THREAT INTELLIGENCE REPORT

When Abuse Reports Go Nowhere: How Registrars Become Silent Partners in Cybercrime

Ref. **PD-TI-2026-46949** Published **10 July 2026** Source **phishdestroy.io/registrar-abuse-response-failure**

INVESTIGATION • 15—18 min read

We send evidence-packed abuse reports — VirusTotal detections, screenshots, blacklist data, antivirus scans. Registrars receive them and do nothing. Some phishing domains survive **1,788 hours** and **13 separate reports** . This isn't a system failure — it's a design choice. Here's the data.

~8 min read · Updated **March 2026** · PhishDestroy Intelligence

The Broken System

Every abuse report we send follows a clear protocol: domain URL, category (phishing, crypto drainer, fake casino), VirusTotal detection count, screenshot evidence, and blacklist status. These aren't vague complaints — they're forensic packages. And yet, domain after domain stays online for **weeks and months** after the first report.

There is no universal standard for how registrars must handle abuse reports. No SLA. No mandatory response time. No accountability metric. Each registrar decides on its own whether a domain flagged by **16 antivirus engines** deserves attention — or a template reply and a closed ticket.

1,788h
payscrow[.]bet — active for 75 days despite 6 reports and 16 VirusTotal detections. Registrar: Tucows / Identity Digital.

Who Overrules 16 Antivirus Engines?

This is the question no registrar wants to answer. When **Kaspersky, ESET, Fortinet, BitDefender, Sophos, G-Data** and ten more security vendors flag a domain as malicious on VirusTotal — and the registrar's abuse team decides *"no action needed"* — who exactly made that call?

Consider the absurdity: a single abuse analyst at a registrar overrules the combined threat intelligence of **16 independent antivirus engines** , each with billions of data points, dedicated research labs, and decades of experience. On what basis? What scanning infrastructure does an abuse team at NiceNIC or GlobalDomainGroup operate that surpasses Kaspersky's?

The answer is simple: none. They don't scan. They don't verify. They either don't look at the report at all, or they apply a financial calculation: a live domain generates revenue; a suspended domain does not.

farewex[.]com — 13 abuse reports sent. 13 VirusTotal detections. Active for 1,352 hours (56 days). The registrar (apiname.com / Verisign) received evidence from antivirus vendors, threat intelligence platforms, and ICANN compliance. **The domain is still live.** Who decided this is acceptable?
Let's be explicit about what this means: someone at the registrar looked at evidence from 13 independent security vendors and 13 separate abuse reports — and decided their own judgment was superior. That's not a mistake. That's a policy.

No Authority They Respect

Name a single antivirus vendor that registrars treat as authoritative. You can't — because there isn't one.

- **Kaspersky** — detects the domain? Ignored.
- **ESET** — flags it as phishing? Ignored.
- **Fortinet** — blocks it at the network level? Ignored.
- **BitDefender** — warns millions of users? Ignored.
- **Google Safe Browsing** — the largest web safety system on Earth? Still ignored.

There is **no detection threshold** at which a registrar is obligated to act. Not 5 engines. Not 10. Not 16. A domain can be flagged by every antivirus vendor on VirusTotal, appear on multiple blacklists, and have a dozen abuse reports filed — and the registrar is under no enforceable obligation to do anything.

This isn't a gap in the system. **This is the system.** The domain registration industry has successfully avoided any binding standard that would require them to respect the findings of security researchers, antivirus vendors, or threat intelligence platforms. When 16 out of 70 engines detect a domain — that's

not a "maybe." That's a consensus. And the registrar's abuse team, with zero scanning infrastructure and a financial interest in keeping the domain alive, overrules that consensus.

0

The number of antivirus vendors whose findings registrars are **obligated** to act on. Not Kaspersky. Not ESET. Not Google. Zero.

50,000+ abuse reports filed. The registrar wall stands. Domains stay online.

The Financial Incentive

Domain registrars charge annual fees for every domain. Every suspension is lost revenue. Every takedown is a refund risk. There is a direct, measurable financial incentive to keep domains active — and no financial penalty for ignoring abuse reports.

This is not the case for all infrastructure providers. **Cloudflare** , for example, processes abuse reports efficiently and does not earn revenue from domain registrations in the same way. The distinction matters: when the company processing your report profits from the domain staying online, the conflict of interest is structural.

