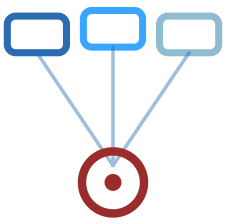
Principal Brief // two-minute read

DOMAIN & DNS | OSINT | MISIDENTIFICATION



# Why a Shared Registrar Proves Nothing

> *Investigators link domains by where they were registered. Two companies now own three in five accredited registrars, and one platform sits behind 13,000 reseller brands. "Same registrar" and "different registrars" both mean less than they did.*

### WHAT HAPPENED

The registrar market consolidated behind its brand names. Newfold Digital runs Bluehost, HostGator, Network Solutions, Register.com, and three more as separate storefronts under one private-equity owner. Tucows runs the wholesale platform behind 13,000 reseller brands. By September 2026 one drop-catching company held more than 1,500 of ICANN's 3,323 accreditations, almost all shells. Attribution methods that cluster by registrar did not change.

### WHY IT REACHES YOU

Twice. A protective-intelligence report that ties a hostile domain to a person because both used the same registrar makes a weak inference sound strong, and the person it names could be you or someone close to you. And your own domains, spread across three brands, may sit on one backend with one account-recovery process between an attacker and all of them.

## *THREE THINGS TO TAKE FROM THIS*

**1**

### The receipt is not the operator

Reseller brands, multi-brand owners, and shell accreditations mean a registrar name identifies a storefront, not a control plane.

**2**

### The error runs both ways

Registrar clustering links domains that share only a label and separates ones that share a backend. Wrong systematically, so wrong confidently.

**3**

### Ask what else connects them

Nameserver history, certificate timing, hosting, content. If a report linking domains to a person has only the registrar, it has nothing.

## *DO THIS*

- [ ] **YOU, WHEN A REPORT NAMES SOMEONE**
  Ask which evidence beyond the registrar connects the domains. No answer means the name comes out until there is one.
- [ ] **YOU, WITH YOUR FAMILY OFFICE**
  List the registrar of record and nameservers behind every domain brand you use. Diversify by those, not by storefront.
- [ ] **YOU, WITH YOUR SECURITY LEAD**
  Have past investigations that clustered by registrar re-run on infrastructure signals before anyone relies on them again.

### NOT THE STORY YOU MAY HAVE HEARD

This brief does not say registrar data is useless or that consolidation is sinister. Registrar identity is fine as context and often right. It says "same registrar, therefore related" and its mirror "different registrars, therefore independent" no longer hold as evidence, and anyone naming a person on that basis has not done the work.

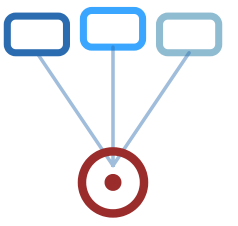
### HOW SURE WE ARE

High on the market structure, shown by the companies' own statements, ICANN accreditation data, and our review of 116 entities. Moderate on how widespread technical backend reuse is beyond the registrar layer.

THE FULL COMMAND BRIEF FOLLOWS: THE STRUCTURE BEHIND THE BRANDS, WHY THE METHOD FAILS, THE FIVE AXES, AND POSTURE BY FUNCTION.

CB-053

# Domain Attribution Has Structurally Broken



*"When brand independence decouples from infrastructure independence, registrar identity stops being a sound anchor."*

> *Analysts cluster domains by registrar: two domains at the same registrar look related, two at different registrars look independent. Both inferences are weaker than they look. Of 3,323 ICANN-accredited registrars in September 2026, one drop-catching business controls more than 1,500 and one hosting group more than 500, and a single wholesale platform sits behind more than 13,000 reseller brands. Nominally independent registrars share backends; nominally shared registrars are often shells. For a principal, the protected person at the center of a security program, this matters twice: when an investigator says threatening domains are "linked" because of where they were registered, and when a family's own domains look diversified because the receipts carry different names.*

**BLUF.** Registrar identity is no longer a sound primary anchor for domain attribution. The public structure of the market shows why. Newfold Digital, owned by Clearlake Capital and Siris Capital since February 2021, runs Bluehost, HostGator, Network Solutions, Register.com, Web.com, Domain.com, and CrazyDomains as separate brands on one company, and its SnapNames arm holds more than 500 registrar accreditations. Tucows operates OpenSRS, Enom, Ascio, and EPAG as wholesale platforms behind more than 13,000 reseller brands, with more than 14 million domains on OpenSRS alone. DropCatch's parent, TurnCommerce, held more than 1,500 accreditations by September 2026, about 47 percent of all accredited registrars, most of them numbered shell entities that exist to win expiring names. ObscureIQ's early-2026 review of 116 entities across registrars, resellers, aftermarket platforms, WHOIS and passive-DNS providers, scanners, and threat-intelligence platforms found the same pattern. Of the 71 entities for which an ultimate parent could be established, 48 belong to six companies: Newfold Digital (15 brands), Team Internet (9), GoDaddy (8), Tucows (7), United Internet (6), and Mastercard (3). Three of those groups also operate the WHOIS privacy proxies that appear in public records for their registrars (Domains By Proxy for GoDaddy, Contact Privacy for Tucows, Withheld for Privacy for Namecheap under CVC), so the name on a privacy-shielded record identifies the parent, not the registrant. Annex A carries the map.

