THREAT INTELLIGENCE REPORT

$0 Takedowns, Priceless Tantrums

Ref. **PD-TI-2026-34337** Published **10 July 2026** Source **phishdestroy.io/enemy-one**

Ongoing Intelligence Report

Since 2019, we've removed thousands of phishing domains at zero cost. Scammers retaliated with DDoS attacks, fake companies, mass reports, and forged legal documents. None of it worked. Here's the evidence.

Published May 20, 2025 Updated April 2026 9 min read PhishDestroy Intelligence

$0 Cost per takedown
10+ Attack types
5+ yrs Active since
0 Downtime days
100% Failure rate

How We Operate

Our model is intentionally boring. We scan for phishing infrastructure, archive evidence, file structured abuse reports, and remove domains. No PR wars, no ego plays. Just automation and email.

Detect
Automated crawling + community submissions via Telegram bot. 839K+ domains in our threat database.
Archive
Snapshot sites on Web Archive + local forensic copies before takedown. Evidence preservation is paramount.
Report
One structured SMTP email per domain with everything a registrar/host needs. Automated pipeline. $0 cost.
Key principle
No doxx by default. We focus on infrastructure, not individuals. When threat actors cross legal lines (threats, fraud, identity theft), we escalate to law enforcement with full evidence packages. Otherwise, we just turn off their domains.

What Scammers Tried (and Why It Failed)

Over the years, threat actors have thrown everything they could think of at us. Here's a comprehensive breakdown of every tactic, and why each one was a waste of their money.

Attack	Method	Their Cost	Our Impact	Status
Email floods	2,000-5,000 msgs/day for months	$50-300/mo	Zero	Failed
UK shell company	Paper company + forged "ownership" docs	$500-2,000	Zero	Failed
Social takedowns	Mass-reporting X, Telegram, Medium	$100-500	Accounts suspended, archives live	Nuisance
DDoS attacks	Rented botnets against our lander	$200-2,000	Zero	Failed
Bot farms	Fake followers/likes/reports	$50-300	Zero	Failed
False abuse reports	Fake complaints to our hosting provider	Time	Zero	Failed
Content swapping	Inject illegal content to trigger auto-bans	Time	Zero	Failed
Impersonation	Fake "Russian hacker" forums selling our work	Time	Zero	Failed
DDoS → host kill	283M requests / 1.21 TB — Namecheap dropped us	$2,000+	Migrated to Cloudflare + Hetzner	Nuisance
Fake DMCA	Forged OnlyFans copyright claim to Google	Time	Zero — OnlyFans denied filing	Failed

Attack	Method	Their Cost	Our Impact	Status
Trust user infiltration	Trusted user injected 46 false-positive domains	Time	Caught fast, hardened all roles	Failed
Appeals form spam	9,000+ fake domain appeals via hCaptcha solving	$100-500	Zero — trivially filtered	Failed
Email bombing (ongoing)	400,000+ messages, non-stop, auto-deleted	$500+/mo	Zero	Failed
X/Twitter ban (again)	Gov-style emergency request → account suspended	$3,000+	Not restoring. Done with X.	Nuisance
Reddit ban	Account banned. 1 post from 5 years ago.	Time	Zero	Failed

The economics are simple
They spend $3,000+ per "government-style" social takedown. We spend $0 per domain removal. Our takedown pipeline is email-based automation — the website is optional. DDoS attacks against a lander are like bombing a billboard: the mail trucks keep moving.

Attack Timeline

2019 — Origin
"You don't even have a website!"
Scammers mocked us in a registrar complaint. We built one in 15 minutes. The joke stuck. The takedowns scaled.
2020-2022 — Email Floods
2,000-5,000 messages per day
Bulk inbox bombing sustained over months. We don't rely on inbound email for operations. No impact whatsoever.
2023 — UK Shell Company
Paper company + forged ownership docs
Created a UK-registered company and forged "domain ownership" documents to claim our domain. Domain registered to a private individual — corporate claims fail by design.
2024 — DDoS Campaign
Botnet rental against our lander
Rented botnets to "drop" us. Behind Cloudflare. Email flows continued. Takedowns unaffected. Expensive lesson for them.
Sept 2025 — Telegram Takedown
Mass-reported our Telegram channel
Successfully mass-reported our channel where domains were published for automated banning. We launched a new channel immediately.
2025-2026 — Ongoing
Operations scaled, infrastructure hardened
Automated detection and reporting pipeline expanded. New countermeasures deployed against active phishing infrastructure. Details classified.
March 6, 2026 — DDoS Nuclear Option

283M requests, 1.21 TB — Namecheap dropped us

Massive DDoS attack: 283 million requests and 1.21 TB of bandwidth in 7 days. Namecheap hosting couldn't handle it and terminated our account. We migrated to Cloudflare + Hetzner (from $8/mo to $25/mo). After migration, they tried again — and predictably face-planted. Cloudflare absorbed everything. Zero downtime.

March 30, 2026 — Fake DMCA

Forged OnlyFans copyright claim to Google

Filed a fraudulent DMCA takedown with Google, claiming our domain report page infringed OnlyFans content. The claim was filed by "kanave mogel" using OnlyFans performer names. We contacted OnlyFans directly — they confirmed: *"This notice was not submitted by the OnlyFans team. It did not originate from us."* Case dismissed.

March 2026 — Trust User Infiltration

Trusted user injected 46 false-positive domains

A user with trusted status managed to add 46 legitimate domains to our blocklist. We detected it quickly and rolled back. Result: hardened permission model for all user roles — admins, trusted users, everyone. Thanks for the free security audit.

March-April 2026 — Appeals Form Flood

9,000+ fake appeals via hCaptcha solving

Spammed our domain appeals form with 9,000+ fake submissions, paying for hCaptcha solving. Trivially filtered — the patterns were obvious. Cost them money and time. Cost us nothing.

April 2026 — X/Twitter Suspended Again

Second X account killed. Not restoring.

Our X account was suspended again, likely via gov-style emergency requests. This time we decided: we're done with X. Not worth the effort to restore. We've built alternative communication channels and our operations don't depend on any social platform.

2026 — Reddit Banned

5-year-old account with 1-3 posts. Gone.

