The Domain Name Life Cycle as an Attack Surface: Systematic Threat Mapping and Defense Recommendations

Thomas Fritzler and Michael Massoth
Hochschule Darmstadt (h_da) - University of Applied Sciences
member of European University of Technology (EUt+)
Department of Computer Science
Darmstadt, Germany
email: thomas@fritzler.me, michael.massoth@h-da.de

***Abstract*—This paper presents a phase-based security analysis of the domain-name life cycle - pre-registration, active registration, expiry, and malicious re-registration. Synthesizing peer-reviewed studies, documented incidents, and current threat intelligence (2014-2025), we map key attack vectors (for example typosquatting, dangling records, registrar compromise, expired-domain abuse) to concrete mitigations (registrar hardening, zone hygiene, renewal governance). The result is a concise model and a threat-to-control table aimed at practitioners in enterprises and registrars. This is a conceptual, literature-based synthesis; no new measurements are introduced. We argue that domain names are critical security assets that require continuous management across technical and administrative controls.**

Keywords-Domain Life Cycle; Domain Security; Domain Management; Expired Domains; Cybersecurity Best Practices.

I. Introduction

Domain names form the backbone of navigation on the Internet. They function both as a company's **digital identity** and as **trusted anchors** for users accessing web resources [1]. A compromised domain can therefore trigger wide-ranging consequences - from phishing attacks to the complete takeover of online services. Attackers systematically exploit these weaknesses by operating with legitimate domains or deceptively similar names in order to bypass security mechanisms. In doing so, virtually every attack that relies on a seemingly legitimate sender or web address to evade defenses is facilitated [2].

Against this backdrop, the present paper analyzes the **vulnerabilities throughout the entire life cycle of a domain** - from registration, through operation and expiration, to potential takeover by third parties. The objective is to highlight *technical attack vectors* and *documented incidents* for each phase and to demonstrate their relevance for enterprises. To this end, existing scientific studies, security reports, and recorded attacks are comparatively evaluated. In addition, well-established tools are presented that can help to detect and prevent such weaknesses. **This contribution is a conceptual, literature-based synthesis rather than an empirical measurement study.** We address the following research questions (RQs): **RQ1** - What threats emerge at each phase of the domain name life cycle? **RQ2** - Which technical and organizational controls effectively mitigate them? **RQ3** - Which gaps suggest directions for future empirical validation?

The remainder of this paper is structured as follows: **Section II** reviews related work and outlines our methodology; **Section III** presents the phase-oriented model of the domain name life cycle and a consistent, phase-by-phase threat mapping; **Section IV** discusses implications, provides concrete recommendations, states limitations, and outlines future work.

II. Related Work

Prior studies typically focus on isolated threat surfaces. Typosquatting and other naming-confusion attacks have been analyzed in depth [3][4], while the risks of dangling Domain Name System (DNS) records [5][6] and expired-domain takeovers [7] have been explored separately. Adjibi *et al.* extend this line of research by quantifying how the Fortune 500 pursue *defensive registrations* and showing that roughly three-quarters of look-alike domains remain under third-party control [1]. Their work highlights a critical blind spot - corporate protection tends to begin *after* registration - and therefore does not capture threats that arise *before* or *after* that window (e.g., pre-registration brand monitoring or post-expiration abuse). **In contrast to prior work, this paper systematically maps threats across all four phases and couples them with phase-specific mitigations for practitioners.**

Other surveys take a broader perspective on DNS security. Schmid provides a view on systemic threats in DNS Insecurity [8], while Ramdas *et al.* catalog mitigation techniques against DNS-related attacks [9]. Affinito *et al.* examine domain lifetimes and quantify baseline risks across the ecosystem [10]. However, none of these works integrates security threats across the *entire domain life cycle*.

Methodology: We conducted a structured literature scan (2014-2025) across ACM DL, IEEE Xplore, USENIX, NDSS and selected industry reports. Inclusion: peer-reviewed security work on DNS/domain life cycle, empirical incident reports; Exclusion: marketing/duplicate blog posts. Search keys included "domain life cycle security", "dangling DNS", "expired domains", "typosquatting", "registrar hijacking". Two reviewers screened titles/abstracts; we extracted threats, affected life cycle phase, and mitigation classes. This is a conceptual synthesis without new measurements.

Despite these valuable contributions, the literature still lacks an integrated framework that maps vulnerabilities from pre-registration to post-expiration. This paper closes that gap by

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

Copyright (c) IARIA, 2025. ISBN: 978-1-68558-295-1

TABLE I. COMPARATIVE OVERVIEW OF EXISTING REVIEWS AND HOW THIS WORK DIFFERS

Work	Focus/Method	Life cycle coverage	Added value of this paper
COMST'21 [8]	Broad DNS threats survey	Cross-cutting; not phase-based	End-to-end, phase-based map (P1-P4) with aligned mitigations
ICCS'19 [9]	DNS attack mitigations (short survey)	General DNS; no life cycle lens	Life cycle view + concrete phase-wise controls
TMA'22 [10]	Domain lifetimes / expiry risks	Emphasis on lifetime/expiry	Integrates pre-reg, active, expiry, re-reg threats
NDSS'25 [1]	Defensive registrations (Fortune 500)	Narrow pre/post around reg.	Complements with ops/expiry abuse beyond registration

proposing a phase-oriented security model and by deriving unified mitigation guidelines that link technical, administrative, and policy controls.

