THREAT INTELLIGENCE REPORT

150+ Fake Mozilla Extensions — One Backend & Paid Media

Ref. **PD-TI-2026-82201** Published **10 July 2026** Source **phishdestroy.io/moz-fake-extensions-paid-media**

Investigation • 6—8 min read

Media blamed “Russian bears” for 150+ fake Mozilla extensions. Our findings show Nigerian infrastructure (IP 185.208.156.66), recycled phishing kits, and how paid articles helped spread the myth.

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

Read the full article on Blog

Originally published on Medium — PhishDestroy

The Misleading Narrative

A story about **"150+ fake Mozilla extensions"** tied to a supposed "Russian trail" was amplified across major crypto and security outlets. It sounds dramatic, but our analysis shows this narrative is misleading — and worse, **it shields the real perpetrators** .

150+ Low-Quality Extensions on a Single Backend

All extensions in this campaign were:

- Non-unique, copy-paste quality.
- Only logos and names varied.
- All connected to a **single backend** .

Backend IP: `185.208.156.66`

The backend domain was `alladdsite[.]digital/app.php` . Most domains tied to this IP are now dead, but archives preserved snapshots through Urlscan and WebArchive.

Our Actions Against This Campaign

As a independent threat intelligence group specializing in phishing and scam infrastructure takedowns, we:

- Submitted reports directly to Mozilla to flag malicious extensions.
- Escalated to Seal , requesting professional assistance to accelerate banning.
- Published a report on Chainabuse for community visibility.
- Injected millions of empty seed phrases into the attackers' backend to pollute stolen data.

Why This Is Not "Russian" Infrastructure

Russian-speaking threat actors typically use:

- Distributed backends (Cloudflare Workers, Firebase, Amazon, unique links per campaign).
- Obfuscation and redundancy to avoid single points of failure.

Instead, this campaign showed:

- A **Nigerian hosting provider** .
- Neighboring domains tied to bank scams, fake crypto wallets, fake delivery scams.
- A Telegram account receiving stolen data linked to a **Nigerian operator** .

"Russian groups build sophisticated infrastructures. This was cheap, centralized, and unsophisticated — exactly what we've seen before on Nigerian servers."

The Paid Media Problem

Paid media placements create serious consequences:

1. One paid article in a respected outlet gets published.
2. Hundreds of smaller sites, blogs, and Telegram channels rewrite or translate it.
3. Within days, it becomes a massive fake narrative with the illusion of credibility.

"Victims see 'the Russian trail,' believe the case is closed, and stop reporting to authorities. Real criminals remain untouched."

Example: Angel Drainer

Every major outlet ran headlines about *"Angel Drainer shutdown after devs identified."* But was it true — or just another paid placement repeated until it looked credible? For criminals, buying articles is pocket change; for victims, it changes everything.

Cybersecurity Companies Buying Their Own PR

Cybersecurity companies pay tens of thousands of dollars for articles about themselves, their research, and their impact. This raises fundamental questions:

- Why does a real cybersecurity group need to pay for coverage?
- Are they trying to bury the real hacker's trail?
- Or leverage the hacker's identity for blackmail or competitive gain?
- Is the purpose to strengthen trust — or manipulate perception for profit?

"If cybersecurity becomes another PR game, where facts are shaped by who pays more, then trust in this field collapses."

Evidence of the Market

The practice is not hidden:

- On Fiverr, Upwork, and specialized PR markets, you can directly purchase "guest posts."
- Providers send Google Sheets with dozens of outlets and prices — including well-known cybersecurity brands.
- Some promise: "for an extra fee, no sponsored label."

Stated goals for buying articles include:

- Link Building (SEO).
- Traffic & Sales.
- Brand Awareness.
- Reputation Management (burying negatives).
- Social Verification.
- Publication Lists for Visa Applications.

Costs mentioned include over **$20,000** for paid interview slots from major crypto media outlets.

"This is not journalism. It is a market — where credibility is bought and sold."

Business vs. Lies

Publishing paid content is not illegal — it's business. But when it crosses into **publishing false claims, misdirecting investigations, and disguising PR as fact** , it becomes part of the problem.

Conclusion

PhishDestroy is a independent cybersecurity initiative that doesn't get paid, sell ads, or profit. The facts are clear:

- 150+ Mozilla extensions routed to a single backend on Nigerian hosting.
- Data went to a Nigerian Telegram account.
- The "Russian trail" narrative is fabricated.
- Paid media coverage amplified this fabrication until it looked like truth.
- Even cybersecurity companies themselves pay for self-promotion.

"Selling ads is business. Selling lies as facts shields criminals. And when even cybersecurity sells narratives, the victims — and justice — lose."

