THREAT INTELLIGENCE REPORT

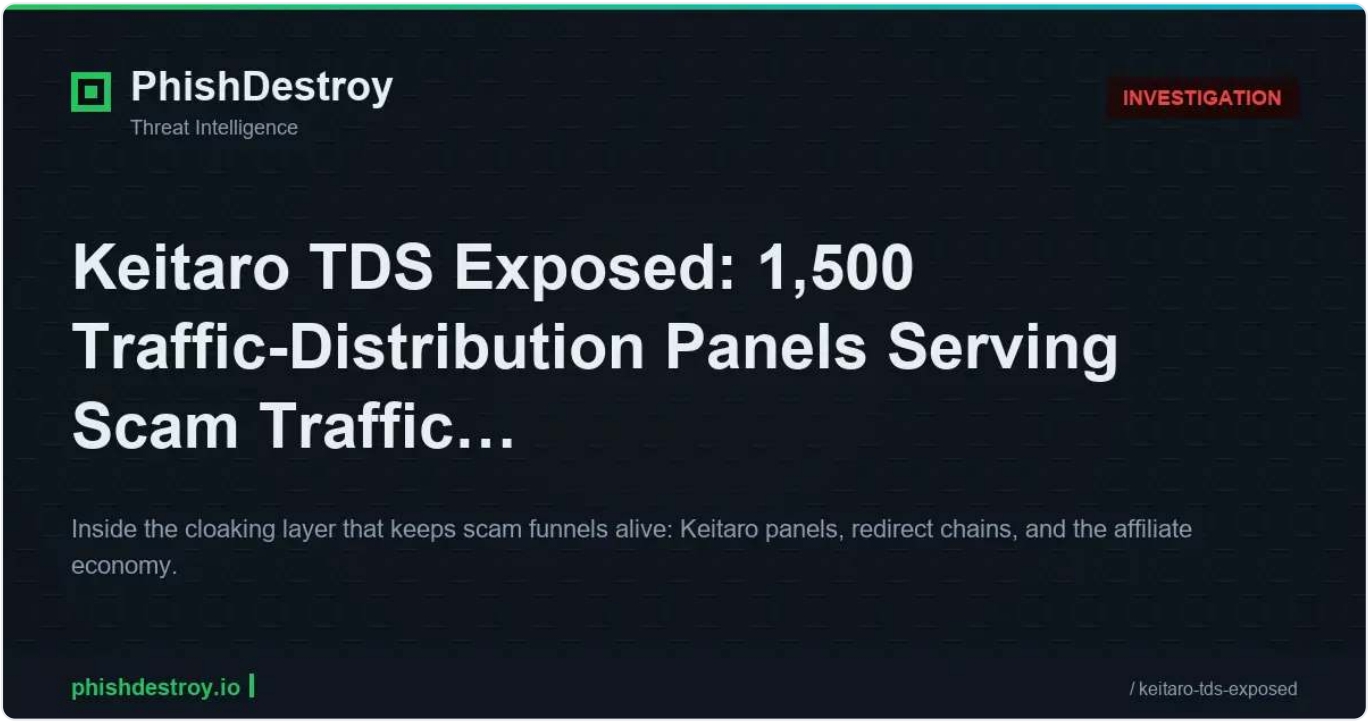
Keitaro TDS: 1,500 Panels Exposed and Zero Legitimate Uses Found

Ref. **PD-TI-2026-17698** Published **10 July 2026** Source **phishdestroy.io/keitaro-tds-exposed**

ScamIntelLogs Investigation + Tool Release

The cloaking engine behind every scam you've never seen. PhishDestroy scanned 50,000+ sites, discovered 1,565 Keitaro TDS admin panels, and found zero legitimate deployments. Every single panel was connected to crypto fraud, phishing, malware distribution, or worse. Clients include EvilCorp, LockBit ransomware, and VexTrio. Open-source detection toolkit, 7-point methodology, and full panel CSV now released.

