“A STRUCTURED REVIEW OF INTERNET DOMAIN RESEARCH: REGISTRATION, MARKET, SECURITY, AND LAW”

Research Paper

Peter Wilfahrt, Swiss School of Business and Management, Geneva, Switzerland, pw@pw.is

“Abstract”

This structured review synthesises the current state of research on Internet domain names across five clusters: market structure and growth, registration behaviour, DNS abuse and cybersecurity, trademark law and cybersquatting, and domain valuation in the secondary market. It draws on registry statistics (Verisign and DNIB), ICANN research (INFERMAL), independent measurement studies (Interisle Consulting Group), WIPO case statistics, the European Commission's DNS abuse study, and peer-reviewed work, most of it published between 2011 and 2026. The global base reached 401.6 million registered domain names in mid-2026 and grew by 8.1% year on year, with new generic top-level domains expanding at more than 30% a year. Abuse grows faster than the market: 19.5 million unique domains were used in malware, phishing or spam attacks in 2025, more than twice the 2024 figure, and at least 10% of all domains newly registered in gTLDs in 2025 were later blocklisted. The evidence, most of it correlational, points to price as the main driver of abuse. Phishing domains cost on average USD 4.71 at registration against USD 8.62 for benign domains, and each one-dollar reduction in price is associated with an estimated 49% increase in malicious registrations. The review documents the legal instruments available to brand owners (UDRP, URS, ACPA, NIS2 Article 28), the economics of the domain aftermarket, and the implications of the ICANN 2026 gTLD round, which closed with more than 1,600 applications. It identifies four research gaps: the cost of domain abuse for small and medium-sized enterprises, econometric evidence on registrar pricing and abuse, the security of blockchain-based namespaces, and the causal effect of registrant verification under NIS2.

Keywords: *Internet domains, DNS abuse, cybersquatting, domain valuation, new gTLDs, registrar pricing, SMEs, NIS2*

1 Introduction

Domain names are the addressing layer of the public Internet. Every website, e-mail address and API endpoint depends on a name that resolves through the Domain Name System (DNS). For a business, the domain is also an economic asset: it carries the brand, it routes customer contact, and it can be sold. Over the past two decades, domains have therefore become a subject of research in computer science, law, economics and marketing at the same time.

This paper synthesises that research. It covers work published mainly between 2011 and 2026 and is organised around five questions. How large is the domain market, and what drives its growth? What distinguishes legitimate from malicious registration behaviour? How is the DNS used for cybercrime, and what does detection cost? Which legal instruments protect trademark owners? And how are domain names priced in the secondary market?

The economic perspective runs through all five clusters. The main finding is that the domain market and the market for domain abuse respond to the same variables: price, automation and verification requirements. Measures that lower the cost of a legitimate registration also lower the cost of a phishing

campaign. The paper pays particular attention to small and medium-sized enterprises (SMEs), which hold most business domains but are almost absent from the empirical literature.

1.1 Methodology

The study is a structured narrative review. Sources were identified in three steps between November 2024 and September 2026. First, primary statistics were taken from registry and industry publications: the Domain Name Industry Brief (DNIB, sponsored by Verisign), WIPO case statistics, ICANN research reports and the measurement studies of Interisle Consulting Group. Second, academic publications were searched in the ACM Digital Library, SSRN, Wiley Online Library and Springer for the terms domain registration, DNS abuse, cybersquatting, typosquatting and domain valuation. Third, practitioner reports from security vendors (DomainTools, Palo Alto Networks Unit 42, CSC) were included where they contain original measurements.

Inclusion required original data or a documented method. Marketing content without a stated method was excluded, as were secondary summaries of studies already covered. Foundational work published before 2011 (Akerlof, 1970; Anderson and Moore, 2006; Moore, Clayton and Anderson, 2009; Moore and Edelman, 2010) is included where it provides the theoretical or measurement basis for later studies. Practitioner guides and law-firm publications (Canella Camaiora, 2025; Dynadot, 2026; Name Experts, 2026; SentinelOne, 2025; Wissen Research, 2023) are cited for definitions and industry conventions, not as empirical evidence. The final corpus comprises the 68 sources listed in the references. Twenty are peer-reviewed journal articles or conference papers: four predate 2011, thirteen appeared between 2011 and 2018, and three since 2019. Three are commissioned studies or working papers (Bayer et al., 2022; Nosyk et al., 2024; Gasimova, 2022). Official documents from ICANN, WIPO, EU institutions and the FBI account for fifteen sources, and registry statistics and independent measurement reports (DNIB, Verisign, Interisle, DNS Research Federation, M3AAWG) for another thirteen. The rest are four security-vendor reports, eight aftermarket data sources and trade-press articles, and the five practitioner guides named above. Where figures from independent sources converge, they are treated as corroborated. Where they diverge, both are reported with their method. All figures were verified against the original publication in September 2026.

1.2 Scope and limitations

The review covers the domain lifecycle from registration through use, abuse, dispute and resale. It does not cover DNS protocol internals, DNSSEC deployment or registrar systems architecture. The geographic scope is global, with country-level data for the United States, the European Union and China where available. Data through the second quarter of 2026 is included.

Five limitations apply. Vendor reports (DomainTools, CSC, Palo Alto Networks) have a commercial interest in documenting threats, and their figures should be read as upper bounds; a similar caveat applies to the DNIB, which is sponsored by Verisign, the operator of .com and .net. Abuse statistics depend on blocklists, which undercount abuse that is never reported and can overcount where compromised legitimate domains or false positives are listed. And the secondary market is opaque: reported sales cover only transactions that sellers choose to publish. The review was conducted by a single author without a formal quality appraisal, so source selection and weighting have not been checked independently. Finally, most of the peer-reviewed measurement studies cited date from 2011 to 2018; for the period since 2019 the review relies largely on ICANN and industry reports, with recent peer-reviewed evidence limited to generated squatting domains and blockchain naming systems.

2 Global Domain Market: Structure and Growth

2.1 Market size and trajectory

At the end of the second quarter of 2026, 401.6 million domain names were registered across all top-level domains (TLDs), an increase of 29.9 million or 8.1% year on year (DNIB, 2026b). Growth has accelerated sharply. In the first quarter of 2025 the base stood at 368.4 million and grew at 1.7% a year (DNIB, 2025a). Five quarters later the annual rate had more than quadrupled. Almost all of the acceleration comes from new generic TLDs (ngTLDs), which added 13.4 million names in twelve months, and from .com, which returned to growth after a decline in 2024.

Behind the net figure sits a high-churn market. New .com and .net registrations alone reached 12.7 million in the second quarter of 2026 (DNIB, 2026b). Renewal rates vary widely by segment: .com and .net renew at about 75% (preliminary estimate), ngTLDs at 31%, and individual low-price extensions such as .shop at 14.2%, .xyz at 17.5% and .top at 18.9% (DNIB, 2026b). A large share of new registrations therefore never survives its first year. Table 1 summarises the key indicators.