III. DOMAIN LIFE CYCLE AND ITS VULNERABILITIES

The life cycle of a domain can be simplified into four phases: **(1) Pre-registration**, **(2) Active Registration**, **(3) Expired Domains**, and **(4) Malicious Re-registration**. While Phase 3 resembles Phase 1 in terms of availability, residual references (e.g., third-party logins, old references to email addresses, or inbound links) may still exist. Each phase poses distinct security threats [10]. *Per phase, we (i) define scope, (ii) enumerate threats, (iii) list recent evidence, and (iv) summarize mitigations.* Table II summarizes the key threats and defenses across the four phases addressed in this work. The following subsections outline these phases and their typical weaknesses.

A. Phase 1: Pre-registration

In the first phase, a domain is completely **freely available** - either never registered before or released by its previous owner - and can be registered anew. Even though no legitimate content exists under such a name, attackers can still **abuse** it by proactively registering it [11].

T1. Typosquatting and look-alike domains: Typosquatting refers to registering domain names that are **confusingly similar** to a well-known brand, usually through typographical errors or minor spelling changes. Users who mistype or fail to notice the difference are silently routed to the wrong site. This technique has deceived users since the early commercial Internet. Typical variants include letter transpositions, character omission or insertion, or using **homographs** - visually similar characters from other scripts. A well-known early case was `goggle.com`, intended to mislead visitors to `google.com`. Modern attackers increasingly rely on Internationalized Domain Names (IDNs) that mix, e.g., Cyrillic and Latin letters - an attack most browsers now detect and block [12].

Despite longstanding defensive efforts, typosquatting remains highly prevalent and continues to evolve. Recent incidents show that this **scheme continues to flourish** and evolve. In 2024, for example, a security vendor reported a surge of Bifrost-Trojan campaigns leveraging VMware typosquats [13]. Fraudulent job sites and even parts of the SolarWinds supply-chain attack also traced back to typosquatting domains [14]. An Akamai analysis found that about 20.1% of all newly observed domains it tracks - roughly 13 million malicious domains every month, i.e., well over three million each week - are flagged as malicious, many of them look-alike registrations [15]. These are not accidental errors but **deliberate registrations by criminals**. The technique now underpins sophisticated fraud schemes, such as combining bogus websites with matching social-media profiles, intercepting emails (e.g., Business-Email-Compromise), or smuggling trojanized code into development environments. One example is the discovery of Python libraries like `"requessts"` or `"reqquests"`, typosquats of popular packages registered on look-alike domains to trick developers [3].

a) Example: the Mastercard typo: A real-world incident underscoring the danger of small DNS errors is the *Mastercard typo*. A **faulty** DNS entry went unnoticed for years, meaning attackers could have registered the misspelled domain and weaponized it [16]. The case shows that even an innocuous typo in a DNS zone can open major security gaps, because customers or internal systems may unknowingly resolve the "wrong" domain.

b) Example: the BYD domain confusion: A recent real-world incident illustrates how brand visibility can backfire when obvious look-alike domains are left unprotected. During UEFA EURO 2024, Chinese electric-vehicle maker BYD bought prominent pitch-side advertising. Curious spectators naturally tried the German country code Top Level Domain (ccTLD) variant `byd.de` - but that name was already owned by an unrelated adult-toy retailer. The unexpected spotlight drove a massive traffic spike to the site, forcing its owners to publish a disclaimer that they were not affiliated with the car company [17]. The episode shows that even legitimate marketing can funnel large crowds to misleading domains, creating fertile ground for fraud or malware if criminals register similar names first. Careful domain-portfolio management across relevant TLDs is therefore essential throughout the life cycle of a brand.

Scientific studies confirm typosquatting's breadth. A 2014 USENIX study analyzing hundreds of thousands of domains found that typosquatting is **widespread** and growing [4]. Actors invest significant resources to monetize these domains. More recent surveys reveal that **74% of look-alike domains** targeting Fortune 500 companies are held by third parties [1], highlighting aggressive coverage by criminals and domain speculators. Such names are often used for **phishing**, fraud, or brand abuse.

T2. Orphaned and published domains: A threat that spans **Phase 1 (Pre-registration)**, also surfaces during **Phase 2 (Active Registration)** through abandoned or misconfigured

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

subdomains, and re-appears in **Phase 4 (Malicious Re-registration)**. Attackers actively look for **domain or subdomain names that are still referenced** - in documentation, configuration files, code snippets, or lingering DNS records - yet are either unclaimed or left dangling. Although these names look legitimate from the outside, they are **not actually under the rightful owner's control**. By claiming an orphaned domain or subdomain, adversaries can invisibly insert themselves into traffic intended for the original destination [5][18][19]. Modern scanners such as *BadDNS* now crawl websites to locate externally referenced, takeover-able domains [20].