The Evidence: Live Data From Our Reports

Below is a sample from our March 2026 abuse escalation log. Every entry represents a real phishing domain that was **still active** at the time of reporting, despite prior reports and confirmed detections.

Domain	Reports	Active (hours)	VT	BL	Registrar Abuse
payscrow[.]bet	6	1,788h	16	—	Tucows
6chicken9[.]top	4	1,783h	4	1	Endurance
apphyena[.]trade	2	1,781h	3	—	NiceNIC
airdrop[.]autos	3	1,364h	4	1	Gname
amlstats[.]com	7	1,363h	14	1	Tucows
amlscore[.]info	7	1,363h	9	1	Tucows
amlwallets[.]io	4	1,363h	10	1	nic.io
aavleaderboard[.]assetavenue[.]capital	2	1,359h	1	—	IdentityDigital
airdropchime[.]com	2	1,359h	1	—	Namecheap
farewex[.]com	13	1,352h	13	—	apiname.com
app[.]whitewhalesmeme[.]com	4	1,330h	14	—	Verisign
zordex[.]us	3	1,314h	14	—	apiname.com
alhpatrademarket[.]com	2	1,278h	15	—	GlobalDomainGroup
angelferno[.]com	2	1,278h	7	1	NiceNIC
ansol[.]cc	4	1,278h	4	1	NiceNIC
amltrackerbot[.]com	2	1,278h	6	1	Tucows
amlstatement[.]info	4	1,228h	16	—	Porkbun
a8vx[.]top	2	1,049h	16	—	Dynadot
amlinfo[.]now	2	1,033h	2	—	Porkbun
xwinner[.]cc	4	1,026h	14	—	GlobalDomainGroup
xerowex[.]com	6	1,021h	14	—	apiname.com
menty[.]sbs	4	985h	16	—	gen.xyz
perowex[.]com	5	971h	14	—	apiname.com
amlbot[.]im	4	965h	6	—	nic.im
3capitalstrading[.]com	2	879h	2	—	GlobalDomainGroup
naebex[.]com	5	826h	11	—	PDR
casbatle[.]com	2	803h	2	—	NiceNIC
amlchecknow[.]digital	2	751h	6	—	PDR
sollfalare[.]top	2	730h	3	—	Endurance
marketcsgo[.]net	2	717h	15	—	GlobalDomainGroup
dinadrop[.]com	2	717h	6	—	GlobalDomainGroup
dotabuff[.]org	2	674h	2	—	PIR

Domain	Reports	Active (hours)	VT	BL	Registrar Abuse
casesbattle[.]org	2	652h	2	—	PIR
763182819[.]top	2	618h	15	—	Gname
kahcas[.]com	5	539h	14	—	INWX
qizaro[.]cc	5	535h	12	—	GlobalDomainGroup
apexresolvefix[.]com	2	496h	3	—	Cosmotown
amlriskscore[.]ru	2	448h	1	—	cctld.ru
patricksstash[.]to	2	427h	2	—	tonic.to
stashhpatrick[.]cc	2	427h	5	—	NiceNIC
stake2win[.]me	2	402h	14	—	domain.me
wazbee[.]me	2	388h	16	—	domain.me
dexscreener[.]at	2	328h	16	—	nic.at
2fa[.]walletpinet[.]com	1	—	16	—	Verisign
appether[.]fi	1	—	13	1	—

VT = VirusTotal detections out of ~70 engines. "Active" = hours since first detection at time of escalation. Data: PhishDestroy abuse escalation log, March 19–21, 2026.

The Numbers Don't Lie

Average Active Time

943h

~39 days average across all domains with known active hours

Maximum Active Time

1,788h

payscrow[.]bet — 75 days, 6 reports, VT:16

Total Reports Sent

150+

Combined reports across all domains in this sample alone

Domains With VT≥10

22

Nearly half of all domains — confirmed malicious by 10+ antivirus engines, still active

The Repeat Offenders: Registrar Breakdown

Not all registrars are equal. Our data shows clear patterns — some registrars appear repeatedly in the worst-performing entries.

apiname.com

- farewex[.]com — 1,352h, 13 reports, VT:13
- zordex[.]us — 1,314h, 3 reports, VT:14
- xerowex[.]com — 1,021h, 6 reports, VT:14
- perowex[.]com — 971h, 5 reports, VT:14

4 domains. Combined: 4,658 hours of criminal infrastructure. 27 reports ignored.

