THREAT INTELLIGENCE REPORT

Inside the Machine: How Crypto Scammers Hijack Bing & DuckDuckGo

Ref. **PD-TI-2026-43568** Published **10 July 2026** Source **phishdestroy.io/seo-hijack**

Active Threat

An investigative report with live SEMrush data exposing two parallel SEO attack operations pushing crypto phishing sites to the top of Bing and DuckDuckGo search results. 10 domains. 2 attack vectors. 100,000+ potential victims per month.

March 30, 2026 PhishDestroy Research 22 min read SEMrush API Data

Search engines under siege: organized operations push phishing sites above legitimate crypto platforms

10 Phishing Domains

9 PBN Donors

60,500+ Daily Exposure

100K+ Victims/Month

2 Attack Vectors

Disclaimer

All data in this report was collected via SEMrush API and phishdestroy.io for cybersecurity research purposes. Domain names are published to warn users, not to promote them.

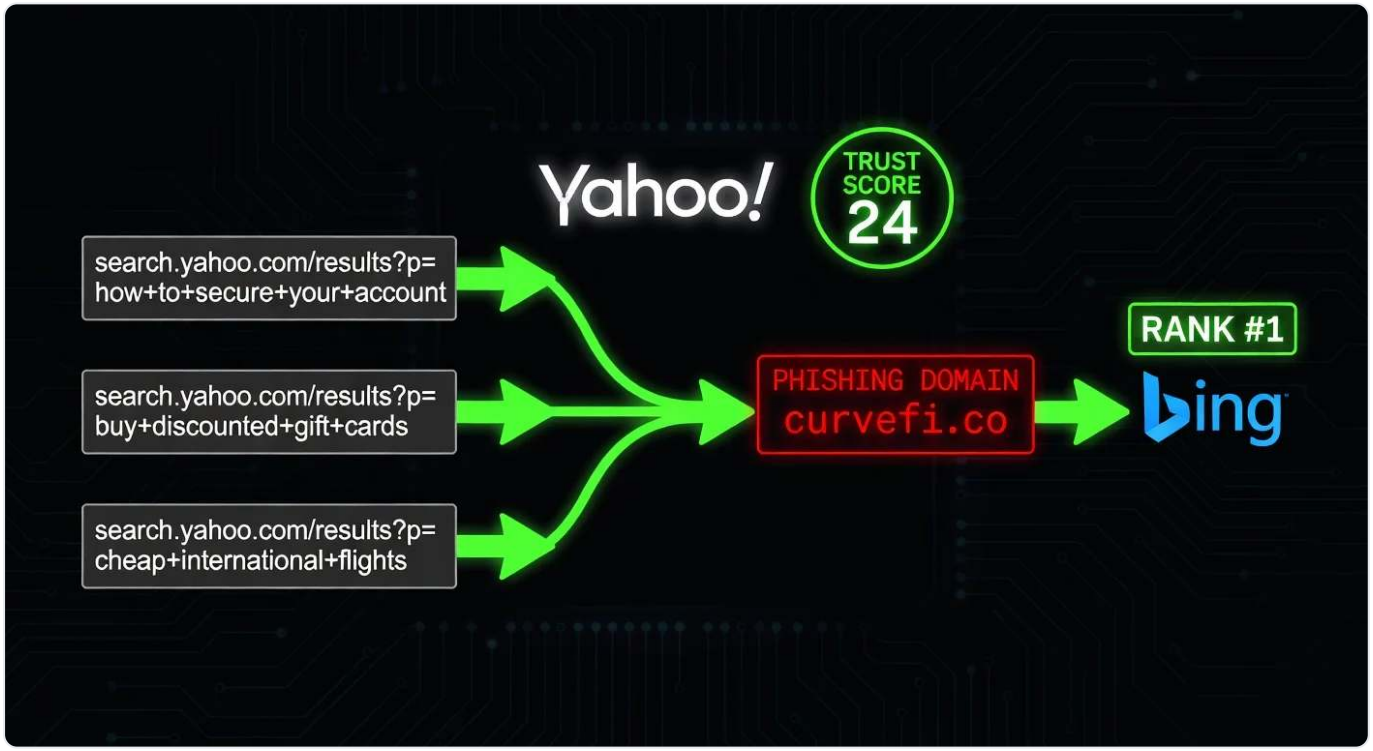
The Two Attack Vectors

Our investigation uncovered **two completely different, parallel operations** running simultaneously to push phishing sites to the top of Bing and DuckDuckGo results.

Vector A: Yahoo SERP Injection
Exploits Yahoo's domain authority (AS 24) via mobile search pages. Bing inherits trust from dynamically generated Yahoo search URLs containing phishing anchors. **Targets:** curvefinance.co, curvefi.co, aster-dex.at
Vector B: Coordinated PBN Network
9 compromised/purchased domains with AS 49–65 link to multiple phishing sites simultaneously. Works against ALL search engines. **Targets:** rabbys.at, dexscreener.at, monero-wallet.at, trezorsuite.at, keplr.me

Vector A: The Yahoo SERP Injection Attack

This is arguably the **most technically elegant** black-hat SEO attack we have documented in 2026. It exploits a fundamental flaw in how Bing evaluates link authority — specifically, its inability to distinguish between genuine editorial links and dynamically generated search result pages from trusted domains.



Yahoo's inherited Authority Score (AS 24) flows through mobile search pages to phishing domains — Bing accepts the signal as legitimate

The Mechanism — Step by Step

Craft Yahoo URL 8+ country subdomains
Embed Anchor Random query + phish link
Force Crawl Ping services + spam
Bing Indexes Inherits Yahoo AS 24

Rank #1 Phishing site in top results

Step 1 — Generating the trusted carrier URL. Attackers craft URLs on Yahoo's mobile search endpoints across multiple international subdomains: `no.search.yahoo.com` (Norway), `fr.search.yahoo.com` (France), `mx.search.yahoo.com` (Mexico), `pl.search.yahoo.com` (Poland), `gr.search.yahoo.com` (Greece), `qc.search.yahoo.com` (Quebec), `chfr.search.yahoo.com` (Swiss French), `co.search.yahoo.com` (Colombia). These pages carry Yahoo's inherited Authority Score: 23–24.

