lists: we did not find a suitable Steam-only public list for a larger census, so we checked lists we considered relevant. None is exclusively Steam scams or phishing; their results are reported separately.

Steam Link Filter responses · percentage of all hosts in each list

List	Tested hosts	Blocked	Blocked %	Ordinary notice

List	Tested hosts	Blocked	Blocked %	Ordinary notice
Steam / Discord feeds	36,724	1,759	4.79%	34,965
PhishDestroy · community + main list	1,086,734	4,010	0.37%	1,082,629

Scroll horizontally to compare the results.

Why these lists?

- **Steam / Discord feeds.** DevSpen and Discord-AntiScam cover gaming-account phishing and related scams. They are close to the Steam ecosystem, but the combined list is not exclusively Steam phishing. DevSpen · Discord-AntiScam.
- **PhishDestroy · community + main list.** Our PhishDestroy community and main lists test broader phishing and scam coverage, including crypto. The supplied results also contain blocked crypto-themed hosts, such as `app-metamask-kyc-auth.com`, `app-trezor-auth.com`, so this is a relevant additional check, not a Steam-only sample. PhishDestroy destroylist.

The two runs contain 1,123,458 host records, with 34,705 hosts in both lists: 1,088,753 distinct hosts after deduplication. We do not pool their block rates.

▼ **Method & verification**

Blocked % = BLOCKED ÷ all tested hosts in that row. The PhishDestroy run also has 78 ERROR, 15 UNKNOWN and 2 INTERNAL results; these 95 are included in the denominator, not counted as ordinary notices. The Steam / Discord run has no residual statuses.

ALLOWED means the ordinary “You are leaving Steam” notice was recorded, not that the destination is safe. These dated results measure the supplied lists; they do not establish that every site was still active or how Valve maintains its filter.

Methodology · English · TXT

Recounted results · JSONIndividual files & signatures · English

The filter’s one demonstrated fluency is the gambling list. Independent threat-intelligence platforms surface live Steam phishing kits in seconds by searching for Steam’s official favicon hash; Valve does not sync with external feeds, does not run hash-based threat hunting, and manually intervenes when compelled by regulators — the 2016 WSGC gambling order — or to protect its trademarked domain strings. The filter reads the gambling list fluently; it has never ingested a phishing feed. [E13]

TELEMETRY,
NOT PROTECTION

A layer that passes 92.5% of live 2025–2026 phishing hosts is not a shield.

It presents a polite “You are leaving Steam” notice with a clickable proceed button, shifts the blame onto the click, and collects the telemetry of the click — while the theft passes through.

Read the 120-domain longitudinal phishing audit ↗

04
THE PUBLIC RECORD

Inspect the evidence.

28 RECORDS
Sources cited in this article appear first. Select “All records” to inspect the complete 107-record register shared by the investigation; the dedicated evidence files retain their own detailed registers.

▼ **Methodology & source notes**
Research date: 10 October 2026. The credential comparison separates user API keys, publisher keys and session JWTs. Historical workflows retain their dates; the supplied JWT fields are transcribed with identifiers redacted. The package-specific checks continue in the extension audit and the three-operator comparison.

The Link Filter records preserve literal request URLs, timestamps, observed headings and continue links. Diagrams illustrate the documented paths; they do not execute account operations. The public-response and ownership analysis remains in Valve and enforcement.

▼ **Original research scope · 10 October 2026**
Research date: **10 October 2026**. This investigation compares the platform’s public policies and dated technical records with Valve’s public statement, Steam’s agreement, account-restriction rules and the filed New York complaint. The supplied RWT warning is reproduced without alteration.

Technical changes are presented on a dated timeline. The Link Filter exhibits preserve literal request URLs, timestamps and observed headings and continue links. The JWT exhibit transcribes the supplied decoded fields with identifiers redacted. The interactive diagrams explain the documented control relationships. The legal-response analysis places Valve’s public framing beside the complaint and the documented control of accounts and items.

The analysis follows the economic mechanism: who supplies the credential, assigns value, verifies delivery, credits the balance, sets transfer conditions, enforces account restrictions and receives fees. Related findings link directly to the Steam Dossier’s underlying records.