B. Phase 2: Active Registration

In Phase 2 the domain is under **active ownership** (typically by an organization) and used for services such as websites, email, or Application Programming Interface (APIs). Although the name is legitimately controlled, numerous **attack vectors arise from misconfiguration or insufficient safeguards**. The main concerns are **DNS configuration**, registrar security, and subdomain management [2].

T1. DNS Misconfigurations and Gaps: A domain is only as secure as its DNS settings. Faulty or negligent configuration can give adversaries opportunities to abuse or manipulate the name. Key issues include:

Missing DNSSEC signing: Domain Name System Security Extensions (DNSSEC) cryptographically signs DNS responses to guarantee their **authenticity and integrity**. Without DNSSEC, domains are vulnerable to cache-poisoning and manipulation - an attacker could inject forged answers and redirect users to malicious IPs. Despite clear benefits, adoption remains low: an APNIC study in 2023 found that **only about 4.3 % of .com domains are DNSSEC-signed** [21]. In other words, more than 95 % lack this protection. Some TLDs fare better - `.nl` reaches roughly 60 % coverage [21] - yet a global gap persists. Technical complexity, operational effort, and limited know-how leave many domains exposed whenever an attacker can influence a resolver or intercept traffic.

Missing CAA records: A **CAA (Certification Authority Authorization)** record lets owners specify which CAs may issue TLS certificates for the domain. Without CAA, any CA could issue a certificate (assuming domain-control checks can be bypassed via DNS tampering or error). CAA therefore reduces the risk of *unintended or fraudulent issuance*. Nevertheless, a 2020 survey showed that **only about 3 % of the Alexa Top-1-Million** domains publish a CAA record. Given the ease of deployment, this figure is strikingly low. A CAA record might restrict issuance to `Let's Encrypt` or `DigiCert`; some domains even use `issue ";"` to permit **no** CA - 358 cases in that study. [22]

Open zone transfers (AXFR): Zone transfers replicate data between authoritative name servers. If a server is misconfigured to allow AXFR from *unauthorized IPs*, attackers can pull a **complete zone dump**. The dump reveals all records - internal subdomains, IP mappings, etc. - and aids further attacks. Although CVE-1999-0532 highlights the risk, Internet scans as late as 2016 still found "large numbers" of exposed servers. Successful leaks expose hidden services such as `vpn.company.com` or `dev.db.company.com`. Mitigation is trivial: allow transfers **only to authorized secondary servers** [23].

Stale or incorrect DNS records: Domains or subdomains often move or services are retired without cleaning all records. Such **stale entries** may point nowhere - or worse, be taken over (see *subdomain takeover*). A special case is **incorrect NS entries**: if registry-level name servers are misspelled or unresponsive, the domain becomes unstable. Attackers have exploited these situations. The 2024 *"Sitting Ducks"* campaign revealed hundreds of thousands of domains with **DNS misconfigurations** (e.g., bad NS pointers) effectively abandoned [24]. Attackers impersonated the intended name servers and seized control [24]. Infoblox found nearly **800,000 vulnerable domains** in three months; about 9 % (>70,000) were **actively hijacked** [24]. These domains - often legitimate but misconfigured - were then abused for phishing, investment fraud, and more [24]. Even a minor lapse (e.g., an outdated NS entry) can turn a domain into *easy prey*.

A common scenario is a DNS record that points to an external domain (e.g., via **CNAME**, **MX**, or **NS**) no longer controlled by the organization. Such a **dangling record** invites abuse: registering the missing domain diverts traffic to the attacker. For instance, `example.com` might include `oldservice.example.com CNAME oldservice-provider.com`, even though `oldservice-provider.com` no longer exists. Whoever registers that domain gains control over every request to `oldservice.example.com`. The same applies to unregistered domains listed as **MX** or **NS**, enabling email interception or name-server takeover [5][19].

In short, during Phase 2 the owner must ensure that all security-relevant DNS settings are correct and current. Misconfiguration directly threatens the **integrity of name resolution**. Additional precautions include avoiding unnecessary internal disclosures (e.g., chatty TXT records or revealing subdomain names) and routinely auditing the zone for **anomalous entries**.