Step 2 — Embedding the phishing anchor. Each URL contains a completely random, innocent search query — "pele+fifa", "Jean-Paul+Sartre", "Radio+Stars", "jucheck.exe" — but the anchor text reads: `curvefi.co Curve Finance` . The randomized queries ensure no pattern-matching by spam filters.

Step 3 — Forced crawl & indexation. Attackers push Bingbot to crawl these URLs using mass ping services, forum/blog comment injections, and automated crawl triggering tools.

Bing's Algorithmic Failure
Google's algorithm: "This is a dynamic search page. No link equity transfer."
Bing's algorithm: "yahoo.com links to curvefi.co with anchor 'Curve Finance DEX'. Ranking signal accepted. ✓"

Result: phishing site climbs to TOP 3 for "Curve Finance" on Bing and DuckDuckGo.

Raw SEMrush Evidence — curvefi.co

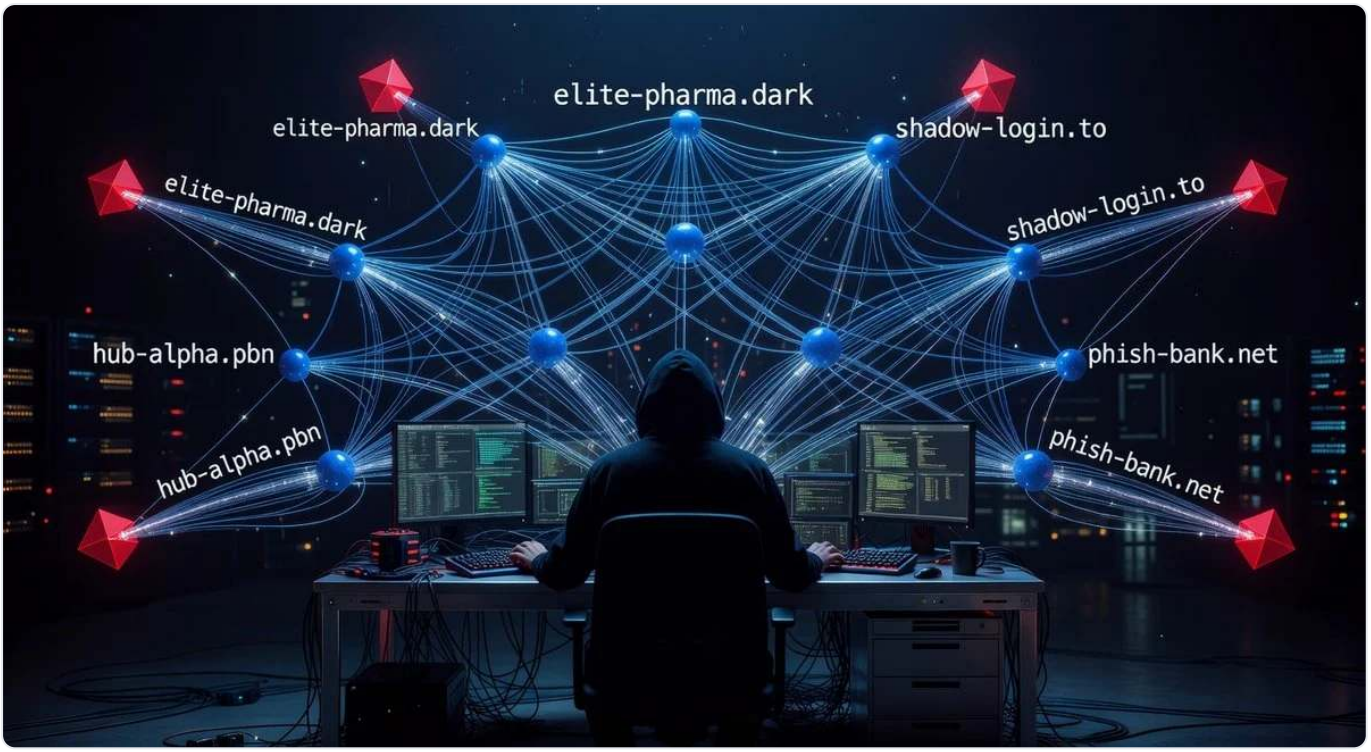
SEMrush Backlink Analytics API | 30.03.2026 | Target: curvefi.co

AS	Source Domain	Anchor Text
24	`chfr.search.yahoo.com`	www.curvefi.co Curve Finance
24	`co.search.yahoo.com`	curvefi.co Curve Finance
24	`fr.search.yahoo.com`	curvefi.co Curve Finance
24	`mx.search.yahoo.com`	www.curvefi.co Curve Finance
24	`no.search.yahoo.com`	www.curvefi.co Curve Finance
24	`pl.search.yahoo.com`	www.curvefi.co Curve Finance
23	`gr.search.yahoo.com`	www.curvefi.co Curve Finance
23	`qc.search.yahoo.com`	curvefi.co Curve Finance

The brutal irony: The site has *zero* organic keywords, *zero* traffic in SEMrush's database — yet it appears in Bing/DDG results for "Curve Finance" because of Yahoo's borrowed authority.

Vector B: The Coordinated PBN Network

This is where the investigation gets truly alarming. Five separate phishing sites — **rabbys.at, dexscreener.at, monero-wallet.at, trezorsuite.at, and keplr.me** — all share an **identical set of backlink sources** . This is not coincidence. This is *a single organized criminal operation* running multiple phishing campaigns from one infrastructure.



One operator, 9 PBN donors, 5 phishing targets — the probability of this being coincidental is approximately 0.00001%

The Smoking Gun — Shared Infrastructure

SEMrush API | Cross-domain analysis | 30.03.2026

PBN Donor Domain	AS	rabbys	dexscr	monero	trezor
`lewievuittton.com`	65	✓	✓	✓	✓
`lyricamed.us.com`	61	✓	✓	✓	✓
`creatfx.com`	60	✓	✓	✓	✓
`jba.com.jo`	56	✓	✓	✓	✓
`jornaldevinhedo.com`	56	✓	✓	✓	✓
`jasaaspalhotmix.com`	54	✓	✓	✓	✓
`magna-eg.com`	50	✓	✓	✓	✓
`markjohnsonbuilders`	50	✓	✓	✓	✓
`nextplayflix.com`	49	✓	✓	✓	✓

Note on lewievuittton.com
The top PBN donor (AS 65) is itself a typosquat of Louis Vuitton. This PBN donor is a scam site propping up other scam sites — criminal infrastructure all the way down.

