THREAT INTELLIGENCE REPORT

Profit Over Players: The BlockBlasters Cover-Up (Steam Scandals, Part 1)

Ref. **PD-TI-2026-95378** Published **10 July 2026** Source **phishdestroy.io/steam-not-good-guy**

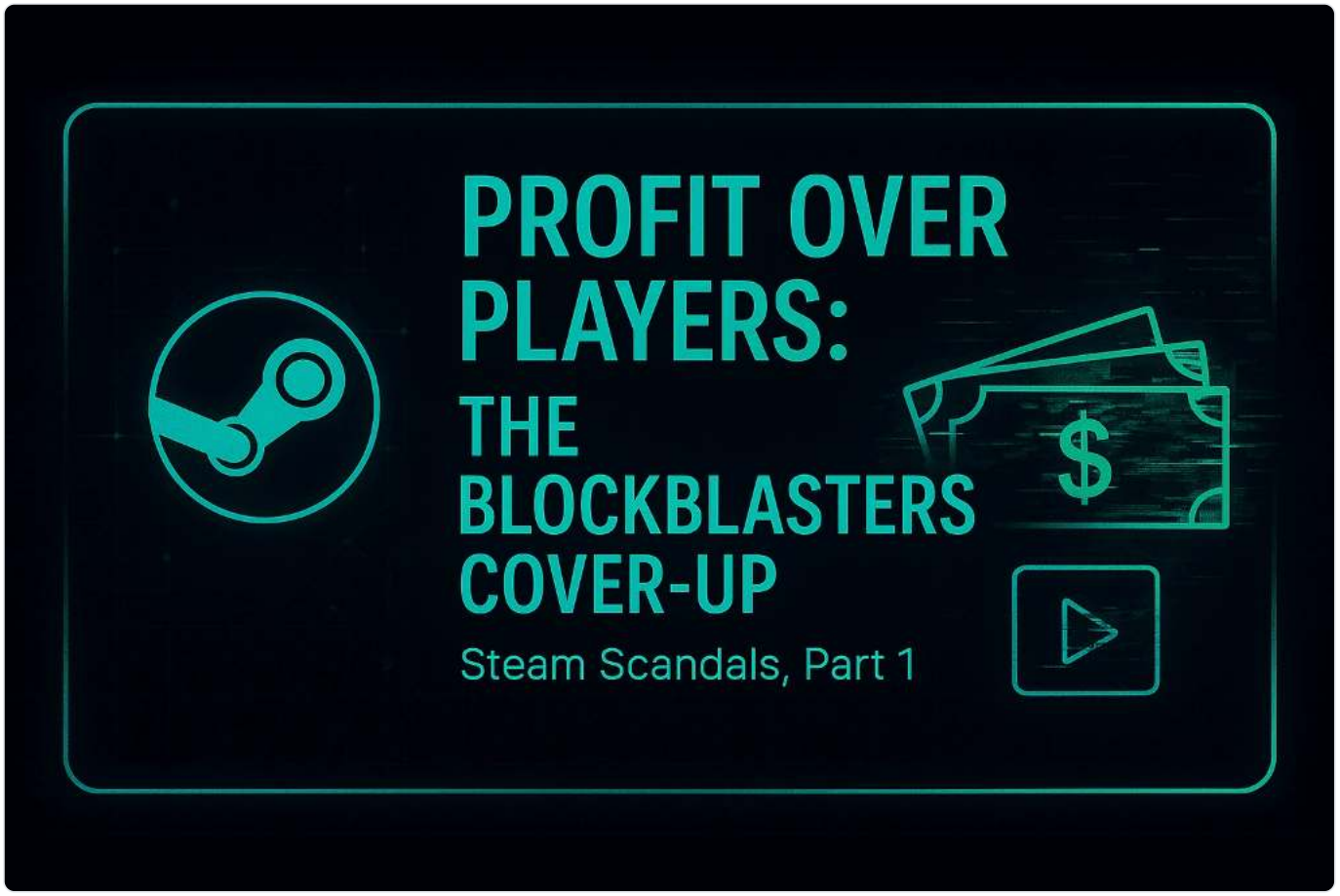
Investigation Corruption

We are launching a multi-part investigation uncovering the hidden truth about Steam revealing the corruption behind its operations, the systemic abuse, exploitation, and negligence that have harmed millions of users, and exposing how a global monopoly turned a gaming platform into a machine of manipulation and silent profit.