Our Reddit account was banned. It had 1 karma, 0 contributions, and a 5-year-old post in r/TREZOR warning about scam apps on Google Play. We're devastated. (We're not.) 😂

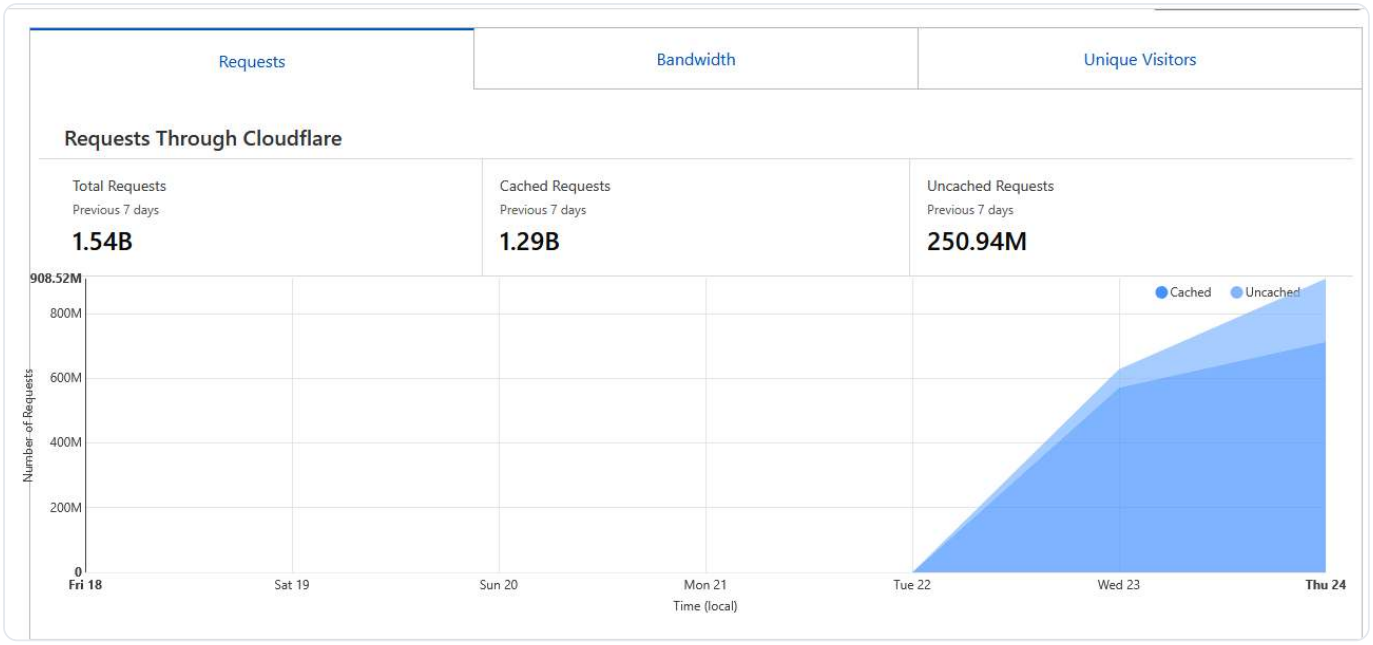
Ongoing — Email Bombing

400,000+ emails and counting

Non-stop email flood, auto-deleted. We genuinely can't tell you the exact count because our filters delete them automatically. Estimated 400K+. Someone is very upset. We must be doing something right.

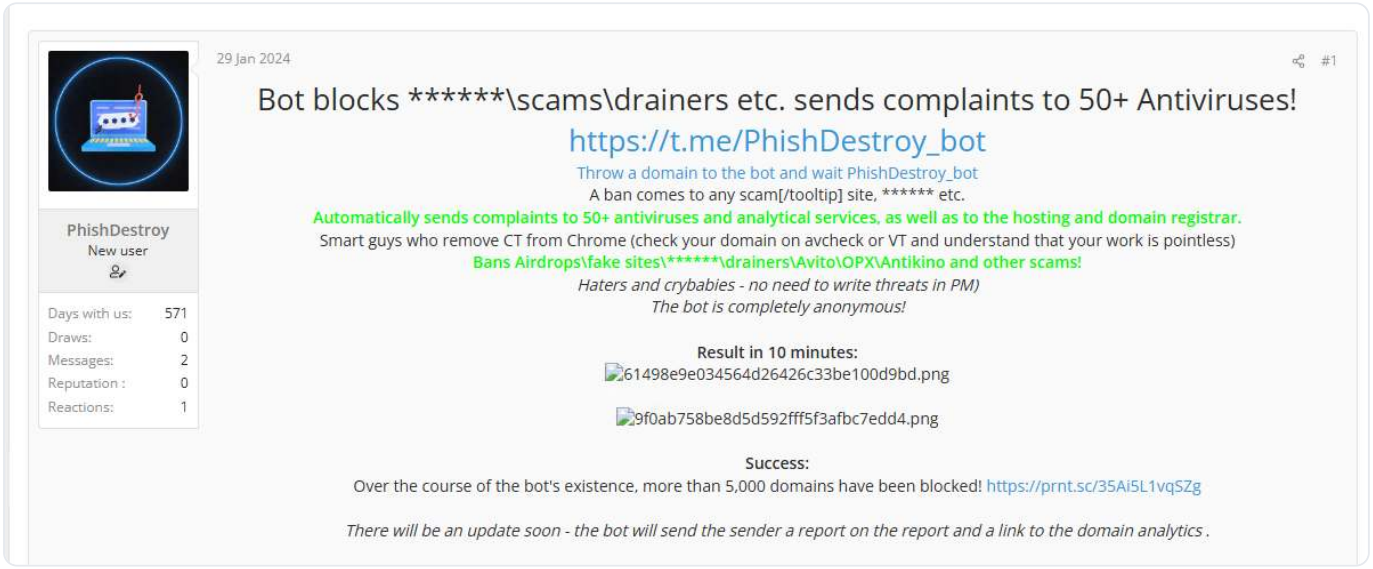
Evidence Archive

Below is documented evidence of specific incidents. Click any card to view the full-size screenshot. All evidence is preserved for transparency and potential legal proceedings.