Disclaimer

We are not accusing any individual, company, or media outlet. All facts are open-source and verifiable through public archives, scanners, and reports. The real question: *why are such narratives controlled and amplified? Who benefits when an unknown security company publishes an inaccurate mega-investigation that shifts attention away from real actors?*

Quick Links

- Report via Telegram bot
- Registrars Enabling Global Scams

- Crypto Drainer Networks
- Anatomy of a Takedown

Found a fake extension or paid-PR campaign hiding real criminals? Report it.

Indicators

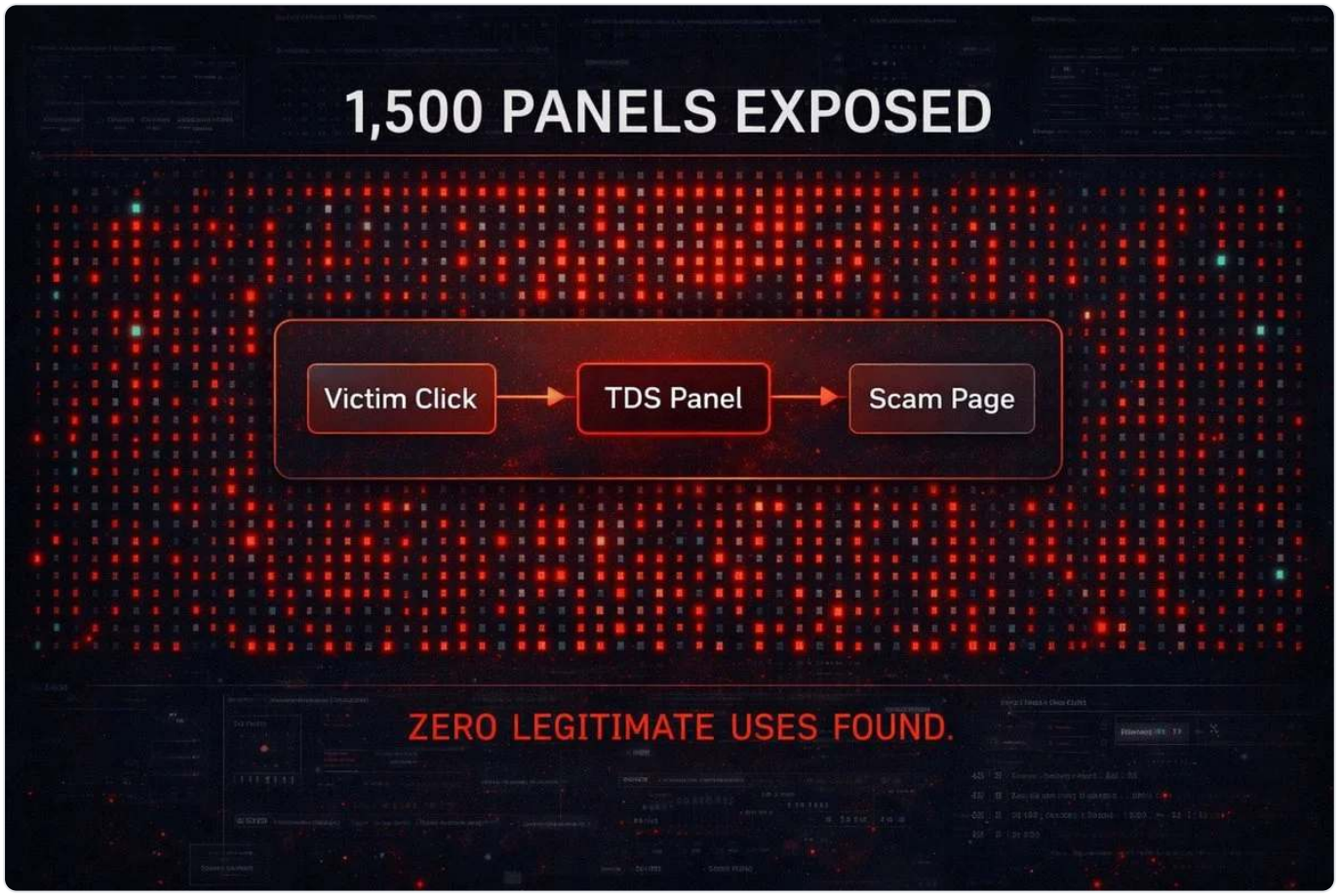
- IP: `185.208.156.66`
- Backend: `alladdsite[.]digital`
- Hosting: Nigerian provider

#MozillaExtensions #PaidMedia #Disinformation #ThreatIntel #OSINT

Share This Investigation

X / Twitter Telegram Reddit LinkedIn

Related Investigations



INVESTIGATION

Keitaro TDS: 1,500 Panels Exposed, Zero Legit Uses

INVESTIGATION

Steam BlockBlasters Malware: Platform Negligence Exposed