THREAT INTELLIGENCE REPORT

The Anatomy of a Takedown: How PhishDestroy Disrupts Cybercrime

Ref. **PD-TI-2026-02167** Published **10 July 2026** Source **phishdestroy.io/takedown-anatomy**

CYBER DEFENSE

From a fledgling initiative in 2019 to a powerhouse disrupting over 400,000 malicious domains, PhishDestroy's journey reveals the power of community, technology, and a hard-earned reputation.

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

Companion piece on Medium: A Direct War on Phishing Operations

In the relentless battle against online fraud, PhishDestroy has emerged as a critical force, evolving from a dedicated initiative in 2019 into a highly effective operation. Our mission is clear: to dismantle phishing and scam infrastructure, protecting users worldwide. This isn't just about blocking malicious links; it's about understanding the anatomy of a cyberattack and disrupting it at its core.

Our Evolution: From Weeks to Minutes

How one phishing link triggers a full takedown chain

When PhishDestroy began, taking down a malicious domain could take weeks. Over the years, we have grown, forged strong alliances, and earned the trust of key players in the cybersecurity landscape. Our

focus has always been laser-sharp on phishing, allowing us to develop specialized expertise and maintain a minimal false positive rate.

Today, what once took weeks can now be reduced to mere minutes. This acceleration is a testament to our continuous innovation and the robust reputation we've built.

The Takedown Process

1. Rapid Detection & Verification

Detection occurs through community reports via our Telegram Bot , automated monitoring, and threat intelligence feeds. Our teams swiftly verify threats to ensure a minimal false positive rate.

2. In-depth Analysis & Evidence Collection

Our analysts delve deep into the threat, identifying its characteristics, targets, and methods. This involves payload analysis, infrastructure mapping, and assessing victim impact. Every piece of evidence is meticulously documented.

3. Strategic Coordination & Action

This is where our reputation comes into play. We have built strong relationships with hundreds of hosting providers, domain registrars, and law enforcement agencies. When PhishDestroy submits a report, **more than 50 systems instantly recognize our request** . If a reported site is indeed phishing, it can be shut down within minutes.

4. Liquidation and Monitoring

The ultimate goal is complete removal. Once a takedown is initiated, we monitor the status to ensure the site is offline and remains so. Our efforts have resulted in the successful disruption of **over 500,000 malicious domains** since 2019, with continuous post-removal verification to catch resurfacing infrastructure within hours.

Operational Methodology: Automation, Accuracy, Scale

Our model combines **community reporting** with **automated detection systems** and precision analytics. The pipeline is designed to scale from a single report to thousands of takedowns per day without sacrificing quality.

- **Custom-built parsers** continuously scan SEO search results, sponsored ad placements, and Google Ads for phishing indicators — capturing threats at the moment of first paid placement.
- Identified threats are automatically submitted to **50+ antivirus vendors** and threat-intelligence feeds, maximizing global block coverage in the first minutes after detection.
- We maintain a **false-positive rate below 0.5%** , with over **100,000 validated reports** — proving our systems are not just fast, but highly accurate.
- Verified contributors who submit **100+ accurate reports** are granted *"trusted"* status, enabling direct submissions without moderation and dramatically reducing time-to-takedown for known reporters.

- A live **damage counter** estimates the financial loss inflicted on scammers — based on average domain value and promo costs (~$15/domain for typical crypto-scam setups).

Detection Sources — Where Threats Surface

Phishing infrastructure rarely hides — it advertises. We harvest leads from:

- **Telegram Bot reports** from our community via @PhishDestroy_bot — primary public intake.
- **SEO & paid-ad parsers** — Google Ads, Bing, Yandex; sponsored crypto-wallet, exchange, and bridge keywords are continuously monitored.
- **Threat-intelligence feeds** shared with us by partners and researchers.
- **Honeypot networks** and seed-phrase canary tokens that ping us when scammers try to use stolen data.
- **WHOIS & certificate transparency** monitoring for newly-registered look-alike domains targeting protected brands.