The governing frame: registrar-based clustering errs in both directions at once. It groups domains that share a brand label but not a control plane, and it separates domains that share a control plane under different labels. Because the error is systematic rather than random, confidence built on it is confidently wrong. Replacing it means classifying on infrastructure dependencies and ultimate control, with registrar identity demoted to context. CB-052 makes the ownership argument for the vendors a principal buys from; this brief makes it for the method those vendors, and a principal's own investigators, use.

**Two independent registrars sharing a backend are one attribution anchor wearing two brand identities.**

## *THE SIGNAL // THE STRUCTURE THE BRAND LAYER HIDES*

RETAIL BRANDS, ONE COMPANY · 2021 ONWARD

Clearlake completed its $3.0 billion acquisition of Endurance International Group on 10 February 2021 and merged it with Web.com to form Newfold Digital, combining Bluehost, HostGator, Network Solutions, Register.com, Web.com, Domain.com, and CrazyDomains, about 6.7 million customers, under one owner. Each brand kept its storefront, its support line, and its name on the invoice. A domain at Bluehost and a domain at Network Solutions share an owner, and often a backend, while a registrar-name cluster treats them as unrelated.

WHOLESALE PLATFORMS · STANDING

Tucows describes its domains business as powering more than 13,000 resellers worldwide through OpenSRS, Enom (acquired 2017), Ascio (2019), and EPAG (2011), with more than 14 million domains on OpenSRS alone. A reseller brand is what a registrant sees; the registrar of record, the nameservers, and the WHOIS privacy service belong to the platform. Thousands of "different registrars" resolve to one operational anchor.

SHELL ACCREDITATIONS · SEP 2026

On 3 September 2026 Domain Incite reported that DropCatch's parent had acquired 300 more numbered shell registrars, taking it past 1,500 accreditations, about 47 percent of the 3,323 registrars ICANN accredits, with Newfold's SnapNames at more than 500. Roughly three in five accredited registrars therefore belong to two companies and exist to catch expiring domains, not to serve registrants. A registrar name drawn from that pool identifies a lottery ticket, not an operator.

OWNERSHIP ABOVE THE BRAND · 2024 TO 2025

The layer above the registrar consolidated too, as CB-052 records: Mastercard now owns Recorded Future and, beneath it, the SecurityTrails passive-DNS history and DNS Spy; Permira owns Squarespace and the former Google Domains book; CVC agreed in September 2025 to a majority stake in Namecheap; Markmonitor moved to Com Laude under PX3 Partners. Public attribution datasets did not update at the same pace, so the gap between the brand-level map and the control-plane map widened.

PRIMARY REVIEW · 2025 TO 2026

ObscureIQ's early-2026 review classified 116 entities in the domain-intelligence landscape by ultimate parent, layer, business model, and the kind of data each holds. Forty-five carried no traceable parent or were independent; of the 71 that did, 48 sat under six parents, and the largest, Newfold Digital, ran fifteen brands spanning retail registrars (Bluehost, HostGator, Domain.com), legacy registrars (Network Solutions, Register.com, Web.com), the aftermarket (SnapNames, NameJet), and wholesale (ResellerClub, LogicBoxes). Team Internet ran nine, from Key-Systems and Hexonet at wholesale to 101domain and SafeBrands in brand protection. Fifty-one of the 116 were WHOIS and ownership lookup tools, most of them reading the same upstream registries. Annex A (CB-053-A) publishes the ownership map; the entity-level notes stay internal.

**SO WHAT** "Registered at the same place" and "registered at different places" both tell you less than they used to. Anyone who links domains to you, or clears them, on that basis is guessing with a straight face.

## THE MECHANISM // WHY THE METHOD FAILS, AND WHO IT FAILS

### THE INFRASTRUCTURE BRANDS OBSCURE

Behind the brand-level map sit shared technical components: nameserver infrastructure, autonomous system numbers, certificate authorities, DNS resolution backends, hosting environments, and pooled WHOIS privacy services. When two independent registrars share nameserver patterns they are operationally one attribution anchor wearing two brands, and the review found this pattern widespread rather than anomalous. The brand-level map and the infrastructure-level control map have decoupled.