10 min read · Updated **March 2026** · PhishDestroy Intelligence

PhishDestroy Team

Investigation Report



Critical Finding

Steam blatantly lies, covers up for criminals, and obstructs the investigation.

Introduction: A Crime of Calculated Negligence

In August 2025, the world's largest gaming platform, Steam, didn't just suffer a security breach; it actively enabled one. Through a cascade of systemic failures and gross negligence, Valve allowed the game **BlockBlasters** (AppID 3872350) to become a Trojan horse for a devastating malware campaign. This wasn't a sophisticated, unavoidable attack. It was a textbook data-stealing operation that succeeded because Steam's security is fundamentally broken. For 22 days, it stole hundreds of thousands of dollars, emptied crypto wallets, and compromised user accounts while Valve did nothing.

When the truth surfaced, Valve's response was not to protect its users, but to protect its image. The company issued a single, deceitful statement blaming a "compromised developer account" a pathetic lie designed to shift blame and shield itself from liability. This article will dismantle that lie. Using forensic data, timeline analysis, and Valve's own policies, we will prove that this incident was not just a failure to act, but a deliberate cover-up of criminal negligence.

Corporate negligence timeline: Day 1 malware published, Day 3 first reports, Day 3 multiple flags, Day 10 zero action with 1,489,500 victims exposed, Day 22 finally removed

Exposed Identity

Steam blatantly lies and hides Valentin Lopes the verified developer behind the malicious application.

The 22-Day Timeline of Inaction

Valve had 22 days to stop this. User reports were flowing in, and platform data showed clear signs of trouble. Their silence was a choice.

July 31, 2025
BlockBlasters launches. A clean, legitimate build is approved by Steam's vetting process.

August 30, 2025
The trap is set. The attackers push Patch Build 19799326. This update, containing the malware payload, is approved by Steam and distributed to all players.

Early September 2025
The first victims sound the alarm. Users flood Steam Support with tickets reporting anomalous CPU usage, suspicious network traffic, and most critically stolen cryptocurrency. These tickets enter a black hole, ignored by Valve.

September 612, 2025
The data screams a warning. Public SteamDB telemetry shows the player count collapsing to single digits, yet the game remains installed on hundreds of machines, silently exfiltrating data. This massive discrepancy is a red flag that any competent monitoring system should have caught.

September 21, 2025
The community acts. Independent security researchers expose the malware's Telegram-based command-and-control infrastructure, forcing the hackers' hand.

September 22, 2025
The proof is undeniable. G DATA CyberDefense AG publishes a full forensic report, confirming the malware's multi-stage attack vector and exposing the technical details of the breach.

The Anatomy of the Attack

This wasn't cutting-edge malware. It was a crude but effective cocktail of common scripts and stealers that should have been trivial for a multi-billion dollar platform to detect.

Stage 1: Initial Compromise (game2.bat)

The initial payload, a simple batch script, performed basic reconnaissance: collecting IP, geolocation, and Steam user details. It then downloaded a password-protected ZIP file (v1.zip)a classic technique to bypass naive automated scanners.

Stage 2: Evasion and Escalation (VBS Loaders)

Using VBS scripts, the malware executed its core components in hidden command windows. It added its own directory to the Microsoft Defender exclusion list an action that should trigger an immediate, high-priority alert on any monitored system.

Stage 3: Data Theft (Client-built2.exe & Block1.exe)

With defenses disabled, the malware deployed its primary payloads: a Python-based backdoor for persistent access and a variant of the StealC infostealer. It targeted browser data, session tokens, and, most importantly, cryptocurrency wallets from Chrome, Edge, and Brave. All stolen data was funneled to two command-and-control servers in unsecured HTTP traffic. The crypto drainer IOCs confirmed Steam as a malware distribution vector for organized theft operations.

Trust Betrayed

It was precisely their trusted certificate and disregard that led to dozens of thefts that they cover up. This represents a textbook supply chain attack exploiting platform trust exploitation at scale.