Evidence Preservation — Permanent Digital Record

Takedowns are only the first step. **Preserving evidence is our core priority** — because a deleted domain is useless to investigators if no record remains.

- Every detected domain is **archived via public scanners** (urlscan.io, Wayback Machine, our own snapshot pipelines) to capture full site fingerprints — HTML, screenshots, network calls, JavaScript payloads.
- Each operation leaves a **digital record** that is immune to deletion by attackers — published openly on GitHub destroylist and the ScamIntelLogs archive .
- Archives include scammer admin panels, Telegram chat exports, payment flows, victim records, and IOCs — supporting attribution and prosecution long after takedown.
- **While scammers wipe traces, we make them permanent.**

Allies and Adversaries Among Registrars

Speed-of-takedown depends entirely on registrar and host responsiveness. Our partner data shows a stark divide:

- **Responsive partners: Namecheap** 's 24/7 abuse team alone has helped eliminate **30,000+ malicious domains** . **GoDaddy** , **Hostinger** , **Squarespace** , and **IONOS** consistently act within hours of a verified report.
- **Persistent enablers: NiceNic** , **Cosmotown** , **NameSilo** , and **Webnic** repeatedly ignore abuse reports — effectively acting as safe havens for cybercriminal operations. See our investigation: How NameSilo, Webnic, and NiceNic Enable Global Scams .

Criminal Retaliation — Confirmation of Impact

Our effectiveness has triggered organized backlash, which we treat as proof of impact rather than disruption:

- **DDoS attacks** against our infrastructure (mitigated by Cloudflare).
- **Coordinated smear and takedown campaigns** via paid PR placements (see how paid media distorts cybersecurity).
- **Mass-reporting** of our social media accounts to silence reporting.
- Our X (Twitter) account with **140,000+ documented phishing reports** was permanently suspended after registrar pressure — see NameSilo Killed Our Twitter . The archive remains public: GitHub archive .

Criminals try to erase their tracks; we ensure their traces stay permanent.

Legal Status & Coordination

We are a **non-profit, operator collective** — not a company, not a legal entity, not affiliated with any government. Everything we do is in the open:

- All reports and evidence are published openly on GitHub, Telegram, and Mastodon — nothing is hidden or stored privately.
- In major investigations involving actor attribution, financial tracing, or infrastructure mapping, we **formally transfer full evidence packages to law enforcement or CERT teams** .
- All such transfers are made in full legal compliance and only when actionable intelligence is verified.
- We **do not store any personal data** of contributors — protecting whistleblowers from retaliation and eliminating data-breach risk.

Our role is to document and destroy malicious operations, then support those with legal authority to act on the evidence.

By the Numbers

- **500,000+** phishing & scam domains disrupted since 2019.
- **130,000+** active threats curated in destroylist .
- **50+** antivirus vendors and threat-intel platforms receive our feeds.
- **30,000+** domains removed via Namecheap partnership alone.
- **<0.5%** false-positive rate across **100,000+** validated reports.
- **140,000+** reports archived after our X account suspension.
- **888K+** community subscribers across feeds.

How You Can Help

- **Report a domain:** @PhishDestroy_bot on Telegram.
- **Subscribe to alerts:** @PhishDestroyAlerts .
- **Use our blocklist** in your firewall, DNS, or security stack: github.com/phishdestroy/destroylist .
- **Read our investigations:** Registrars enabling scams , $100K returned , 150+ fake Mozilla extensions .

> "Collective action is the strongest defense. Our journey highlights what can be achieved when technology, expertise, and community unite against cybercrime."