Cited source records

E09 · Steam Subscriber Agreement

Publisher: Valve

Date: Live agreement

Supports: Valve's licence grant, the absence of ownership interest in marketplace subscriptions, and Steam Wallet restrictions.

Scope: Relevant clauses: §1.C (personal account), §2.A/2.G (licence and commercial use), §3.C/3.D (Wallet and marketplace), §4.D and §9.C (enforcement).

https://store.steampowered.com/agreement/?l=english

E16 · Authentication using Web API Keys

Publisher: Valve / Steamworks

Date: Live documentation

Supports: User-key registration and publisher keys with app associations, permission groups and configurable IP restrictions.

Scope: Sections: User Keys, Publisher Keys and Creating a Publisher Web API Key.

https://partner.steamgames.com/doc/webapi_overview/auth

E04 · WebAPI P2P Solution

Publisher: CSGORoll

Date: 10 Apr 2024

Supports: A dated account of token collection for monitoring trades, including session dependence and expiration.

Scope: Technical record dated 10 April 2024; the subsequent workflow changes appear in E05–E07.

https://www.csgoroll.com/blog/steam-p2p-solution/

E05 · WebAPI Trading Extension

Publisher: CSGORoll

Date: 25 Jun 2024

Supports: The announcement says the extension automatically collects and refreshes the Steam WebAPI token and transmits it to the operator's servers.

Scope: The token collection, refresh and server-transmission workflow announced on 25 June 2024.

https://www.csgoroll.com/blog/csgoroll-trading-extension/

E17 · Decoded JWT fields — redacted transcription

Publisher: Author-supplied notes

Date: Supplied with this investigation

Supports: Declared JWT type, EdDSA algorithm, Steam account subject, web:community audience and supplied timestamp and IP-related field names.

Scope: Field transcription with account and IP identifiers redacted. Signature bytes were not supplied.

https://phishdestroy.io/steam_dossier/case_assets/assets/evidence/jwt-field-excerpt.json

E44 · IEconService — trade history and offer records

Publisher: Valve / Steamworks

Date: Live documentation

Supports: GetTradeHistory, GetTradeOffers and GetTradeOffer as concrete examples of account-economy methods.

Scope: Method reference used to explain what a trading API exposes.

https://partner.steamgames.com/doc/webapi/IEconService

E45 · ISteamUserAuth — publisher ticket authentication

Publisher: Valve / Steamworks

Date: Live documentation

Supports: AuthenticateUserTicket on the publisher host, its publisher key, application ID and ticket parameters.

Scope: A concrete example of the publisher-server access relationship.

https://partner.steamgames.com/doc/webapi/ISteamUserAuth

E43 · Web API Overview — public and publisher hosts

Publisher: Valve / Steamworks

Date: Live documentation

Supports: HTTP method structure, public and authenticated operations, publisher host requirements and access configuration.

Scope: The host and request layer underlying the credential comparison.

https://partner.steamgames.com/doc/webapi_overview

E23 · Steamworks API Overview — native game integration

Publisher: Valve / Steamworks

Date: Live documentation

Supports: The native Steamworks SDK, C++ interfaces, libraries, initialization and game feature integration.

Scope: The game-integration layer contrasted with the HTTP Web API and its account credentials.

https://partner.steamgames.com/doc/sdk/api

E07 · Trade Protection Update

Publisher: CSGORoll

Date: 16 Jul 2025

Supports: Coin-release timing during the seven-day protection window, tier-dependent instant access and consequences for reversals.

Scope: The coin-release mechanism described on 16 July 2025; tiers and limits are adjustable under that policy.

https://www.csgoroll.com/blog/trade-protection-update/

E13 · The Steam Dossier — rules, routes and accountability

Publisher: PhishDestroy

Date: Related investigation

Supports: The parent investigation supplies the historical registration and consent exhibits, transfer-substitution sequence, route register, ownership and recovery records, and correspondence used by this companion investigation.

