账户访问与问责——《Steam档案》

来源: https://phishdestroy.io/steam_dossier/zh/investigation_part2
CC0 1.0 Universal · 2026-09-30

《STEAM档案》/ II

您的账户。他们的访问权限。*谁接电话？*

公共自动化。外包支持。最终承担代价的还是民众。

追踪基础设施状况、已报告的损失以及索赔背后的文件。

追踪基础设施↘
附件 01 / 实时暗网市场监控**550,000+**
Steam 个账号正在 FSB Market (匿名名称；此处不公开原名) 上积极出售
就在这一刻

550,000+ 实时库存 · 231,829 历史抓取语料库（198,320 窃取日志）
被劫持的 Steam 账户的主要地下交易平台，FSB Market (其他相关名称不予公开) 使用 Valve 的官方 Steam OpenID 对买卖双方进行身份验证（openid.realm = https://FSB Market). 每分钟都有超过50万个被盗和遭泄露的账户（来自RedLine/Lumma的窃取日志、钓鱼攻击截获数据、凭证填充数据）以几美分的低价（$0.50–$2.00）被积极挂牌出售。两者均未FSB Market nor相关论坛 被 Valve 的链接过滤器拦截。这是为 63.06% 个付费机器人账户提供支持的“人才库”，而 Valve 在未向受害者提供任何帮助的情况下将其封禁。

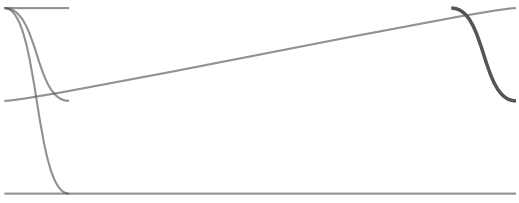
实时情报：暗网市场监控（55万+在线用户）↗ ·打开捕获记录 ↗ ·打开链接过滤器跟踪记录 ↗55万+ 在线

01 / 一个由作者构成的生态系统

自动化已经*书面记录。*

已命名的项目。已发布的功能。追溯工具至其文档，然后检查收集到的开发者关联关系。

252已收录的仓库
3,320GITHUB 个人主页
4,214简介——配置文件与存储库配对
Valve 基础设施 社区图书馆 可重用应用程序



线条表示已记录的集成或依赖关系。选择一个节点以查看其相关信息。

多账户自动化 / JustArchiNET

ArchiSteamFarm

该项目明确宣传可在Steam账户间同时刷卡。其项目文件声明了SteamKit2依赖项。

阅读该项目的官方文档 ↗

SteamKit → ArchiSteamFarm
已声明的依赖项 ↗

《关系集》

40 贡献者标签 · **40** forker标签

以下是贡献者示例。这些标签描述的是代码库之间的关系，而非雇佣关系或审批关系。

@JustArchi @renovate[bot] @JustArchi-ArchiBot @dependabot-preview[bot] (unavailable) @renovate-bot @actions-user @dependabot-support @Abrynos

开发者图所揭示的内容
该图表展示了已公开的贡献者与分支者之间，在指定项目与 GitHub 个人资料之间的关联关系。这些都是公开记录——仓库分支、贡献列表、个人资料关联。关键在于，已公开的能力和开发者关系所留下的这些“纸质痕迹”要求 Valve 回答什么问题，而不是这项调查杜撰了什么。源代码哈希值保存在地图来源.

探索整个网络 ↗ 存储库源数据 ↓

02 / 不同的凭证，不同的权限。

哪个键*我们说的是什么？*

玩游戏并不要求玩家提供个人 Web API 密钥。这正是本调查的核心区别所在。

01 / 用户账户

个人 Web API 密钥

`steamcommunity.com/dev/apikey`
由用户账户签发，用于允许的 API 调用。密钥的创建、可见性、撤销和滥用检测均属于账户安全问题。

02 / 游戏后端

发布商 Web API 密钥

Steamworks 合作伙伴使用发行商凭据来执行受支持的后台操作，包括与游戏相关的服务。玩家的个人密钥则是另一种凭据。

03 / 身份与会话

OpenID / 会话令牌

OpenID 用于向网站验证身份。而 Steam 会话令牌或刷新令牌则具有不同的用途。不应将这些机制混为一谈，视作一个可互换的“API 密钥”。

What this means — OpenID and openid.realm
OpenID is the sign-in standard behind the “Sign in with Steam” button: the site does not receive the password, Steam confirms the identity to it. **openid.realm** is the field carrying the address of the site asking for the sign-in, and **openid.return_to** the address Steam is to send the user back to. Steam receives both on every request and prints the realm on its own login page — which is why this dossier can name the host each platform authenticates through.