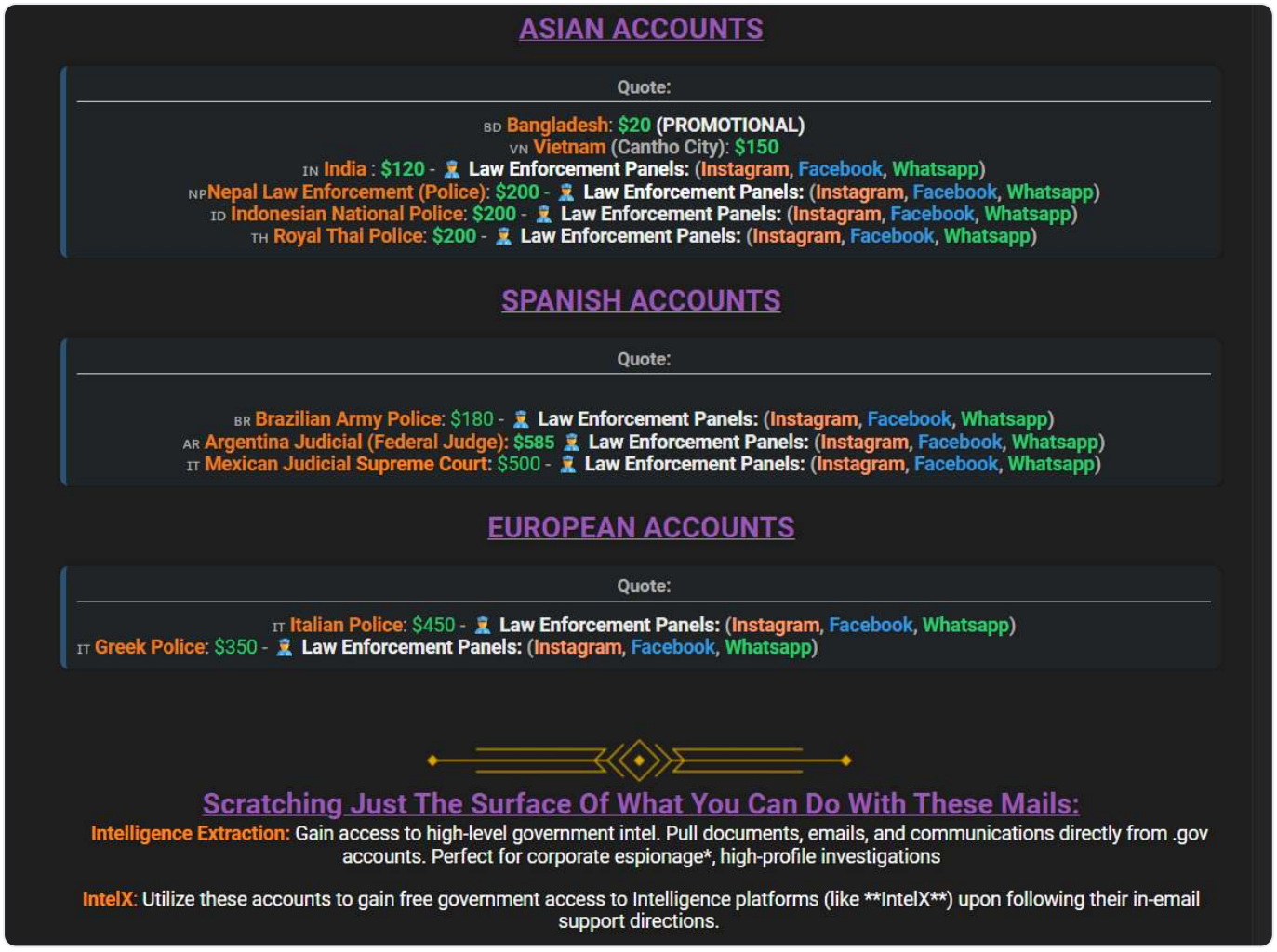
DDoS Attack Graph

Traffic spikes from rented botnets. Behind Cloudflare. Zero operational impact on email-based takedowns.



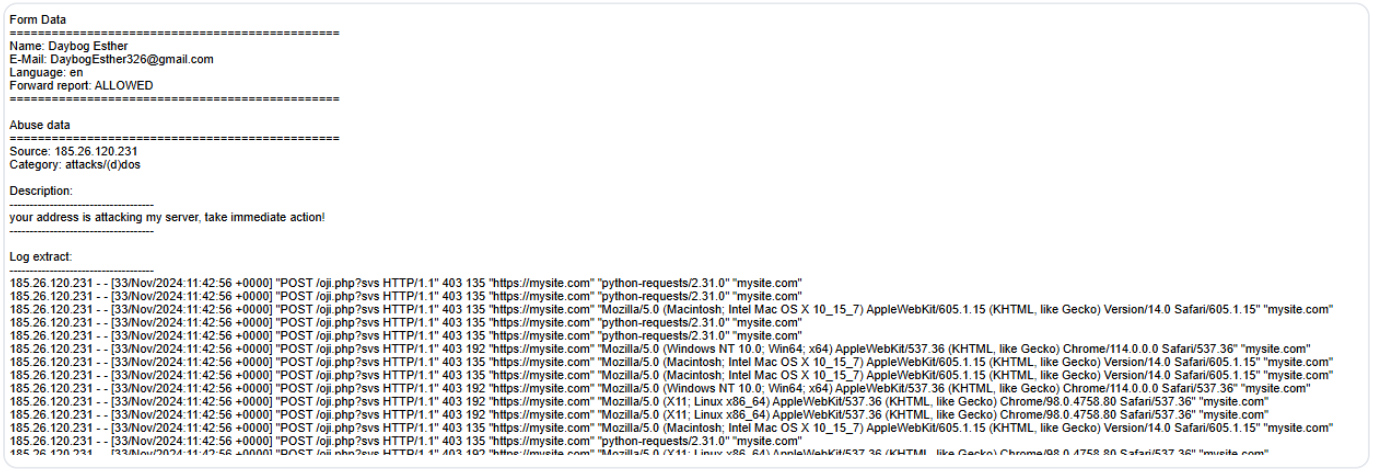
Fake "Russian Hacker" Forum

Scammers created faux-RU boards and paraded our work as their "service". Screenshot preserved for documentation.