GlobalDomainGroup

- xwinner[.]cc — 1,026h, VT:14
- marketcsgo[.]net — 717h, VT:15
- dinadrop[.]com — 717h, VT:6
- qizaro[.]cc — 535h, VT:12
- csgomy[.]com — 356h, VT:9
- tastdrop[.]com — 357h, VT:2
- casebatle[.]com — 327h, VT:6
- casebatltle[.]com — 327h, VT:2
- chestix[.]net — 293h, VT:1
- ggddrop[.]com — 365h, VT:1

10 domains. The single largest cluster in our dataset. A pattern, not an accident.

Tucows / IdentityDigital

- payscrow[.]bet — 1,788h, 6 reports, VT:16
- amlstats[.]com — 1,363h, 7 reports, VT:14, BL:1
- amlscore[.]info — 1,363h, 7 reports, VT:9, BL:1
- amltrackerbot[.]com — 1,278h, 2 reports, VT:6, BL:1

Tucows: 22 combined reports, 5,792 hours of fraud. amlstats received 7 reports — one per week — and survived them all.

NiceNIC (nicenic.net)

- apphyena[.]trade — 1,781h, VT:3
- angelferno[.]com — 1,278h, VT:7, BL:1
- ansol[.]cc — 1,278h, 4 reports, VT:4, BL:1
- casbatle[.]com — 803h, VT:2
- stashhpatrick[.]cc — 427h, VT:5
- casebaetle[.]com — 310h, VT:2
- casebattle[.]info — first report, VT:1
- appalmanak[.]live — first report, VT:2

8 domains. 5,877+ combined hours. Previously investigated: NiceNIC Verdict — zero legitimate uses found.

Porkbun

- amlstatement[.]info — 1,228h, 4 reports, VT:16
- amlinfo[.]now — 1,033h, 2 reports, VT:2
- amlspace[.]com — 712h, 2 reports, VT:1

amlstatement[.]info: 16 antivirus detections, 4 reports, and 51 days online. What did Porkbun's abuse team decide was acceptable?

Dynadot

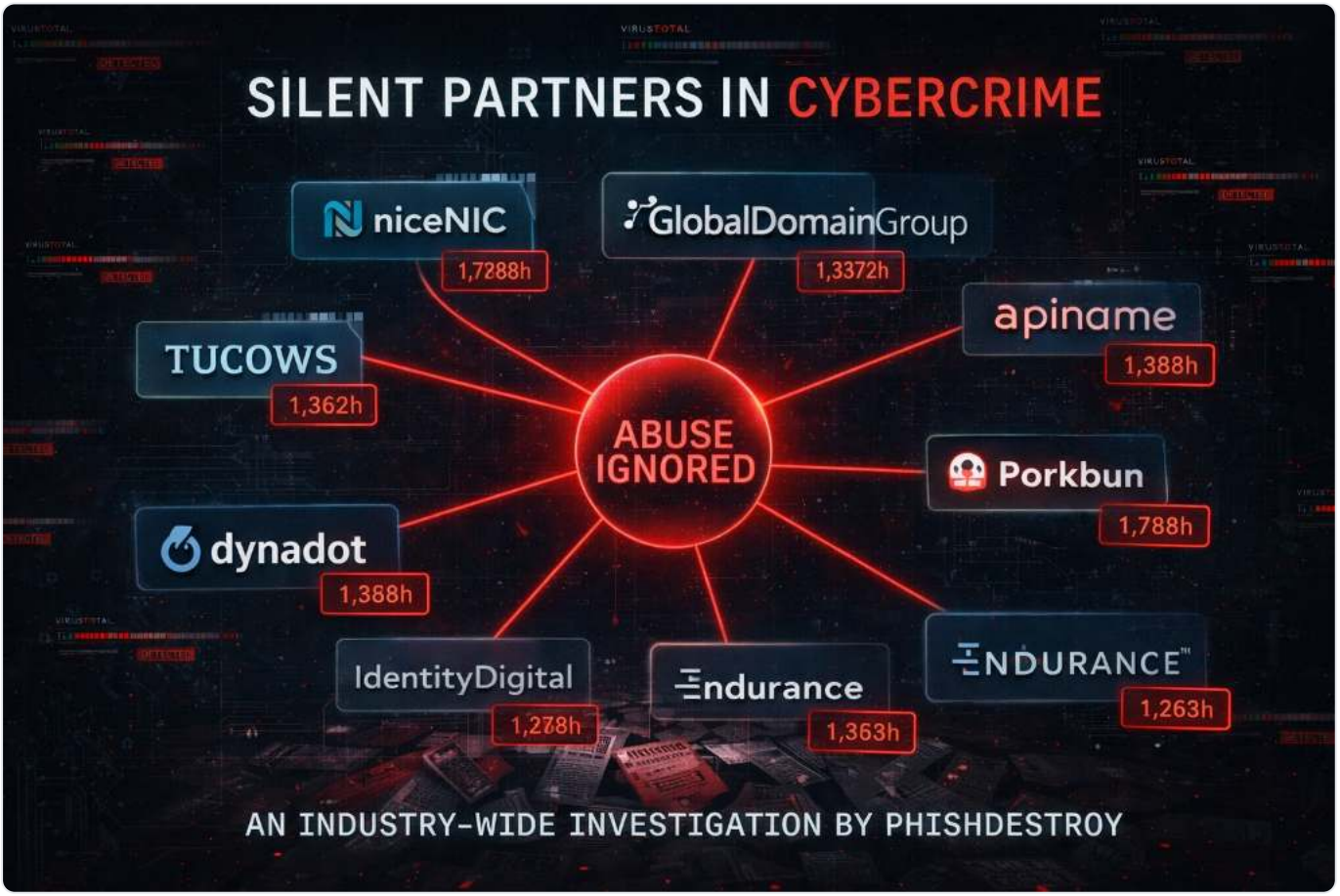
- a8vx[.]top — 1,049h, 2 reports, VT:16
- aave[.]events — first report, VT:2, BL:1
- aavetrading[.]net — first report, VT:9