Geographically, the ccTLD space is led by .cn, .de, .uk, .ru and .nl. At the end of the first quarter of 2026, the ten largest ccTLDs held 57.6% of all 146.3 million ccTLD registrations, and 316 ccTLDs are delegated in the root zone (DNIB, 2026a). For the registry industry, the market is profitable: Verisign, which operates .com and .net, reported revenue of USD 435 million and operating income of USD 296 million in the second quarter of 2026, an operating margin of 68% (Verisign, 2026).

Indicator	Value	Source
Registered domains worldwide (Q2 2026)	401.6 million	DNIB (2026b)
Year-on-year growth (Q2 2026)	+29.9 million (+8.1%)	DNIB (2026b)
.com and .net combined (Q2 2026)	179.1 million	DNIB (2026b)
ccTLD registrations (Q2 2026)	148.6 million	DNIB (2026b)
ngTLD registrations (Q2 2026)	52.9 million (+34.0% YoY)	DNIB (2026b)
ngTLD share of all registrations (Q2 2026)	13.2%	DNIB (2026b)
Renewal rate, .com and .net / ngTLDs	75.2% (preliminary) / 31.0%	DNIB (2026b)
TLDs delegated in the root zone (Q4 2025)	1,265	DNIB (2025b)
Verisign quarterly revenue (Q2 2026)	USD 435 million	Verisign (2026)
Domains used in cyberattacks (2025)	19.5 million	Interisle (2025a)
UDRP cases filed with WIPO (2025)	6,282	WIPO (2026)

Table 1. Key indicators of the global domain market and its abuse, 2025-2026.

2.2 TLD ecosystem: legacy gTLDs, ccTLDs and new gTLDs

The namespace has three segments with very different economics. Legacy gTLDs (.com, .net, .org and a handful of others) hold about 200 million names, renew reliably and command the highest resale prices. ccTLDs hold 148.6 million names and are governed nationally; their renewal rates, between 72% for .ru and 82% for .fr, are the highest in the industry (DNIB, 2026a). New gTLDs, introduced from 2013 onwards, hold 52.9 million names, 13.2% of the market at mid-2026 (12.4% at the end of

2025), and their combined renewal rate of 31% shows that most of their volume is speculative or short-lived (DNIB, 2025b; 2026b).

That pattern was visible from the start. Halvorson et al. (2015) analysed the first 480 new gTLDs launched in 2013 and 2014 and found that most registrations were speculative or defensive: a large share of names were parked, and only a minority resolved to content that differed from the registrant's existing sites. The 31% renewal rate a decade later indicates that the segment has not outgrown that profile.

The three segments also differ in price. Verisign charges registrars USD 10.26 a year for a .com name, rising to USD 10.97 on 1 November 2026, and registrars add their margin on top (Allemann, 2026a). Many ngTLDs are sold at first-year promotional prices below one dollar, in bulk, through automated interfaces (Interisle, 2023; Nosyk et al., 2024). That pricing model explains both the growth of the ngTLD segment and, as sections 3 and 4 show, its share of abuse. The ICANN Notice of Breach issued against the .top registry in July 2024 for failing to act on abuse reports, cured only in June 2025, illustrates how thin the operational margin for low-price registries can become (ICANN, 2025a).

.com remains the reference asset. It accounts for 59% of sales at Sedo and 74% of the dollar volume in the reported aftermarket (Sedo and InterNetX, 2025; Allemann, 2025). Among ccTLDs, .ai (Anguilla) has become a special case: repurposed for artificial-intelligence companies, it quadrupled in size between 2022 and 2025 and doubled its aftermarket dollar volume in 2024 alone (SIDN, 2025; Allemann, 2025).

2.3 The registrar and registry business model

The contracted supply chain has three tiers. ICANN contracts with registries (which operate a TLD) and accredits registrars (which sell names to registrants); resellers and hosting companies form a fourth, unregulated layer. Revenue is annual and recurring, which gives the industry the economics of a subscription business with very low marginal cost. Verisign's 68% operating margin, earned mainly on .com, is the extreme case (Verisign, 2026). Registrars operate on thinner margins and compete on price, bundling and automation. The economic incentive to maximise registration volume, regardless of who registers, is built into the model. Section 4.3 shows what that incentive produces.

2.4 ICANN's 2026 gTLD round

ICANN opened the second application window for new gTLDs on 30 April 2026, the first since 2012. The window closed on 12 August 2026 with more than 1,600 applications (ICANN, 2026a; 2026b). The 2012 round had drawn about 1,930 applications and produced more than 1,200 new extensions. The evaluation fee is USD 227,000 per application. Compared with 2012, the Applicant Guidebook adopted on 30 October 2025 introduces an Applicant Support Programme for applicants from underserved regions, a Registry Service Provider pre-evaluation, applications in 27 scripts for internationalised domain names, and stricter contractual obligations on DNS abuse (ICANN, 2026a). Closed generic strings, single-registrant applications for dictionary words, remain excluded until a public-interest framework exists.

For brand owners the round has two sides. A .brand TLD removes dependence on third-party registries and gives IT departments full control of the namespace. At the same time, every new open extension adds a namespace in which a brand can be squatted. Interisle (2026) warns that without stronger registration controls the round will add supply to a market in which criminals already buy one in ten newly registered gTLD names.

3 Domain Registration Behaviour

3.1 Legitimate demand drivers

Legitimate demand has four sources: business formation, the digitalisation of existing firms, brand strategy including defensive registrations, and investment. In the European Union, 79.0% of enterprises operated a website in 2025, with rates above 90% in Finland, Denmark, Austria, the Netherlands, Germany and Sweden and below 60% in Bulgaria, Romania and Greece (Eurostat, 2026). Since SMEs make up 99.8% of EU enterprises (European Commission, 2025), the large majority of business domains in Europe belong to small firms. The same firms show the lowest levels of digital skills investment: 21% of SMEs provided ICT training in 2024 against 73% of large enterprises (Eurostat, 2025).

Lindenthal (2018) models the primary market as a monocentric system in which registrants trade off name quality against price and distance from the .com centre, in the same way that households trade off location against rent. The model explains why short, generic .com names are exhausted and why demand spills over into ccTLDs and ngTLDs. Sedo reports that mid-range transactions from start-ups and SMEs, rather than headline sales, drove aftermarket growth in 2024 (SIDN, 2025), which is consistent with the model.

3.2 Malicious registration patterns

Hao et al. (2013) provided the first large-scale evidence on how spammers register domains. Using five months of .com registration data, they showed that spammers register in bursts, favour a small number of registrars, reuse name servers and often re-register domains that had previously expired. Earlier work by the same group showed that malicious domains display distinctive DNS behaviour within hours of registration (Hao, Feamster and Pandrangi, 2011). Both findings anticipated the design of time-of-registration detection systems (Hao et al., 2016).

The ICANN INFERMAL study is the most comprehensive analysis to date (Nosyk et al., 2024). Over two years the authors compared 14,500 phishing domains with a matched set of benign domains across 73 registrar and registry features. The most consistent result is price sensitivity. Phishing domains cost on average USD 4.71 at registration; benign domains cost USD 8.62. In the regression model, each one-dollar reduction in price is associated with a 49% increase in malicious registrations, and the availability of free add-on services such as hosting is associated with an 88% increase in phishing. Bulk discounts, unrestricted API access and anonymous payment methods all raise abuse; mandatory e-mail or phone verification and restrictive registration policies lower it. ICANN's own reading of the study is that registrar and TLD policy decisions shape the threat landscape and that targeted friction, such as restricted API access and identity verification, reduces abuse without excluding legitimate registrants (ICANN, 2025b).