Section 3 — the observed routes →

Valve 同时记录了用户和发布商的 Web API 密钥。因此，整个 Web API 并非独立于 Steamworks 之外。
API 密钥文档 ↗ 已归档 2026-09-15 ↗ ·游戏会话认证 ↗ 已归档 2026-08-29 ↗

由该工具作者记录 / 2024年3月

自动化不仅可以使用 API 密钥。

Trade Offer Manager 的维基文档描述了在没有单独 API 密钥的情况下，如何在 Web API 的部分功能中使用会话访问令牌。该文档还记录了自 2023 年末起，创建 API 密钥时需要进行手机验证。维护者指出，Valve 不支持此类令牌用法；这只是文档中过时的说法，并非针对当前环境的绕过测试。

查看维护者的说明 ↗ 已归档 2026-09-24 ↗

人性层面 / 一个具有说明性的网络钓鱼路径

还在玩。*已经曝光了。*

来自朋友的一条消息。一个投票请求。一个“感谢”页面。对玩家而言，任务已经完成。但被入侵的会话可能比这一刻持续得更久。

在播放器屏幕上

F
一位朋友的叙述
“你能给我们的团队投一票吗？”

该请求通过Steam聊天功能从一个熟悉的账号发来。在此情况下，链接的页面会在客户端的浏览器中打开。

《看不见》

信任的建立早于网站的建立。

被劫持的朋友账户可能会让钓鱼链接显得更具可信度。周围的 Steam 界面并不能证明目标网站的安全性。

已知发件人 / 外部收件人

在出售任何商品之前，账户安全是首要考虑的问题。
该玩家并非有意创建自动化凭证或授权他人控制。重新登录游戏并不能证明该账户是安全的。Valve 保存着会话日志、API 密钥创建记录以及设备关联数据，而受害者则没有。这种信息不对称正是问责问题所在。

会话访问和凭据类型
API 密钥和登录会话是两种具有不同权限的凭据。撤销密钥不会终止当前的活动会话。Valve 的官方文档中对这两者均有说明；Valve 保存着日志，这些日志可显示在任何存在争议的操作发生时，究竟是哪一种凭据处于活动状态。 要求的是披露该记录——而非调查方凭空推断出的结论。维护者关于令牌处理的文档 ↗ 已归档 2026-09-24 ↗ ·Valve 关键文档 ↗ 已归档 2026-09-15 ↗

03 / 正规市场存在价格上限

该物品可能是稀有物品。*限制依然存在。*

如果报价超过挂牌上限，则无法通过在社区市场进行一次全价挂牌来实现该价格。

参考要价$5,000更改商品的标价
$100 $20,000
此为已公布的限额示意图，并非估值或交易建议。simplified-chinese

上市上限 ≈ **$1,800**
钱包帽 ≈ **$2,000**
超过已公布的挂牌上限。

钱包中的资金无法提现至银行账户。这些限制催生了第三方皮肤市场所满足的需求：这种需求由上架限制和钱包额度限制所产生，而Valve自身的规则却禁止商业运营商满足这一需求。

Steam的市场限额 ↗ 已归档 2026-09-21 ↗

04 / 支持边界内部

受托管理数据。*负责访问管理。*

Valve的隐私政策明确规定，在提供支持所必需的情况下，可与第三方支持服务提供商共享个人数据。

《玩家》 **账目与凭证**
→
VALVE **恢复过程**
→
支持提供商 **委托访问**
隐私政策 §5.2 ↗ · Valve的内部政策允许第三方支持人员进行访问。目前尚待澄清的问题包括：授予了哪些权限、存在哪些审计记录，以及在据称发生访问权限滥用时发生了什么。

2015

该秤是公开的

Valve 承认了账户被盗现象普遍存在，并介绍了相应的防护措施。

Valve 出版物 ↗ 已归档 2026-08-09 ↗

2015

Valve 将该岗位外包了——并且也这么说了

Valve 设有一个小型内部 Steam 支持领导团队，并表示*“雇了几家不同的公司”* 以处理支持服务（Erik Johnson、Valve，向Kotaku）；其隐私政策第5.2条授权这些第三方访问用户数据。**哪家承包商拥有账户恢复权限，Valve从未透露过** — 社区讨论中提到了Concentrix等供应商，但均未得到Valve确认。该外包服务台早在以下两则声明发布之前数年就已经设立。