a8vx[.]top: 16 VT detections and 44 days of criminal activity. Dynadot is an ICANN-accredited registrar.

domain.me

- wazbee[.]me — 388h, VT:16
- stake2win[.]me — 402h, VT:14

Both domains with 14–16 antivirus detections. Both still active after second report.



Every node is an ICANN-accredited registrar. Every number is hours of confirmed criminal infrastructure left online after abuse reports.

Combined Hours of Inaction by Registrar

NiceNIC
5,877h
Tucows
5,792h
GlobalDomainGroup
5,520h+
apiname.com
4,658h
Porkbun
2,973h
Endurance
2,513h
Dynadot
1,049h+
domain.me
790h

Combined active hours of all reported domains per registrar in our March 2026 dataset. Not total registrar abuse — just what we observed in one sample.

What We Send vs. What They Do

Every PhishDestroy abuse report includes:

Our Report Contains

- Domain URL and registration data
- VirusTotal score with vendor names
- Full-page screenshot of the phishing site
- Category classification (phishing, drainer, scam casino)
- Blacklist status from multiple feeds
- URLscan.io or similar scan results
- Prior report history and timeline

Registrar Response

- No response at all (most common)
- Template acknowledgment, no action
- "We will review" — weeks pass, domain stays
- "We cannot verify the claim" — despite 16 VT detections
- Ticket closed without resolution
- Request for evidence already provided

After registrar inaction, we escalate to **ICANN Compliance** (compliance@icann.org). In every case shown above, ICANN was CC'd on the second or subsequent report. The results? Equally absent.

The ICANN Standard That Doesn't Exist

ICANN's **Registrar Accreditation Agreement (RAA), Section 3.18** requires registrars to maintain an abuse contact and to "take reasonable and prompt steps to investigate and respond appropriately" to reports of abuse.

In practice, "reasonable and prompt" means whatever the registrar decides it means. There is:

- **No maximum response time** — a registrar can wait weeks and claim it was "reasonable"
- **No mandatory suspension threshold** — 16 VT detections doesn't automatically trigger anything
- **No public reporting requirement** — registrars don't have to publish how many reports they receive or act on
- **No meaningful penalty** — ICANN has rarely revoked accreditation for abuse inaction

The result: registrars treat abuse handling as a cost center to minimize, not a safety obligation to fulfill.

What the standard should be: 24-hour acknowledgment. 72-hour action for domains with VT≥10. Automatic suspension after 3+ independent reports. Public quarterly reporting on abuse metrics. Financial penalties for systematic non-compliance.