Interisle's measurements confirm the pattern at market scale. Of the 19.5 million domains used in attacks in 2025, 7.3 million had been registered in bulk, an increase of 177% over 2024 (Interisle, 2025a). Registrations that exactly match a brand name grew by 97% in a single year (M3AAWG, 2025). Event-driven surges are well documented: CSC (2024) counted about 59,000 third-party registrations around the 2024 US presidential election, and Hao et al. (2013) observed the same burst behaviour a decade earlier.

4 DNS Abuse and Cybersecurity

4.1 Scale and distribution of abuse

Abuse is growing faster than the market. Interisle recorded more than 26 million malware, phishing and spam events in 2025, 60% more than in 2024, involving 19.5 million unique domains compared with 8.6 million a year earlier (Interisle, 2025a). Domains registered specifically for criminal use rose by 149%. DomainTools (2024) reported 395,000 confirmed malicious domains among 106 million

registrations in 2024, a rate of 0.37%. Interisle's later estimate, based on blocklists rather than a single vendor's risk score, is far higher: of the nearly 85 million domains newly registered in gTLDs in 2025, at least 8.5 million, about 10%, had been blocklisted by mid-May 2026, and projections that add future blocklisting and associated unlisted domains raise the estimate to 16.8 million, or 20% (Interisle, 2026). The gap between the two figures reflects different years, different denominators and different methods, so the two figures are compatible. Vendor risk scores flag abuse confirmed by one vendor; aggregated blocklists capture abuse reported by many.

Abuse concentrates. In 2025, new gTLDs held 12% of all registrations but 47% of cybercrime domains, nearly four times their market share, and more than half of the domains registered for criminal purposes (Interisle, 2025a). Within the ccTLD space, five extensions account for 77% of reported abuse (Interisle, 2025b). At registrar level the concentration can be extreme: at one registrar, 88% of 2025 registrations were identified as malicious (Interisle, 2026). Interisle (2023) found that 90% of phishing domains in new gTLDs sit in just 25 extensions. The share of phishing domains registered in ngTLDs rose from 25% to 42% in a single year (Interisle, 2025c).

The concentration is not new. Korczyński et al. (2018) compared abuse rates across legacy and new gTLDs for 2014 to 2016 and found that new gTLDs already carried a disproportionate share of spam and phishing domains, and that abuse concentrated in a small number of registries and registrars with permissive policies. Since then the structure has stayed the same and the scale has grown. The European Commission's DNS abuse study, the largest independent measurement of the EU namespace, confirms the pattern for 2021: new gTLDs held an estimated 6.6% of the market but 20.5% of abused domains, while EU ccTLDs accounted for only 0.8% of abused domains (Bayer et al., 2022). The same study cautions that about 25% of phishing domains and 41% of malware-distribution domains had been registered by legitimate users and compromised later, so abuse counts do not measure registration decisions alone.

4.2 Abuse typology

The literature converges on a small set of abuse types, regardless of vocabulary. Phishing domains impersonate a brand to harvest credentials. Typosquatting exploits predictable typing errors. Cybersquatting registers a brand-identical or confusingly similar name for resale or leverage. Malware distribution and botnet command-and-control use domains as infrastructure rather than as bait. Bitsquatting, the rarest form, relies on hardware bit errors to divert traffic (Stobbs IP, 2024). ICANN's contractual definition of DNS abuse, taken from SSAC report SAC115, covers malware, botnets, phishing, pharming and spam used as a delivery vehicle (GNSO, 2025). Cybersquatting and trademark infringement fall outside that definition and are handled by the dispute mechanisms in section 5.

All types share a lifecycle. Hao, Feamster and Pandrangi (2011) showed that malicious domains are used within hours of registration, and later work confirmed that most abuse is visible within the first week (Hao et al., 2016). The economic corollary is that a phishing domain has to earn back its registration fee in days. Cheap domains make that arithmetic work; verified, higher-priced domains do not.

4.3 The economics of abuse: price, automation and verification

Three variables explain most of the variation in abuse rates between registrars and TLDs. The first is price. INFERMAL's USD 4.71 against USD 8.62 comparison and its 49% price-effect estimate are the strongest quantitative evidence available (Nosyk et al., 2024). An earlier natural experiment points the same way: when the .cn registry ended promotional pricing and introduced documented registrant checks in December 2009, spam-advertised domains moved to other TLDs within months (Liu et al., 2011). Two caveats apply to the INFERMAL estimates. They are conditional correlations from a generalised linear model, not causal effects, as ICANN's own clarification stresses (ICANN, 2025b), and they cover phishing only. The second variable is automation. Bulk registration through APIs allows an attacker to buy thousands of names in minutes, and bulk-registered attack domains grew by 177% in 2025 (Interisle, 2025a). The third is verification. Registries that verify identity at registration,

including many European ccTLDs, record consistently lower abuse rates (Bayer et al., 2022; DNS Research Federation, 2025).

Vendor telemetry adds infrastructure-level detail. DomainTools (2024) identifies specific registrar, name-server and hosting combinations as reliable predictors of malicious activity. Palo Alto Networks Unit 42 (2020) found that squatting operators cluster around financial, social-media and e-commerce brands and use free TLS certificates to appear legitimate. Interisle (2025a) reports that the number of IP addresses used for hosting attacks fell by 20% while the number of domains more than doubled, which suggests that criminals now treat domains as the disposable resource and hosting as the stable one.

4.4 Detection methodologies

Detection has moved from reactive blocklisting to prediction at registration time. PREDATOR (Hao et al., 2016) classified domains at the moment of registration using registrar, name-server, registrant history and lexical features and achieved 70% detection at a 0.35% false-positive rate, days before the domains appeared on any blocklist. Vissers et al. (2017) showed for the .eu zone why registration data carry so much signal. Using registrant information from 14 months of registrations, they traced at least 80% of malicious domains to just 20 campaigns, whose processes were only partly automated. Registrant and infrastructure data, more than the name string, are what give such campaigns away.

At the policy level, ICANN's Domain Abuse Activity Reporting (DAAR) system publishes monthly abuse rates per gTLD, and the 2024 amendments to the Registry and Registrar Agreements require contracted parties to act on well-evidenced abuse reports (GNSO, 2025). Interisle (2025a) and INFERMAL agree on the practical recommendations: identity verification for bulk registrants, rate limits on API registration, and the removal of promotional pricing below cost.

5 Trademark Law and Cybersquatting

5.1 The UDRP and its caseload

The Uniform Domain Name Dispute Resolution Policy (UDRP), adopted by ICANN in 1999 on WIPO's recommendation, is the primary instrument against cybersquatting. A complainant must show three things: that the domain is identical or confusingly similar to a mark in which the complainant has rights, that the registrant has no rights or legitimate interests in it, and that the domain was registered and is being used in bad faith (ICANN, 1999, para. 4(a); Gasimova, 2022). The remedy is transfer or cancellation of the domain; damages are not available. At WIPO, the fee for one to five domain names is USD 1,500 before a single panelist and USD 4,000 before a three-member panel, plus counsel; an expedited service delivers a decision within one month of commencement for USD 4,000 (WIPO, no date).