Indicators of Compromise (IoCs)

File	SHA256	Classification
`game2.bat`	`aa1a1328e0d0042d071bca13ff9a13116d8f3cf77e6e9769293e2b144c9b73b3`	BAT.Trojan-Stealer.StimBlaster.F
`launch1.vbs`	`c3404f768f436924e954e48d35c27a9d44c02b7a346096929a1b26a1693b20b3`	Script.Malware.BatchRunner.A@ioc
`test.vbs`	`b2f84d595e8abf3b7aa744c737cacc2cc34c9afd6e7167e55369161bc5372a9b`	Script.Malware.BatchRunner.A@ioc
`Client-built2.exe`	`17c3d4c216b2cde74b143bfc2f0c73279f2a007f627e3a764036baf272b4971a`	Win64.Backdoor.StimBlaster.L6WGC3
`Block1.exe`	`59f80ca5386ed29eda3efb01a92fa31fb7b73168e84456ac06f88fdb4cd82e9e`	Win32.Trojan-Stealer.StealC.RSZPXF

Deconstructing the Lie: The "Hacked Account" Is Complete Bullshit

Cover-Up Exposed

Steam lies and helps victims, while their company checks developers and gives the highest certificate of trust to their content.

Let's call Valve's "hacked developer" excuse what it is: **a pathetic and easily disproven lie.** It's an insult to the intelligence of their user base, a narrative crafted to shield them from the consequences of their own negligence. This entire fantasy collapses the moment you look at Steam's own mandatory procedures.

- **The $100 Wall and Identity Verification:** To publish on Steam, every developer must go through the Steam Direct program. This involves paying a $100 fee and completing a Know Your Customer (KYC) process, providing legal names, banking information, and tax documents. The perpetrator was not an anonymous ghost; Valve had their verified identity and financial details on file. This makes their inaction a conscious choice to protect a verified partner over their own users.
- **The 22-Day Blackout Myth:** Steamworks provides developers with robust tools to secure their accounts. A legitimate developer who lost control could file a "lost access to publisher credentials" ticket. This process is designed to be fast, freezing publishing rights and builds within hours, not weeks. The idea that a developer could be locked out for over 20 days while their game distributes malware is absurd. It implies one of two scenarios, both of which indict Valve: either the developer was complicit, or Valve ignored their frantic support tickets in addition to the dozens of user complaints.

- **Systematic Neglect of User Complaints:** Dozens of users filed detailed reports of financial theft, malware behavior, and account compromise. These weren't vague complaints; they were actionable intelligence. A competent support system would have flagged these, escalated the issue, and frozen the app page pending investigation within 24 hours. Valve's failure to do so for 22 days is not an oversight; it's a policy of willful ignorance.

The Core Deception: Tampering with a Digital Crime Scene

This is where Valve's cover-up graduates from simple negligence to what can only be described as **tampering with a digital crime scene.** Let this be stated without ambiguity: Valve did not remove the infected game.

Forensic evidence and analysis from security researchers tracking the C2 infrastructure confirm it unequivocally: the criminals themselves deleted their malicious builds from Steam's servers. They did this on September 21st, only after their Telegram control group was publicly exposed. They executed a "scorched earth" exit, destroying the evidence to cover their tracks.

Tampering with a digital crime scene - Steam/Valve hand reaching past do not cross tape while PhishDestroy investigates with magnifying glass

Valve's claim of taking action is a blatant fabrication. By waiting for the attackers to erase their own tracks before stepping in to remove the store page, Valve effectively allowed the primary evidence to be destroyed. This wasn't damage control; it was obstruction. They weren't protecting users; they were protecting themselves by ensuring the crime scene was clean.

The Human Cost of Corporate Indifference

Valve's negligence had real-world consequences for which it has taken zero responsibility.

- **Financial Ruin:** Over $150,000 USD was stolen (looks like more than $1,000,000 USD). For many, this was life-altering money. One streamer lost $32,000 during a live charity broadcast for cancer treatment.
- **Betrayal of Trust:** Hundreds of users had their accounts compromised, their data stolen, and their systems infected.
- **Absolute Silence:** To this day, Valve has offered no refunds, no compensation, and no genuine apology. Their form-letter response was an insult to every victim.

The Motive: Profit Over People

Why would Valve allow this to happen? The motive is as simple as it is cynical: **it was cheaper.**

A real security overhaul implementing sandboxed testing for all builds, separating developer credentials, hiring a competent security team, and publishing transparency reports would cost millions. Paying restitution to victims would set a costly precedent.

The alternative? Issue a vague, misleading statement, let the news cycle move on, and absorb the minimal PR hit. It was a calculated business decision where user safety was deemed an acceptable loss.

This pattern of negligence is not new. From PirateFi (2024) to Chemia (2025), Valve has repeatedly ignored warnings and allowed malware onto its platform, only acting after public outcry. BlockBlasters was not an anomaly; it was the inevitable result of a rotten security culture.

Final Verdict: Guilty as Charged

Let the facts speak for themselves.