They Act on Typosquatting — But Not on Phishing

Here's what makes this even more absurd. Some of the same registrars that ignore phishing reports for months are extremely efficient at one specific type of abuse: **typosquatting** — domains that are confusingly similar to established brand names.

Why? Because typosquatting targets **corporations with legal budgets** . When Google, Apple, or Microsoft files a UDRP complaint about a lookalike domain, registrars act within days. The threat of litigation and ICANN sanctions for trademark abuse is real and immediate.

But when a phishing domain steals money from individual victims? When a crypto drainer empties someone's life savings? When a fake casino steals credit card data from gamers? **No corporate legal team. No UDRP filing. No urgency.** The registrar's abuse department applies a different standard — one where the victim's financial loss doesn't trigger the same response as a brand's trademark concern.

Typosquatting Report

- Brand owner files UDRP
- Registrar responds in days
- Domain locked/suspended quickly
- Legal consequences for inaction

Phishing/Scam Report

- Victims/researchers file abuse reports
- Registrar ignores for weeks/months
- Domain stays active until expiry
- Zero consequences for inaction

The message is clear: **registrars protect brands, not people.** They respond to legal power, not to evidence of harm. Our reports contain more objective evidence than any UDRP filing — VirusTotal scans, antivirus detections, blacklist confirmations, screenshots — and yet they sit unanswered.

We Do Their Job — For Free

PhishDestroy is a **independent, non-commercial project** . We scan domains. We classify threats. We generate VirusTotal reports. We take screenshots. We write detailed abuse reports and send them to registrars, registries, and ICANN. **We do the security work that registrars should be doing themselves.**

And here's the uncomfortable truth: **some registrars actually do this work.** Some registrars run their own domain scanning infrastructure, use private threat intelligence feeds, and proactively suspend malicious domains before anyone even reports them. They exist. They prove it's possible.

Registrars That Act

- Run internal scanning tools (private, non-public)
- Proactively suspend obvious fraud domains
- Respond to abuse reports within hours
- Cooperate with researchers and law enforcement
- Accept VirusTotal and blacklist data as evidence

These registrars prove that fast abuse response is technically and economically feasible.

Registrars That Protect Scammers

- No scanning infrastructure whatsoever
- Wait for reports, then ignore them
- Template replies, ticket closed, domain active
- Deny receiving reports (NameSilo pattern)
- Overrule 16 antivirus engines with zero evidence

These registrars chose revenue over safety. Their inaction is subsidized by the security community doing their work for free.

The question isn't whether fast abuse response is possible. **It is.** The question is why some registrars choose not to do it. And the answer, every time, circles back to the same structural incentive: **live domains generate revenue. Suspended domains don't.**

Authoritative Standards That Should Apply

The framework for holding registrars accountable already exists — it's just not enforced:

ICANN RAA §3.18

The Registrar Accreditation Agreement requires registrars to maintain abuse contacts and investigate reports promptly. Enforcement is effectively non-existent.

APWG

The Anti-Phishing Working Group publishes quarterly phishing trend reports showing the scale of the problem. Registrars participate in APWG — and still ignore reports.

FTC Actions

The FTC warning letter to NameSilo (Dec 2024) explicitly called out failure to address fraud. ICANN's own Compliance department receives our escalations and returns silence.

DNSAI

The DNS Abuse Institute (by PIR) develops tools like DAAR and promotes best practices. Yet PIR's own registry hosts dotabuff[.]org (674h active, VT:2) and casesbattle[.]org (652h).

50,000 Domains and Counting

The examples above are a **sample from a single week** . The real scale is staggering.

50K+
Active phishing domains in our destroylist that have received abuse reports. Most are **still online** .
Our continuously updated threat feed at content_active.txt contains over 50,000 domains that have been reported as malicious. Each one received at least one abuse report. Many received multiple. The registrars received the evidence — the VirusTotal scans, the screenshots, the blacklist confirmations — and chose their client over the safety of the public.

Because that's what this is: **a choice** . The registrar's client is the person who registered the domain — the scammer. The registrar's client is not the grandmother who lost her savings to a fake banking page, or the crypto user whose wallet was drained, or the gamer whose Steam account was stolen. The registrar chose the scammer. Every time.