T2. Threats from subdomain takeover: Many organizations delegate subdomains to external cloud providers - e.g., `shop.example.com` for SaaS or `cdn.example.com` for a CDN - via **CNAME** records (such as `shop.example.com CNAME shopsaas.com`). While the service is active and configured, no issue arises. **The threat arises when external services are decommissioned but DNS entries remain.** The subdomain then points to a *non-existent* target - a *dangling DNS record*. Attackers can **re-register** or claim that resource (e.g., the freed **cloud host name or account**) to seize control [5][19]. This is known as a **subdomain takeover**. The attacker "captures" a victim's subdomain by obtaining the referenced external domain or resource. Once in control, they can serve content or intercept traffic under the trusted hostname. Cloud platforms are frequent targets: Azure Web Apps, AWS S3 buckets, GitHub Pages, Heroku, and more. If the CNAME is left behind after

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

deletion, an attacker can spin up an identically named service and **take over** the subdomain [5][19].

Empirical work shows subdomain takeover is not rare but a **systemic risk**: in 2016 researchers identified 467 vulnerable subdomains among the Alexa Top-10k plus university sites [6]. Follow-up scans across cloud platforms found over **700 000 vulnerable DNS entries** overall [5][7].

Root causes are usually poor cleanup: projects end, services migrate, yet DNS records linger. Especially in DevOps and cloud cultures where teams create subdomains autonomously, visibility is lost. Companies should schedule **regular audits** of their DNS zones to detect *dangling* entries. Tools such as **Subjack**, **Subzy**, takeover modules in scanners like **Nuclei**, or the comprehensive **BadDNS** can automate detection by checking CNAME/MX/NS targets for registrability [20].

T3. Weaknesses in Registrar Security: Domain protection also depends heavily on the **security of the registrar account** - the portal where the name is registered and managed. An attacker who gains access can **seize the entire domain**: redirect name servers, change ownership details, or transfer the domain to another account.

Numerous incidents of **domain hijacking** stem from social engineering or registrar breaches. Attackers exploit weak passwords, absent two-factor authentication, or technical flaws at smaller registrars. A prominent example is the **"Sea Turtle"** campaign (2017-2019), in which a state-sponsored actor compromised registrars and DNS providers to hijack high-profile domains - mainly in the Middle East - by phishing credentials and altering DNS to their own servers, even acquiring valid TLS certificates [25]. This illustrates that even perfectly configured DNS zones fail if **registrar infrastructure is breached**.

Cyber-criminals without state backing also hijack domains. Often they first compromise the owner's email address (e.g., by registering an expired domain from Phase 3), then trigger a **password reset**. Support staff may also be fooled into **unauthorized transfers**. High-value domains - famous brands or premium .com generics - regularly appear in news reports after such thefts [25]. In 2015, for instance, Lenovo's domain was redirected to a defacement server, allegedly via registrar account compromise [26].

Key **weak points** include absent **multi-factor authentication**, lack of **Registry Lock** (a service that blocks critical changes unless manually approved), and poor credential hygiene. Registry Lock is highly effective yet mainly adopted by large firms: **46 % of companies using enterprise registrars** employ it, versus only 7 % using mass-market registrars. Many SMEs may not know or purchase the feature, and some registrars do not actively promote it [27].

Altogether, Phase 2 requires a **holistic defense** of the domain: both technical DNS parameters and administrative access must be secured, or attackers may gain total control - with potentially catastrophic outcomes such as fraud, reputation damage, or data breaches.

C. Phase 3: Expired Domains

Domains are typically registered for periods of 1 to 2 years and must be renewed regularly. If a domain is **not renewed in time**, it enters an expiry workflow. The registrar first places it in a short **grace period** (typically 30-45 days, during which the original holder can recover it for a fee), optionally followed by a **redemption period** (another $\sim$30 days, usually with a higher restoration fee). Finally, the domain is deleted and released for **re-registration** [10]. From a corporate perspective, allowing a domain to lapse is usually unintentional, yet still occurs frequently, whether through organizational errors (missed reminder emails, staff changes) or because the name is deemed no longer important (e.g., after rebranding or project shutdown). Older corporate domains or those of acquired subsidiaries are especially prone to "slipping through" [28]. Once a domain becomes available, attackers have an excellent opportunity to register and exploit it. Phase 3 therefore shows the threats posed by **expired domains**.

T1. Abuse of expired domains for phishing and fraud: A **released domain** can be registered by anyone - professional domain traders (*drop-catchers*) often run automated scripts to acquire attractive names the moment they drop. Criminal actors monitor such drop lists for **promising targets**. Domains previously owned by well-known organizations are highly valuable because they **inspire trust**. Attackers re-register them and deploy **convincing replicas** of the original content to deceive users. A typical pattern is launching a **fake webshop** on a formerly legitimate domain [29]. Brian Krebs [30] chronicled how a photographer's lapsed portfolio domain was re-registered by fraudsters and converted into a counterfeit sneaker store. Visitors seeking her work unknowingly entered card details, which criminals harvested and resold. Besides reputational damage, the photographer lost access to linked accounts because attackers also seized her former email address [29]. Automated renewal management and systematic SaaS deprovisioning ensure that critical domains never lapse and that dormant integrations are fully removed after project shutdowns.