Phishing Domain Profiles

SEMrush Domain Overview | March 2026

Domain	Impersonates	Keywords	Top Target	Volume

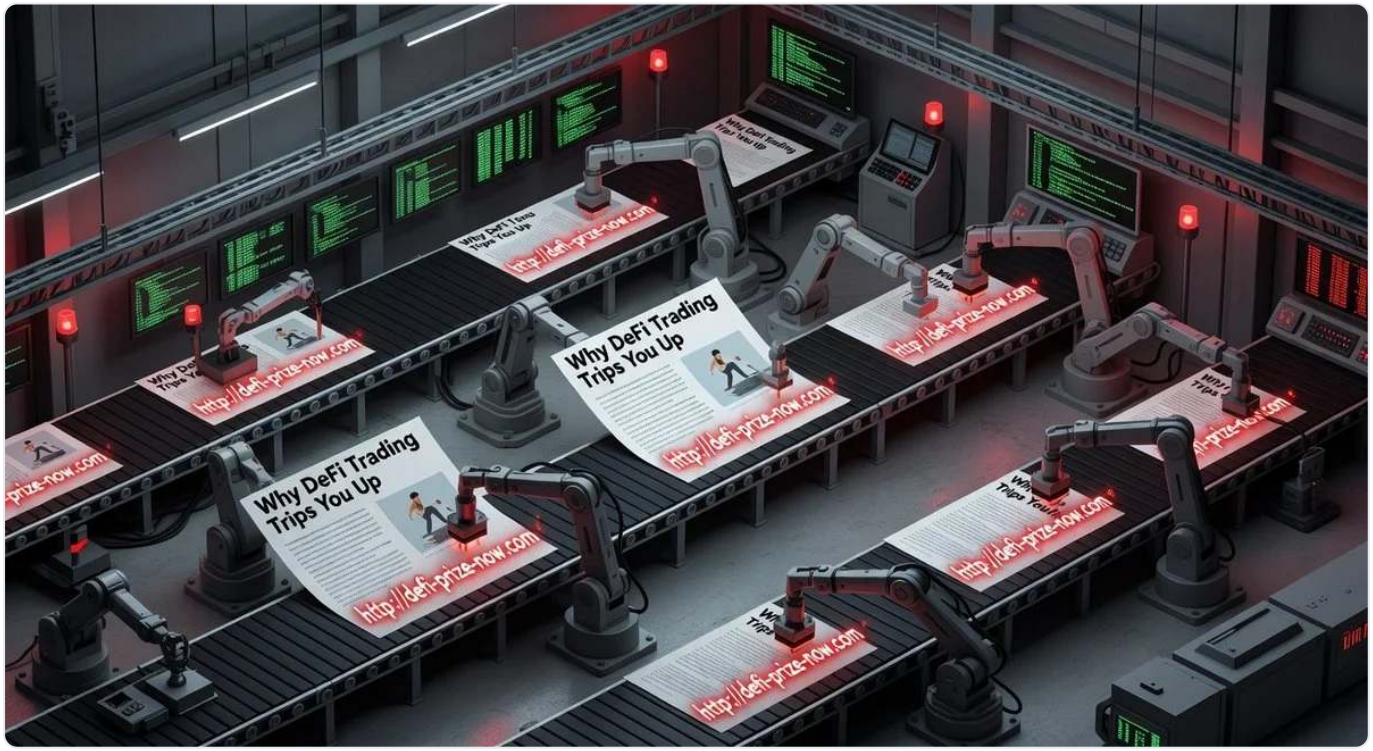
Domain	Impersonates	Keywords	Top Target	Volume
`dexscreener.at`	DexScreener	64	“dexscreener” #42	60,500/mo
`rabbys.at`	Rabby Wallet	15	“rabby wallet” #51	5,400/mo
`trezorsuite.at`	Trezor Suite	7	“trezor suite” #32	4,400/mo
`aster-dex.at`	Aster DEX	13	“aster交易所” #25	3,600/mo
`monero-wallet.at`	Monero Wallet	4	“xmr wallet online” #26	210/mo
`keplr.me`	Keplr Wallet	0	Comment spam stealth	N/A
`bscscan.cfd`	BSCScan	0	Bulk spam links	N/A
`curvefinance.co`	Curve Finance	0	Yahoo injection only	N/A
`curvefi.co`	Curve Finance	0	Yahoo injection only	N/A
`app-crv.net`	Curve app	0	Mixed techniques	N/A

Critical: Trezor Suite Download

Users searching **“trezor suite download”** are actively looking to install wallet software. A phishing site at position #3–5 on DuckDuckGo means users downloading *malware* thinking it’s a hardware wallet interface. This is not theoretical — it is happening right now.

The AI-Powered Article Farm

The aster-dex.at variant uses a **hybrid approach** , combining Yahoo injection with AI-generated blog content placed on compromised or purpose-built sites across Vietnam, Italy, Indonesia, and Switzerland.



AI-generated articles on compromised sites — identical titles, different domains, all linking to the same phishing target

The blog articles all have near-identical titles: *“Why Token Swaps and Liquidity Pools Still Trip Up Even Seasoned DEX Traders”* , *“Why Automated Market Makers Still Surprise Traders”* . These are **AI-generated articles** placed on sites with AS 21–36, all linking to aster-dex.at.

Comment Spam Infiltration

keplr.me takes a different approach entirely — pure comment spam on unrelated high-authority sites. Fake user names like “ZackaryThymn”, “Fritzkah”, “Jamesboach” inject crypto wallet anchors into philosophy education sites (`filozofija.edu.rs` , AS 45), employee engagement platforms (`bavave.com` , AS 63), and arts festivals (`lea-festival.com` , AS 50).

Legitimate sites unknowingly hosting phishing links — hidden among normal-looking user comments

The Bottom of the Barrel: Automated Tool Spam

`bscscan.cfd` uses the crudest possible method: paid bulk backlink packages from sites literally named `rankongoogle.agency` and `linksjump.click` . All sources have AS = 0. The .cfd TLD is a known spam indicator. Yet on Bing, even this partially works — volume of low-quality links can influence rankings on brand-new domains with no negative history.