The abuse report conveyor belt: domains come in with VT:16 detections, get stamped "NO ACTION," and keep running. Registrar names glow above the line they created.

From Report to Victims: Every Hour Counts

The moment we send an abuse report, a clock starts. From that moment, the registrar is **officially aware** that a domain under their management is being used to commit fraud. Every hour of inaction after that notification is an hour of **informed complicity** .

Many domains in our dataset don't just survive a few reports — they survive until their **registration period expires** . They run the full cycle: register, scam, get reported, get reported again, get escalated to ICANN, continue scamming, expire naturally. The registrar collected the registration fee. The scammer collected the stolen funds. The victims collected nothing.

NameSilo has publicly denied receiving abuse reports that we have documented proof of sending.
When a registrar lies about receipt of reports to avoid accountability, what recourse do victims have? Perhaps it's time for an independent audit of registrar abuse handling — one that compares reports sent vs. actions taken, with public results.
A timely domain suspension is not just an administrative action. It's not just "an inconvenience for the registrant." **It's a rescue operation.** Every domain banned in time is a wallet not drained, a credential not stolen, a savings account not emptied. Registrars who frame takedowns as "censorship" or "business disruption" are revealing exactly whose interests they serve.

Should Registrars Compensate Victims?

Here is the question the entire domain registration industry refuses to engage with:

If a registrar receives an evidence-based abuse report — with VirusTotal detections, screenshots, and blacklist confirmations — and chooses not to act, is the registrar liable for damages caused to victims after that point?
Think about it. Once the registrar receives the report, they are **no longer ignorant** . They have been informed, with evidence, that a domain under their control is being used to steal money, credentials, and identities. From that moment, continued inaction is not negligence — it is a **conscious decision** to allow harm.

- **Is the registrar willing to accept liability** for every dollar stolen through a domain they were warned about?
- **Is the registrar prepared to compensate victims** who lost funds after the abuse report was filed and ignored?
- **Does the registrar's legal team** understand that "we reviewed and found no issue" — when 16 antivirus engines disagree — is not a defensible position?

If the answer to all three is "no" — then there is no legitimate reason to keep the domain active. **Suspend first, investigate later.** That's how responsible infrastructure providers operate. That's how Cloudflare operates. That's how hosting providers like Hetzner and OVH increasingly operate. Only domain registrars cling to a model where the scammer's convenience outweighs the victim's safety.

Who Pays the Price

Every hour a phishing domain stays online translates directly to victims:

- **Crypto drainer domains** (farewex, perowex, xerowex, naebex) — wallets emptied in seconds. The 4,658 combined hours of apiname.com domains represent thousands of potential wallet drains.
- **Fake casino / CS:GO scams** (casebattle variants, csgomy, ggddrop, tastdrop) — credit card fraud, identity theft, and rigged outcomes targeting gamers.
- **Fake service impersonation** (dexscreener[.]at, trustwallet[.]receipts[.]sh, amlbot[.]im, dotabuff[.]org) — brand impersonation leading to credential theft and financial loss.
- **Carding infrastructure** (patricksstash, stashhpatrick) — selling stolen payment data to other criminals.

75

days that payscrow[.]bet was operational — the equivalent of leaving a pickpocket in a shopping mall for 2.5 months after security was told about them, showed them the footage, and identified the suspect.

What Must Change

The current model is broken by design. Registrars profit from domains staying active. ICANN has no enforcement teeth. Victims have no recourse. Here's what would fix it:

1. **Mandatory SLA for abuse response:** 24-hour acknowledgment, 72-hour initial action, 7-day escalation path. Measurable. Auditable.
2. **Automatic suspension threshold:** Any domain with VirusTotal detections ≥10 and 2+ independent reports must be suspended pending review — not the other way around.
3. **Public abuse transparency reports:** Every ICANN-accredited registrar must publish quarterly: reports received, average response time, actions taken, domains suspended.
4. **Financial penalties for non-compliance:** Graduated fines for registrars that systematically fail to act. Loss of accreditation for repeat offenders.
5. **Independent abuse ombudsman:** A third-party body that can review registrar decisions, override inaction, and fast-track suspensions for critical threats.
6. **Cross-registrar ban list:** When a registrant is confirmed as a serial abuser, all accredited registrars should be notified. No more domain shopping.

What PhishDestroy Has Done About It

We don't write reports and wait for the industry to fix itself. We build systems that force transparency and create consequences for inaction.