Scope: The parent PhishDestroy investigation; linked as the wider editorial and infrastructure context.

https://phishdestroy.io/steam_dossier/

E34 · Steam Web API Documentation

Publisher: Valve / Steam Community

Date: Public developer documentation

Supports: Website-developer use of Steam data, user-key registration and the Steam OpenID identity mechanism.

Scope: The public web-service documentation linked to Steam Community account-key registration.

https://steamcommunity.com/dev?l=en

E28 · Release notes — inventory visibility

Publisher: Valve / Counter-Strike

Date: 2 Apr 2024

Supports: Purchased and traded Counter-Strike items made invisible for ten days to other users viewing a Steam inventory.

Scope: Dated official release-note archive, entry for 2 April 2024.

https://store.steampowered.com/news/posts/?appids=730&enddate=1714088148&feed=steam_community_announcements

E06 · New Escrow, Dispute and Penalty Systems for Trades

Publisher: CSGORoll

Date: 01 Oct 2024

Supports: Platform-defined manual completion after ten minutes, disputes, escalating penalties and inventory-based verification; a token-free route was described for certain skins.

Scope: Dated record of the manual verification, dispute and penalty workflow introduced in October 2024.

https://www.csgoroll.com/blog/new-trading-system/

E08 · In-Game Item Trading Update

Publisher: Valve

Date: 13 Jul 2016

Supports: Valve’s account of identity verification and automated trading used by gambling services, its stated prohibition and its denial of business relationships with those sites.

Scope: Valve’s public statement from July 2016, retained here as a historical infrastructure record.

https://store.steampowered.com/oldnews/22883

E11 · RFC 7519 — JSON Web Token

Publisher: IETF / RFC Editor

Date: May 2015

Supports: JWT represents claims in a token format. A service uses its own verification and authorisation rules when accepting the token.

Scope: Technical definition of the JWT format; endpoint permissions are determined by the receiving service.

https://www.rfc-editor.org/rfc/rfc7519

E25 · RFC 8037 — EdDSA in JOSE

Publisher: IETF / RFC Editor

Date: Jan 2017

Supports: The EdDSA algorithm identifier used for signatures in the JOSE framework.

Scope: Section 3.1; relevant to the declared alg value in the supplied header.

https://www.rfc-editor.org/rfc/rfc8037

E24 · RFC 7515 — JSON Web Signature

Publisher: IETF / RFC Editor

Date: May 2015

Supports: Compact signed-token structure, encoded header and payload, signature input and verification.

Scope: Sections 3.1 and 5 describe compact serialization and signing/validation.

https://www.rfc-editor.org/rfc/rfc7515

E33 · Steam Web API Terms of Use

Publisher: Valve

Date: Page marked last updated July 2010

Supports: The established API-key signup framework, applications and websites, confidentiality obligations and Valve's access controls.

Scope: The terms describe the account-key service and the API access relationship.

https://steamcommunity.com/dev/apiterms

E48 · How FloatDB Tracks Skins — the original-ID endpoint and its closure

Publisher: CSFloat engineering

Date: 3 Jul 2020

Supports: The former original-ID field, closure of its endpoint in 2017 and the replacement matching approach using float, seed and paint properties.

Scope: Firsthand technical history of item tracking and its limitations.

https://blog.csfloat.com/how-floatdb-tracks-items/

E38 · People of New York v. Valve Corporation — filed complaint

Publisher: New York Attorney General / NYSCEF

Date: 25 Feb 2026

Supports: Court, filing date, index 450952/2026, allegations, statutory bases and requested remedies.

Scope: NYSCEF document 2; 52-page court-stamped complaint. Requested relief appears on PDF pages 50–51.

https://ag.ny.gov/sites/default/files/court-filings/new-york-v-valve-corporation-complaint-2026.pdf

E41 · Steam Online Conduct — commercial activity

Publisher: Valve

Date: Live rules

Supports: Gambling is explicitly included under the commercial-activity prohibition.

