



Malanta:

MALANTA RESEARCH · TECHNICAL REPORT

Different Brands. The Same Traffic Machine.

Malanta flagged 466 brand lookalikes for sending visitors to flagged destinations. Their shared nameservers exposed one operator's infrastructure of about 115,000 domains. It imitates brands in every sector and dozens of markets, screens its visitors, and sells their visits to whoever pays, including, in one observed case, a malware dropper. Sector relevance alone can miss the platform.

Malanta Research Team; Yossi Dantes

20 Oct 2026 · Data cutoff 20 Oct 2026 · About 20 minutes

AT A GLANCE

What Malanta found

466

brand lookalikes flagged by Malanta's signals

all but one with at least two independent signal families

18 · 76

industry sectors · brand markets

133 organizations among the seeds; every sector category in the wider footprint

11 · 20

nameserver domains · nameserver IPs

one family, registered 2009-2022

≈115,000

domains on the operator's nameservers

20 Oct 2026; full list in the indicator CSV

Contents

- 01 Executive summary
- 02 Not my sector?
- 03 Key findings
- 04 From signals to shared infrastructure
- 05 One operator's infrastructure
- 06 Every sector, many markets
- 07 Who sees what
- 08 Threats running on the infrastructure
- 09 Flagged months before it woke up
- 10 What was already known
- 11 Who gains what
- 12 Defensive implications
- 13 Methodology
- 14 References
- A Indicator appendix

OBSERVATION WINDOWS

Signals and seed redirects: 6-13 Oct 2026

Expansion and enrichment: 8-20 Oct

Followed visits: 19 Oct

Malware encounter: 20 Oct

PUBLICATION

Malanta Research Team; Yossi Dantes

20 Oct 2026

Data cutoff 20 Oct 2026

About 20 minutes

EXECUTIVE SUMMARY

Executive summary

Threat-intelligence programmes that filter for actors targeting one sector or region can miss a shared traffic platform that serves all of them.

What we found.

Malanta's lookalike monitoring flagged 466 brand lookalikes that redirected visitors to already-flagged destinations. Shared private nameservers opened about 115,000 front domains on 11 linked nameserver domains (20 nameserver IPs). About 28% of the fronts are lookalike names. The seeds alone impersonate 133 organizations in 18 industry sectors; the wider footprint imitates brands with main markets in 76 countries.

How it works.

Domain owners park inventory on the platform. The operator screens visitors and sells visits through ad feeds. Buyers decide the landing: affiliate and search ads, adult and gambling offers, unanalysed downloads, or, in one observed case, a fake-CAPTCHA macOS dropper with a blockchain dead-drop.

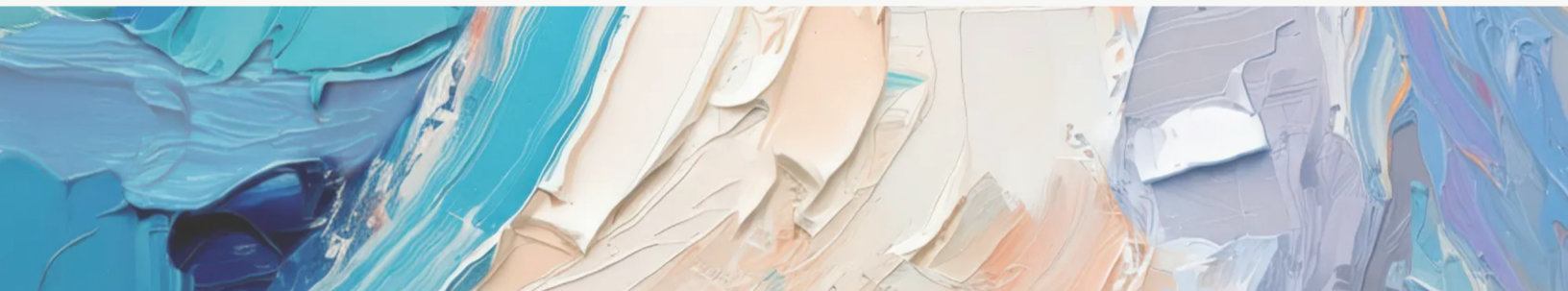
Why sector filters fail.

The operator does not select targets by sector. Brand sector mostly changes which offer is attached. Visitor location, device, and buyer delivery rules decide who is exposed.

What to do.

Correlate across sectors. Act on relationships (nameserver family, parking networks, gate fingerprint, seller identifiers), not only per-domain verdicts. Test suspicious domains with several visitor profiles. Block confirmed threat hosts; treat shared ad-tech and CDNs with care. Full indicators and RPZ guidance are in the appendix.

Data cutoff 20 Oct 2026. Confidence labels appear on each key finding below.



01

Not my sector?

Many threat-intelligence programmes still filter for "actors that target our sector in our region". Sector relevance alone can fragment the view of shared infrastructure.

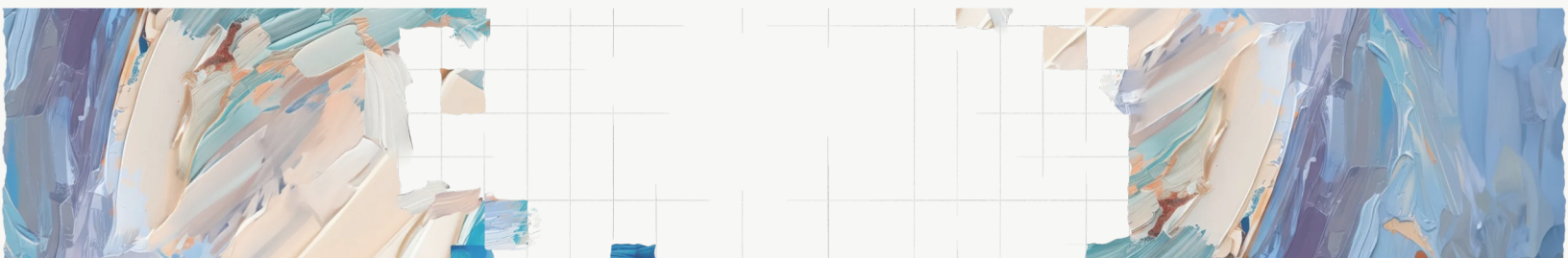
This investigation started from 466 brand lookalikes Malanta flagged in October 2026. Each redirected visitors to a destination that was already flagged. Together they impersonate 133 organizations in 18 industry sectors. Their shared private nameservers opened a wider footprint: about 115,000 domains that imitate brands with main markets in 76 countries.

The operator does not pick targets by sector. It collects typing mistakes across brands, sorts visitors by device and location, and sells their visits to whoever bids. Those domains imitate banks and credit bureaus; retailers and software vendors; insurers and health services; government portals and gaming sites.

What a visitor finally receives depends on who buys the visit. On 20 October 2026, a Malanta researcher opened [iuntuit\[.\]com](#), Intuit's name with an extra letter inserted, in an ordinary browser. The browser was redirected to a page that showed a familiar "I am not a robot" check. Clicking it silently copied a command to the clipboard, and the page asked for it to be pasted into a terminal.

Decoded, the command downloads a script that installs a hidden macOS launch agent. That agent looks up its command server in a smart contract on the Polygon blockchain, then fetches and runs whatever that server sends. Two weeks earlier, a visit to the same domain from a cloud address had found only a parking-style search page.

This report follows how Malanta's pre-attack signals, correlated across sectors, exposed the platform behind apparently unrelated lures.



02

Key findings

01

From individual signals to shared infrastructure

Malanta's lookalike monitoring flagged 466 brand lookalikes for sending visitors to destinations that were already flagged. All but one carried at least two independent families of signals: lexical, registration, mail, content and reputation. Together they impersonate 133 organizations in 18 industry sectors. Their shared nameservers led to the wider infrastructure.

[High](#)

02

One infrastructure behind them

A reverse nameserver lookup from the seeds' nameservers listed about 115,000 domains delegated to 11 linked nameserver domains. About 32,000 of the 115,000 (28%) are lookalike domain names. Shared nameservers alone could mean a reseller, so we checked further. 99.9% of the domains' address records point to 125 dense parking addresses tied to this family. The nameserver domains share registration batches and servers, and the front domains arrived in bulk waves, each moved onto one nameserver domain. A shared gate fingerprint appeared across the family on tested domains, and sampled domains on six of the nameserver domains shared one observed publisher account.

[High for a shared platform](#)

03

Every sector, many markets

The imitated brands span every sector category we use, and main markets in 76 countries. The front domains sit on 193 top-level domains, including country domains of 30 countries. US brands dominate, but no sector or region is excluded.

[High](#)

04

Visitors are screened, then sold

In controlled visits with different visitor profiles, the same domain sent different visitors to different places, and we captured each redirect chain. Visits that looked like crawlers, scripts or data-centre traffic got parking pages. Selected real-user profiles were handed to ad feeds, which ran their own browser checks.

[High, on the tested domains](#)

05

What the visits reached

Seen at the end of the operator's routes: **confirmed malicious**: a fake CAPTCHA that installs a macOS dropper with a blockchain dead-drop resolver; **not analysed**: a MEGA download behind a six-day-old redirector, and an Android app outside Google Play; **commercial**: brand-keyword search pages, adult and gambling offers, and paid or affiliate links to at least 19 brands' own sites.