~10 min read · Updated **March 2026** · PhishDestroy Intelligence
1,565 Panels Found 100% Malicious Rate 7 Detection Methods 4 Tools Released



0
Admin Panels Found
50,000+
Sites Scanned
0%
Legitimate Uses
7
Detection Methods

What Is Keitaro TDS?

Keitaro TDS is a commercial Traffic Distribution System sold by **Apliteni OU** , a company incorporated in **Estonia** . On the surface, it markets itself as a traffic management tool for affiliate marketers. In practice, it is the single most widely deployed cloaking engine in the global scam ecosystem.

Cloaking is the art of showing different content to different visitors. When a security researcher, ad reviewer, or law enforcement officer visits a URL, Keitaro identifies them and serves a clean, innocent page. When a real victim visits the same URL, they get redirected to crypto scams, phishing pages, malware downloads, or fraudulent e-commerce sites. The victim never sees the clean version. The analyst never sees the scam.

Keitaro's pricing ranges from **€40 to €400 per month** , positioning it as enterprise-grade fraud infrastructure. It stores visitor data for up to **9.75 years** , giving operators a massive dataset of victim fingerprints, geographic data, and behavioral profiles. All of this data is stored on **AWS infrastructure** , meaning Amazon is unknowingly hosting the backend for thousands of scam operations.

Corporate Shell

Apliteni OU operates from Estonia, leveraging the country's e-Residency program and favorable corporate privacy laws. The company maintains a veneer of legitimacy through professional marketing, documentation, and customer support — while every measurable deployment of their product is connected to criminal activity. They charge €40–400/month for what is effectively a scam-as-a-service platform with nearly a decade of data retention.

The Numbers: 1,565 Panels, Zero Legitimate

PhishDestroy's investigation began with a simple hypothesis: if Keitaro TDS has legitimate uses, we should find them at scale. We scanned **50,000+ sites** using a combination of automated tools and manual verification, specifically looking for Keitaro TDS fingerprints. What we found was unambiguous.

1,565 active Keitaro admin panels were discovered. We analyzed every single one. The result: **zero legitimate deployments** . Not one panel was being used for lawful affiliate marketing, A/B testing, or any other benign purpose. Every panel — 100% — was connected to criminal activity.

1,565
Active Panels
100%
Malicious Rate
50K+
Sites Scanned
9.75yr
Max Data Retention

Abuse Categories Breakdown

The 1,565 panels were distributed across six primary abuse categories. Many panels served multiple categories simultaneously, using Keitaro's traffic routing to direct victims to different scam types based on geography, device, or time of day.

Abuse Category	Description
Crypto Scams	Fake investment platforms, wallet drainers, pig-butchering landing pages
Phishing	Credential harvesting for banks, email providers, social media
Malware Distribution	Loader delivery, ransomware staging, drive-by downloads
E-commerce Fraud	Fake shops, counterfeit goods, payment card skimming
Dating Scams	Romance fraud, sextortion landing pages, fake profiles
Gambling Fraud	Unlicensed casinos, rigged betting platforms, deposit theft

Methodology Note

Every panel was verified through at least two independent detection methods before being classified. False positives were manually reviewed and excluded. The 1,565 count represents only confirmed, active Keitaro installations — the true number of deployments, including those behind additional layers of protection, is certainly higher.

Criminal Client Roll Call

Keitaro TDS isn't just used by small-time scammers. It is the cloaking infrastructure of choice for some of the most dangerous cybercriminal organizations on the planet. Here are the documented clients:

EvilCorp

The sanctioned Russian cybercrime syndicate uses Keitaro to bust through international sanctions. By cloaking their operations behind Keitaro's traffic distribution, EvilCorp evades the very security controls designed to shut them down. Every click routed through Keitaro is a sanctions violation enabled by Apliteni OU's software.