Scope: Read beside the account-enforcement record and Valve's public transferability language.

https://store.steampowered.com/online_conduct/

E14 · About the New York Attorney General lawsuit against Valve

Publisher: Valve

Date: 11 Mar 2026

Supports: The public collectibles comparison, optional and cosmetic framing, transferability argument, account-ban total, privacy objections and legislative position.

Scope: Corporate public response dated 11 March 2026; linked alongside the filed complaint and the investigation's analysis.

https://help.steampowered.com/en/faqs/view/6300-A6C4-519D-A3F5

E19 · October 2016 response to the Washington State Gambling Commission

Publisher: Valve / legal correspondence

Date: October 2016

Supports: Valve's explanation of Steam trading, OpenID, notices to more than forty sites and account-level enforcement.

Scope: Public document copy linked by the Steam Dossier; the letter itself is dated 17 October 2016.

https://fr.scribd.com/document/328063293/Valve-s-Oct-18th-response-to-Washington-State-Gambling-Commission-s-cease-and-desist

E18 · Link Filter — 20-URL observation record

Publisher: PhishDestroy / public Steam responses

Date: 10 Oct 2026 · 19:02–19:03 / 20:27 UTC

Supports: Four ordinary notices with continue anchors and sixteen hard blocks for the exact supplied wrapper URLs, including both CSGORoll hostname variants.

Scope: Unauthenticated HTTPS requests; classification by returned page heading and continue-anchor presence. Exact URLs and timestamps preserved.

https://phishdestroy.io/steam_dossier/case_assets/assets/evidence/linkfilter-2026-10-10.json

E46 · Introducing Big Picture — the built-in web browser

Publisher: Valve

Date: Original product presentation

Supports: Valve's presentation of web browsing within the original Big Picture interface.

Scope: Historical product presentation, used to identify the browser surface discussed in the submitted notes.

https://store.steampowered.com/bigpicture/

E47 · Exploiting Steam: Usual and Unusual Ways in the CEF Framework

Publisher: DARKNAVY

Date: 27 Jun 2024

Supports: Firsthand technical description of steamwebhelper and its Chromium Embedded Framework architecture.

Scope: Documents Steam's embedded Chromium architecture and its exploitation history, dated June 2024. The shipped configuration, patch cadence and present protection of steamwebhelper are part of the record requested from Valve.

https://www.darknavy.org/blog/exploiting_steam_usual_and_unusual_ways_in_the_cef_framework/

E36 · Link Filter — literal-address comparison

Publisher: PhishDestroy / public Steam responses

Date: 10 Oct 2026 · 19:09–19:10 UTC

Supports: Returned headings and continue anchors for five literal csgofast-related address probes.

Scope: Exact request strings and responses are preserved, including separate percent-encoded request results.

https://phishdestroy.io/steam_dossier/case_assets/assets/evidence/linkfilter-pattern-2026-10-10.json

EDITION NOTES / TRACEABLE FILES

Read the claim. Check its source.

This reading edition was prepared on 18 October 2026 from the current English article. It retains the authored discussion and analytical tables in the source HTML. Navigation and interactive controls are removed. Interactive datasets remain linked rather than expanded into thousands of printed rows.

Selected source images remain linked to their publications or retained copies. The PDF does not independently authenticate the participants in a screenshot, verify every report in a collection, or determine the merits of a legal allegation.

Check this edition

The detached OpenPGP signature covers the exact bytes of the article JSON. That JSON includes the exported text, source identity and SHA-256 of this PDF. It is not a PDF document signature, and it does not certify the truth of underlying third-party material.

Article JSON · OpenPGP signature · JSON SHA-256
Published verification key · Verification instructions

```
Signing-key fingerprint
129FC7F39C40C69D2EF3C329BFCF9E8DD295EE01

Source HTML SHA-256
6d73894b2123fc2bc39dc7e3ae8fcf413c8e2d9c7b57f7ce1b12c53604fc789c
```

Reuse and attribution

Authored research is released under CC0 1.0 Universal. Third-party statements, screenshots and other source material retain their own rights and attribution. The original rights statement is a separate signed object.

```
Build 2026-10-18T12:03:18.956Z
Source: https://phishdestroy.io/steam_dossier/steam-access
```