Forum Pricing — "Gov Access"

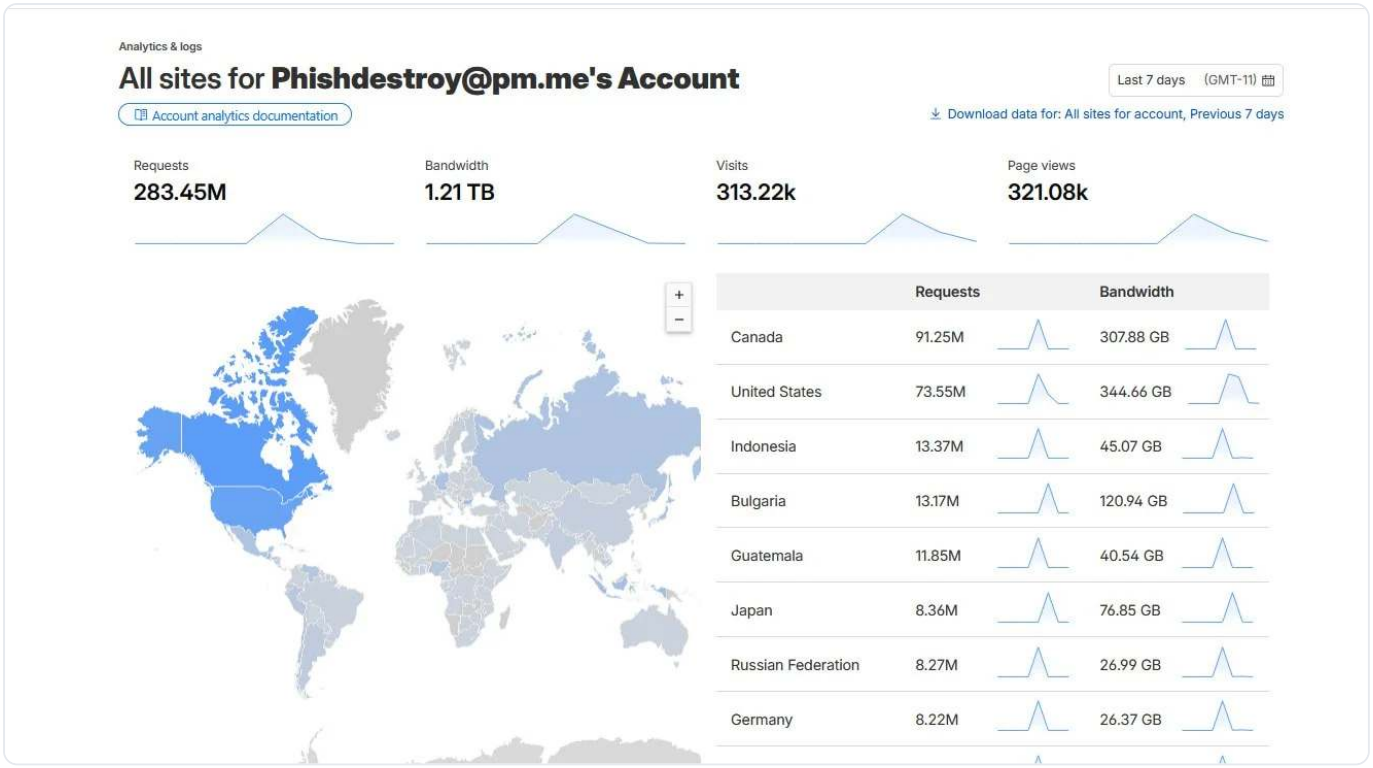
Public scam forum pricing. They offer turnkey services and automated law enforcement dashboard access.



```
Form Data
==========
Name: Daybog Esther
E-Mail: DaybogEsther326@gmail.com
Language: en
Forward report: ALLOWED
==========

Abuse data
==========
Source: 185.26.120.231
Category: attacks/(d)dos

Description:
---
your address is attacking my server, take immediate action!
---

Log extract:
---
185.26.120.231 - - [33/Nov/2024:11:42:56 +0000] "POST /oji.php?svs HTTP/1.1" 403 135 "https://mysite.com" "python-requests/2.31.0" "mysite.com"
185.26.120.231 - - [33/Nov/2024:11:42:56 +0000] "POST /oji.php?svs HTTP/1.1" 403 135 "https://mysite.com" "python-requests/2.31.0" "mysite.com"
185.26.120.231 - - [33/Nov/2024:11:42:56 +0000] "POST /oji.php?svs HTTP/1.1" 403 135 "https://mysite.com" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Safari/605.1.15" "mysite.com"
185.26.120.231 - - [33/Nov/2024:11:42:56 +0000] "POST /oji.php?svs HTTP/1.1" 403 135 "https://mysite.com" "python-requests/2.31.0" "mysite.com"
185.26.120.231 - - [33/Nov/2024:11:42:56 +0000] "POST /oji.php?svs HTTP/1.1" 403 135 "https://mysite.com" "python-requests/2.31.0" "mysite.com"
185.26.120.231 - - [33/Nov/2024:11:42:56 +0000] "POST /oji.php?svs HTTP/1.1" 403 192 "https://mysite.com" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36" "mysite.com"
185.26.120.231 - - [33/Nov/2024:11:42:56 +0000] "POST /oji.php?svs HTTP/1.1" 403 135 "https://mysite.com" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Safari/605.1.15" "mysite.com"
185.26.120.231 - - [33/Nov/2024:11:42:56 +0000] "POST /oji.php?svs HTTP/1.1" 403 135 "https://mysite.com" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Safari/605.1.15" "mysite.com"
185.26.120.231 - - [33/Nov/2024:11:42:56 +0000] "POST /oji.php?svs HTTP/1.1" 403 192 "https://mysite.com" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36" "mysite.com"
185.26.120.231 - - [33/Nov/2024:11:42:56 +0000] "POST /oji.php?svs HTTP/1.1" 403 192 "https://mysite.com" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.80 Safari/537.36" "mysite.com"
185.26.120.231 - - [33/Nov/2024:11:42:56 +0000] "POST /oji.php?svs HTTP/1.1" 403 192 "https://mysite.com" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.80 Safari/537.36" "mysite.com"
185.26.120.231 - - [33/Nov/2024:11:42:56 +0000] "POST /oji.php?svs HTTP/1.1" 403 135 "https://mysite.com" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Safari/605.1.15" "mysite.com"
185.26.120.231 - - [33/Nov/2024:11:42:56 +0000] "POST /oji.php?svs HTTP/1.1" 403 135 "https://mysite.com" "python-requests/2.31.0" "mysite.com"
```