- **Fact:** Valve's automated systems approved a build containing trivial malware.
- **Fact:** Valve's support team ignored direct warnings from victims for three weeks.
- **Fact:** Valve only acted after the hackers themselves removed the malicious files.
- **Fact:** Valve's official statement was a deliberate misrepresentation of events designed to avoid accountability.

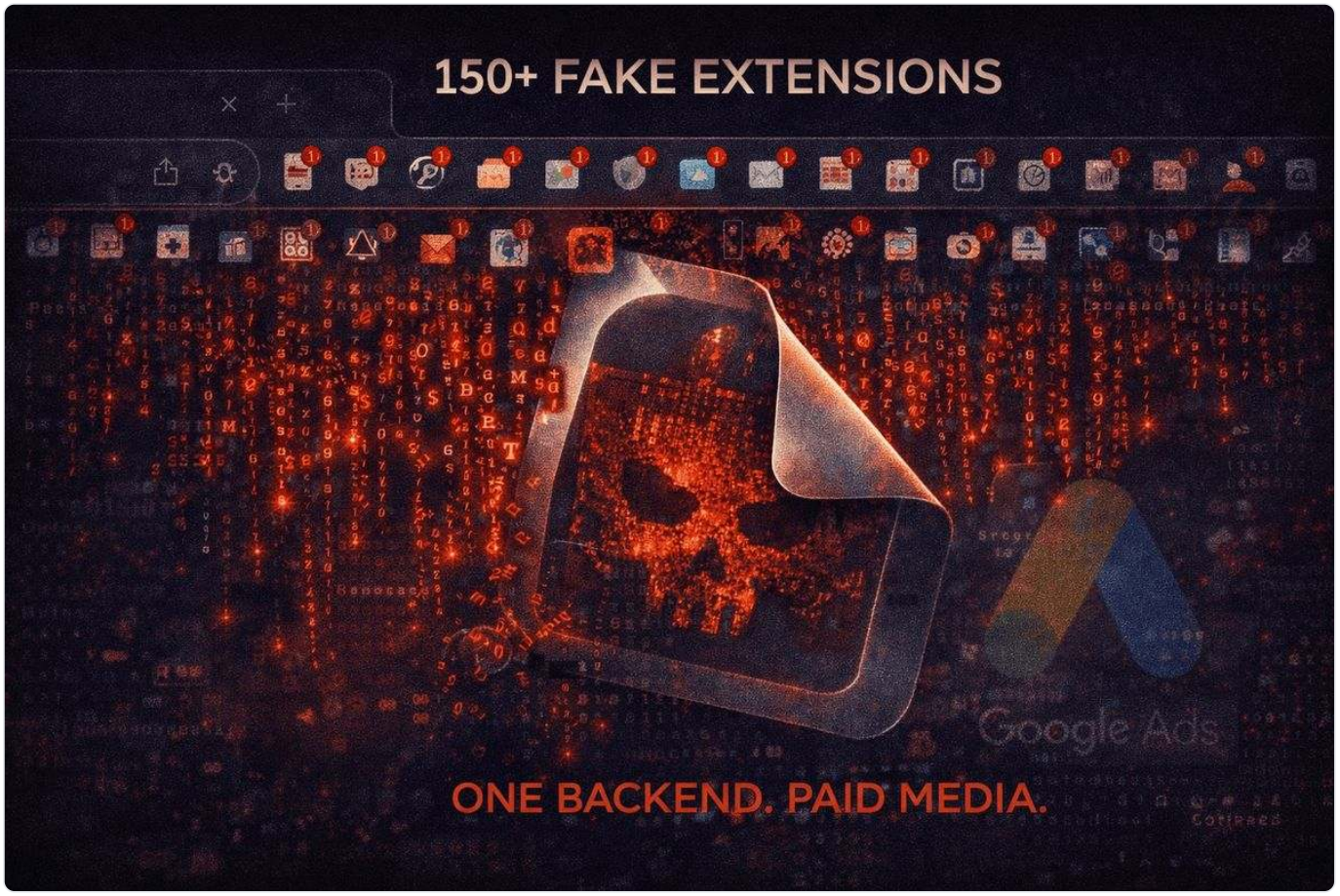
Valve didn't just fail. It lied. It covered up its own negligence, protected its profits, and left its users to pay the price. The trust that the community placed in Steam has been irrevocably broken. This wasn't a mistake; it was a betrayal.