[High for the dropper's behaviour](#) · [Medium for how the visit reached it](#)

06

Flagged months before it woke up

A batch of 25 domains, registered on one day in September 2025 and flagged by Malanta that November and December, sat parked for about eight months. Then, in late August 2026, Quad9 saw its lookups jump to about seven times those of comparable domains, together, for about three weeks.

[High for the pattern](#) · [Low-Medium for the cause](#)

07

Earlier research, extended

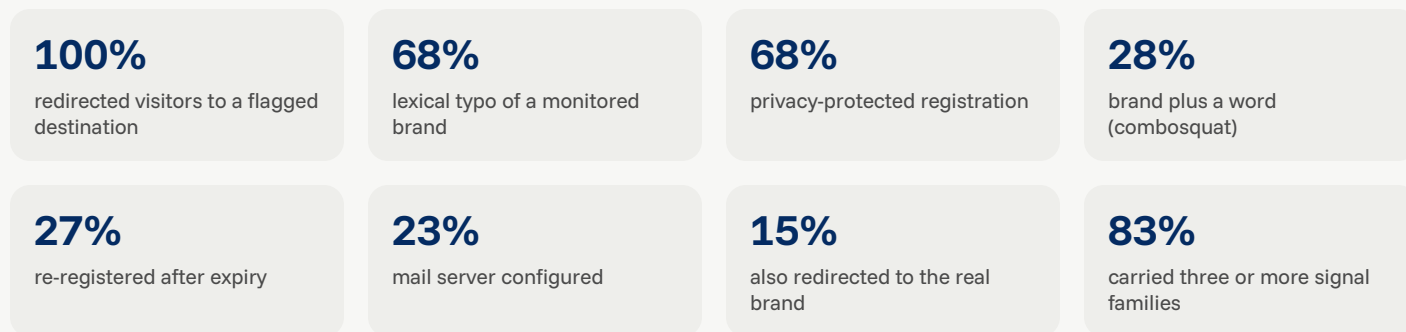
Infoblox reported two of the 11 nameserver domains in December 2025, as two different actors. This research places both, and nine more, on one co-located infrastructure.

[Medium for a single platform beneath Infoblox's two actors](#)

From individual signals to shared infrastructure

Lookalike domain names closely imitate the domain of a specific popular website, for example with a one-character typo, a swapped domain ending or a missing "www." dot. Attackers use them to deceive users. Malanta's lookalike monitoring watches for domains that imitate monitored brands. It scores them on independent evidence families, so that a single coincidence cannot convict a domain.

This investigation started from 466 lookalikes that it flagged in October 2026. Each sent visitors to a destination that was flagged at the time, by Malanta reputation or by multiple public DNS blocklists. Each seed had its own profile:



None of these signals is damning alone. Typos are common, privacy services are everywhere, and expired names are bought and sold every day. What made them worth following was what they shared: all 466 delegated DNS to private-label nameservers: ten nameserver domains with unrelated names that turned out to belong to one family.

The seeds were not aimed at one industry. The shares below are of the seeds whose imitated organization has a recorded sector, 82% of them. An organization can belong to more than one sector, so the shares add up to more than 100%:



≈2% or less each: communications, insurance, automotive, transport, commercial services, education, chemicals, healthcare, aerospace, pharma, defence

Among the impersonated brands were QuickBooks, TransUnion, Walmart, YouTube, Ticketmaster, GEICO, Coinbase, Scotiabank, Yandex and Marriott.

From signals to infrastructure

Each stage uses different evidence. Boxes are not to scale.

1 · SIGNALS

466

lookalikes, each with its own suspicious signals

Each redirected visitors to a flagged destination; all but one carried at least two independent signal families. 133 imitated organizations, 18 sectors.

2 · CORRELATION

11

linked private nameserver domains

The seeds sat on ten of them. Same-day registrations, shared nameserver addresses and nameservers inside the parking networks link them, and an eleventh, into one family.

3 · EXPANSION

≈115,000

domains delegated to the family

Reverse nameserver lookup in Malanta DNS data. Checked against hosting (99.9% on 125 dense parking addresses in 21 networks), registration records and tests on sample domains.

Figure 1. The discovery path. (1) Malanta's lookalike monitoring flagged the seeds on their own signals. (2) Their nameserver delegations pointed to ten private nameserver domains, which registration and server records linked, with an eleventh, into one family. (3) A reverse nameserver lookup in Malanta DNS data listed every domain delegated to the family. Address records, WHOIS and tests on sample domains were then used to check that link (section 4). Source: Malanta lookalike evidence, DNS, hosting and registration data, 6-20 Oct 2026.

04

One operator's infrastructure

On 20 October, **about 115,000 domains** were delegated to 11 private-label nameserver domains: domains that run nameservers for one customer base rather than selling DNS to the public. Ten of them carry live delegations. The eleventh, [squirreldns\[.\]com](#), still resolves to the same servers as [redfoxdns\[.\]com](#), but its former domains have moved to [redfoxdns](#) or left the family.

How the set was built. Membership is defined by delegation: a domain is in the set if its current nameserver records name one of the 11 nameserver domains. We listed those domains with a reverse nameserver lookup over Malanta's DNS data on 20 October. Shared nameservers alone could mean a reseller serving unrelated customers, so we tested the link further with:

- the domains' address records;
- the nameserver domains' registration and server records;
- WHOIS;
- behaviour on tested domains.

The table below lists what each check showed.

No single link below proves common control. Taken together, they point to one shared platform.

Converging evidence that the nameserver domains form one operator's infrastructure (Malanta data and live DNS, 19-20 Oct 2026)

Strand	What we observed	What it shows on its own
Nameserver registration batches	Nameserver domains registered on the same day: <code>redfoxdns</code> , <code>badgerdns</code> , <code>squirreldns</code> (27 Jun 2022, animal names); <code>tacomadc</code> , <code>redmondcd</code> , <code>rentondc</code> (17 Dec 2015, Washington-state city names).	Planning by one hand, weakly
Domain acquisition waves	Grouped by the nameserver domain they use today, the front domains arrived in waves, each through one dominant registrar: <code>tacomadc</code> in 2018-19 and <code>redfoxdns</code> in 2019-21, through Media Elite; <code>badgerdns</code> from 2022, through CommuniGal and Tucows, peaking in September-December 2025; <code>redmondcd</code> in August-October 2025, through OnlineNIC. On single days, one registrar added up to several hundred names that all point to the same nameserver domain. About a fifth of dated domains arrived in same-day groups of 50 or more.	Bulk, planned acquisition feeding specific nameserver domains
Shared servers	<code>squirreldns[.]com</code> resolves to exactly the two nameserver IPs of <code>redfoxdns[.]com</code>	One DNS operator for both nameserver domains
Network proximity	Ten of the eleven nameserver domains have a nameserver host in the same /24 network as dense parking servers. <code>ns1.hastydns[.]com</code> shares a /28 with twelve of them. The front domains of each nameserver domain point to their own address block, and those blocks sit side by side at seven hosting providers.	Provisioning by the same hands or reseller
Hosting concentration	99.9% of the domains' address records point to 125 parking addresses, each serving at least 20 of the domains, in 21 networks.	Dedicated parking infrastructure for this family, not a general-purpose host
Lookalike inventory	About 32,000 of the 115,000 (28%) are lookalike domain names. Every nameserver domain with live delegations carries them, from about 16% to 54% of its front domains.	The same kind of inventory across the family, weakly
Shared gate	The same loading page and signed token appeared on tested domains across the family, in samples taken on 8 and 19 Oct	The same software at the front door, where it appears
Shared routes	Typos on six different nameserver domains were all sent through the same redirector, <code>rhcdom[.]com</code> , to the same search page	One routing configuration across nameserver domains
Seller identifier	One ad-feed publisher account (<code>publisher=230041</code> , <code>pubfeed=965920</code>) on traffic from sampled domains across six nameserver domains	One commercial account monetizing those domains

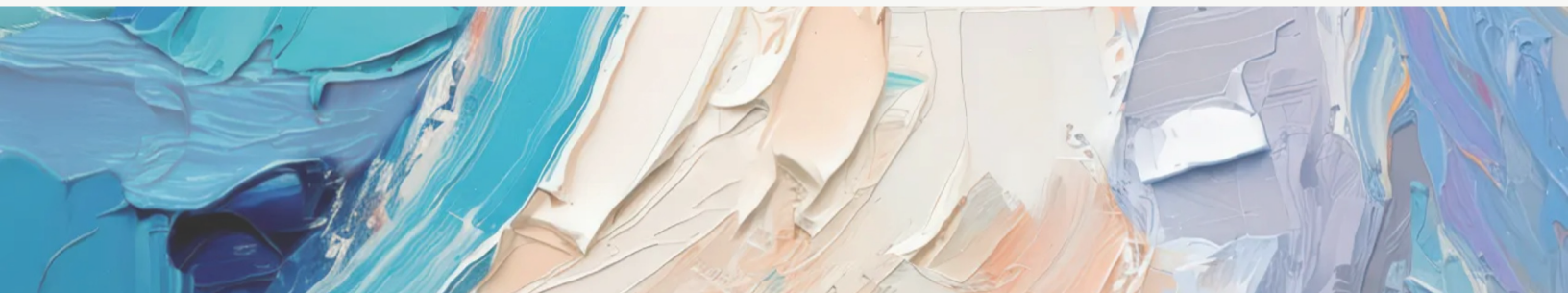
One operator, several owners. Registration records cover 95% of the footprint. They show at least four distinct groups of domain owners:

- **Fundacion Privacy Services / Media Elite Holdings** account for about four in ten domains. That registrant has lost typosquatting disputes since 2018.^{3,4,5}
- **badgerdns** holds a separate book registered through CommuniGal and Tucows.
- **redmondnc** is dominated by OnlineNIC registrations.
- **smtmdns** and **rentondc** lean on Fabulous, Gransy and Above.com.