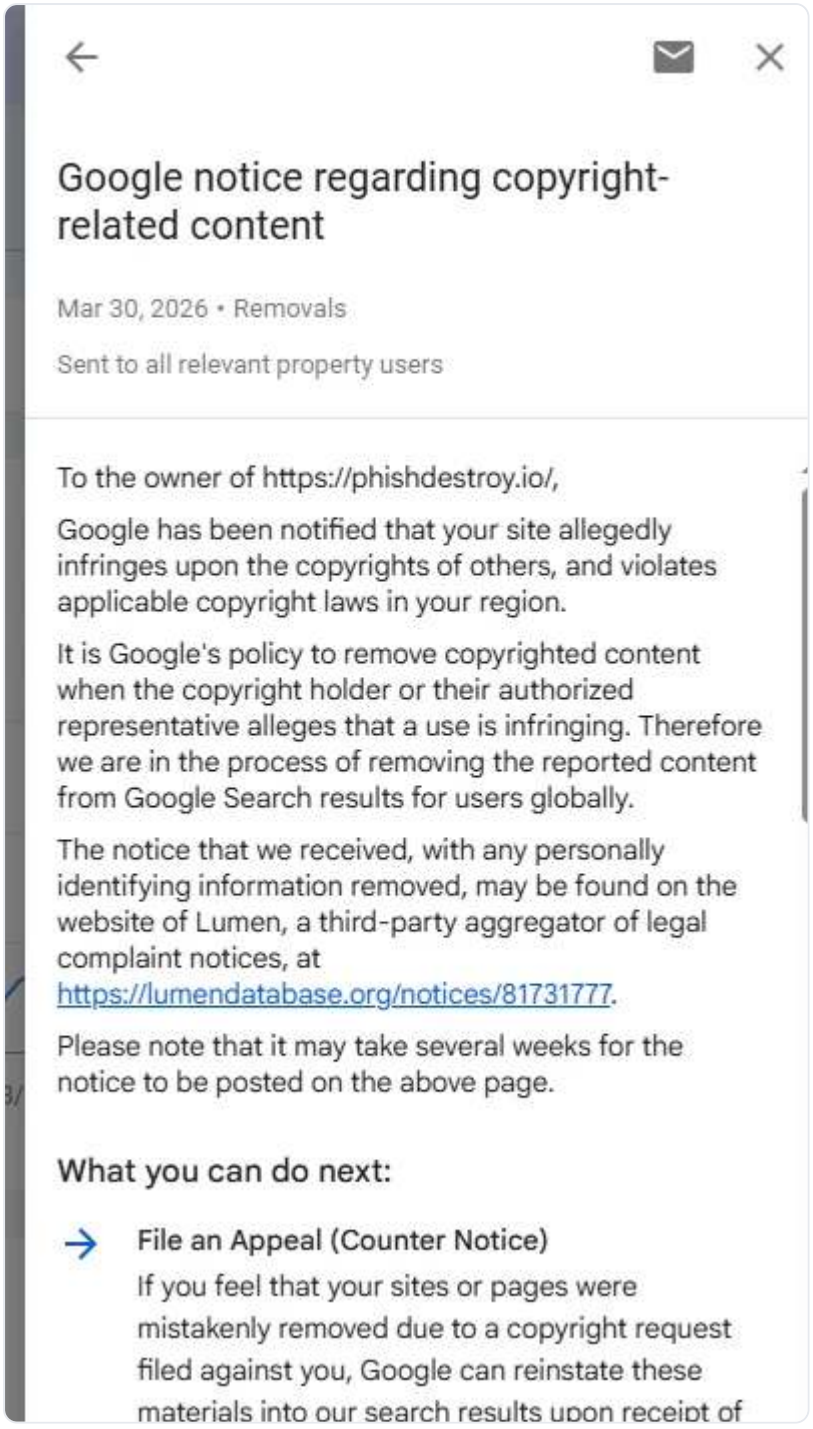
False Abuse Report

They hid the real domain as "mysite.com" in a report. It wasn't DDoS — it was their seed-capture auth endpoint.