T2. Email and account takeovers: If a company abandons a domain once used for email addresses (e.g., `@oldcorp.com`), an attacker who re-registers it can intercept all future mail. They can impersonate the firm, send **phishing mails from the genuine domain**, or reset passwords of existing accounts [31]. Many online services rely on email for password recovery. If a former employee signed up to a cloud service with `name@oldcorp.com`, the new domain owner can use "forgot password" to gain access. Researchers warn that **trade secrets can leak** or attackers may penetrate personal accounts of ex-staff [31]. A 2025 report showed that registering domains of defunct start-ups yielded access to countless SaaS accounts. Examples included ChatGPT, Slack, Notion, Zoom, and even HR systems still tied to old email addresses [32]. Attackers viewed sensitive data such as tax forms, payslips, and applicant information [32]. The study exposed a *design problem* in single-sign-on: many providers

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

identify users solely by email domain (the `hd` claim in Google OAuth), so a fresh Google account under the captured domain is treated as the original user [32]. Even without historical mail access, simply re-creating the address **preserves perceived identity** and unlocks accounts [32].

T3. Threats from lingering integrations: Beyond email, an expired domain may still be embedded in security infrastructure. Examples include **OAuth redirect URIs** or API callbacks. If such URLs point to a domain later relinquished, an attacker who captures it can control the OAuth flow. One case involved an integration using a subdomain of a now-defunct firm as its OAuth redirect; [32] after researchers bought the domain, they could masquerade as an *authenticated* organization and access data [32]. Likewise, **Single Sign On (SSO) endpoints**, API keys, or license servers may rely on the old domain. Re-using former names thus creates **bridges into previously protected areas** that the victim no longer monitors [31][32].

T4. Drop-catching and domain speculation: Drop-catching - automated registration of recently expired names - is not inherently criminal; an entire legitimate industry resells such domains. Fraudsters, however, also exploit it as a **business model**. With little effort they obtain domains that already **carry trust** (user familiarity, positive mail reputation, inbound links) [29]. These names are then *monetized*: directly for phishing or fraud, resold to the original owner (cybersquatting/extortion), or used for **spam/SEO** [33]. Studies show most seized domains end up in **black-hat SEO** networks - injecting links and redirects to boost dubious sites [33][34].

A headline example illustrating speculative risk occurred in 2021: Google's official Argentinian domain, `google.com.ar`, briefly lapsed and was bought for about $3 USD by a local web designer [35]. No harm ensued - he promptly returned it - but the incident shows even a tech giant can stumble, and the potential impact had an attacker acted maliciously [35].

Phase 3 therefore focuses on **keeping expired domains out of adversaries' hands**. As shown, both external users (customers) and the organization itself (through account takeover) can fall victim otherwise. For attackers, orphaned domains are attractive **attack platforms**, cloaked in legitimacy and leveraging existing trust relationships.

D. Phase 4: Malicious Re-registration

Phase 4 examines the situation after a domain has been taken over by a *new owner* - often an attacker or speculator. The central question is: **How can a captured domain be exploited or monetized?**

T1. Threats from domain speculation and trading: Some actors register domains merely to resell them at a profit. In the harmless case, these are generic terms (e.g., `domaintrading.net`) or catchy names awaiting a buyer [36]. It becomes problematic when speculators register domains clearly linked to a company or product and then try to sell them back to the rightful owner - often at inflated prices. This practice is known as **cybersquatting**. Victims may feel extorted into repurchasing the domain to prevent abuse or protect their brand. Immediately after expiration, fraudsters can seize a domain and demand a ransom for its return [1].

Large-scale domain parking is another issue: studies show that a significant share of *re-registered* or never-used domains are **parked** - they host no original content, only ad links, redirects, or placeholders. According to [33], major parking providers control hundreds of thousands of such domains. Besides *trademark concerns*, parking poses *security threats*: parked domains can be repurposed for phishing or malware without notice, and it is hard for outsiders to judge whether a parked domain is benign or simply "waiting" for abuse [33].

T2. Criminal monetization options: Once attackers gain control of a domain - whether through typosquatting, expiration, or takeover - they acquire a highly valuable asset. **Possible revenue streams** include:

Phishing and fraudulent sites: As in Phase 3, a reputable domain can host convincing phishing pages. Login portals or data-theft forms seem trustworthy because the URL looks legitimate. **Fake shops** are equally common [29][37].

Malware delivery and command-and-control: Attackers distribute malicious files or run **Command-and-Control (C2) infrastructure** for botnets and trojans on the domain. A name absent from blacklists enjoys better initial reach. Some *Sitting Ducks* domains were used for traffic-distribution systems (TDS), spam, and **malware C2** servers [24][29].

Spam and email scams: A freshly registered (or hijacked) domain can host mail servers to send spam. A legacy corporate domain may still have a **good sender reputation**, reducing filter hits [1][38]. Crime groups deliberately set up mail on lapsed domains and even used them to seize social-media or SaaS accounts, as noted earlier [29].