The ages are mixed: about a fifth were created in 2010 or earlier, while 15% were created or re-registered in 2025-26. Most of the new ones came in a burst between September and December 2025, largely on **badgerdns**. That wave also moved away from **.com** toward cheap newer top-level domains such as **.live**, **.xyz**, **.click** and **.bet**. Earlier waves were almost all **.com**. The batched names are lookalikes about as often as the footprint as a whole, roughly three in ten, so the waves bought mixed inventory: typos and expired names together. **High for the waves**

Our reading is that one operator runs the nameservers and parking servers, and the gate and publisher account seen on the tested domains, and that several domain owners park their inventory with it. By "operator" we mean whoever runs this shared platform. A reseller that rents private-label nameservers and dedicated parking to several customers would fit much of the same evidence; in that case the reseller is the operator in our sense, and its customers are the owners. **High for the shared platform · Medium for the owner/operator split**

Why the family matters. The nameserver family is not evidence of an unusually difficult technical build. Its significance is the concentration it exposes: a large, diverse domain inventory operating through a small set of related DNS services, with shared screening and monetisation observed across the tested domains. The durable investment appears to be the traffic inventory, the automation and the commercial relationships behind the names. **Medium**

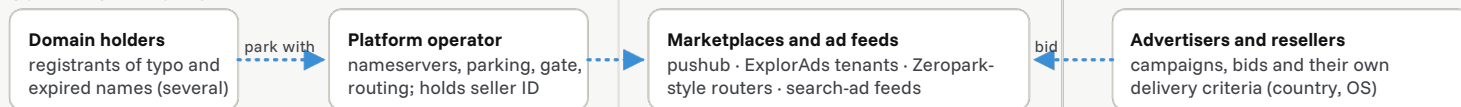


FRONT · ACQUISITION AND FIRST SCREENING

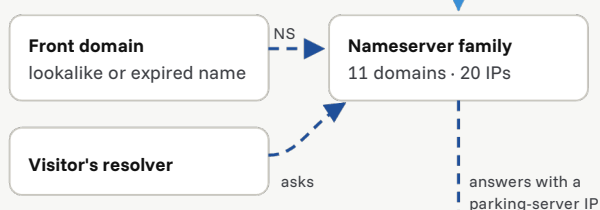
MIDDLE · SALE AND FILTERING

LANDING · WHAT IS REACHED

COMMERCIAL ROLES



DNS RESOLUTION



BROWSER NAVIGATION (HTTP)

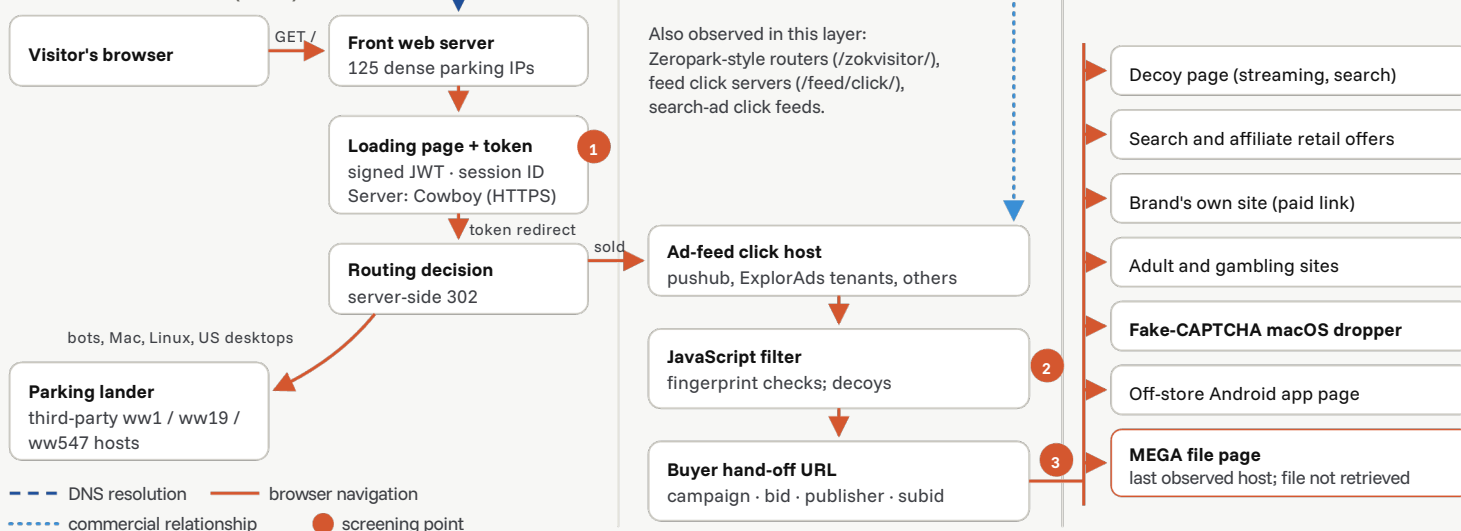


Figure 2. The three layers, with three kinds of relationship drawn separately: **DNS resolution** (dashed) tells a resolver where the front server is. Browsers never pass through a nameserver. **Browser navigation** (solid) is what the visitor follows. **Commercial relationships** (dotted) pay for each hop. Screening happens at least three times: at the front gate (1), at the ad feed's filter (2), and in the buyer's own delivery rules (3).

TEXT VERSION OF FIGURE 2

Commercial: domain owners park names with the platform operator, which sells visits to ad feeds and marketplaces; the tested domains used one seller ID. Advertisers and resellers bid for visits.

DNS: each front domain delegates to the nameserver family, which answers with a parking-server address.

HTTP: the browser gets a loading page and signed token, then a server-side decision sends it either to a third-party parking page or to an ad feed. The ad feed filters again and hands the visit to a buyer. Landings include decoys, affiliate offers, brands' own sites via paid or affiliate links, adult and gambling sites, an off-store Android app, a MEGA download and a fake-CAPTCHA malware dropper.

05

Every sector, many markets

To see what the whole footprint imitates, we matched every domain against the Tranco list of the most popular sites.¹⁵ We kept only the most reliable match types, which a reviewed sample showed to be right 80-100% of the time. Each imitated site was then classified by sector and main market. The charts show shares of the reliably matched lookalikes that could be classified.

A separate check against Malanta's own organization registry reached the same conclusion with a different taxonomy. It found 23 industry sectors, including aerospace, defence, energy and pharmaceuticals.