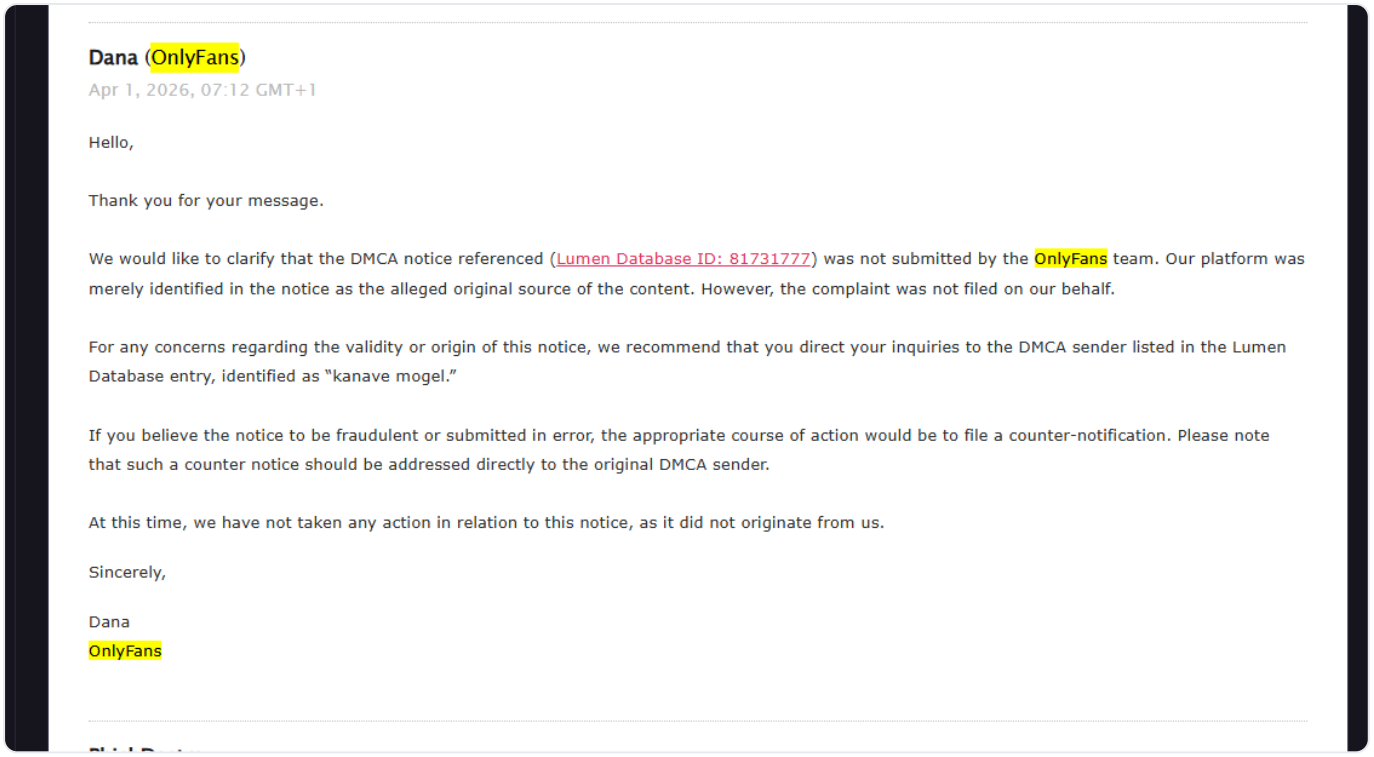
DDoS: 283M Requests / 1.21 TB

March 6, 2026. The attack that killed our Namecheap hosting. Canada, US, Indonesia, Bulgaria — global botnet. Migrated to Cloudflare.



Fake DMCA via Google

Forged OnlyFans DMCA to remove our domain report. Filed by "kanave mogel". OnlyFans confirmed they never filed it.



Dana (OnlyFans)
Apr 1, 2026, 07:12 GMT+1

Hello,

Thank you for your message.

We would like to clarify that the DMCA notice referenced (Lumen Database ID: 81731777) was not submitted by the OnlyFans team. Our platform was merely identified in the notice as the alleged original source of the content. However, the complaint was not filed on our behalf.

For any concerns regarding the validity or origin of this notice, we recommend that you direct your inquiries to the DMCA sender listed in the Lumen Database entry, identified as "kanave mogel."

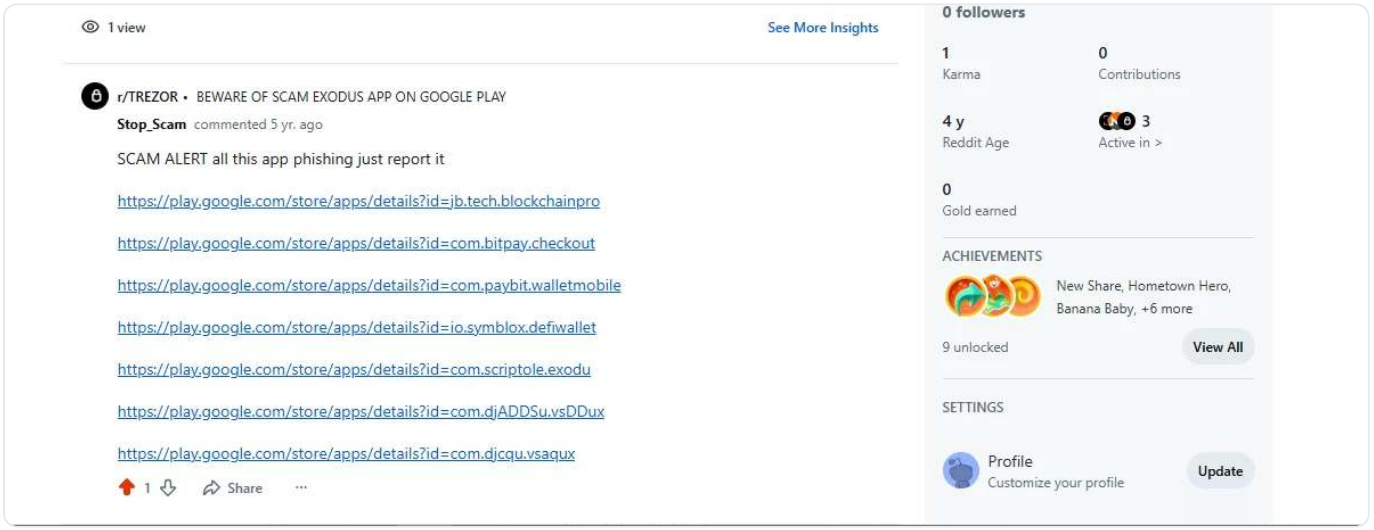
If you believe the notice to be fraudulent or submitted in error, the appropriate course of action would be to file a counter-notification. Please note that such a counter notice should be addressed directly to the original DMCA sender.

At this time, we have not taken any action in relation to this notice, as it did not originate from us.

Sincerely,

Dana
OnlyFans

OnlyFans: "Not From Us"
Official reply from Dana at OnlyFans: "This notice was not submitted by the OnlyFans team. It did not originate from us."



1 view
See More Insights

r/TREZOR • BEWARE OF SCAM EXODUS APP ON GOOGLE PLAY
Stop_Scam commented 5 yr. ago
SCAM ALERT all this app phishing just report it
https://play.google.com/store/apps/details?id=jb.tech.blockchainpro
https://play.google.com/store/apps/details?id=com.bitpay.checkout
https://play.google.com/store/apps/details?id=com.paybit.walletmobile
https://play.google.com/store/apps/details?id=io.symblox.defiwallet
https://play.google.com/store/apps/details?id=com.scriptole.exodu
https://play.google.com/store/apps/details?id=com.djADDSu.vsDDux
https://play.google.com/store/apps/details?id=com.djcqu.vsaqux
1 Share ...

0 followers
1 Karma
0 Contributions
4 y Reddit Age
3 Active in >
0 Gold earned
ACHIEVEMENTS
New Share, Hometown Hero, Banana Baby, +6 more
9 unlocked
View All
SETTINGS
Profile
Customize your profile
Update

Reddit Account Banned
1 karma. 0 contributions. A 5-year-old post warning about scam apps. Truly a threat to society.