Caseload has risen with the market. WIPO administered 6,282 cases in 2025, the highest number since the policy began, after 6,168 cases from complainants in 133 countries in 2024 and 6,192 in 2023 (WIPO, 2025; 2026; Allemann, 2026b). Cumulatively WIPO has resolved more than 80,000 cases, of which more than 70,000 concern gTLDs and nearly 10,000 ccTLDs (WIPO, 2026). .com accounts for by far the largest share of disputes, followed by .shop, .net and .org (Allemann, 2026b). The most active complainant sectors are banking and finance, biotechnology and pharmaceuticals, fashion and retail; the leading complainant representatives are corporate domain-management firms such as CSC, Nameshield and IP Twins rather than law firms (WIPO, 2025). The UDRP applies to all gTLDs; for ccTLDs it applies only where the national registry has adopted it or a variant, and WIPO now provides dispute-resolution services for 87 ccTLDs (WIPO, 2026).

5.2 Other legal instruments

Four further instruments matter in practice. The Uniform Rapid Suspension system (URS), introduced with the 2012 gTLD round, offers a cheaper and faster procedure for clear-cut cases in new gTLDs,

but the remedy is only suspension for the remaining registration term, which limits its use (ICANN, 2019). The US Anticybersquatting Consumer Protection Act (ACPA) of 1999 allows trademark owners to sue in federal court for statutory damages of USD 1,000 to 100,000 per domain name (15 U.S.C. § 1117(d)), which the UDRP cannot award, at the cost of litigation timelines. The Trademark Clearinghouse gives mark holders a sunrise period of at least 30 days and trademark-claims notices for at least the first 90 days of general registration in every new gTLD launch (ICANN, no date) and is likely to remain the main defensive tool in the 2026 round.

The fourth instrument is regulatory. When the GDPR took effect in May 2018, registrars redacted most personal data from the public WHOIS, and ICANN suspended its contractual WHOIS obligations through a Temporary Specification (DNS Research Federation, 2025). Brand owners and law enforcement lost the ability to identify registrants quickly. Article 28 of the NIS2 Directive (Directive (EU) 2022/2555) reverses part of that. It requires TLD registries and registrars operating in the EU to collect and maintain accurate and complete registration data, to verify it, to publish non-personal data such as legal-entity information, and to disclose personal data to legitimate access seekers within 72 hours of a substantiated request (DNS Research Federation, 2024). Transposition was due by October 2024 and is uneven across member states. For registrars the article adds a verification cost per registration; for abuse researchers it restores a data source that had disappeared. INFERMAL's finding that verification requirements reduce malicious registrations suggests the two effects are linked.

5.3 Forms of cybersquatting

The literature distinguishes two groups of conduct. The first exploits proximity to an existing brand: classical cybersquatting (registering the brand for resale), typosquatting (predictable misspellings) and brandjacking (using the brand for phishing or counterfeit sales). The second operates on the namespace itself: registering high-value generic terms, geographic names, or brand strings in newly launched extensions such as .app, .shop or .ai (Wissen Research, 2023; SentinelOne, 2025). Reverse domain-name hijacking, in which a trademark holder uses the UDRP against a legitimate registrant, is the mirror case and is sanctioned by panels. Unit 42 measured the scale of the first group in 2019: 13,857 squatting domains were registered per day, of which 18.6% were actively malicious and a further 36.6% were rated high risk (Palo Alto Networks Unit 42, 2020).

The academic measurement literature on typosquatting is older and more precise than the vendor reports. Moore and Edelman (2010) estimated that at least 938,000 typosquatting domains targeted the 3,264 most popular .com sites and that most were monetised through pay-per-click advertising, which made search-advertising networks the main funders of the practice. Szurdi et al. (2014) extended the analysis to the long tail of the .com zone and found that about 20% of .com registrations were typosquats, mostly of less popular sites. Agten et al. (2015) tracked typosquatting of the top 500 sites over seven months and showed that 95% of targets were squatted at some point and that the domains changed hands and monetisation strategies frequently. Kintis et al. (2017) identified a further category, combosquatting, in which a brand is combined with another word (for example, paypal-security), and found it more prevalent and longer-lived than typosquatting and harder to detect lexically. Together these studies establish that squatting is an economically rational activity with measurable revenue, which is the premise on which the pricing argument of section 4.3 rests.

5.4 Business impact

For large companies the cost of cybersquatting is mostly enforcement and monitoring. CSC's annual review of the Forbes Global 2000 has found, for five consecutive years, that a majority of the largest companies have not deployed registry locks or DNSSEC on their core domains (CSC, 2024). Since search engines no longer reward keyword domains, the contemporary damage is reputational and operational rather than a loss of search traffic: a squatted domain is used for phishing employees, customers and suppliers (Canella Camaiora, 2025).

For SMEs the cost structure is different and largely unmeasured. A UDRP complaint costs several thousand dollars in fees and counsel, a sum that is trivial for a bank and material for a firm with ten employees. Business e-mail compromise through look-alike domains hits the payment processes of small firms directly. The scale of the exposure is visible in aggregate: the FBI's Internet Crime Complaint Center recorded USD 16.6 billion in reported losses in 2024, of which USD 2.77 billion came from 21,442 business e-mail compromise complaints, and phishing was the most reported crime category with 193,407 complaints (FBI IC3, 2025). Those figures are not broken down by firm size or by attack vector, and no peer-reviewed study quantifies domain-related losses for SMEs. WIPO does not publish complainant size either, but its leading complainant representatives are corporate brand-protection firms whose clients are large companies (WIPO, 2025). The absence of SMEs from the dispute statistics is more plausibly a sign of cost barriers than of low exposure. Section 8 returns to this gap.

6 Domain Valuation and the Secondary Market

6.1 Market scale

The domain aftermarket is the market in which already-registered names change hands. It consists of listing marketplaces (Afternic, Sedo, Atom, Dan.com), auction platforms for expiring names (GoDaddy Auctions, DropCatch, NameJet), brokers and escrow services. Reported transactions are a lower bound for the market, since private sales are rarely published. NameBio recorded 144,700 reported sales worth USD 185 million in 2024, a 32.8% increase in dollar volume on 2023 despite a lower number of transactions; .com accounted for 74.4% of the value (Allemann, 2025). A later count of the same database, including private and off-market entries added afterwards, gives 160,800 sales for 2024 (Freename, 2025); the difference shows how much reported figures depend on the cut-off date. In the first half of 2025 reported sales reached 93,100 transactions and USD 122 million, 42.7% more than a year earlier (NameBio, 2025). The largest disclosed transaction of 2024 was chat.com, bought by OpenAI for USD 15.5 million (SIDN, 2025).