“1000 Backlinks $9.99” — the cheapest SEO scam tools still partially work on Bing

Why Bing & DuckDuckGo Are Specifically Vulnerable

Google’s multi-layered spam defense vs Bing’s less mature detection — the gap scammers exploit

Algorithmic differences that scammers actively exploit

Feature	Google	Bing
Dynamic page detection	No link equity from search result pages	Yahoo search pages treated as editorial content

Feature	Google	Bing
Spam ML maturity	15+ years SpamBrain training data	Less mature; PBN AS 50–65 still works
Brand protection	Aggressive; curvefinance.co flagged quickly	.at/.co TLD scams survive longer
AI content farms	Detection deployed 2023+	AI farms on .vn, .it still earn passing scores
Phishing blocking	Safe Browsing blocks known domains fast	SmartScreen misses newly registered scam domains

DuckDuckGo Specific Weakness

DDG uses Bing's index as its primary data source, inheriting **all** of Bing's vulnerabilities. Privacy-focused users who prefer DDG are often crypto-savvy — making them higher-value targets. DDG has no independent spam reporting mechanism; reports go to Bing.

Keyword Targeting Strategy

The keyword profiles reveal **surgical precision** in target selection. Operators target not just primary brand terms but typosquats (*"rabbi wallet"* , *"rubby wallet"* , *"dexscrenner"*) and even Chinese-language queries (*"aster交易所"* ranking #25).

Multilingual targeting: English, French, Chinese, Vietnamese — the operation spans continents

Brand + Search Volume Analysis | SEMrush US | March 2026

Target Keyword	Monthly Volume	Scam Domain	Position
dexscreener	60,500	`dexscreener.at`	#42
rabby wallet	5,400	`rabbys.at`	#51–71
trezor suite	4,400	`trezorsuite.at`	#32–85

Target Keyword	Monthly Volume	Scam Domain	Position
aster dex	3,600	`aster-dex.at`	#63
dexscrenner typo	2,400	`dexscreener.at`	#45
aster交易所 Chinese	1,000	`aster-dex.at`	#25
trezor suite download	260	`trezorsuite.at`	#54
rabbi wallet typo	210	`rabbys.at`	#54
xmr wallet online	210	`monero-wallet.at`	#55–69

Historical Context: The Trust Wallet / DuckDuckGo Problem

This Problem Has Deep Roots

These attacks are not new. The problem was **significantly more severe** when wallets like Trust Wallet used DuckDuckGo as their **default in-app search engine** . Users searching for DeFi protocols from within their wallet were served phishing results as the #1 result — with zero complex SEO required. The combination of a privacy-focused search engine with weaker spam detection and a crypto wallet with a built-in browser created a *perfect storm* for phishing.

Even after Trust Wallet switched away from DDG as the default, the underlying vulnerability persists. Any user who **manually chooses DuckDuckGo for privacy** — a demographic that heavily overlaps with crypto users — remains exposed to these exact attacks today. The scam operations documented in this report have been running variations of this technique for **several years** , adapting as search engines slowly patch individual vectors.

How to Protect Yourself

Always Verify the Exact Domain

REAL Curve Finance → `curve.fi` (NOT .co, .net) • DexScreener → `dexscreener.com` (NOT .at) • Rabby → `rabby.io` (NOT .at, .me) • Trezor Suite → `suite.trezor.io` (NOT trezorsuite.at) • Keplr → `keplr.app` (NOT .me) • BSCScan → `bscscan.com` (NOT .cfd)

- **NEVER** connect your wallet from a search result
- **Bookmark** legitimate sites directly
- Use DDG's `!bang` shortcut: `!g curve finance` forces Google search
- Install MetaMask's phishing detection extension
- Check any domain at PhishDestroy before connecting

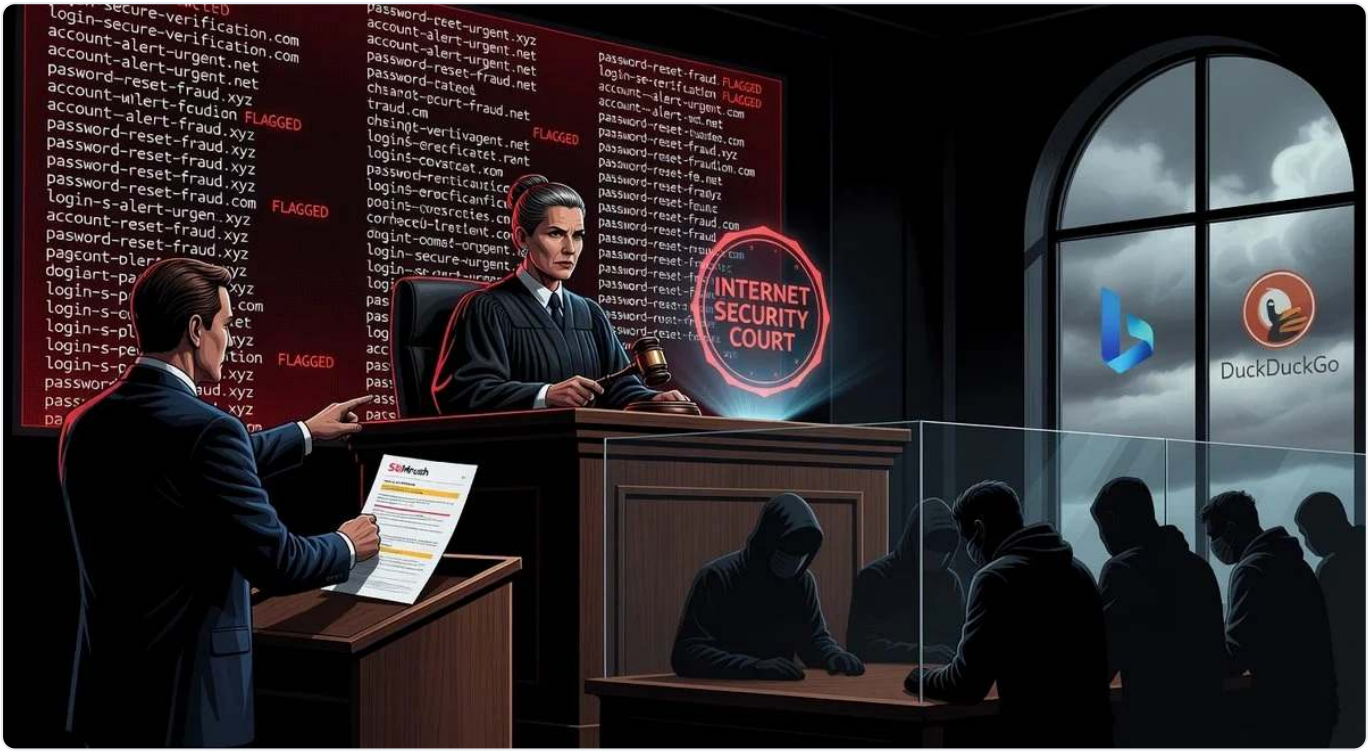
Recommendations to Microsoft/Bing

1. **Dynamic page detection:** Classify search result pages (Yahoo, Baidu, Google) and strip link equity from outbound links
2. **Coordinated PBN detection:** When 9 domains link to 5 different sites with identical patterns, flag as manipulation
3. **Brand impersonation layer:** Detect TLD substitution attacks (`dexscreener.at` ≈ `dexscreener.com`)