### WHY SINGLE-AXIS ENRICHMENT FAILS

Traditional workflows take a domain, look up its registrar, and cluster on registrar identity. When registrar identity decouples from infrastructure identity, the cluster is wrong two ways at once: it groups domains that share a brand label but not a control plane, and it misses domains that share a control plane under different labels. The error is systematic, not random, so risk scoring produces high-confidence conclusions about relationships that do not exist while missing ones that do.

### HOW IT REACHES A PRINCIPAL: THE REPORT THAT NAMES YOU

Attribution errors travel. A protective-intelligence report that links a harassing domain to a principal's former employee, a competitor, or a named individual because both registered through the same reseller brand is making the weak inference in its confident form. CB-246 sets the validation gate for any deliverable that names a person; a registrar match on its own does not pass it. Ask what else connects the domains: nameserver history, certificate issuer and timing, hosting, content, registrant data where lawfully available. If the answer is only "same registrar," the answer is nothing.

### HOW IT REACHES A PRINCIPAL: THE FOOTPRINT THAT LOOKS DIVERSIFIED

The same decoupling runs the other way for a principal's own domains. A family's personal, foundation, and operating-company domains registered through three different brands may sit on one Newfold backend or one Tucows platform, with one privacy service, one support queue, and one account-recovery process between an attacker and all of them. Diversification by logo is cosmetic, as CB-052 says of intelligence feeds. Check the registrar of record and the nameservers, not the storefront.

FIGURE 1 // THE REGISTRAR LAYER IN NUMBERS

| | | | |
|---|---|---|---|
| **3,323** | **47%** | **13,000+** | **48/71** |
| ICANN-accredited registrars, September 2026. | Share held by one drop-catching business, more than 1,500 numbered shells. | Reseller brands on Tucows' wholesale platforms; 14M+ domains on OpenSRS alone. | Reviewed entities with a traceable parent that belong to just six companies. |
| DOMAIN INCITE, 3 SEP 2026 | DOMAIN INCITE, 3 SEP 2026 | TUCOWS / OPENSRS | OBSCUREIQ LANDSCAPE REVIEW, EARLY 2026 (ANNEX A) |

FIGURE 2 // WHAT REPLACES REGISTRAR IDENTITY: FIVE ATTRIBUTION AXES

| | |
|---|---|
| **CORPORATE CONTROL** | Ultimate ownership and financial control, not the brand on the invoice. |
| **INFRASTRUCTURE** | Technical dependencies: nameservers and their history, ASNs, certificate authorities and issuance timing, hosting. |
| **FUNCTIONAL ROLE** | Where the entity sits in the domain lifecycle: registry, registrar of record, reseller, DNS operator, host, privacy proxy. |
| **USE-CASE ALIGNMENT** | Which intelligence use case the data actually serves, and what it was collected for. |
| **VISIBILITY DEPTH** | Depth and temporal reach of the visibility the entity holds: a snapshot, a history, or a live feed. |

> **SO WHAT** Three in five "registrars" are shells owned by two companies, and thousands more are storefronts on one platform. A registrar name is a starting question, not a finding.

## *THE STEELMAN // THE CASE THAT REGISTRAR CLUSTERING STILL WORKS*

**THE BEST CASE FOR THE OTHER SIDE**

+ Registrar-based clustering is fast, cheap, and correct for the large majority of domains that are not deliberately structured to hide.
+ Multi-axial, infrastructure-anchored attribution is heavy and expensive, and few teams have the tooling to run it.
+ The shell-registrar figure overstates the problem: drop-catch accreditations register almost nothing a principal will ever meet, so the operative market is far more concentrated and far more legible than 3,323 names suggest.

Concede that registrar clustering is cheaper and often right, that multi-axial work is heavier, and that the third point is fair: the shell count is a symptom, not the mechanism. The mechanism is the reseller and multi-brand structure, and it applies exactly to the domains a principal does meet. The error it produces is systematic and confident: it manufactures relationships that do not exist and hides ones that do, and it does so precisely where an adversary has structured for it. Heavy is no longer optional overhead. It is the minimum competence for a landscape where brand independence has decoupled from infrastructure independence, and the first thing to demand of anyone who hands a principal a report that links domains to people.