Leveraging residual integrations: If the original organization still references the domain in webhooks, OAuth redirects, or API keys, the new owner can exploit that linkage. Documented cases show attackers gaining **access to enterprise data** by posing as legitimate endpoints [29][32].

Redirects and traffic parking: A subtler yet harmful tactic is funneling all residual traffic to ad or affiliate sites. High-traffic domains earn click revenue via automated parking platforms. While not always illegal, such redirects can tarnish brand reputation - e.g., a former corporate site suddenly points to gambling or adult content [29][33].

Overall, Phase 4 demonstrates that **attackers have many ways to profit from a seized domain**, whether financially or within larger campaigns. A domain in hostile hands becomes a **"weapon"** that slips past defenses thanks to its trusted name. For enterprises, **preventing** such takeovers must be top priority, because **damage control** afterwards is costly. Once criminals register the domain, recourse is often limited to lengthy legal action (e.g., a UDRP proceeding) or an expensive settlement - long after harm may already be done.

IV. Conclusion and Future Work

Domains are critical security assets; a life cycle view shows distinct weaknesses before registration, during operation, after

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

TABLE II. SYSTEMATIC THREAT MAPPING ACROSS DOMAIN LIFE CYCLE PHASES

Phase	Threat (ID)	Recent evidence	Primary controls
P1	T1 Typosquatting / look-alikes	USENIX'14 [4]; NDSS'25 [1]	Defensive regs; brand watch
P1	T2 Orphaned/published names	NDSS'23 [18]; Unit 42 [19]	Monitoring; claims; cleanup
P2	T1 DNS misconfig	CISA [23]; Infoblox [24]	DNSSEC; CAA+CT; restrict AXFR; audits
P2	T2 Subdomain takeover (dangling)	CCS'16 [6]; NSDI'24 [5]	Quarterly scans [20]; cleanup
P2	T3 Registrar account compromise	IMC'22 [25]; The Guardian [26]	MFA; Registry Lock; two-party recovery
P3	T1 Phishing / fraud on expired domains	S&P'22 [29]; KrebsOnSecurity [30]	Auto-renew; renewal governance; brand watch
P3	T2 Email / account takeovers	IMC'24 [31]; The Hacker News [32]	Deprovisioning; retirement checklist
P3	T3 Lingering integrations (OAuth / SSO / API)	IMC'24 [31]; The Hacker News [32]	Deprovisioning; OAuth/SSO audit; key revocation
P3	T4 Drop-catching / speculation	TMA'22 [33]; BBC News [35]	Backorder; legal (UDRP); retain redirects
P4	T1 Speculation/parking abuse	TMA'22 [33]; WIPO [34]	Monitoring; legal recourse
P4	T2 Criminal monetization (phishing / C2 / spam)	Infoblox [24]; SRLabs [37]	Takedowns; blocklists; incident response

expiration, and after re-registration.

Derivation: The conclusions synthesize the phase-wise mapping in Table II with the structured literature scan in Section II, answering RQ1-RQ2.

Implications: Domain security must be run as a continuous program across DNS configuration and registrar governance; safer defaults by registrars, registries, and CAs reduce systemic risk.

Recommendations (priority): DNSSEC on apex and critical zones; CAA; hardened registrar accounts (MFA, Registry Lock, two-party recovery); scheduled zone hygiene and takeover scans; renewal governance with deprovisioning.

Limitations: Conceptual, literature-based synthesis without new measurements; evidence focuses on 2014-2025 English-language sources; prevalence is out of scope.

Future work: (i) DNSSEC/CAA measurement; (ii) WHOIS-based re-registration/abuse analysis; (iii) registrar-security defaults; (iv) audits of SaaS/OAuth residuals during retirement.

REFERENCES

[1] B. V. Adjibi, A. Avgeditis, M. Antonakakis, M. Bailey, and F. Monrose, "The guardians of name street: Studying the defensive registration practices of the fortune 500," in *Proceedings of the 32nd Network and Distributed System Security Symposium (NDSS 25)*, San Diego, CA, USA: Internet Society, Feb. 2025. DOI: 10.14722/ndss.2025.241202.

[2] Y. Zhang *et al.*, "Cross the zone: Toward a covert domain hijacking via shared DNS infrastructure," in *33rd USENIX Security Symposium (USENIX Security 24)*, Philadelphia, PA: USENIX Association, Aug. 2024, pp. 5751–5768, ISBN: 978-1-939133-44-1. [Online]. Available: https://www.usenix.org/conference/usenixsecurity24/presentation/zhang-yunyi-zone.

[3] S. Neupane, G. Holmes, E. Wyss, D. Davidson, and L. De Carli, "Beyond typosquatting: An in-depth look at package confusion," in *Proceedings of the 32nd USENIX Conference on Security Symposium*, ser. SEC '23, Anaheim, CA, USA: USENIX Association, 2023, ISBN: 978-1-939133-37-3.