Public Threat Database

We created and maintain the destroylist — a public, continuously updated database of 50,000+ malicious domains. Every abuse report we send now informs the registrar: **this domain will be listed in a public database** . Potential victims of their client's domains will see when the report was filed and how long the registrar ignored it. This is uncomfortable for registrars — and that's the point.

Domain Threat Pages

Every domain we flag now has a dedicated page at phishdestroy.io/domain — with full analysis, AI-generated threat description, and a **Threat Response Pipeline** showing the exact processing stages: detection, report sent, escalation, ICANN notification. Statuses update in real time. We are now adding exact timestamps of every follow-up report for full transparency. Anyone can see exactly when the registrar was notified and how long they chose to do nothing.

Escalation System — Not Report Flooding

We do **not** flood registrars with duplicate reports. In 98% of cases, we send a single initial report and do not repeat it — both because of daily email limits and because we believe mass duplication is the wrong approach. We only send a follow-up report when a domain is **re-detected as active** during a new scan. If we spammed every active domain daily, that would be 50,000 emails per day. We don't. Our escalation system generates follow-up reports (#2, #3, etc.) with AI-analyzed threat summaries, updated VirusTotal scores, and a count of hours the registrar has ignored the threat.

Community Re-Report Tool

In our Telegram bot @PhishDestroy_bot , users can now submit **re-reports** for domains they've found still active after our initial report. Because too many registrars allow scammers to operate freely and ignore catastrophic damage, we give the community a voice. If a registrar won't listen to us, maybe they'll listen to the volume of independent reports from real users.

A note to scam project owners and negligent registrars: If you think we're "attacking" you with mass reports — we're not. We send one report per detection event. If you're receiving many reports, it's because you have many malicious domains. The reports are all different, for different domains, with different evidence. The problem isn't our reporting volume — it's **your domain portfolio** .

PhishDestroy — we don't protect brands. We don't defend victims. **We destroy phishing and scam infrastructure.**

Conclusion

When 16 antivirus engines say a domain is malicious and a registrar says "no action," the registrar isn't exercising judgment — it's protecting revenue. When 13 separate abuse reports go unanswered and a domain stays live for 1,352 hours, the registrar isn't processing a backlog — it's enabling crime.

The data in this article isn't theoretical. It's our live abuse escalation log from a single week in March 2026 — and behind it sit **50,000+ reported domains** in our continuously updated threat feed. This is not an isolated problem with one registrar. This is an **industry-wide failure** that the domain registration ecosystem has no interest in fixing, because the current model is profitable.

There is no antivirus vendor whose findings registrars are obligated to respect. There is no detection threshold that triggers mandatory action. There is no SLA, no accountability, no consequences. The registrar collects the fee, ignores the reports, and the victims pay the price.

Registrars are not neutral infrastructure providers. They are gatekeepers who choose — every day, with every ignored report — to keep criminal infrastructure online. They are informed of the harm. They have the power to stop it. They choose not to. And until someone asks them the only question that matters — *"Are you willing to compensate the victims of domains you refused to suspend?"* — nothing will change.

The industry's silence on this question is the loudest answer of all.

Quick Links

- Destroylist (auto-updated)
- Registrar Statistics
- NiceNIC Verdict
- Registrars Enabling Scams
- NiceNIC Investigation

Found a domain ignored by its registrar? Report it to our bot for faster disruption.

Report a Threat

Telegram Bot phish.report Ban Tool

The Scale

Our threat feed contains **50,000+** reported domains:

destroylist/content_active.txt

Key Takeaway

If 16 antivirus engines detect a domain and 13 reports are sent, and the domain stays online for 1,352 hours — the registrar's abuse department is either incompetent or complicit. There is no third option. And if they're complicit — **who compensates the victims?**
#AbuseReports #ICANN #Registrars #VirusTotal #PhishingTakedown #Investigation #CyberSecurity

Related Research

Registrars Enabling Global Scams
How NameSilo, Webnic, and NiceNic keep scam infrastructure alive by ignoring abuse reports.
NiceNIC Verdict
Every NiceNIC domain reviewed — zero legitimate uses found across the entire portfolio.
NiceNIC Investigation
Exposing IANA 3765 — the ICANN registrar powering global cybercrime with a phishing score of 1,141.74.