#CyberDefense #Takedown #Phishing #Community

Share This Article

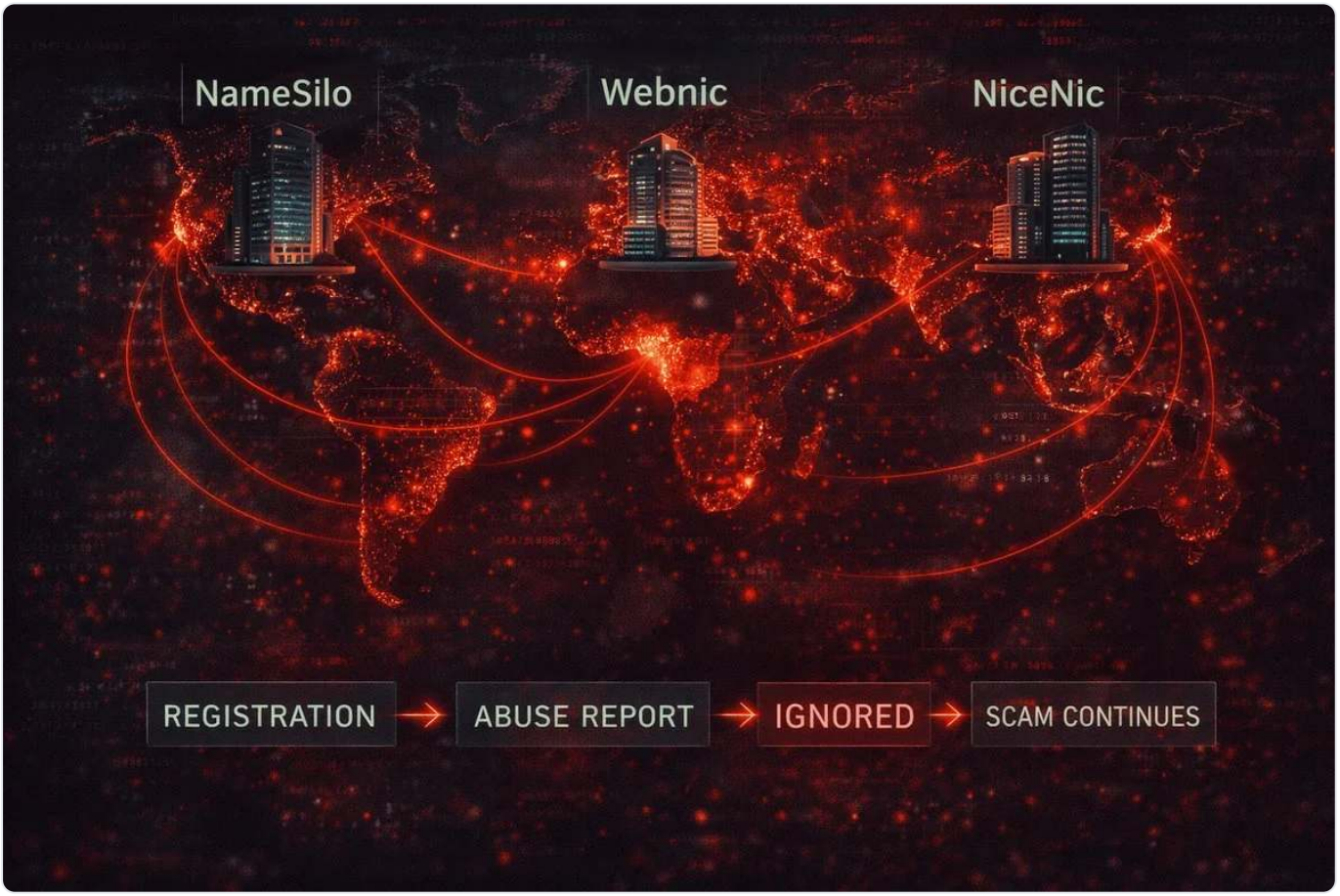
Related Investigations

INVESTIGATION

$0 Takedowns: How We Disrupt Phishing Infrastructure

METRICS

Impact Metrics: 500K+ Phishing Threats Neutralized



INVESTIGATION

NameSilo, Webnic, NiceNic: Registrars Enabling Scams