## ASSESSMENT

FIGURE 3 // ANALYTIC CONFIDENCE BY CLAIM

| | |
|---|---|
| The registrar layer is heavily concentrated behind separate brands: multi-brand owners, wholesale platforms, and shell accreditations. | **STRONG / PUBLIC RECORD** |
| Registrar identity alone is an unsound primary attribution anchor; it errs in both directions systematically. | **STRONG** |
| Ownership concentration extends across the reviewed landscape: 48 of 71 parented entities under six companies, with privacy proxies owned by the same groups. | **STRONG / OBSCUREIQ REVIEW OF 116 ENTITIES, ANNEX A** |
| Infrastructure reuse across competing brands is widespread at the DNS, hosting, and certificate layers as well. | **MODERATE / ENTITY-LEVEL EVIDENCE INTERNAL** |
| Multi-axial, infrastructure-anchored attribution is the minimum competence for anyone linking domains to people. | **STRONG / AS A STANDARD, NOT A MARKET OBSERVATION** |
| How quickly vendors and buyers adopt the heavier methodology. | **MODERATE / FORWARD** |
| Domains at the same registrar are related; domains at different registrars are independent. | **REJECTED / NEITHER INFERENCE SURVIVES THE STRUCTURE ABOVE** |

## POSTURE

### FOR PRINCIPALS

→ When a report links domains to a person, including you, ask what connects them beyond where they were registered. Nameserver history, certificate timing, hosting, and content are evidence; a shared registrar or reseller brand is context. A report that cannot answer has not met the CB-246 gate for naming anyone.

→ For your own domains, ask which registrar of record and which nameservers sit behind each brand you use. Three storefronts on one platform are one account-recovery process away from all three.

### FOR FAMILY OFFICES

→ Reset vendor evaluation. Vendors claiming breadth by brand-level count may not possess it, so evaluate on demonstrable ability to surface infrastructure-level relationships across brand identities, not on logo count. Ask a candidate vendor to show two brands it knows to share a backend, and how it knows.

→ Diversify domain holdings by registrar of record and nameserver operator, not by brand, and confirm that privacy-proxy and account-recovery controls differ where the brands do.

### FOR SECURITY & LEGAL FUNCTIONS

→ Audit existing attribution work. Where past investigations relied on registrar-name clustering, re-cluster against infrastructure-level signals before relying on prior conclusions, and downgrade anything tagged high confidence under the broken method until reverified. Any conclusion that names a person on registrar evidence alone is withdrawn until it passes on other axes.

→ Move to nameserver patterns, ASN clustering, certificate-issuer convergence, and hosting reuse as primary axes, with registrar identity demoted to context, and record which axis carried each link so a reviewer can see what the confidence rests on. This is intelligence analysis, not legal advice.

**CONFIDENCE** High on the public structure of the registrar layer: Newfold's brands and ownership are in its own releases, Tucows' reseller and domain counts are its own statements, and the accreditation counts are from Domain Incite's reporting of ICANN data in September 2026. High on the methodological claim that registrar identity alone errs systematically, which follows from that structure. High on the ownership concentration figures, which come from ObscureIQ's early-2026 classification of 116 entities and are published as Annex A. Moderate on the breadth of technical infrastructure reuse at the DNS, hosting, and certificate layers, where the entity-level evidence remains internal. Moderate on adoption timing.

**METHOD** Revised edition. First published 2 May 2026; facts re-verified and analysis revised 10 September 2026. The revision grounds the argument in public market structure (multi-brand owners, wholesale reseller platforms, shell accreditations), publishes the ownership figures from the internal review as Annex A, adds the two principal-facing mechanisms (misattribution in reports that name people; cosmetic diversification of a family's own domains), aligns the ownership section with the revised CB-052, corrects the Namecheap date, adds a Rejected row, and sets the brief to public release. Cross-read against CB-052, CB-054, and CB-246.

**SOURCES** Newfold Digital on its formation (10 February 2021). Tucows / OpenSRS, About (reseller and domain counts as stated). Domain Incite, "DropCatch acquires 300 more registrars" (3 September 2026). CB-052 and its sources for the Mastercard, Squarespace, Namecheap, and Markmonitor transactions. ObscureIQ Domain Intelligence Landscape review, early 2026 (116 entities; ownership map published as CB-053-A; entity-level notes internal).

*Scope note: the review's entity-level notes are not published; its ownership map is (CB-053-A); the public figures are as stated by the companies and by Domain Incite and were not independently recomputed from ICANN's registrar list. Accreditation share is a structural indicator, not a measure of the domains a principal is likely to encounter. This is intelligence analysis, not legal advice.*

---

OBSCUREIQ INTERNAL ANALYSIS // ARCHIVE COMM-053-DOMAIN-ATTRIBUTION-2026Q2 // XREF **CB-053-A CB-052 CB-054 CB-246** // ACCESS PUBLIC · PUBLIC-INTEREST RELEASE · REVISED 10 SEP 2026