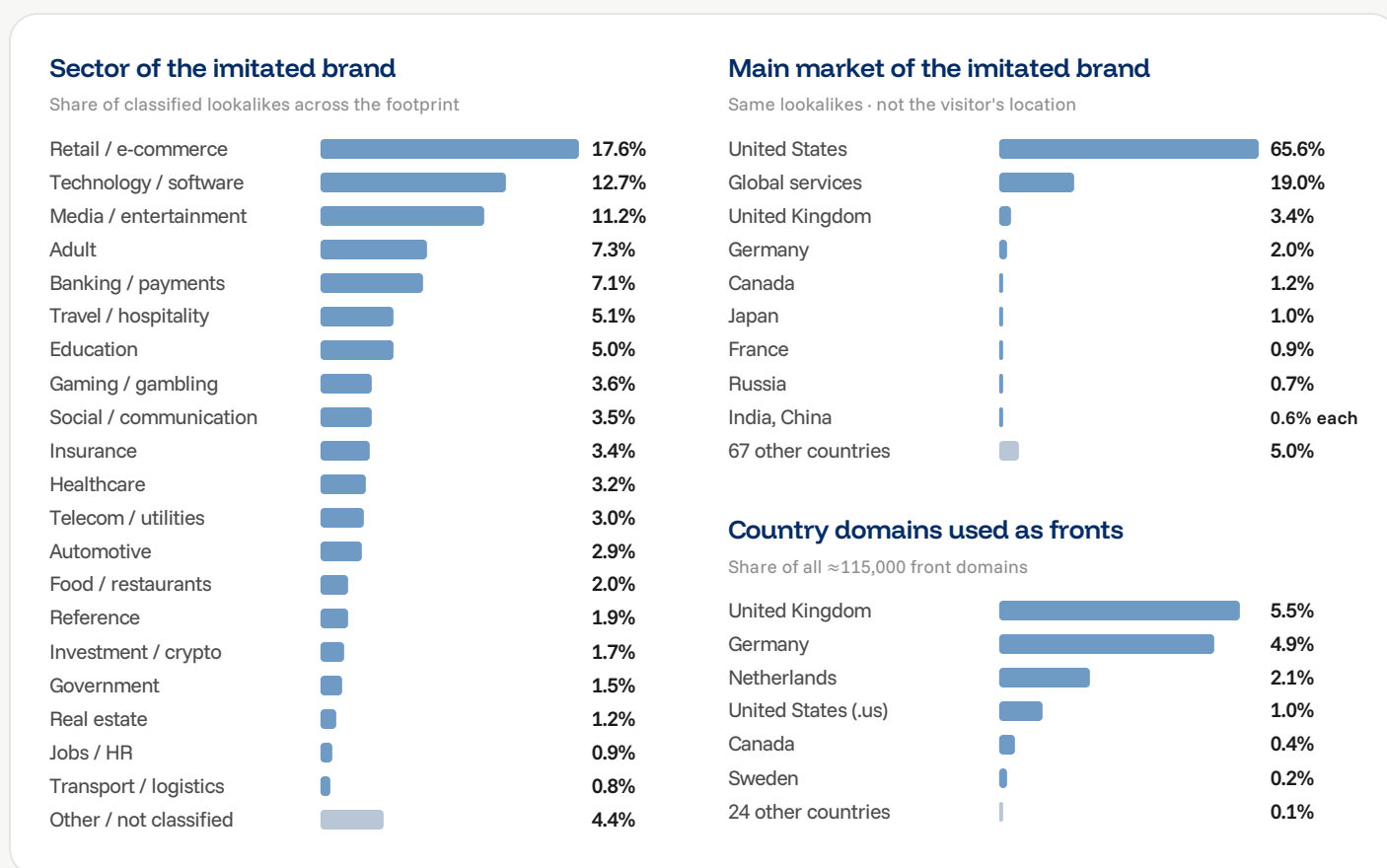


Figure 3. What the footprint imitates and where its fronts live: **Sector and market:** shares of the reliably matched lookalikes that could be classified. Sectors and markets were assigned by classifier. **Country domains:** shares of all front domains. The rest use generic domains (64% .com) across 193 top-level domains. Source: Malanta DNS data, 20 Oct 2026; Tranco list 467YX; Malanta classification.

Three geographies, decided by three parties

- **The imitated brand's market:** mostly the US, with brands from 76 countries.
- **The visitor's location and device:** the operator's routing responds to these (section 6).
- **The buyer's delivery rules:** for example, a download lure that only Brazilian Windows visitors received.

A US-brand typo can be monetized in Germany. A UK typo can be sold to a buyer who only wants phones. Sector does not decide who is exposed here; it mostly changes which offer is attached. Geography still matters, because buyers choose where and to whom they deliver.

06

Who sees what

One domain we followed shows how the screening works. `apypal[.]com` is a PayPal typo on `hastydns`. On 19 October we visited it many times, from cloud addresses in several regions, presenting as different kinds of visitor. Each visit recorded the full redirect chain, status codes and response headers. Most visits passed through these steps; the rest skipped the loading page and were redirected straight away:

1. The domain served a tiny "Loading..." page.
2. Its script reloaded the domain with a signed token and a session ID.
3. A server-side redirect decided where the visit went: the parking server, or an ad feed.
4. The ad feed ran its own browser checks, such as language and screen size.
5. Visits that failed those checks got a decoy, such as a music-streaming page or Google's homepage, instead of an offer.

Who we appeared to be decided where we ended up:

- **Search-engine crawlers and simple bots** were sent to the parking server, which turned them away.
- **Mac and Linux desktops, and Windows desktops in the US**, mostly got a parking page.
- **Windows desktops in Europe and Asia** were handed to an ad feed, with "paypal" as the search keyword. The feed's own checks sent most of them to the decoy.
- **Some visits from a Windows desktop in São Paulo** went through a different click host to a six-day-old redirector, and on to a file on MEGA (threat example 2).
- **Android phones** mostly got a streaming-app link, the feed's decoy. Some were sent to an off-store app page or a live-cam site.

The routing decision is made on the server, so we see its inputs (who we appeared to be, and from where) and its outputs (where each visit went), not its code. We call a difference screening only when it held between visitor profiles in the same region and repeated across visits. The other domains we followed behaved the same way, behind the same gate. On those domains, the visitor, not the sector of the typo, decided the routing.

Captured redirect chains for [apypal\[.\]com](#), 19 Oct 2026, one visit per profile (tokens and IDs shortened)

Visitor profile, region	Captured chain	Ended at
Googlebot user agent, Tokyo	apypal[.]com → 302 → ww547.apypal[.]com	Parking server, 401 "forbidden"
Mac desktop browser, US West	apypal[.]com → 302 → ww547.apypal[.]com	Parking page
Windows desktop, US East	apypal[.]com → 302 → ww547.apypal[.]com	Parking page
Windows desktop, Tokyo	apypal[.]com ("Loading...") → apypal[.]com/?ch=1&js=<signed token>&sid=... → xml-v4.pushub[.]net/click → live.pushub[.]net/filter?q=paypal → xml-v4.pushub[.]net/click2	Music-streaming decoy
Windows desktop, São Paulo	apypal[.]com → click-v4.junclickrmedi[.]com/click → retroanimesege[.]cfd/index51.php?...&country=br&city=São Paulo&os=Windows 10 → mega[.]nz/file/fAoHTKQT	MEGA file page
Android phone browser, Tel Aviv	apypal[.]com → xml-v4.pushub[.]net/click → live.pushub[.]net/filter?q=paypal → xml-v4.pushub[.]net/click2?...ss=412x915&ws=981x1958... → forkstrong[.]com → apkpure[.]com app page	Off-store app page

The `click2` step carries what the feed's script measured in the browser, such as screen and window size (`ss=`, `ws=`). That is direct evidence of the feed's own checks.

The gate's fingerprint, and its limits

The token is a JSON Web Token carrying the default claims of `Joken`, an Elixir library.⁹ The HTTPS responses carry `Server: Cowboy`, the Erlang web server.¹⁰ Both are reliable implementation fingerprints for proxy logs and crawlers. They identify neither the operator nor the routing logic.

Cloud addresses are screened too. A visit from a non-cloud address on the same day reached routers that our cloud visits never saw, and the malware in section 7 appeared only in an ordinary browser. A defender who checks a suspicious domain from a scanner or a data-centre address will usually see a parking page like the one below.

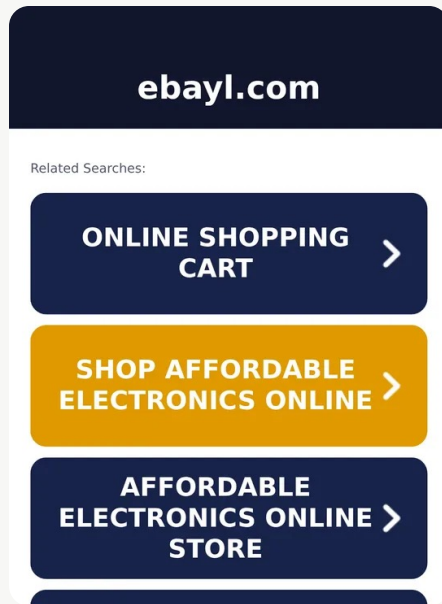


Figure 4. What a search engine is shown: the parking page served for an eBay typo on the same infrastructure to a browser presenting as Googlebot. 19 Oct 2026. Malanta capture.

07

Threats running on the infrastructure

The operator's infrastructure does the acquiring and the screening. What visitors finally receive is decided by whoever buys their visit. The examples below were all observed on traffic leaving this operator's domains. We separate confirmed malicious delivery, downloads and apps we did not analyse, and commercial destinations.

Confirmed malicious delivery

THREAT EXAMPLE 1 · MALWARE

A fake CAPTCHA that installs a macOS dropper

Observed on 20 October 2026, when a Malanta researcher browsed [iuntuit\[.\]com](https://iuntuit[.]com). It's an Intuit typo on redfoxdns, and one of the 466 seeds. We decoded every stage statically; nothing was executed.

1. **Lure page.** [iuntuit\[.\]com](https://iuntuit[.]com) redirected the browser to [hxxps://sso.crypsend\[.\]click/idcheck/vantdot.html](https://sso.crypsend[.]click/idcheck/vantdot.html), which displayed the fake check (Figure 5). [crypsend\[.\]click](https://crypsend[.]click) was registered at NameCheap on 20 Oct 2026, the same day as the visit, and sits behind Cloudflare.
2. **Clipboard.** Clicking "I am not a robot" copied a base64-wrapped command that pipes [hxxps://7ulk.irvinaurus\[.\]fit/clear-cache.sh](https://7ulk.irvinaurus[.]fit/clear-cache.sh) into the shell. [irvinaurus\[.\]fit](https://irvinaurus[.]fit) was registered on 23 Jul 2026.
3. **Script.** The script runs a hidden AppleScript, rebuilt from character codes and padded with junk variables.

4. **Persistence.** It writes a launch agent, `com.Apple.ddjnmuymodzjkyov`, that restarts at every login, and starts it immediately.
5. **Blockchain dead drop.** The agent queries a smart contract on Polygon (`0xA3a603F8...C2A0`) through public RPC nodes. It reads the contract's stored string as its command server; on 20 Oct that was `secdarwin2026[.]icu`.
6. **Next stage.** It posts a campaign ID to that server and runs whatever AppleScript comes back with the user's rights. The final payload was not retrieved.