LockBit Ransomware

The LockBit ransomware group leveraged Keitaro for malware distribution, using its cloaking capabilities to ensure that only genuine targets received ransomware payloads while security sandboxes and researchers saw benign content. Keitaro was a force multiplier for one of the most destructive ransomware operations in history.

VexTrio

The largest known Keitaro client. VexTrio operates with **60+ affiliates** and controls **86,832+ domains** , all funneling traffic through Keitaro's distribution engine. This single operation represents a massive portion of the internet's malicious ad traffic, and Keitaro is the backbone that keeps it invisible.

ClearFake

ClearFake injects fake browser update prompts into compromised websites, delivering malware when victims click "Update." Keitaro's cloaking ensures that only real visitors see the malicious overlay — security scanners see the original, clean website. The result: malware delivery with near-zero detection rates.

FakeBat

FakeBat is a malware loader distributed through malicious advertising campaigns. Keitaro routes ad traffic through a decision engine: security tools get redirected to legitimate software download pages, while real users are served trojanized installers. Keitaro makes FakeBat's malvertising campaigns virtually invisible to ad platform safety teams.

Doppelganger

A Russian state-linked disinformation campaign that uses Keitaro to distribute propaganda across Western social media. Keitaro's geographic and device fingerprinting ensures that content moderators and fact-checkers see different content than targeted populations. Information warfare, powered by commercial Estonian software.

"We found Keitaro fingerprints in every major cybercrime operation we investigated in the past 18 months. It's not a coincidence — it's the industry standard for criminals."

— PhishDestroy Research Team

7-Point Detection Methodology

Over the course of this investigation, PhishDestroy developed seven independent methods for identifying Keitaro TDS deployments. Each method targets a different fingerprint that Keitaro leaves behind, and together they form a comprehensive detection framework that is now available as open-source tooling.

1. `/click_api/v3` Endpoint

Keitaro's core API endpoint for processing click events. This path is hardcoded into the software and present on every installation. Probing for this endpoint is the single fastest way to confirm a Keitaro deployment. A 200 or 302 response at this path is a near-certain positive identification.

2. `_lp` / `_token` / `_subid` URL Parameters

Keitaro appends distinctive tracking parameters to URLs during redirect chains. The `_lp` parameter identifies the landing page, `_token` carries session authentication, and `_subid` tracks sub-affiliate sources. These parameters are unique to Keitaro and rarely appear in legitimate traffic management systems.

3. Keitaro-Specific Cookies

Keitaro sets distinctive cookies to track visitor sessions and maintain cloaking state. These cookies follow naming conventions that differ from standard analytics platforms, making them identifiable through browser inspection or automated cookie analysis.

4. Response Header Patterns

Keitaro's server responses contain distinctive HTTP header patterns, including specific cache-control directives, custom headers, and server identification strings that differ from standard web servers. These headers persist even when operators attempt to customize their installations.

5. JavaScript Redirect Chains

Keitaro implements multi-stage JavaScript redirects to evaluate visitor fingerprints before deciding whether to show the scam or the clean page. These redirect chains follow predictable patterns — specific variable names, timing sequences, and evaluation logic — that can be detected through static and dynamic JavaScript analysis.

World heat map: 1,565 Keitaro TDS panels detected across the globe, 0 legitimate uses found

6. Domain Pattern Analysis

Keitaro operators tend to register domains following predictable naming conventions and registration patterns. Bulk domain analysis reveals clusters of domains with similar WHOIS data, registration dates, nameserver configurations, and hosting providers — all pointing back to coordinated Keitaro deployments.

7. Admin Panel Fingerprinting

Keitaro admin panels are accessible at known paths and return distinctive HTML structures, CSS class names, and JavaScript files. Even when operators change the default login URL, the panel's frontend framework leaves identifiable artifacts that can be detected through path enumeration and content fingerprinting.

Defense In Depth

No single detection method is foolproof. Sophisticated operators may disable or modify individual fingerprints. That's why the 7-point methodology works as a layered system — even if an operator eliminates three or four signatures, the remaining methods will still flag the deployment. In our testing, every Keitaro panel was detectable by at least four of the seven methods.