The market is illiquid. The annual sell-through rate of a .com portfolio is 3 to 4%, against 10 to 20% in residential real estate (Freename, 2025). Marketplace commissions range from 9% to 20%, and 69% of Sedo's sales close at a fixed buy-now price rather than by negotiation or auction (Sedo and InterNetX, 2025). The median sale price at Sedo was USD 549 in 2024, up 7%, which reflects the growth of mid-range demand from start-ups and SMEs (SIDN, 2025).

Between registration and resale, most speculative domains are parked. Alrwais et al. (2014) studied the parking ecosystem and found that a significant share of parking traffic was monetised through click fraud and redirection to malicious content, so that the revenue streams of legitimate speculation and abuse overlap in the same infrastructure.

6.2 Value determinants

Lindenthal (2014) built the first constant-quality price index for domain names from a large data set of domain sales covering 2006 to 2013 and showed that domain prices behave like those of an asset class: they co-move with technology equities and online advertising revenue, albeit loosely (the monthly correlation with the NASDAQ-100 is 0.19), and registrations and resale prices form a long-run equilibrium that indicates supply constraints in the namespace. The hedonic regressions identify the pricing factors that practitioners still use: extension (.com carries the premium), length, dictionary-word status, absence of hyphens and digits, and commercial keyword value. Later practitioner guides add existing traffic, backlink authority, domain age and a clean abuse history (Dynadot, 2026; Name Experts, 2026).

The .ai extension shows how quickly determinants can shift. A ccTLD assigned to a territory of 16,000 people became a premium namespace within three years because its string acquired a generic meaning, and its aftermarket dollar volume rose 107% in 2024 while .io, its predecessor as the start-up extension, declined (Allemann, 2025; Sedo and InterNetX, 2025).

6.3 Valuation methods

Three methods dominate practice. Automated appraisals (GoDaddy, Estibot, Atom) regress keyword volume, extension and comparable sales and are useful for portfolio triage below a few thousand dollars. Comparable-sales analysis using NameBio or DNJournal data is the standard for negotiated transactions. Broker appraisal adds qualitative judgement on brandability and end-user demand for high-value names. Name Experts (2026) formalises the resulting spread as a three-tier structure: retail price (what an end user pays), investor price (40 to 60% of retail) and liquidation price (20 to 30% of retail). Lindenthal's (2014) index work suggests why the spread is so wide: because buyer motivation is not observable in advance, no algorithm predicts individual transaction prices reliably, but portfolio-level returns are measurable.

7 Emerging Trends

7.1 Artificial intelligence on both sides

AI changes the cost structure on both sides of the abuse market. On the offensive side, attackers increasingly register generated squatting domains that avoid the brand string altogether. Koide et al. (2023) collected 205,000 such names over 150 days; of 3,498 domains their detector flagged in a four-week trial, 2,821 hosted phishing sites within a month. Language models also create new targets. Asked about 913 global brands, the models tested by Unit 42 hallucinated some 250,000 plausible but unregistered domains, and adversaries have begun registering them to capture AI-generated traffic (Palo Alto Networks Unit 42, 2026). On the defensive side, the same techniques are being turned into detectors: PhishReplicant groups new registrations by linguistic similarity to known attack domains (Koide et al., 2023), and Unit 42 predicted registrations of hallucinated domains 18 to 51 days before adversaries acted (Palo Alto Networks Unit 42, 2026). The net effect is unclear from the evidence so far. Interisle's 2025 figures (Interisle, 2025a) show attack volume and domain consumption doubling in a year, which suggests that, for now, automation has lowered attacker costs faster than defender costs.

AI has also created demand, most visibly for the .ai extension (sections 2.2 and 6.2). Automated appraisal tools marketed as AI-driven are proliferating, but they rest on the same comparable-sales regressions as their predecessors, and this review found no published evaluation showing that they predict transaction prices better.

7.2 Blockchain-based namespaces

Systems such as the Ethereum Name Service and Unstoppable Domains issue names as tokens outside the ICANN root. They promise censorship resistance and user control, and they are not covered by the UDRP or by ICANN's abuse obligations. Adoption remains limited, and the names serve mainly as wallet identifiers: 67.3% of ENS record settings point to blockchain addresses (Xia et al., 2022). From an economic standpoint they are a parallel namespace without a dispute mechanism, which makes them attractive for the same reasons that cheap ngTLDs are attractive. The first peer-reviewed measurements show the familiar pattern. Xia et al. (2022) found thousands of squatting ENS names as well as scam addresses and malicious websites in ENS records. Muzammil et al. (2024) analysed 4.9 million names across ENS, Unstoppable Domains and ADA Handles and documented typosquatting of popular names, where a single typo transfers funds irreversibly to an attacker. A population-level abuse rate comparable to DNS blocklist statistics, and any evidence on dispute handling, are still missing, a gap discussed in section 8.

7.3 The 2026 gTLD round and its consequences

The more than 1,600 applications described in section 2.4 could produce around 1,000 new extensions from 2027 onwards, if the 2012 ratio of applications to delegations holds (ICANN, 2026b). The historical pattern is consistent: every new open extension attracts a wave of speculative and abusive

registrations in its first year, and extensions that launch with sub-dollar pricing attract the most (Interisle, 2023; Nosyk et al., 2024). Stobbs IP (2024) documented the security concerns raised by .zip and .mov, whose strings collide with file suffixes. The contractual abuse obligations in the 2026 base registry agreement are stronger than in 2012, but enforcement depends on ICANN compliance capacity that the .top breach case showed to be slow (ICANN, 2025a). Brand owners should register in the Trademark Clearinghouse, budget for sunrise registrations in relevant strings, and monitor the new extensions from delegation onward.

8 Discussion and Research Gaps

The evidence reviewed here supports a single economic reading. Domain abuse is a demand-side phenomenon that responds to price. INFERMAL's price-effect estimate, Interisle's concentration data and the .cn natural experiment all indicate that criminals buy where domains are cheapest, fastest to obtain and least verified. Only the .cn case approximates a natural experiment; the rest of the evidence is correlational. That has a policy implication which the industry has been slow to accept: abuse is shaped by pricing and onboarding decisions made by registries and registrars. Interisle (2026) makes the point directly: some registries grow without attracting disproportionate abuse, so the outcome is a choice.

This reading has a theoretical basis in the economics of information security. Anderson and Moore (2006) argued that security failures persist where the party able to prevent harm does not bear its cost. Domain registration is a textbook case: the registrar earns the fee and the victim bears the loss, so abuse is a negative externality of the registration business (Moore, Clayton and Anderson, 2009). The market also has an information problem of the kind described by Akerlof (1970). A registrar cannot cheaply distinguish a legitimate bulk buyer from a phisher, and the low price that attracts the former attracts the latter. Verification requirements are the screening device that restores the distinction, at a cost that falls on all registrants. The policy question is therefore less whether verification reduces abuse, on which INFERMAL and the European ccTLD experience give consistent if correlational evidence, than who pays for it. Table 2 summarises the findings against the five research questions.