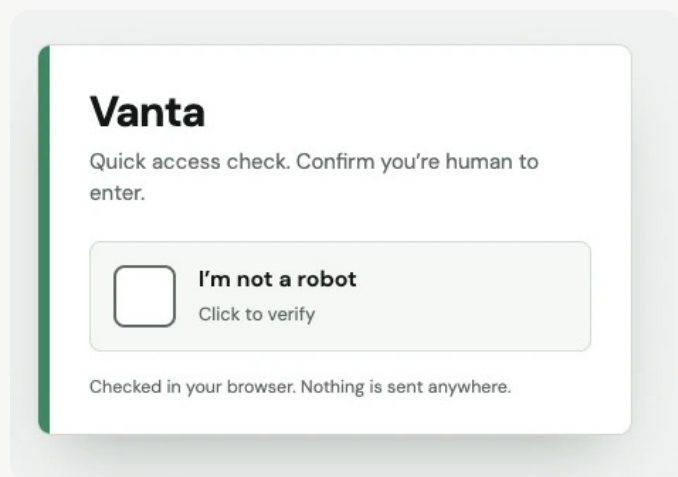


Figure 5. The fake check on `sso.crypsend[.]click`, reached from `iuntuit[.]com` in an ordinary browser, 20 Oct 2026. Ticking the box copied the command to the clipboard, despite the promise that nothing is sent anywhere. Researcher capture.

What the malware does rests on a static analysis of the script the researcher received. [High for the script's behaviour](#)

How the visit reached it is less certain. The visit started on one of the operator's front domains and was redirected to the lure page on `sso.crypsend[.]click`. Whether other routing hops sat in between was not recorded, so we cannot say which party bought or placed the lure. Visits to the same domain from cloud addresses saw only a search page. [Medium for the link to the traffic chain](#)

Downloads and apps we did not analyse

THREAT EXAMPLE 2 · DOWNLOAD LURE

A MEGA file behind a six-day-old redirector

On 19 October, Windows visitors from Brazil, on several of the domains we followed, were sent through ad-feed click hosts to `retroanimesega[.]cfd`. That domain was registered six days earlier, and it passed every one of them to the same MEGA file page. Its URL described the visitor: country, city and operating system. The file's name and content are encrypted by MEGA, and we did not retrieve them. A fresh redirector, country targeting and a cloud-storage file are a common pattern for malware delivery. [Medium](#)

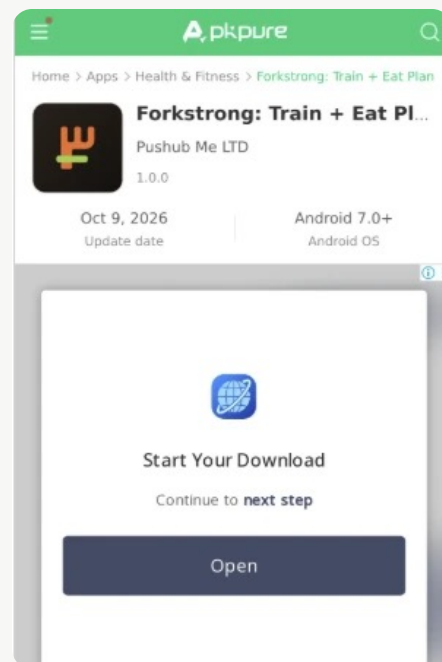
THREAT EXAMPLE 3 · OFF-STORE APP

An Android app pushed from outside Google Play

Android visitors sold to the ad feed were sent through [forkstrong\[.\]com](https://forkstrong[.]com), registered 30 Sep 2026, to a third-party store page for an app that Google Play does not list. Sideloading bypasses store review. The store lists the app's developer as "Pushub Me LTD", the same name as the ad feed these visits passed through; we have not verified whether the two are connected. We did not analyse the app.

Medium

Figure 6. Where threat example 3 ended: a third-party store page for an app not listed on Google Play. Android profile. Researcher capture.



Commercial destinations

THREAT EXAMPLE 4 · BRAND-KEYWORD SEARCH PAGES

Typo traffic turned into "login" and "download" ads

Seeds on six different nameserver domains ended on [findakey\[.\]net](https://findakey[.]net), usually through the redirector [rhcdom\[.\]com](https://rhcdom[.]com). The pages look like parking pages, but they are built from the imitated brand: "QuickBooks Workforce Online Login", "Intuit TurboTax Login Tax Return", "SonicWall NetExtender Download", "Malwarebytes Anti-Malware Free". Each line is an ad slot. Pairing a brand with "login" or "download" invites fake login and fake download ads; we did not capture where those clicks lead.

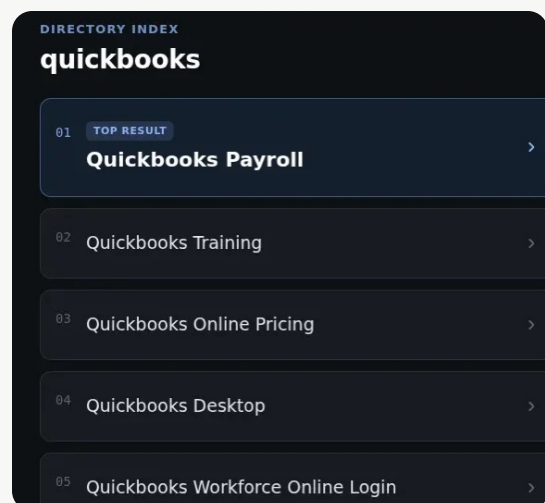


Figure 7. A brand-keyword search page reached from QuickBooks typos. Real browser, 6 Oct 2026. Malanta capture, cropped.

THREAT EXAMPLE 5 · PAID AND AFFILIATE ROUTES

Brand traffic routed through paid and affiliate links

Some seeds ended on the imitated brand's own website, through paid or affiliate redirects. Typos of Walmart, Ticketmaster, Best Buy, Constant Contact, Merrell, Marriott, Coinbase, AT&T, Xfinity, Disney+ and others passed through [q1.quotes\[.\]com](#), [flexlinkspro\[.\]com](#) and short affiliate redirectors. On 19 October, US visitors to [t-mmobil\[e.\]com](#) went through a search-ad feed and the advertiser's own click tracking to T-Mobile's real site. The click record named the typo domain as its source. These routes are consistent with paid-click or affiliate monetisation; we did not verify that any brand was billed.

Medium

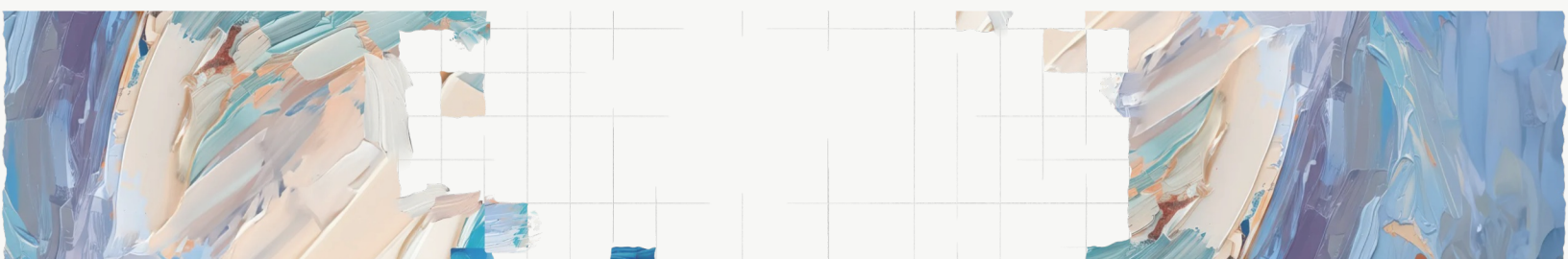
THREAT EXAMPLE 6 · ADULT, GAMBLING AND GREY OFFERS

The rest of the order book

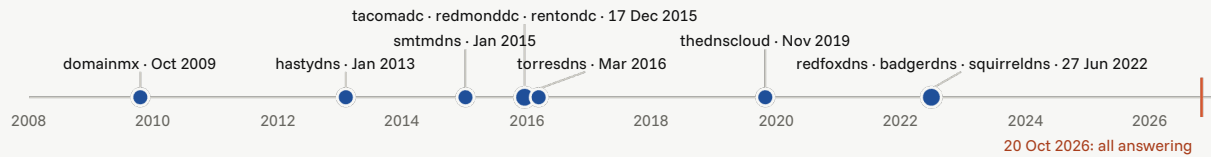
Other visits were sold to:

- live-cam and adult sites, through a dedicated redirect domain;
- UK gambling brands;
- "adblocker" browser-extension pages;
- credit-score offers for credit-bureau typos;
- survey-prize pages, game sign-ups and app subscriptions;
- a competitor's shop, for a sportswear typo.

The same routes served typos of a bank, a ticket seller, a hotel chain and a shoe brand. The sector of the typo seemed mainly to decide which offer was attached.