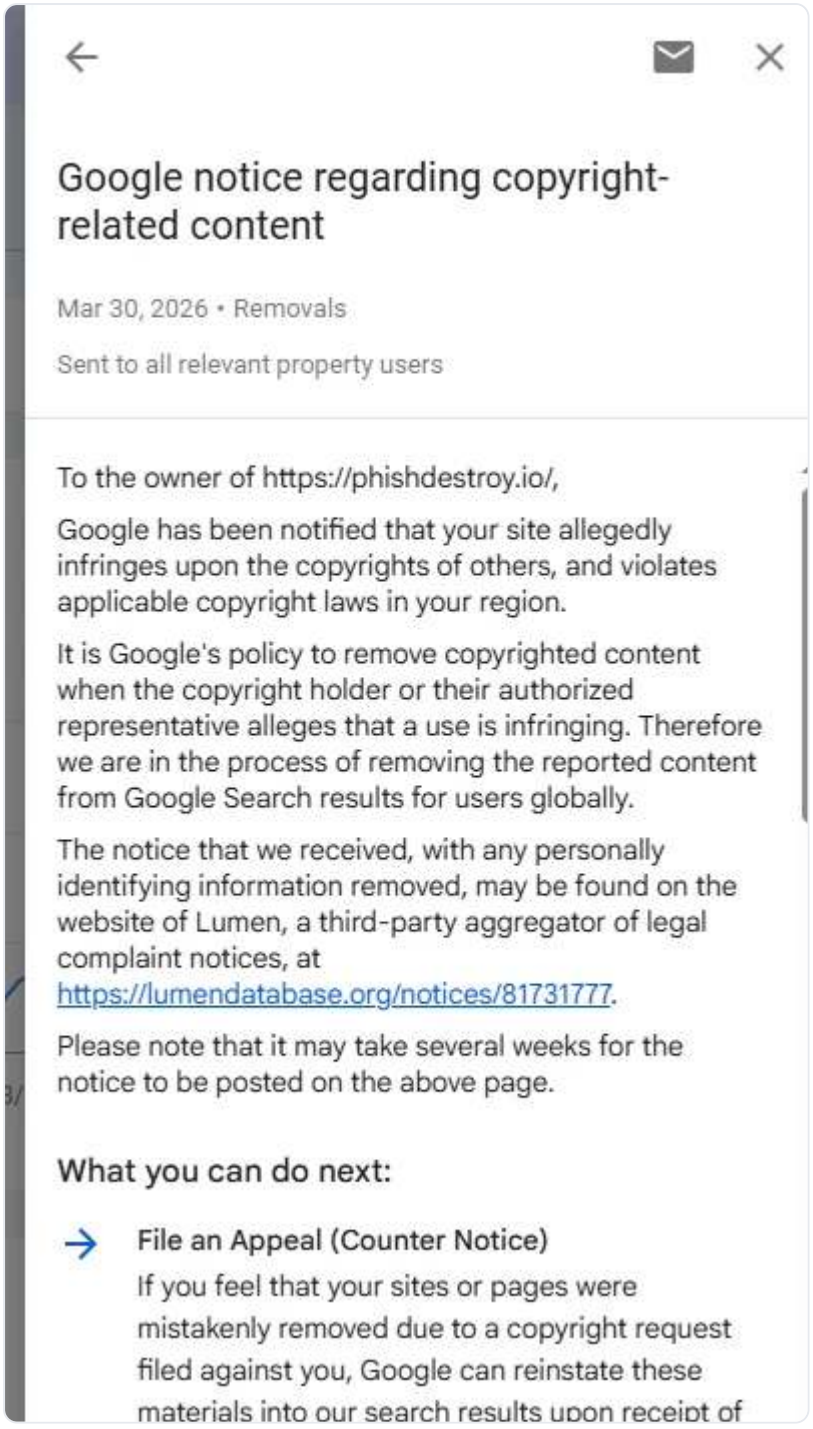
March 2026: The DDoS That Killed Our Hosting

On March 6, 2026, scammers launched the largest DDoS attack against our infrastructure to date: **283.45 million requests** and **1.21 TB of bandwidth** in just 7 days. The attack came from a global botnet spanning Canada (91M requests), United States (73M), Indonesia (13M), Bulgaria (13M), Guatemala (12M), Japan, Russia, and Germany.

Cloudflare analytics: 283M requests, 1.21 TB bandwidth. The attack that forced our hosting migration. Namecheap's $8/month hosting couldn't handle it and terminated our account. We migrated to Cloudflare + Hetzner ($25/month). After migration, they tried again — and predictably face-planted. Cloudflare absorbed everything without breaking a sweat. **Zero downtime. Zero impact on takedown operations.**