[4] J. Szurdi *et al.*, "The long "taile" of typosquatting domain names," in *Proceedings of the 23rd USENIX Security Symposium (USENIX Security '14)*, San Diego, CA, USA: USENIX Association, Aug. 2014, pp. 191–206, ISBN: 978-1-931971-15-7. [Online]. Available: https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-szurdi.pdf.

[5] J. Frieß, T. Gattermayer, N. Gelernter, H. Schulmann, and M. Waidner, "Cloudy with a Chance of Cyberattacks: Dangling Resources Abuse on Cloud Platforms," in *Proceedings of the 21st USENIX Symposium on Networked Systems Design and Implementation (NSDI '24)*, USENIX Association, 2024, pp. 1977–1994, ISBN: 978-1-939133-39-7. [Online]. Available: https://www.usenix.org/conference/nsdi24/presentation/friess.

[6] D. Liu, S. Hao, and H. Wang, "All Your DNS Records Point to Us: Understanding the Security Threats of Dangling DNS Records," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*, New York, NY, USA: Association for Computing Machinery, Oct. 2016, pp. 1414–1425, ISBN: 978-1-4503-4139-4. DOI: 10.1145/2976749.2978387. [Online]. Available: https://doi.org/10.1145/2976749.2978387.

[7] M. Squarcina, M. Tempesta, L. Veronese, S. Calzavara, and M. Maffei, "Can i take your subdomain? exploring SameSite attacks in the modern web," in *30th USENIX Security Symposium (USENIX Security 21)*, Vancouver, B.C., Canada: USENIX Association, Aug. 2021, pp. 2917–2934, ISBN: 978-1-939133-24-3. [Online]. Available: https://www.usenix.org/system/files/sec21-squarcina.pdf.

[8] G. Schmid, "Thirty years of dns insecurity: Current issues and perspectives," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2429–2459, 2021. DOI: 10.1109/COMST.2021.3105741.

[9] A. Ramdas and R. Muthukrishnan, "A survey on dns security issues and mitigation techniques," in *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*, 2019, pp. 781–784. DOI: 10.1109/ICCS45141.2019.9065354.

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

[10] A. Affinito *et al.*, "Domain name lifetimes: Baseline and threats," English, in *Proceedings of the 6th edition of the Network Traffic Measurement and Analysis Conference (TMA Conference 2022)*, International Federation for Information Processing (IFIP), Jun. 2022, ISBN: 978-3-903176-47-8. [Online]. Available: https://tma.ifip.org/2022/.

[11] G. C. M. Moura *et al.*, "Characterizing and mitigating phishing attacks at cctld scale," in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '24, Salt Lake City, UT, USA: Association for Computing Machinery, 2024, pp. 2147–2161, ISBN: 979-8-40-070636-3. DOI: 10.1145/3658644.3690192.

[12] M. Wang, X. Zang, J. Cao, B. Zhang, and S. Li, "Phishhunter: Detecting camouflaged idn-based phishing attacks via siamese neural network," *Computers & Security*, vol. 138, p. 103 668, Mar. 2024. DOI: 10.1016/j.cose.2023.103668. [Online]. Available: https://doi.org/10.1016/j.cose.2023.103668.

[13] Palo Alto Networks Unit 42, *The art of domain deception: Bifrost's new tactic to deceive users*, https://unit42.paloaltonetworks.com/new-linux-variant-bifrost-malware/, Retrieved: Jun. 2025, Mar. 2024.

[14] Insikt Group, "SOLARDEFLECTION: C2 Infrastructure Used by NOBELIUM in Company Brand Misuse," Recorded Future, Tech. Rep., May 2022, Retrieved: Jun. 2025. [Online]. Available: https://go.recordedfuture.com/hubfs/reports/cta-2022-0503.pdf.

[15] S. Tilborghs and G. Ferreira, "Flagging 13 million malicious domains in 1 month with newly observed domains," *Akamai Security Blog*, Sep. 2022, Retrieved: Jun. 2025. [Online]. Available: https://www.akamai.com/blog/security-research/newly-observed-domains-discovered-13-million-malicious-domains.

[16] B. Krebs, "Mastercard dns error went unnoticed for years," Retrieved: Jun. 2025, Jan. 2025, [Online]. Available: https://krebsonsecurity.com/2025/01/mastercard-dns-error-went-unnoticed-for-years/.

[17] L. Nguyen, "Byd-domain führt in deutschland zu sexspielzeug," Retrieved: Jun. 2025, Jul. 2024, [Online]. Available: https://sz.de/lux.J5FGj79Eq9c5ThRgCzKaqM.

[18] X. Li *et al.*, "Ghost domain reloaded: Vulnerable links in domain name delegation and revocation," in *Proceedings of the 2023 Network and Distributed System Security Symposium (NDSS '23)*, San Diego, CA, USA: The Internet Society, 2023. DOI: 10.14722/ndss.2023.23005.