Research question	Main finding	Key evidence
1. Market size and drivers	401.6 million domains, growth 8.1% a year; acceleration driven by low-price ngTLDs (+34%, 31% renewal) and a .com recovery	DNIB (2026a; 2026b); Halvorson et al. (2015)
2. Registration behaviour	Malicious registrants are price-sensitive; USD 4.71 vs 8.62; bulk, API access and anonymous payment raise abuse	Nosyk et al. (2024); Hao et al. (2013); Interisle (2025a)
3. DNS abuse and detection	19.5 million attack domains in 2025; ngTLDs 12% of market, 47% of abuse; registration-time detection reaches 70% at 0.35% false positives	Interisle (2025a; 2026); Korczyński et al. (2018); Hao et al. (2016)
4. Legal protection	UDRP record 6,282 cases in 2025; URS, ACPA and TMCH complement it; NIS2 Art. 28 restores registrant data in the EU	WIPO (2026); DNS Research Federation (2024)
5. Valuation	Domains price like an asset class; .com premium, length and keyword value dominate; market illiquid (3 to 4% sell-through)	Lindenthal (2014); Allemann (2025); Freename (2025)

Table 2. Summary of findings by research question.

The externality reading also has a distributional implication. The costs of abuse fall on users, brand owners and public institutions, while the revenue from the registrations falls to the registrar. The market therefore externalises a cost, and the instruments that internalise it, such as verification requirements under NIS2 Article 28 or the stricter contractual obligations in the 2026 round, are imposed by regulation or by ICANN contract.

Four gaps in the literature stand out. First, the cost of domain abuse for SMEs is unquantified. Empirical work on business impact focuses on Forbes Global 2000 companies and the most popular brands and websites (CSC, 2024; Palo Alto Networks Unit 42, 2020; Moore and Edelman, 2010), while SMEs hold most business domains and appear rarely in UDRP statistics. A study combining survey data on incident costs with passive DNS data on look-alike registrations for a sample of SME domains would fill this gap and could be run at the level of a single ccTLD registry.

Second, the relationship between registrar pricing and abuse has been estimated once, for phishing, by INFERMAL. It has not been replicated for malware or spam, not been estimated across ccTLDs, and not been tested against the full population of ICANN-accredited registrars with controls for market share and customer mix. ICANN itself lists these as open questions (ICANN, 2025b). A cross-registrar panel study would give the GNSO policy process the quantitative basis it currently lacks.

Third, blockchain-based namespaces have no population-level abuse rate and no dispute mechanism; the existing studies measure squatting, not its cost (Xia et al., 2022; Muzammil et al., 2024). As adoption grows, the question of whether a permissionless namespace can support trademark enforcement at all deserves empirical and legal analysis before, rather than after, the first large-scale abuse campaign.

Fourth, NIS2 Article 28 offers the natural experiment the field has lacked. Because member states transposed the verification requirement at different dates, abuse rates in EU ccTLDs and at EU-based registrars can be compared before and after transposition in a difference-in-differences design. Such a study would test the causal claim that section 4.3 can state only as a correlation. Table 3 sets out a research design for each of the four gaps.

Research gap	**Proposed design**	**Data sources**
Cost of domain abuse for SMEs	Incident-cost survey linked to look-alike registrations for a sample of SME domains	ccTLD zone files, passive DNS, SME panel survey
Registrar pricing and abuse	Cross-registrar panel regression with registrar fixed effects; price changes as natural experiments	ICANN registrar reports, DAAR, blocklists, retail price data
Abuse in blockchain namespaces	Population-level measurement of squatting and scam rates; legal analysis of enforcement options	On-chain registration logs (ENS, Unstoppable Domains), scam address lists
Causal effect of registrant verification	Difference-in-differences across EU member states by NIS2 transposition date	EU ccTLD and registrar abuse rates, transposition records

Table 3. Research agenda: proposed designs for the four gaps.

9 Conclusion

The domain market is growing at its fastest rate in a decade, driven by new gTLDs sold at promotional prices, and abuse is growing faster still. Both trends are tied to the same conditions. The evidence from ICANN's own research, from independent measurement and from the academic literature is consistent: price, bulk automation and the absence of verification predict where abuse occurs, and the segments that combine all three, the low-price new gTLDs, held 12% of the market in 2025 and nearly half of its abuse.

For registrars and registries the levers are known: verify identity for bulk buyers, limit API registration, and stop selling below cost. For brand owners preparing for the 2026 round, the tools are the Trademark Clearinghouse, sunrise registrations and continuous monitoring, and for clear-cut cases the UDRP, which resolved a record 6,282 disputes in 2025. For policymakers, NIS2 Article 28 shows that verification can be mandated where the market does not supply it.

For researchers the agenda is specific. Measure what abuse costs the small firms that hold most business domains. Replicate the price effect across registrars and abuse types. Examine blockchain namespaces before they matter. And use the staggered transposition of NIS2 Article 28 to test whether verification causes the drop in abuse with which it is associated. The 2026 round could add around 1,000 extensions to the root from 2027 onwards. Whether they repeat the pattern of 2014 or break it depends on decisions that are being made now, by registries setting launch prices.

References

Agten, P., Joosen, W., Piessens, F. and Nikiforakis, N. (2015) 'Seven months' worth of mistakes: a longitudinal study of typosquatting abuse', in Proceedings of the 22nd Network and Distributed System Security Symposium (NDSS 2015). San Diego, CA: Internet Society.

Akerlof, G.A. (1970) 'The market for "lemons": quality uncertainty and the market mechanism', Quarterly Journal of Economics, 84(3), pp. 488-500. doi: 10.2307/1879431.

Allemann, A. (2025) 'Domain name sales hit $185 million in 2024', Domain Name Wire, 3 January [Online]. Available at: https://domainnamewire.com (Accessed: 22 September 2026).

Allemann, A. (2026a) 'Breaking: VeriSign raising wholesale .com prices', Domain Name Wire, 23 April [Online]. Available at: https://domainnamewire.com/2026/04/23/breaking-verisign-raising-wholesale-com-prices/ (Accessed: 23 September 2026).

Allemann, A. (2026b) 'WIPO handles record number of domain disputes in 2025', Domain Name Wire, 15 January [Online]. Available at: https://domainnamewire.com/2026/01/15/wipo-handles-record-number-of-domain-disputes-in-2025/ (Accessed: 23 September 2026).

Alrwais, S., Yuan, K., Alowaisheq, E., Li, Z. and Wang, X. (2014) 'Understanding the dark side of domain parking', in Proceedings of the 23rd USENIX Security Symposium. San Diego, CA: USENIX Association.

Anderson, R. and Moore, T. (2006) 'The economics of information security', Science, 314(5799), pp. 610-613. doi: 10.1126/science.1130992.

Bayer, J., Nosyk, Y., Hureau, O., Fernandez, S., Paulovics, I., Duda, A. and Korczyński, M. (2022) Study on Domain Name System (DNS) Abuse: Technical Report. Appendix 1 to the Study on DNS Abuse for the European Commission, 31 January [Online]. Available at: https://arxiv.org/abs/2212.08879 (Accessed: 23 September 2026).

Canella Camaiora (2025) Are domain names still a powerful asset for businesses? Cybersquatting, SEO, and digital strategies [Online]. Available at: https://www.canellacamaiora.it (Accessed: 22 September 2026).

CSC (2024) 2024 in Review: Trends and Insights in Domain Security and Brand Protection. Wilmington, DE: CSC Digital Brand Services [Online]. Available at: https://www.cscdbs.com (Accessed: 22 September 2026).