STABLE · NAMESERVER DOMAINS, BY REGISTRATION DATE (ALL ANSWERING ON 20 OCT 2026)



CHANGING · ROUTING, LANDING AND THREAT HOSTS, REGISTRATION → FIRST SEEN

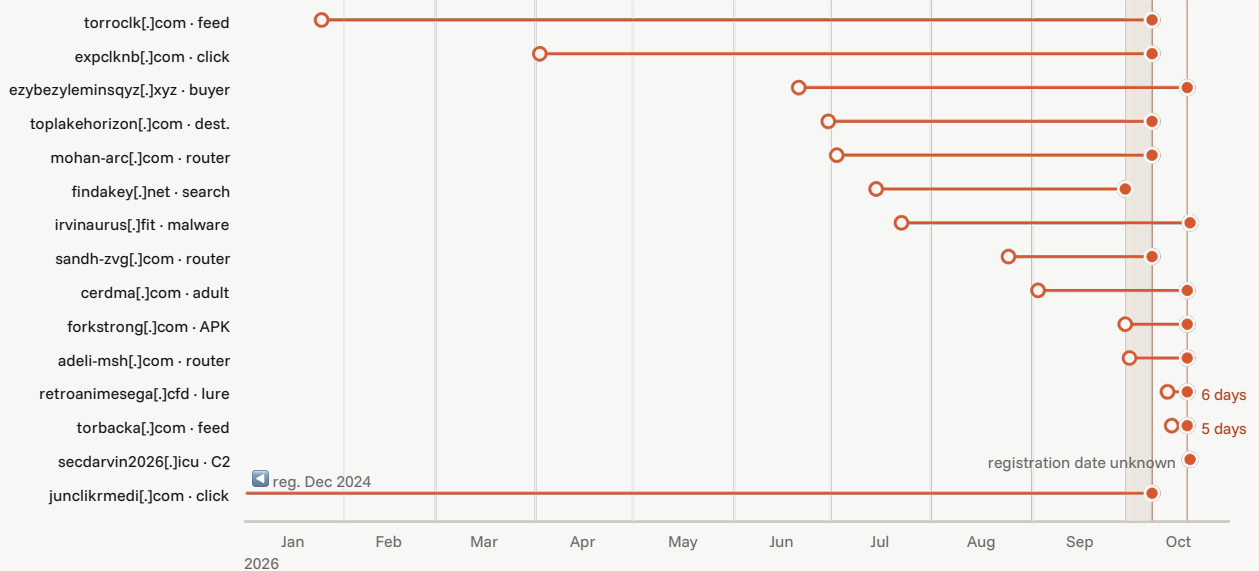


Figure 8. The infrastructure is stable; the threats on top of it rotate. **Nameserver domains:** registered over 13 years, all still answering. **Routing, landing and threat hosts:** mostly registered in 2026, several within weeks of use. A feed server even changed its name while keeping its address.

Flagged months before it woke up

Quad9 shares DNS telemetry with Malanta for domains on Malanta's indicator list. One example from that data shows how attacker infrastructure on these nameservers is staged and then put to use:

- **Bought in bulk.** On 24 September 2025, 25 domains were registered on the same day through one registrar and delegated to `badgerdns`. Most are random seven-letter `.com` names, such as `djcxtew[.]com`, `fmwesgr[.]com` and `kyyepzh[.]com`. The rest read like lures: `ibanking-dbs-verify[.]com`, `mygovau funds[.]com`, `vz-help[.]com`.
- **Flagged early.** Malanta classified most of them as malicious between 30 November and 15 December 2025, about ten weeks after registration. Several of the names were already known to Malanta from earlier registrations in 2023.
- **Left to sit.** They then stayed parked on the operator's addresses for about eight months.
- **Switched on together.** In the week of 23 August 2026, their Quad9 lookups jumped to about seven times those of comparable domains on the same nameserver domain and ending. They stayed there for about three weeks, then fell back by late September.

Random strings do not attract mistyped traffic, so something referred to these names together during those weeks, such as a spam or link run, bots or scanning. DNS data shows the timing, not the purpose. [High for the pattern](#) · [Low-Medium for the cause](#)

The sequence is a common way to stage attacker infrastructure: buy names in bulk, let them age quietly on parked servers, then use them together in a short burst. For defenders, the timing is the point. These domains were on Malanta's list eight to nine months before the burst.

FROM BULK REGISTRATION TO A TRAFFIC BURST · QUAD9 LOOKUPS PER DOMAIN PER DAY

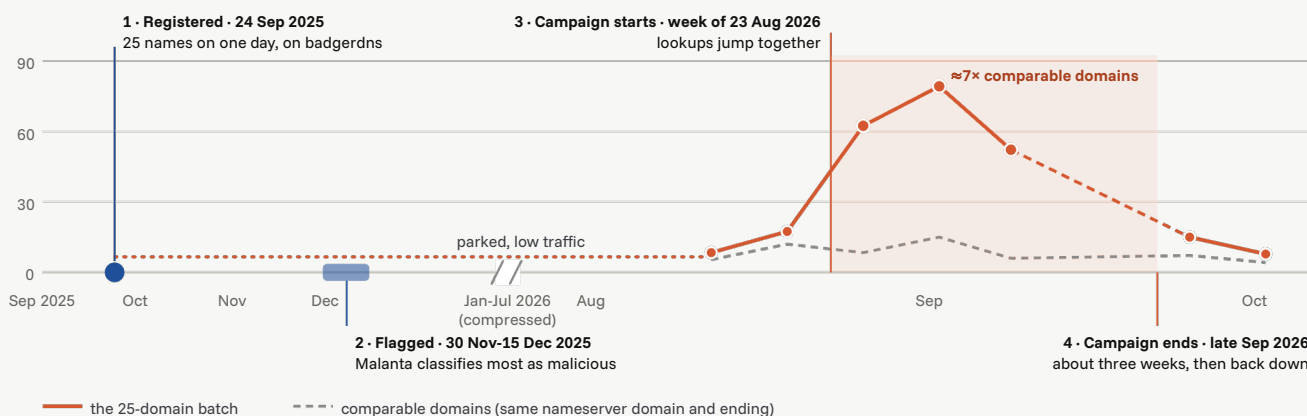


Figure 9. The 24 September 2025 batch, from bulk registration to a traffic burst: Quad9 lookups per domain per day (weekly averages) for the batch and for comparable domains on the same nameserver domain and ending. The time axis is compressed between January and July 2026. The telemetry starts on 9 August 2026; earlier traffic is drawn as low. Source: Quad9 DNS telemetry shared with Malanta; Malanta registration and reputation data, 21 Oct 2026.

09

What was already known, and what this adds

Infoblox Threat Intel published the most detailed prior account in December 2025: [Parked Domains Become Weapons with Direct Search Advertising](#).¹ Krebs on Security covered it the same day.² We credit it for establishing much of the ecosystem described here.

Infoblox (16 Dec 2025) compared with this report (data to 20 Oct 2026)

Topic	What Infoblox reported	What this report adds
Actors	Three portfolios: a torresdns actor (~3,000 lookalikes); a "double fast flux" actor (~80,000 domains) rotating ten nameservers, including hastydns ; a domaincontrol actor (~30,000).	torresdns and hastydns sit in one co-located family of 11 nameserver domains with ~115,000 front domains. Nine of them were not named by Infoblox. Infoblox's other listed nameservers carry about 82,000 domains today on an adjacent but separate parking pool. One of them shares redfoxdns 's exact servers.
Screening	Cloud, VPN, scanner and bot traffic gets parking pages; residential traffic is redirected	Routing followed per visitor profile and region on example domains. The front gate is fingerprinted (Joken token, Cowboy server).
Platforms	Zeropark, Trillion Direct Search, ExplorAds, AdventureFeeds, Skenzo parking, Above.com, RichAds, Sedo, Team Internet	The publisher account at the ad feed pushub, seen on sampled domains across six nameserver domains. The pushub, ExplorAds and other click hosts run on one ad-serving platform. ⁷ Search-ad feeds and affiliate routers (quotes[.]com , flexlinkspro[.]com).
Harm	Over 90% of residential visits in its experiments ended in scams, malware or unwanted content. Tedy malware lure hosted on MEGA; Babar via ClickFix; scareware; business-email compromise via gmail[.]com .	A macOS ClickFix dropper with a Polygon smart-contract dead drop; a MEGA lure; an off-store APK; brand-keyword search pages; paid or affiliate routes to 19+ brands' own sites
Indicators	13 nameserver domains, 8 landing and redirect domains, 3 file hashes, 1 IP, with more on its GitHub	Nameserver IPs; dense parking networks; the seller identifiers; new routing, landing and threat hosts (appendix)
Sources cited	USENIX Security 2014 (under 5% malicious, then); Trinity Cyber; CISA AA25-093A on fast flux; Kinto Technologies; APNIC; TechTarget; sandbox and scanner reports	Malanta lookalike evidence, DNS, WHOIS, hosting and reputation data; multi-profile visits to example domains; a static malware analysis
Discovery	Large-scale scanning from residential proxies and Tor	Pre-attack signals on 466 lookalikes, correlated through shared nameservers into the full infrastructure