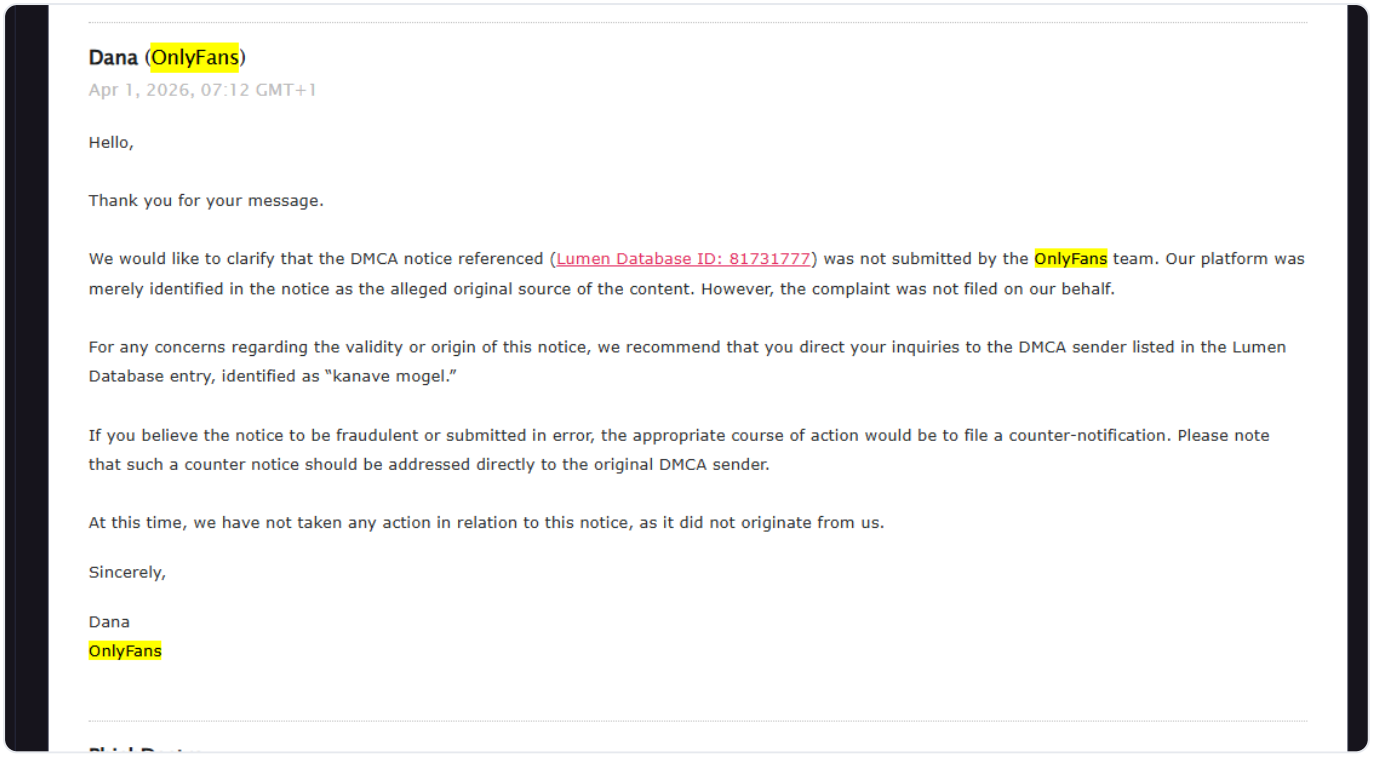
Fake DMCA Attack

On March 30, 2026, Google notified us of a copyright complaint against our domain report page `phishdestroy.io/domain/hbmhcw.net/` . The claim alleged that our page contained copyrighted OnlyFans content belonging to performers "Mibadbitch, Bri naranjo, or Brianna naranjo". The complaint was filed by someone named **"kanave mogel"** .



Google Copyright Notice

Mar 30, 2026. Google removes our domain report page from search results based on fraudulent DMCA claim.



Dana (OnlyFans)
Apr 1, 2026, 07:12 GMT+1

Hello,

Thank you for your message.

We would like to clarify that the DMCA notice referenced (Lumen Database ID: 81731777) was not submitted by the OnlyFans team. Our platform was merely identified in the notice as the alleged original source of the content. However, the complaint was not filed on our behalf.

For any concerns regarding the validity or origin of this notice, we recommend that you direct your inquiries to the DMCA sender listed in the Lumen Database entry, identified as "kanave mogel."

If you believe the notice to be fraudulent or submitted in error, the appropriate course of action would be to file a counter-notification. Please note that such a counter notice should be addressed directly to the original DMCA sender.

At this time, we have not taken any action in relation to this notice, as it did not originate from us.

Sincerely,

Dana
OnlyFans

OnlyFans: Not From Us
Dana from OnlyFans: "This notice was not submitted by the OnlyFans team. It did not originate from us."
We contacted OnlyFans directly. Their response was clear: *"The DMCA notice referenced (Lumen Database ID: 81731777) was not submitted by the OnlyFans team. Our platform was merely identified in the notice as the alleged original source of the content. However, the complaint was not filed on our behalf."*

Lumen Database record
lumendatabase.org/notices/81731777 — The full fraudulent DMCA notice is public record. Filed by "kanave mogel". A scammer trying to use copyright law to remove evidence of their phishing domains from our reports.

Social Media Takedowns

Our social accounts are systematically targeted. X (Twitter), Telegram, Medium, Reddit — all suspended or banned via mass reports, likely using forged government emergency requests. Our latest X account was killed in April 2026. **We've decided not to restore it.** We're done playing whack-a-mole with platform suspensions.

X/Twitter — permanently abandoned
After the second suspension, we decided: enough. We're not wasting time restoring accounts on platforms where scammers with money can file fake government requests to kill accounts. Our operations never depended on social media. The takedowns continue regardless.

Alternative channels
We tell the truth and help block what needs to be blocked. Some people don't like that. They think banning or deleting our accounts will stop us or hurt us. We're not complaining — it's honestly funny at

this point. We're ready for any bans and takedowns. Scammers with money and no brains = buying attacks and attempting to destroy us. But PhishDestroy is still here. And we destroy.
X Archive
140K+ takedown posts preserved.
GitHub Repo
Medium Archive
All blog posts preserved and mirrored.
View Archive
New Channel
Rebuilt immediately after takedown.
Join Channel

Evidence Preservation Protocol

Every action we take follows a strict evidence preservation protocol designed for maximum transparency and potential legal proceedings:

- **Pre-takedown archiving:** Web Archive snapshots + local forensic copies of every phishing site before reporting
- **Chain of evidence:** All communications with registrars, hosting providers, and law enforcement are logged and timestamped
- **Escalation protocol:** When identity is confirmed and legal lines are crossed, evidence packages are passed to authorities
- **No vendetta policy:** We prefer infrastructure removal to person-centric hunts. It's cleaner, faster, and scales better

Related reading
Infosecurity Magazine: Law Enforcement & Government Emails — Registrar response quality varies dramatically. Namecheap consistently acts fast; others, less so.

The $0 Model in Practice

Our cost structure is intentionally asymmetric. Every dollar they spend on retaliation is wasted. Every domain we remove costs us nothing.

Their spend	Our spend
$3,000+ per "government-style" social takedown	$0 per automated abuse report
$200-2,000 for DDoS botnet rental	$0 — behind Cloudflare, email flows continue
$500-2,000 for UK paper company + legal forgeries	$0 — private registration, claims auto-rejected
$50-300/mo for email flood services	$0 — we don't use inbound email for operations
$50-300 for bot farm fake reports	$0 — reported and wiped by platforms

The Scoreboard

They burn thousands trying to stop us. We spend **$0** to remove their infrastructure. Our automation scales. Their panic doesn't. We warn them: *"your infra turns off soon"* — then chaos begins on their end. Meanwhile, we keep it boring: scan, archive, report, remove.

Want to Help?

If you've encountered a phishing site or want to contribute to the fight against crypto scams, here's how:

Transparency notice. PhishDestroy is a non-commercial, independent project. Our research may reflect an inherent bias against scam infrastructure and the services that enable it. We encourage readers to evaluate all material critically and independently. Read our full transparency statement →