Global Infrastructure Map

The 1,565 Keitaro panels are distributed across a global hosting infrastructure that favors cheap VPS providers and jurisdictions with slow abuse response times. Here's where the panels live:

Region	Hosting Providers	Notes
United States	DigitalOcean, Vultr	Largest concentration of panels. US-based hosting provides fast response times for North American victims.

Region	Hosting Providers	Notes
Netherlands	Various VPS	Popular for European-targeted campaigns. Permissive hosting policies.
Germany	Hetzner, various	Major hub for EU-targeted phishing and e-commerce fraud operations.
Russia	Various bulletproof	Home base for many operators. Hosting providers with zero abuse enforcement.
United Kingdom	Various cloud	Used for targeting UK financial institutions and government services.
Hong Kong	Femo cluster	Distinct cluster of panels associated with Asian-targeted crypto scams. The "Femo cluster" operates as a coordinated group.

US Dominance

The United States hosts the largest concentration of Keitaro panels, primarily on DigitalOcean and Vultr. These are mainstream cloud providers that process abuse reports — but the volume of deployments and the speed at which operators spin up new instances means abuse teams are perpetually playing catch-up.

The Femo Cluster

A distinct cluster of Keitaro panels operating from Hong Kong infrastructure, targeting Asian markets with crypto scams and gambling fraud. The "Femo cluster" shows coordinated deployment patterns suggesting a single operator or organized group managing dozens of panels simultaneously.

AWS Backend

Regardless of where the frontend panels are hosted, Keitaro's core data storage runs on **Amazon Web Services (AWS)** . This means visitor fingerprints, redirect logs, and targeting data for potentially millions of scam victims are sitting on Amazon infrastructure. With data retention of up to 9.75 years, AWS is hosting one of the largest scam victim databases in existence.

Open-Source Tools Released

Alongside this investigation, PhishDestroy is releasing a complete open-source detection toolkit. Every tool is free, requires no API keys, and can be deployed immediately. The full dataset of 1,565 panels is included.

checker.html
Web-based Keitaro panel checker. Open in any browser, enter a URL, and get instant detection results. No installation required. Uses the 7-point methodology client-side.

keitaro_hunter_4.py
Python scanner for bulk Keitaro detection. Feed it a list of domains and it runs all 7 detection methods, outputting confirmed panels with confidence scores. Designed for security teams and researchers.

worker.js
Cloudflare Worker for real-time Keitaro detection. Deploy to your Cloudflare account and it intercepts requests in real-time, flagging Keitaro-cloaked traffic before it reaches users. Zero-latency protection

at the edge.

panels.csv

Complete dataset of all 1,565 confirmed Keitaro admin panels. Includes IP addresses, hostnames, detection methods triggered, hosting providers, and geographic data. Updated regularly.

Full Evidence Repository

All tools, data, and evidence are published at phishdestroy.github.io/ScamIntelLogs/keitaro/ . The repository is public and will be updated as new panels are discovered. Community contributions and additional detection methods are welcome.

#KeitaroTDS #TrafficDistribution #Malvertising #ScamInfra #Investigation

Related Research

Fake Casino Epidemic: 5 Panels Exposed

Comparative anatomy of 4 casino PaaS operations with 383 verified victims across 30+ countries.

Crypto Drainer Toolkit Exposed

How TRXDrop and NiceCrypto weaponize wallet connections to steal crypto assets.

TheProject: $10M Scam Empire

Inside the scam empire running industrialized fraud operations at massive scale.

Scam Teams Compared

Side-by-side comparison of organized scam team structures, tools, and operational methods.

PhishDestroy Tools & Services

Full suite of open-source detection, analysis, and reporting tools for security researchers.

Anatomy of a Takedown

Step-by-step walkthrough of how we take down phishing infrastructure.