DNIB (2025a) The Domain Name Industry Brief Quarterly Report, Q1 2025 [Online]. Available at: https://www.dnib.com/articles/the-domain-name-industry-brief-q1-2025 (Accessed: 22 September 2026).

DNIB (2025b) The Domain Name Industry Brief Quarterly Report, Q4 2025 [Online]. Available at: https://www.dnib.com/articles/the-domain-name-industry-brief-q4-2025 (Accessed: 22 September 2026).

DNIB (2026a) The Domain Name Industry Brief Quarterly Report, Q1 2026 [Online]. Available at: https://www.dnib.com/articles/the-domain-name-industry-brief-q1-2026 (Accessed: 22 September 2026).

DNIB (2026b) The Domain Name Industry Brief Quarterly Report, Q2 2026 [Online]. Available at: https://www.dnib.com/articles/the-domain-name-industry-brief-q2-2026 (Accessed: 22 September 2026).

DNS Research Federation (2024) NIS2 and domain names: an explainer [Online]. Available at: https://dnsrf.org/blog/nis2-and-domain-names---an-explainer (Accessed: 22 September 2026).

DNS Research Federation (2025) Trends in the transposition journey of Article 28 of NIS2 [Online]. Available at: https://dnsrf.org/blog/trends-in-the-transposition-journey-of-art-28-of-nis2/index.html (Accessed: 22 September 2026).

DomainTools (2024) Domain Intelligence Year in Review 2024. Seattle, WA: DomainTools [Online]. Available at: https://www.domaintools.com (Accessed: 22 September 2026).

Dynadot (2026) 'How domain value is calculated', Dynadot Blog [Online]. Available at: https://www.dynadot.com/blog (Accessed: 22 September 2026).

European Commission (2025) Annual Report on European SMEs 2024/2025: SME Performance Review. Luxembourg: Publications Office of the European Union [Online]. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC142263 (Accessed: 22 September 2026).

Eurostat (2025) Digitalisation in Europe: 2025 edition [Online]. Available at: https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2025 (Accessed: 22 September 2026).

Eurostat (2026) E-business integration: Statistics Explained [Online]. Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-business_integration (Accessed: 22 September 2026).

FBI IC3 (2025) Internet Crime Report 2024. Washington, DC: Federal Bureau of Investigation, Internet Crime Complaint Center [Online]. Available at: https://www.ic3.gov (Accessed: 23 September 2026).

Freename (2025) Domain Aftermarket Report, Q1 2025 [Online]. Available at: https://freename.com/blog/domain-aftermarket-report-q1-2025 (Accessed: 22 September 2026).

Gasimova, C. (2022) 'Domain name and trademark infringement (cybersquatting) in the digital age', SSRN Electronic Journal, Paper No. 4344891. doi: 10.2139/ssrn.4344891.

GNSO (2025) Final Issue Report on DNS Abuse Mitigation. Los Angeles, CA: ICANN Generic Names Supporting Organization, 4 December [Online]. Available at: https://gnso.icann.org (Accessed: 22 September 2026).

Halvorson, T., Der, M.F., Foster, I., Savage, S., Saul, L.K. and Voelker, G.M. (2015) 'From .academy to .zone: an analysis of the new TLD land rush', in Proceedings of the 2015 ACM Internet Measurement Conference (IMC '15). Tokyo, 28-30 October. New York: ACM.

Hao, S., Feamster, N. and Pandrangi, R. (2011) 'Monitoring the initial DNS behavior of malicious domains', in Proceedings of the 2011 ACM SIGCOMM Internet Measurement Conference (IMC '11). Berlin, 2-4 November. New York: ACM, pp. 269-278. doi: 10.1145/2068816.2068842.

Hao, S., Thomas, M., Paxson, V., Feamster, N., Kreibich, C., Grier, C. and Hollenbeck, S. (2013) 'Understanding the domain registration behavior of spammers', in Proceedings of the 2013 ACM Internet Measurement Conference (IMC '13). Barcelona, 23-25 October. New York: ACM, pp. 63-76.

Hao, S., Kantchelian, A., Miller, B., Paxson, V. and Feamster, N. (2016) 'PREDATOR: proactive recognition and elimination of domain abuse at time-of-registration', in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). Vienna, 24-28 October. New York: ACM, pp. 1568-1579.

ICANN (1999) Uniform Domain Name Dispute Resolution Policy, adopted 26 August [Online]. Available at: https://www.icann.org/resources/pages/policy-2012-02-25-en (Accessed: 23 September 2026).

ICANN (2019) 5 things every domain name registrant should know about ICANN's Uniform Domain Name Dispute Resolution Policy (UDRP) and Uniform Rapid Suspension (URS) system [Online]. Available at: https://www.icann.org/resources/pages/5-things-registrants-know-udrp-urs-2019-09-25-en (Accessed: 23 September 2026).

ICANN (2025a) '.TOP Registry cures Notice of Breach', ICANN Contractual Compliance, 2 June [Online]. Available at: https://www.icann.org/compliance (Accessed: 22 September 2026).

ICANN (2025b) Insights and Clarifications on the INFERMAL Study. Los Angeles, CA: ICANN Office of the Chief Technology Officer, June [Online]. Available at: https://www.icann.org/resources/pages/inferential-analysis-maliciously-registered-domains-infermal-2024-12-03-en (Accessed: 22 September 2026).

ICANN (2026a) 'ICANN opens application window for new generic top-level domains', Press release, 30 April [Online]. Available at: https://www.icann.org/resources/press-material/release-2026-04-30-en (Accessed: 22 September 2026).

ICANN (2026b) 'ICANN 2026 Round closes with more than 1,600 new gTLD applications', Announcement, August [Online]. Available at: https://newgtldprogram.icann.org/en/application-rounds/round2 (Accessed: 22 September 2026).

ICANN (no date) Trademark Clearinghouse FAQs [Online]. Available at: https://newgtlds.icann.org/en/about/trademark-clearinghouse/faqs (Accessed: 23 September 2026).

Interisle (2023) Phishing Landscape 2023: An Annual Study of the Scope and Distribution of Phishing. Boston, MA: Interisle [Online]. Available at: https://interisle.net (Accessed: 22 September 2026).

Interisle (2025a) Cybercrime Supply Chain 2025: Measurements and Assessments of Cyber Attack Resources and Where Criminals Acquire Them. Boston, MA: Interisle, 18 November [Online]. Available at: https://interisle.net/insights/cybercrimesupplychain2025 (Accessed: 22 September 2026).

Interisle (2025b) 'Supply Chain 2025: cybercrime across the TLD name space', Interisle Insights, 10 December [Online]. Available at: https://interisle.substack.com/p/supply-chain-2025-cybercrime-across (Accessed: 22 September 2026).

Interisle (2025c) Phishing Landscape 2025: A Study of the Scope and Distribution of Phishing. Boston, MA: Interisle, 9 September [Online]. Available at: https://interisle.net/insights/phishing-landscape-2025-an-annual-study-of-the-scope-and-distribution-of-phishing (Accessed: 22 September 2026).