Kotaku：Valve 对其支持 ↗ 已归档 2025-07-11 ↗

2023

第一次入学

Valve的《CS:GO》战队就其帮助请求流程导致账号被盗一事以书面形式承担责任，并撤销了相关交易。

打开外包案例 ↓

2025

第二次入学

33个月后，Steam 客服回复称，一名技术人员“未按我们的流程操作，导致您的账户被恢复给了其他人”。同样的渠道。同样的结果。

Dexerto，2025年11月14日 ↗

案件档案 / HFB 与外包指控

进入的方式正是Steam支持本身。*Valve 以书面形式表示了这一点。*

在Dexerto转载的客服回复中，Valve的CS:GO战队承认其账号遭入侵一事应由该队负责**通过求助流程** — 这是其自有渠道，既非钓鱼页面，也非用户所为。相关资产已被追回，交易已撤销，而这正是Valve告诉其他受害者根本不存在的补救措施。据报道，HFB的库存为**$2,000,000+** 当天以及**$3,000,000+** 在后续工作中；**Qkss 也以同样的方式输掉了 $1,000,000+，一无所获**.

支持回复 / 转载自 DEXERTO · 2023年2月21日

> “因一则技术支持请求而遭到入侵，CS:GO团队对此承担责任”

阅读报道及转载的消息 ↗ 已归档 2025-08-18 ↗
01 / 哪个阀门开了

其自有支持渠道便是切入点

该回复涉及被入侵的账户及其交易的撤销。Valve已撤销这些交易——因此这些交易是可以撤销的。原始的经过认证的交易单不在此集合中。

02 / 解雇未能解决的问题

2025年11月，那扇门再次敞开了

该承包商解雇了其全部 Steam 名支持人员——此消息由 Mzkshow 通过 Dexerto 报道，并非来自 Valve 的人事声明。 三十三个月后，Steam Support 致信另一位用户称：“处理该求助请求的技术支持人员未遵循我们的流程，导致您的账户被恢复给他人。”这是 Valve 本人关于同一渠道的陈述。

第二次入学，2025年11月14日 ↗
03 / 什么是“开放”

Valve从未透露过该承包商的名称

这些消息来源既未指明承包商，也未指明具体地点。这并非报道中的漏洞——而是Valve尚未披露谁拥有用户账户的访问权限。

该案的当代记载 ↗
有三个问题Valve尚未回答：谁可以绕过账户恢复机制、访问审计发现了什么，以及此后发生了什么变化。

保存下来的支持档案中后来的指控
2024年Reddit上的两篇帖子披露了Mzkshow的进一步调查——一起发生于2024年7月的VAC禁令撤销案例和一起发生于2024年12月的$13,000库存案例。这些是分别报告的事件。 每起事件中的问责问题都是一样的：谁拥有覆盖权限，审计发现了什么，以及发生了哪些变化。

2024年7月14日 · 报告已康复 / VAC-禁令案例 ↗ 2024年12月2日 · 报告了 $13,000 库存案例 ↗ 已归档 2025-08-05 ↗ 两条已保存的帖子、来源行和哈希值 ↓

05 / 追随损失

每个金额*需要一个保护套。*

10起案例，时间跨度为2022年6月至2026年3月。每个金额均采用其所引用的来源公布的数值——**$6,300,000**,**$2,000,000+**,**$1,000,000+**,**≈$320,000**,**≈$300,000**，降至288欧元。Valve保存着每笔交易的交易日志、会话记录和支持审计轨迹，但均未提供任何相关记录。

支持渠道 21 6月2022
$2,000,000+

HFB — the largest inventory in the game

报告的库存估值 · 在2月2023后续报道中上调至3百万美元以上

七件“龙之传说”纪念品和#1蓝宝石卡兰比特刀，仅那把刀的价格就约为1.26。账户已闲置三年，认证标识仍未移除；已通过客服账户恢复渠道更改了邮箱和密码。Valve撤销了交易——并以书面形式承担了责任。 在撤销交易之前，据报告已有200,000+的交易收益通过market.csgo.com提现，该平台支持现金和加密货币结算。撤销交易仅退还皮肤，不会返还用户已存入账户的资金。 此次回滚还引发了其他问题：一名买家将他的“纪念版龙之传说”藏在游戏内的储物箱中，脚本无法查看该容器内部；Valve在撤销一起盗窃时，将一件价值$130,000的物品复制了一份——这一问题通过物品ID和社区举报被发现，该物品已于7月被删除2022，，买家的退款由BUFF而非Valve处理。