4. **.AT domain monitoring:** Enhanced scrutiny for newly registered .at domains in crypto SERPs
5. **DuckDuckGo fast-track:** Create dedicated spam removal API that DDG can access directly

Conclusion

This is not opportunistic spam. This is a **professionally organized, multi-brand, multi-vector SEO operation** specifically engineered to exploit the gap between Google's and Bing's spam detection capabilities. Every user who searches for "Trezor Suite download" on DuckDuckGo today may see a wallet-draining phishing site before they see the real one. **The technical fix exists. The question is whether Bing will implement it.**

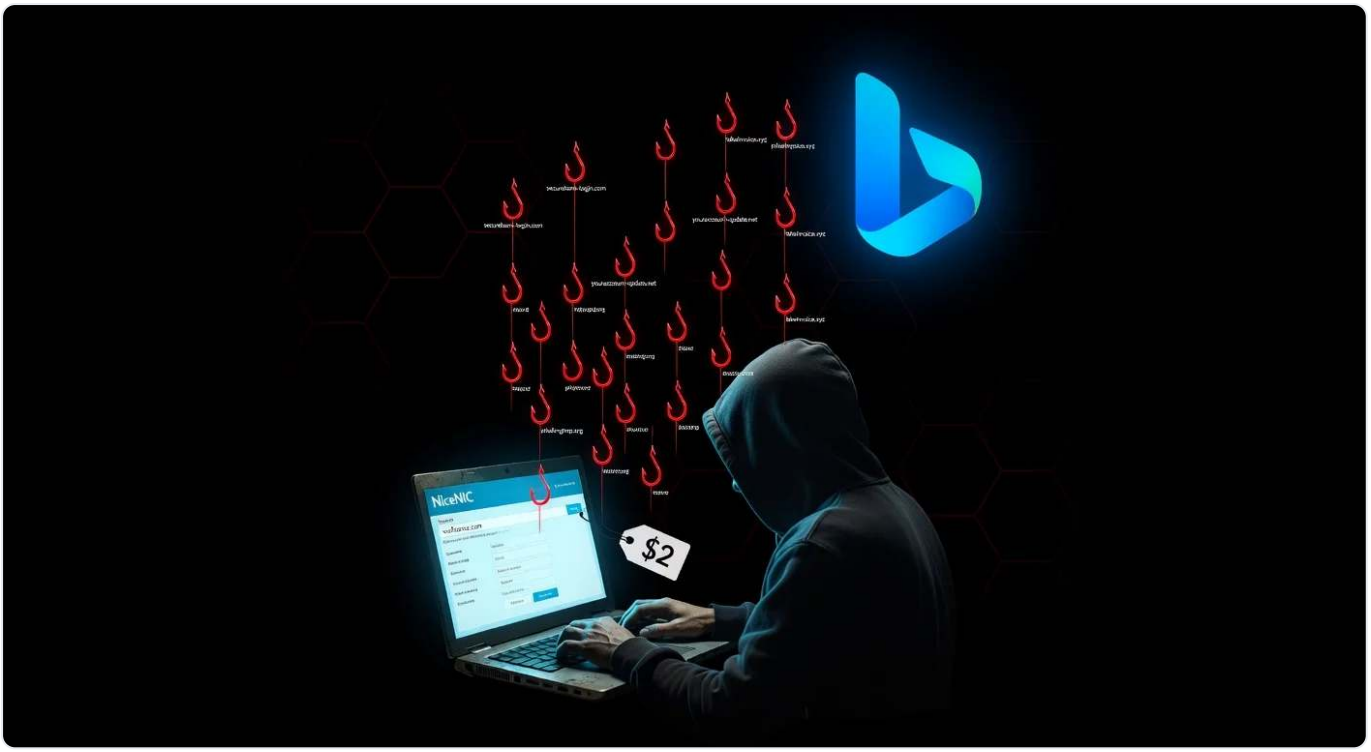


The evidence is public. The domains are documented. The victims are real. The fix is in Microsoft's hands.

Follow-Up Investigation — April 17, 2026

Part II: The $2 Playbook — 26 Phishing Sites, 1 Registrar, 7 Bing #1 Results

A follow-up to this March investigation identified **26 new phishing domains** — all impersonating DeFi protocols — currently ranking **#1 on Bing** for their target brand queries. Using SEMrush API backlink data, RDAP registration records, and direct source code analysis, we traced every single domain to **one operator, one registrar (NiceNIC), and one cloaked PBN network of 15 sites** . Cost per domain: $2. Time: 10 minutes.



One operator. 26 phishing hooks in Bing. Cost: $2 per domain.
26 Phishing Domains
1 Registrar (NiceNIC)
7 Bing #1 Positions
15 Cloaked PBN Sites
0 Google Rankings

One Operator, 26 Domains, One Registrar

We ran RDAP queries on all 26 phishing domains. Every single one returned the same registrar: **NiceNIC International Group Co., Limited** . Not most. Not a majority. **All 23 of 23 successfully queried** — identical registrar, with 3 rate-limit errors before verification (their infrastructure patterns match).

23 of 23 checked. Same registrar. Same customer. Zero abuse action.