Who gains what

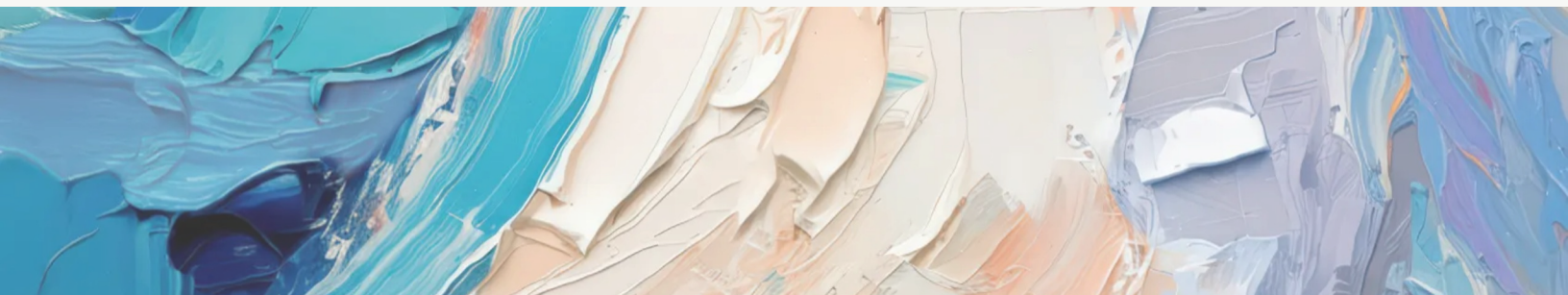
Each party gains something different:

- **The operator** sells mistyped and expired-domain traffic; on the tested domains it did so under one publisher account. It hides the sale from crawlers and analysts.
- **Domain owners** earn from inventory they park on the platform.
- **Ad feeds and marketplaces** resell the visits. They are commercial services, probably being abused, not the operator.
- **Buyers** decide the outcome:
 - affiliates and search-ad resellers can earn commissions, possibly from the imitated brands themselves;
 - adult and gambling advertisers buy cheap reach;
 - malware distributors can receive screened, real users in chosen countries, as the dropper example suggests.
- **Visitors** carry the risk.
- **Brands** lose traffic, and may pay commissions or click fees for visitors they would have had anyway.

Where the money goes: a scenario estimate

Maintaining a portfolio of this size plausibly costs its holders seven figures a year: about 115,000 names at wholesale renewal prices of roughly \$10 or more each comes to \$1 million or more. The shared DNS and redirect infrastructure, about 150 addresses on rented servers at commodity hosting providers, may cost only tens of thousands of dollars a year. This is a scenario-based estimate, not observed expenditure.

The economic investment lies mainly in acquiring and retaining traffic-producing domains, not in the servers that route their visitors. **Low: scenario estimate**



Defensive implications

Correlate across sectors. Sector relevance alone can fragment the view of shared infrastructure. Correlating across sectors exposes the platform behind apparently unrelated lures. Geography still matters to delivery, because buyers choose countries and devices. Across lures, the things that stay put are:

- the nameservers;
- the parking networks;
- the gate fingerprint;
- the seller identifiers.

Act on relationships, not only verdicts. One at a time, most of the operator's front domains look like ordinary parked typos. What gives them away is their delegation to this nameserver family. A policy built on that relationship covers every domain, whether or not it has been judged on its own.

- **Monitor new delegations** to the 22 nameserver hostnames, and new hostnames on the 20 nameserver addresses. Hundreds of same-day registrations pointing at one nameserver domain are an early sign of a new wave. The [indicator CSV](#) lists every front domain as of 20 October.
- **Correlate DNS, proxy and brand-abuse data.** Resolver logs show which clients queried which lookalike. Proxy logs show the gate (`?ch=1&js=`), the seller fields and the router paths.
- **Test with several visitor profiles:** Windows abroad, Android, a real browser, non-cloud egress. Scanner checks see parking pages.
- **Hunt for the malware example on macOS fleets:**
 - user launch agents named `com.Apple.*`;
 - `osascript` launched from `bash`;
 - `curl` calling public Polygon RPC endpoints;
 - clipboard commands piping a downloaded script into the shell.
- **Evaluate nameserver-based DNS policy** (RPZ `NSDNAME` / `NSIP`) where your resolver supports it.^{11,12,14} Validate support, run log-only, allowlist legitimate exceptions, then enforce. We found one functioning business with mixed delegation to the family, and some vendors already treat malicious nameservers as a category.¹³
- **Block specific confirmed hosts, not platforms.** Block the fake-CAPTCHA page, the payload host, the command server and the MEGA file URL. Leave out shared ad-tech, CDNs, cloud providers, third-party parking services, app stores and MEGA itself.

Plan for replacement, not a single takedown. There is no single permanent takedown for a replaceable infrastructure business. Defenders can, however, keep protection on known front domains as the operator changes nameservers, hosting and destinations. Combining domain-level enforcement, validated nameserver policies and continuous infrastructure discovery turns a one-time disruption into sustained denial of access.

Proposed operational metrics (suggestions; no measured values in this report)

Metric	What it tells you
New family members per week	Growth and churn of the operator's front layer
Time from first delegation to policy coverage	Whether nameserver policy keeps pace
Outcome difference by visitor profile	How much a single-profile check misses
Legitimate-domain exceptions	Allowlist size and age, including mixed delegations
User exposures via the family	Resolver hits per user and per typo, for awareness and brand notification

MITRE ATT&CK, limited to what was observed¹⁶

Who	Technique	Observed as
Operator	T1583.001 Domains · T1583.002 DNS Server · T1583.004 Server	Typo and expired-domain inventory; private nameserver domains; dedicated parking pools
Traffic buyers	T1583.008 Malvertising	Download lure and off-store APK reached through ad feeds; the fake CAPTCHA's route was not recorded
Malware operator (example 1)	T1204.004 Malicious Copy and Paste · T1059.002 AppleScript · T1059.004 Unix Shell · T1027 / T1140 Obfuscation · T1543.001 Launch Agent · T1036.005 Masquerading · T1102.001 Dead Drop Resolver · T1105 Ingress Tool Transfer	Clipboard command → script → launch agent → smart-contract C2 → next-stage AppleScript

Methodology

How the set was built:

1. **Seeds.** 466 lookalikes that Malanta's lookalike monitoring flagged, 6-13 Oct, for redirecting visitors to destinations already flagged by Malanta reputation or by multiple public DNS blocklists.
2. **Nameserver family.** The seeds' nameserver delegations pointed to ten private-label nameserver domains. Three kinds of evidence linked them, and an eleventh, into one family:
 - same-day registration batches;
 - shared and adjacent nameserver addresses;
 - nameservers inside the parking networks.
3. **Expansion.** A reverse nameserver lookup over Malanta's DNS data (current NS records, 20 Oct) listed every domain whose nameservers belong to the family: about 115,000. The full list is in the [indicator CSV](#).
4. **Checks.** Three checks tested the link:
 - the domains' address records: 204 addresses, of which 125 dense ones carry 99.9% of the records;
 - WHOIS (95.5% coverage), to separate the domains' owners from the platform operator;
 - behaviour on tested domains: the gate fingerprint, the routes and the publisher account.

Page-similarity hashing, certificate clustering and IP geolocation were not used.

How screening was tested. On 19 October we ran a controlled multi-profile crawl of a sample of front domains chosen across sectors and nameserver domains:

- **Regions:** nine AWS cloud regions (US East and West, São Paulo, London, Frankfurt, Tel Aviv, Mumbai, Singapore and Tokyo).
- **Visitor profiles:** seven (a search-engine crawler user agent, a plain script, Mac, Linux and Windows desktop browsers, and an Android phone).
- **Clients:** a scripted HTTP client and a real browser, with four referrer types.
- **Recorded per visit:** the full redirect chain, status codes, response headers, the final page and, in the browser, a screenshot.

A visit to each domain from a non-cloud address the same day checked whether cloud traffic was itself screened. Live checks on 8 and 19 Oct recorded the gate on further samples.

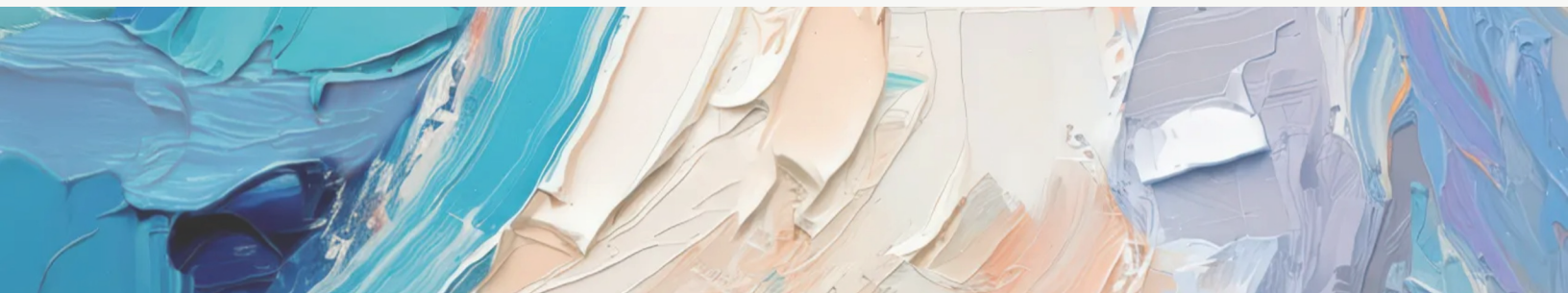
Other sources:

- Malanta DNS, WHOIS, hosting, IP-clustering and reputation data (to 20 Oct);
- Malanta captures and screenshots;
- Quad9 DNS telemetry shared with Malanta for domains on Malanta's indicator list (daily activity periods, 9 Aug-15 Oct 2026);
- live DNS, HTTP and TLS checks (8, 19 and 20 Oct);
- a static analysis of the malware the researcher encountered (20 Oct). The command server was resolved by reading public blockchain state, without contacting it.