Dexerto，失窃当天 ↗

钱包与购买 07 7月2022
>$500

44 disputed Market purchases

申报的钱包消费额 · 美元

有用户反映，其账户遭人擅自购买了低价值的《Dota》2游戏道具，且客服的回应令人不满。

阅读投诉内容及相关截图 ↗

平台安全漏洞 14 8月2022
$6,300,000

CS.Money — 19,000+ 机器人生成的皮肤

估值 · 初步估价1.6百万美元

攻击者窃取了该交易平台交易机器人的手机验证器文件并清空了其中的内容，还将部分赃款转给知名交易员以混淆视听。 社区研究人员在数小时内就追踪到了55上的攻击者账户。Valve并未进行任何反向追踪——据Steam透露，该第三方网站位于Steam之外，而该平台的库存、交易API及账户系统全程参与了此次盗窃。

阅读当代记载 ↗

支持渠道 报道来源：21 2月2023
$1,000,000+

Qkss——同一扇门，同一位演员，截然不同的答案

报告的存货估值

以HFB案为参照——由同一位当事人通过相同的客服求助请求提出——HFB案已在八个月前得到了全额赔偿，而Qkss案则未获全额赔偿。在已公开的记录中，除受众规模外，这两起案件并无任何区别。

Dexerto关于Mzkshow调查的报道 ↗

支持渠道 报道于2月2023
≈ $320,000

内幕交易本身——持续了一年

约一年内的营业收入 · 非存货估值

技术支持团队查阅到了长达15年的账户历史记录：第一个CD密钥、第一封电子邮件、第一张信用卡——这些正是账户恢复流程所要求的证据。 无论谁掌握数据库，在与账户持有者的争执中总是占据上风。一把被盗的 M4A4 Howl（附带 iBUYPOWER 和 Titan Katowice 2014 全息贴纸），以 $35,000 的价格售出，最终落入 NAVI 战队的 b1t 手中，而他对此毫不知情。承包商的应对之策是解雇所有在 Steam 客服部门工作的员工。

Escorenews关于同一项调查的报道 ↗

钱包与购买 09 DEC 2023
€288

尽管采用了两步验证保护，钱包仍遭丢失

TRUSTPILOT · 来源索引 16

该评论者反映其账户遭到黑客入侵，且对方拒绝协助处理Market消费问题。该导出文件中未包含单独的评论链接。

检查来源出处 ↗

账户恢复 02 DEC 2024
$13,000

《马特维》——解雇事件两年后

作者的存货估算

向某人授予了账户恢复权限，因为该人提供了账户所有者本人无法匹配的账户数据。在承包商清空其 Steam 支持服务台后，采取了同样的流程，结果也一样。

阅读已存档的指控 ↗

账户恢复 09 MAY 2025
≈ $10,000

通过他人的车票进行补票

索赔物品丢失 · 美元

一位魁北克用户称，客服应他人要求重置了密码并取消了账户保护。

阅读这篇第一人称投诉 ↗

支持渠道 13 11月2025
≈ $300,000

Hawkeye337 —— 以及Valve的第二份书面供词

卡托维兹2014全套全息图集

攻击者索要1比特币，并开始将该收藏品刮取到Negevs上以销毁它。Steam 客服回复：“处理该求助请求的一名技术支持人员未遵循我们的流程，导致您的账户被恢复给了其他人。” 自首次承认问题以来已过去三十三个月，情况依然如故。该帖子在X上成为热门话题后数小时内，账户便被恢复。Qkss则没有那么大的受众群体。

Dexerto, 14 Nov 2025 ↗

钱包与购买 29 MAR 2026
$50

未经授权的充值和赠送游戏

TRUSTPILOT · 来源索引 290

该评论者指控存在未经授权的消费以及退款申请未获批准的情况。导出文件中缺少该条评论的具体链接。

检查来源出处 ↗

来源及金额均按各来源的报告为准。Valve 保存了所有这些案例的交易日志、会话记录和支持审计轨迹。请提供这些资料。一篇被保留下来的 Reddit 帖子无法解决这个问题——Valve 自身的记录才能解决。

“系列” / “核对后”

231,829个账号正在出售。*Valve 保存了每个的日志。*

354 → 201

Trustpilot 记录

已删除 153 行重复记录。导出文件中未保留单个评论的 URL。

231,829

Steam 账户列表

33,509 归类为“自行登记”；198,320 归类为“收藏家盗窃品”。列表中的商品并不代表已成交。

应收账款审计 ↓ 搜索源代码存档 ↗