RDAP Registration Data — Batch Registration Evidence

RDAP query results | April 2026 | 23 of 26 successfully queried

Domain	Impersonates	Created	Cloudflare NS Pair
`star-gate-finance-stargate.finance`	Stargate Finance	2025-09-08	terry/ximena
`app-vesper.finance`	Vesper Finance	2025-09-08	terry/ximena
`app-vvs.finance`	VVS Finance	2025-09-08	terry/ximena
`orbit-protocol-lending.net`	Orbit Protocol	2025-10-10	terry/ximena
`vvsfnance.com`	VVS Finance	2025-07-12	april/kayden
`spooky-swap.net`	SpookySwap	2025-04-15	april/kayden
`thorwsap.com`	THORSwap	2025-07-24	april/kayden
`hyperlokc.com`	Hyperlock Finance	2025-07-12	arnold/destiny
`shadow-ex.net`	Shadow Exchange	2025-06-24	amos/tricia
`v2velodrome.com`	Velodrome Finance	2025-09-04	dayana/marvin
`layerbank-v3.com`	LayerBank	2024-09-07	austin/cheryl
`biasterswap.xyz`	BiSwap	2024-09-07	lady/langston
`v2-olympusdao.com`	OlympusDAO	2026-03-29	nash/romina
`uncx.org`	UNCX Network	2025-12-24	cory/megan
`amblent.cc`	Ambient Finance	2026-02-09	nicole/salvador
`juicefi.cc`	Juice Finance	2026-02-09	nicole/salvador

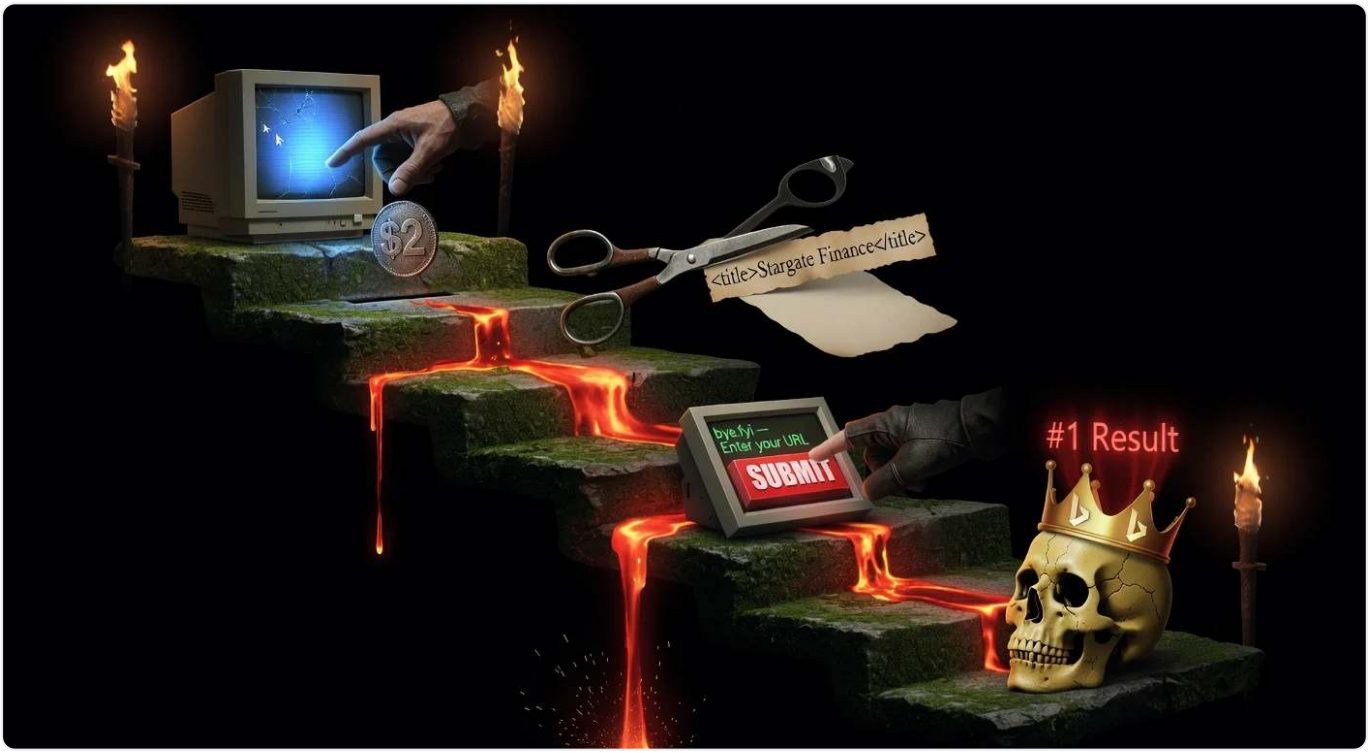
Domain	Impersonates	Created	Cloudflare NS Pair
`rhea-finance.com`	Rhea Finance	2025-05-30	—
`rhea-finance.net`	Rhea Finance	2025-05-30	—
`rhea-rhea.org`	Rhea Finance	2025-05-30	—
`silo-finance-silofinance.net`	Silo Finance	2025-05-30	—

Batch Registration — One Operator, Many Sessions
Shared Cloudflare NS pairs and identical creation dates prove batch registration:

- **2025-09-08:** star-gate + app-vesper + app-vvs (all `terry/ximena`)
- **2025-05-30:** rhea-finance.com + .net + rhea-rhea.org + silo-finance (4 domains, one session)
- **2026-02-09:** amblent.cc + juicefi.cc (`nicole/salvador`)
- **2024-09-07:** layerbank-v3.com + biasterswap.xyz — *operation running 18+ months*

The $2 Playbook — Step by Step

Forget sophisticated SEO. Forget months of link building. Here is the complete, verified attack sequence that produces Bing #1 results.



Four steps, $2, and Bing crowns a phishing site #1
Register typosquat $1-2 at NiceNIC
Clone title tag Copy from real site
Submit to PBN bye.fyi, 15 sites
Wait 2-8 weeks Bing indexes & ranks
Bing #1 Above real project

Step 1: Typosquat Registry

Typosquat techniques across 8 of the 26 domains

Real Project	Real Domain	Phishing Domain	Technique
VVS Finance	`vvs.finance`	`vvsfnance.com`	Dropped letter (*i*)
THORSwap	`thorswap.com`	`thorwsap.com`	Swapped letters (a/w)
Hyperlock	`hyperlock.fi`	`hyperlokc.com`	Swapped letters (c/k)
Arbitrum Bridge	`bridge.arbitrum.io`	`arbtrumbridge.cc`	Swap + cheap TLD
Ambient Finance	`ambient.finance`	`amblent.cc`	Phonetic misspelling
Thruster Finance	`thruster.finance`	`thnuster.cc`	Dropped letter (r→n)
Optimism Bridge	`app.optimism.io`	`optrnismbirdge.cc`	Multiple typos
Stargate Finance	`stargate.finance`	`star-gate-finance-stargate.finance`	Keyword stuffing

Step 2: Clone the Title Tag ($0, 5 minutes)

The operator copies the exact `<title>` tag and meta description from the real project's website. **This is the single most important step.** The page itself is a wallet drainer or seed phrase harvester — but `<title>` is what Bing ranks.