References

1. Infoblox Threat Intel, "Parked Domains Become Weapons with Direct Search Advertising," 16 December 2025. infoblox.com
2. Krebs on Security, "Most Parked Domains Now Serving Malicious Content," December 2025. krebsonsecurity.com
3. WIPO Arbitration and Mediation Center, Case D2018-0979. wipo.int
4. ADR Forum, Claim 1831258. adrforum.com
5. WIPO Arbitration and Mediation Center, Case D2020-0665. wipo.int
6. Zeropark documentation, "Redirect RTB integration." doc.zeropark.com
7. AdGuard cname-trackers, issue 58 (ak-is2[.]net). github.com
8. urlscan.io, domain record for [junclickmedi\[.\]com](https://junclickmedi[.]com). urlscan.io
9. Joken, "Joken.Config" documentation. hexdocs.pm
10. Nine Nines, Cowboy HTTP server. github.com
11. IETF DNSOP, "DNS Response Policy Zones (RPZ)," draft-ietf-dnsop-dns-rpz-00, 2017. datatracker.ietf.org
12. Infoblox, "Response Policy Zones (RPZ)," DNS Security Resource Center. infoblox.com
13. Infoblox, "Configuring Infoblox Threat Intelligence Feed," NIOS 8.5 documentation. docs.infoblox.com
14. Zytrax, "BIND9 Response Policy Zone Configuration." zytrax.com
15. Tranco, list 467YX. tranco-list.eu
16. MITRE ATT&CK: [T1583.001](https://attack.mitre.org/tactics/TA0001/t1583.001), [T1583.002](https://attack.mitre.org/tactics/TA0001/t1583.002), [T1583.004](https://attack.mitre.org/tactics/TA0001/t1583.004), [T1583.008](https://attack.mitre.org/tactics/TA0001/t1583.008), [T1204.004](https://attack.mitre.org/tactics/TA0001/t1204.004), [T1543.001](https://attack.mitre.org/tactics/TA0001/t1543.001), [T1102.001](https://attack.mitre.org/tactics/TA0001/t1102.001).

Lookalike matching used the Tranco list [467YX](https://tranco-list.eu) and only the most reliable match types. Sector and market labels come from a classifier and from Malanta's organization registry. Sector and geography figures are shares of the lookalikes that could be classified.



APPENDIX

Indicators

All indicators are defanged and were observed between 30 Sep and 20 Oct 2026. Review before any enforcement. The tables below list the infrastructure and threat hosts.

Download the full indicator list: github.com/malanta-ai/iopas · [Typosquat-Traffic-Machine-Nameserver-Family](#)

About 115,000 front domains with their nameserver domain, plus every indicator below, each with a recommended use.

Nameserver family, as resolved on 20 Oct 2026: candidates for RPZ [NSDNAME](#) / [NSIP](#) after log-only assessment

Nameserver domain	ns1	ns2
badgerdns[.]com	208.115.240[.]174	77.247.179[.]81
redfoxdns[.]com	208.115.240[.]170	77.247.182[.]241
hastydns[.]com	69.162.80[.]50	85.17.21[.]143
thednscloud[.]com	207.244.109[.]97	94.75.199[.]68
redmondcd[.]com	192.211.55[.]138	45.82.67[.]21
smtmdns[.]com	172.98.192[.]42	95.211.134[.]248
tacomadc[.]com	192.211.55[.]134	213.227.156[.]65
domainmx[.]com	23.92.212[.]226	212.92.105[.]225
torresdns[.]com	23.92.212[.]162	78.41.207[.]71
rentondc[.]com	172.98.192[.]98	85.17.5[.]93
squirrelldns[.]com	208.115.240[.]170	77.247.182[.]241

Dense parking networks (20 Oct 2026). Provider blocks also host other customers, so validate before IP-level action.

216.245.197[.]0/24 · 77.247.179[.]0/24 · 77.247.182[.]0/24 · 216.245.213[.]0/24 · 69.162.80[.]0/24 · 212.7.194[.]0/24 · 199.193.114[.]0/24 · 23.92.212[.]0/24 · 172.98.192[.]0/24 · 23.105.175[.]0/24 · 212.32.254[.]0/24 · 45.82.67[.]0/24 · 212.92.105[.]0/24 · 94.75.193[.]0/24 · 78.41.207[.]0/24 · 213.227.156[.]0/24 · 37.48.110[.]0/24 · 85.17.5[.]0/24 · 62.212.89[.]0/24

Two further dense networks are in shared cloud space and carry only a few dozen domains each; they are not listed.

Threat example hosts:

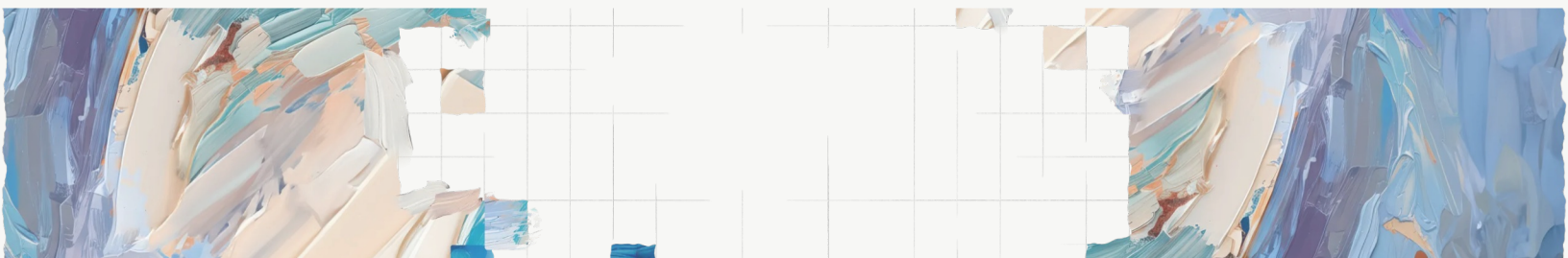
- **Malware chain:**
 - Fake-CAPTCHA page `hxxps://sso.crypsend[.]click/idcheck/vantdot.html`
 - `hxxps://7ulk.irvinaurus[.]fit/clear-cache.sh`
 - Polygon contract `0xA3a603F8a454a9c905b4c579Bb72628F7C15C2A0` (selector `0x2686ecea`)
 - C2 `secdarwin2026[.]icu` (20 Oct)
 - Launch agent `~/Library/LaunchAgents/com.Apple.ddjnmuymodzjkyov.plist`
- **Download lure:** `retroanimesega[.]cfd` and `hxxps://mega[.]nz/file/fAoHTKQT` (block the file URL, not MEGA).
- **Off-store app:** `forkstrong[.]com`.
- **Search pages:** `findakey[.]net`, via `rhcdom[.]com` and `manifcook[.]com`.
- **Destinations:** `toplakehorizon[.]com`, `studiowaterarts[.]com`, `survey-smiles[.]com`.
- **Feed servers:** `torroclk[.]com` and `torbacka[.]com` on 104.248.224[.]96.

Commercial ad-tech and affiliate routers (categorize, do not attribute): `xml-v4.pushub[.]net`, `live.pushub[.]net`, `click-v4.expclknb[.]com`, `click-v4.junclikrmedi[.]com`⁵, `click-v4.plarclck[.]com`, `q1.quotes[.]com`, `track.flexlinkspro[.]com`, `verifiedbrandsite[.]com`, `click.validclick[.]net`, `query.pureleads[.]com`, and the Zeropark-style routers⁶ `sandh-zvg[.]com`, `mohan-arc[.]com`, `adeli-msh[.]com`.

Do not block on association: the third-party parking landers on 208.91.196[.]145 and 34.160.121[.]137, public Polygon RPC providers, CDN and cloud addresses.

Behavioural strings:

- a ~470-byte `<title>Loading...</title>` page with `?ch=1&js=;`
- token prefix `eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdWQiOiJKb2t1biIs`
- `publisher=230041` or `pubfeed=965920`;
- `/zokvisitor/` with `campaignid=;`
- `txid=e91825a83c4bb6415101cd03a2f422f8` posted to a C2.



MALANTA RESEARCH

Different Brands. The Same Traffic Machine.

Malanta Research Team; Yossi Dantes · Data cutoff 20 Oct 2026 · Indicators are defanged and provided for defensive use.

FULL INDICATOR LIST

Download the full indicator list: github.com/malanta-ai/iopas-Typosquat-Traffic-Machine-Nameserver-Family

About 115,000 front domains with their nameserver domain, plus every indicator in the appendix, each with a recommended use.



Malanta:

Pre-Attack Prevention. Hit the source.

MALANTA.AI