Sources

- G DATA CyberDefense AG (Sept 22, 2025)
- SteamDB - BlockBlasters
- Gamalytic
- GamesRadar - Steam malware report
- The Verge - BlockBlasters malware coverage
- Tom's Hardware - Steam malware analysis
- Community incident logs

#Steam #Valve #CryptoDrainer #Malware #GamingSecurity

Related Investigations

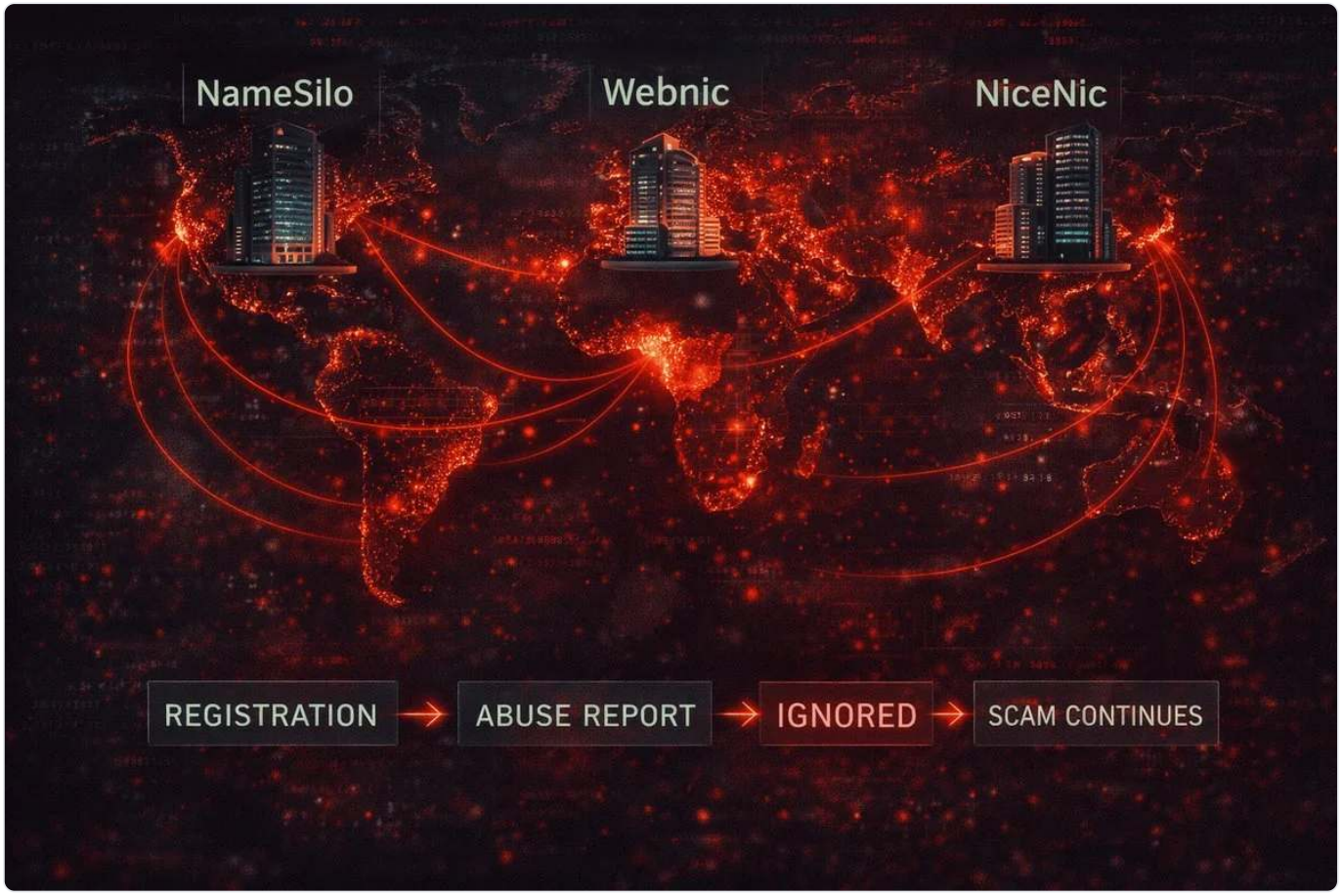


INVESTIGATION

150+ Fake Mozilla Extensions: One Backend, One Network

INVESTIGATION

$0 Takedowns: How We Disrupt Phishing Infrastructure



INVESTIGATION

NameSilo, Webnic, NiceNic: Registrars Enabling Scams