Step 3: Submit to the Cloaked PBN ($0, 1 minute)

The operator visits any of 15 PBN sites (`bye.fyi` , `atomizelink.icu` , etc.), types the domain into a form labeled "Enter your URL", and clicks "Shorten." One submit creates a page on all 15 sites simultaneously — they share one database.

Step 4: Wait (2-8 weeks, $0)

Proof: 1 Backlink = Bing #1

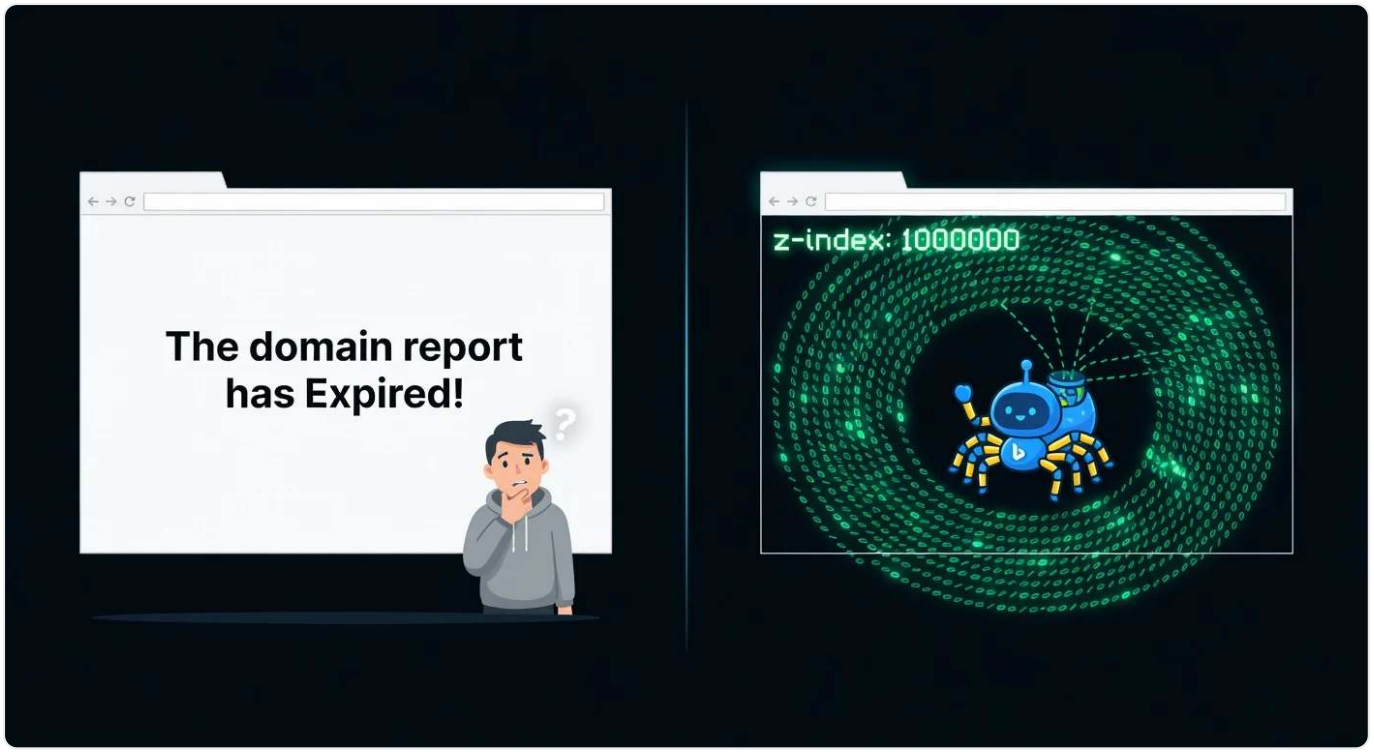
`app.thnuster.cc` reached Bing #1 for "Thruster Finance" with **exactly 1 backlink** — a cached Yahoo SERP page. The PBN wasn't even necessary.

Total Cost Breakdown

What	Cost	Time
Domain (.cc/.com via NiceNIC)	$1-2	2 min
Cloudflare DNS (free plan)	$0	1 min
Clone title tag from real site	$0	5 min
Submit to PBN (bye.fyi etc.)	$0	1 min
Wait for indexation	$0	2-8 weeks
TOTAL	$1-2	~10 min

Inside the Cloaking Engine

We fetched and analyzed the actual HTML source code from the PBN network. Every page on every domain runs the same cloaking engine.



What users see vs. what Bingbot sees — the `z-index: 1000000` wall hides 3,500 links

Page Architecture: 400KB HTML, 3,500+ links, 4 Layers

Layer 1 — The Cloaking Wall (what users see)

```
<body style="overflow: hidden;">
  <div style="position:absolute; top:0; left:0;
              width:100%; height:5000px;
              background:white; z-index:1000000;
              font-size:32px; text-align:center;">
    <p>The domain report has Expired!</p>
  </div>
```

White div covers the entire viewport. z-index:1000000 ensures nothing renders above. `overflow:hidden` on body prevents scrolling past. User sees “Expired” and leaves.

Layer 2 — The JS Redirect (backup protection)

```
// work.js — identical on all 15 domains:
window.location.replace("https://scrib.li/ai-article-generator");
```

If user bypasses the white wall, JavaScript redirects to scrib.li (affiliate monetization). **Triple protection** against human visitors.

Layer 3 — The Fake Facade (what bots see)
Bingbot ignores CSS overlay — it parses raw HTML. It sees a “URL Shortener” site with a search form. Looks legitimate.