Interisle (2026) Malicious Registrations in the Domain Name Market: An Analysis of 2025 gTLD Registrations and Cybercriminal Demand. Boston, MA: Interisle, June [Online]. Available at: https://interisle.net/insights/cybercriminaldomaindemand (Accessed: 22 September 2026).

Kintis, P., Miramirkhani, N., Lever, C., Chen, Y., Romero-Gómez, R., Pitropakis, N., Nikiforakis, N. and Antonakakis, M. (2017) 'Hiding in plain sight: a longitudinal study of combosquatting abuse', in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17). Dallas, TX. New York: ACM.

Koide, T., Fukushi, N., Nakano, H. and Chiba, D. (2023) 'PhishReplicant: a language model-based approach to detect generated squatting domain names', in Proceedings of the 39th Annual Computer Security Applications Conference (ACSAC '23). Austin, TX, 4-8 December. New York: ACM. doi: 10.1145/3627106.3627111.

Korczyński, M., Wullink, M., Tajalizadehkhoob, S., Moura, G.C.M., Noroozian, A., Bagley, D. and Hesselman, C. (2018) 'Cybercrime after the sunrise: a statistical analysis of DNS abuse in new gTLDs', in Proceedings of the 2018 Asia Conference on Computer and Communications Security (ASIACCS '18). Incheon. New York: ACM.

Lindenthal, T. (2014) 'Valuable words: the price dynamics of internet domain names', Journal of the Association for Information Science and Technology, 65(5), pp. 869-881. doi: 10.1002/asi.23012.

Lindenthal, T. (2018) 'Monocentric cyberspace: the primary market for internet domain names', Journal of Real Estate Finance and Economics, 57(1), pp. 1-29. doi: 10.1007/s11146-016-9547-2.

Liu, H., Levchenko, K., Félegyházi, M., Kreibich, C., Maier, G., Voelker, G.M. and Savage, S. (2011) 'On the effects of registrar-level intervention', in Proceedings of the 4th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '11). Boston, MA: USENIX Association.

M3AAWG (2025) 'M3AAWG co-sponsors new global report on cybercrime supply chain finding another year of dramatic growth fueled by security gaps', M3AAWG Blog, November [Online]. Available at: https://www.m3aawg.org (Accessed: 22 September 2026).

Moore, T., Clayton, R. and Anderson, R. (2009) 'The economics of online crime', Journal of Economic Perspectives, 23(3), pp. 3-20. doi: 10.1257/jep.23.3.3.

Moore, T. and Edelman, B. (2010) 'Measuring the perpetrators and funders of typosquatting', in Sion, R. (ed.) Financial Cryptography and Data Security (FC 2010). Lecture Notes in Computer Science, vol. 6052. Berlin: Springer, pp. 175-191.

Muzammil, M., Wu, Z., Harisha, L., Kondracki, B. and Nikiforakis, N. (2024) 'Typosquatting 3.0: characterizing squatting in blockchain naming systems', in Proceedings of the 2024 APWG Symposium on Electronic Crime Research (eCrime). IEEE, pp. 94-108. doi: 10.1109/eCrime66200.2024.00013.

Name Experts (2026) 'How to value a domain name' [Online]. Available at: https://www.nameexperts.com (Accessed: 22 September 2026).

NameBio (2025) Domain sales statistics, first half of 2025 [Online]. Available at: https://namebio.com (Accessed: 22 September 2026).

Nosyk, Y., Korczyński, M., Maroofi, S., Bayer, J. and Duda, A. (2024) INFERMAL: Inferential Analysis of Maliciously Registered Domains. Los Angeles, CA: ICANN Office of the Chief Technology Officer, 8 November [Online]. Available at: https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf (Accessed: 22 September 2026).

Palo Alto Networks Unit 42 (2020) 'Cybersquatting: attackers mimicking domains of major brands', Unit 42 Threat Research, 1 September [Online]. Available at: https://unit42.paloaltonetworks.com/cybersquatting/ (Accessed: 22 September 2026).

Palo Alto Networks Unit 42 (2026) 'Phantom squatting: AI-hallucinated domains as a software supply chain vector', Unit 42 Threat Research, 30 June [Online]. Available at: https://unit42.paloaltonetworks.com/phantom-squatting-hallucinated-web-domains/ (Accessed: 23 September 2026).

Sedo and InterNetX (2025) Global Domain Report 2025. Cologne: Sedo GmbH [Online]. Available at: https://sedo.com (Accessed: 22 September 2026).

SentinelOne (2025) 'What is cybersquatting? Types, prevention and examples', Cybersecurity 101 [Online]. Available at: https://www.sentinelone.com (Accessed: 22 September 2026).

SIDN (2025) 'Global Domain Report 2025: trends and sales in domains', SIDN News, September [Online]. Available at: https://www.sidn.nl/en/news-and-blogs/global-domain-report-2025-trends-and-sales-in-domains (Accessed: 22 September 2026).

Stobbs IP (2024) 'A new analysis of the newest new-gTLDs', CircleID, 7 May [Online]. Available at: https://circleid.com (Accessed: 22 September 2026).

Szurdi, J., Kocso, B., Cseh, G., Spring, J., Félegyházi, M. and Kanich, C. (2014) 'The long "taile" of typosquatting domain names', in Proceedings of the 23rd USENIX Security Symposium. San Diego, CA: USENIX Association.

Verisign (2026) 'Verisign reports second quarter 2026 results', Press release, 23 July [Online]. Available at: https://investor.verisign.com (Accessed: 22 September 2026).

Vissers, T., Spooren, J., Agten, P., Jumpertz, D., Janssen, P., Van Wesemael, M., Piessens, F., Joosen, W. and Desmet, L. (2017) 'Exploring the ecosystem of malicious domain registrations in the .eu TLD', in Dacier, M., Bailey, M., Polychronakis, M. and Antonakakis, M. (eds.) Research in Attacks, Intrusions, and Defenses (RAID 2017). Lecture Notes in Computer Science, vol. 10453. Cham: Springer, pp. 472-493. doi: 10.1007/978-3-319-66332-6_21.

WIPO (2025) 'WIPO Domain Name Report 2024: UDRP case filings remain strong', 15 January [Online]. Available at: https://www.wipo.int/amc/en/domains/news/2025/news_0001.html (Accessed: 22 September 2026).

WIPO (2026) '2025 marks record-breaking year for WIPO domain name disputes', 14 January [Online]. Available at: https://www.wipo.int/amc/en/domains/news/2026/news_0001.html (Accessed: 22 September 2026).

WIPO (no date) Schedule of Fees under the UDRP [Online]. Available at: https://www.wipo.int/en/web/amc/domain-name-disputes/fees/index (Accessed: 23 September 2026).

Wissen Research (2023) 'Cybersquatting involving trademarks and service marks' [Online]. Available at: https://www.wissenresearch.com (Accessed: 22 September 2026).

Xia, P., Wang, H., Yu, Z., Liu, X., Luo, X., Xu, G. and Tyson, G. (2022) 'Challenges in decentralized name management: the case of ENS', in Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22). Nice, 25-27 October. New York: ACM, pp. 65-82. doi: 10.1145/3517745.3561469.