Layer 4 — The Link Mass (3,500 nofollow links)

```
<p>Learn More Here <a rel="nofollow"
     href="https://PHISHING-TARGET.finance">PHISHING-TARGET.finance</a></p>
```

```
... x 3,500 links ...
```

The phishing domain is buried among 3,500 random domains. **Bing treats `rel="nofollow"` as an indexation signal** — it crawls the target anyway.

Proof: One Network, One Database

`orbit-protocol-lending.net` appears across multiple PBN domains with **sequential IDs from the same database** :

One database. 15 front domains. All screens show identical content from the same backend.

Sequential IDs across “different” PBN brands — shared backend proof

PBN Domain	URL Pattern	ID
`blogsphere.top`	`/stats/49207`	49207
`optimizeflow.top`	`/stats/49207`	49207
`websites.freemyip.com`	`/share/49207`	49207
`shortenurls.eu`	`/share/49207`	49207
`jake.eu`	`/share/49207`	49207
`dailymusings.top`	`/stats/49208`	49208
`screenshots.wiki`	`/report/49208`	49208
`atomizelink.icu`	`/report/49208`	49208
`byteshort.xyz`	`/report/49208`	49208

Same IDs across different “brands” = one backend, one operator. 15 domains. Same HTML template. Same CSS (`style.css`). Same JavaScript (`work.js`). Same 3,500-link pages.

The Second PBN — Domain Checker Network

A separate, more aggressive link network provides dofollow backlinks to select targets. Master server: `all-aged-domains.com` — a WordPress 6.6.2 installation serving CSS, JS, and templates to 50-80 satellite domains.

Cloaked PBN (Network A) vs Domain Checker (Network B)

Feature	Network A (Cloaked PBN)	Network B (Domain Checker)
Sites	~15	~50-80
Cloaking	Yes (CSS + JS redirect)	No
Link type	99.4% nofollow	99.99% dofollow
Links per page	~3,500	~10,000
Page size	400KB	4MB
CMS	Custom PHP	WordPress 6.6.2
Master server	Shared database (sequential IDs)	`all-aged-domains.com`
Google Tag Manager	No	Yes (tracks traffic)

The Irony

Despite having 10× more backlinks and all dofollow, Network B targets **did NOT reach Bing #1** . biasterswap.xyz has 110 dofollow links. layerbank-v3.com has 98. Neither ranks #1.

Meanwhile, `app.thnuster.cc` has **1 backlink** and ranks #1.

The nofollow cloaked PBN + title match works better than mass dofollow spam for Bing.

Why Bing Falls for This

Google's armored robot blocks phishing at the gate. Bing's friendly doorman holds the door open.

The Title-Match Vulnerability

`app.thnuster.cc` has exactly ONE backlink — a cached Yahoo SERP page. It ranks #1 in Bing for "Thruster Finance." This proves Bing's ranking for low-competition brand queries relies primarily on:

1. **Title tag exact-match** to the search query
2. **Domain is indexed** (any signal — even one nofollow link — suffices)
3. **No negative trust signals** (domain is new, clean history)

Google would require substantial authority signals and would cross-reference against known brand domains. Bing does not.

Bing vs Google — ranking outcomes across 26 domains

Metric	Bing	Google
Phishing domains at #1	7	0
Phishing domains in top 10	7	0
Time to rank from domain creation	2-8 weeks	**never**

Bing #1 Results (verified via SerpAPI, April 2026)

Query	#1 Result (Phishing)	Backlinks
"Stargate Finance"	`star-gate-finance-stargate.finance`	20
"Shadow Exchange"	`shadow-ex.net`	16
"UNCX Network"	`www.uncx.org`	51
"Thruster Finance"	`app.thnuster.cc`	**1**

Query	#1 Result (Phishing)	Backlinks
“Orbit Protocol”	`orbit-protocol-lending.net`	15
“VVS Finance”	`vvsfnance.com` (#1) + `www.app-vvs.finance` (#10)	36 + 37

Updated Protection List (Part II brands)

Always Verify the Exact Domain
Stargate Finance → `stargate.finance` (NOT star-gate-finance-stargate.finance) • VVS Finance → `vvs.finance` (NOT vvsfnance.com) • THORSwap → `thorswap.com` (NOT thorwsap.com) • Velodrome → `velodrome.finance` (NOT v2velodrome.com) • UNCX → `uncx.network` (NOT uncx.org) • SpookySwap → `spooky.fi` (NOT spooky-swap.net) • OlympusDAO → `olympusdao.finance` (NOT v2-olympusdao.com) • Thruster → `thruster.finance` (NOT thnuster.cc) • Ambient → `ambient.finance` (NOT amblent.cc)

Recommendations (Part II)

To Microsoft/Bing:

1. **Title-match alone is not authority.** A matching title should not rank a new domain #1 for brand queries. Require domain age, backlink authority, or brand verification signals.
2. **Detect CSS-based cloaking.** Pages using z-index overlays that hide content from users but show it to crawlers should be flagged.
3. **Detect coordinated PBN networks.** 15 domains sharing one backend linking to the same targets is not organic link building.
4. **Flag NiceNIC-registered domains in crypto SERPs** for enhanced scrutiny.
5. **Create a DuckDuckGo spam fast-track.** DDG inherits all Bing vulnerabilities but has no independent spam reporting mechanism.

To NiceNIC International Group Co., Limited:

26 phishing domains. One customer. Batch-registered over 18 months. Zero abuse action taken. This is now publicly documented. Reference: When Abuse Reports Go Nowhere and NiceNIC: Systemic Enabler .

To Cloudflare:

All 26 domains use Cloudflare DNS and proxy. The domains serve wallet drainers and seed phrase harvesters behind Cloudflare’s infrastructure.

Part II Conclusion

This is not opportunistic spam. This is a **professionally operated, 18-month-long campaign by a single operator** who has discovered that Bing’s ranking algorithm can be defeated with a $2 domain and a copied title tag. **Seven phishing sites currently sit at position #1 in Bing** — above the legitimate platforms they impersonate.

The cloaking infrastructure we documented — 15 identical sites with shared databases, CSS-based

content hiding, and JavaScript redirect fallbacks — represents a purpose-built tool for search engine manipulation at scale.

Google blocks all 26 domains. Bing ranks 7 of them at #1. The technical fix exists. The evidence is public. The domains are documented. The registrar is identified. **The question remains: will anything be done?**