[19] P. A. N. Unit 42, *Dangling domains: Security threats, detection and prevalence*, https://unit42.paloaltonetworks.com/dangling-domains/, Retrieved: Jun. 2025.

[20] H. N. Security, *Baddns: Open-source tool checks for subdomain takeovers*, https://www.helpnetsecurity.com/2025/02/03/baddns-open-source-tool-check-domain-subdomain-takeover/, Retrieved: Jun. 2025.

[21] R. Future, *Dnssec: What is it? how does it work?* https://www.recordedfuture.com/threat-intelligence-101/tools-and-techniques/dnssec, Retrieved: Jun. 2025.

[22] S. I. S. Center, *Quick status of the caa dns record adoption*, https://isc.sans.edu/diary/26738, Retrieved: Jun. 2025.

[23] CISA, *Dns zone transfer axfr requests may leak domain information*, https://www.cisa.gov/news-events/alerts/2015/04/13/dns-zone-transfer-axfr-requests-may-leak-domain-information, Retrieved: Jun. 2025.

[24] I. T. Intel, "DNS Predators Hijack Domains to Supply their Attack Infrastructure," Retrieved: Jun. 2025, Nov. 2024, [Online]. Available: https://blogs.infoblox.com/threat-intelligence/dns-predators-hijack-domains-to-supply-their-attack-infrastructure/.

[25] G. Akiwate *et al.*, "Retroactive identification of targeted dns infrastructure hijacking," in *Proceedings of the ACM Internet Measurement Conference (IMC '22)*, Nice, France: Association for Computing Machinery, Oct. 2022, pp. 14–32. DOI: 10.1145/3517745.3561425.

[26] A. Hern, "Lenovo website hacked and defaced by lizard squad in superfish protest," Retrieved: Jun. 2025, The Guardian, Feb. 2015, [Online]. Available: https://www.theguardian.com/technology/2015/feb/26/lenovo-website-hacked-and-defaced-by-lizard-squad-in-superfish-protest.

[27] C. Global, *Csc's 2023 domain security report finds many global 2000 companies neglect their .ai domain extensions despite surge in popularity for artificial intelligence*, https://www.cscglobal.com/service/press/many-global-2000-companies-neglect-their-ai-domains/, Retrieved: Jun. 2025.

[28] D. Chiba, H. Nakano, and T. Koide, "Domaindynamics: Advancing lifecycle-based risk assessment of domain names," *Computers & Security*, vol. 153, p. 104 366, 2025. DOI: 10.1016/j.cose.2025.104366. [Online]. Available: https://doi.org/10.1016/j.cose.2025.104366.

[29] J. So, N. Miramirkhani, M. Ferdman, and N. Nikiforakis, "Domains do change their spots: Quantifying potential abuse of residual trust," in *2022 IEEE Symposium on Security and Privacy (SP)*, 2022, pp. 2130–2144. DOI: 10.1109/SP46214.2022.9833609.

[30] B. Krebs, *That domain you forgot to renew? yeah, it's now stealing credit cards*, *KrebsOnSecurity* (blog), Retrieved: Jun. 2025, Nov. 2018. [Online]. Available: https://krebsonsecurity.com/2018/11/that-domain-you-forgot-to-renew-yeah-its-now-stealing-credit-cards/.

[31] R. Li *et al.*, "Bounce in the wild: A deep dive into email delivery failures from a large email service provider," in *Proceedings of the 2024 ACM on Internet Measurement Conference*, ser. IMC '24, Madrid, Spain: Association for Computing Machinery, 2024, pp. 659–673, ISBN: 979-8-40-070592-2. DOI: 10.1145/3646547.3688425.

[32] T. H. News, *Google oauth vulnerability exposes millions via failed startup domains*, https://thehackernews.com/2025/01/google-oauth-vulnerability-exposes.html, Retrieved: Jun. 2025.

[33] J. Zirngibl *et al.*, "Domain parking: Largely present, rarely considered!" In *Proceedings of the 6th Network Traffic Measurement and Analysis Conference (TMA '22)*, International Federation for Information Processing (IFIP), 2022, pp. 1–9. [Online]. Available: https://dl.ifip.org/db/conf/tma/tma2022/tma2022-paper26.pdf.

[34] W. I. P. O. (WIPO), *Wipo domain name report 2024: Udrp case filings remain strong*, Retrieved: Jun. 2025, 2025. [Online]. Available: https://www.wipo.int/amc/en/domains/news/2025/news_0001.html.

[35] J. Clayton, "Google argentina's domain name bought by man for £2," Retrieved: Jun. 2025, Apr. 2021, [Online]. Available: https://www.bbc.com/news/technology-56870270.

[36] Afnic Studies Team, "The global domain name market in 2023," Afnic – Association Française pour le Nommage Internet en Coopération, Tech. Rep., Jul. 2024, Retrieved: Jun. 2025. [Online]. Available: https://www.afnic.fr/wp-media/uploads/2024/07/study-afnic-the-global-domain-name-market-in-2023.pdf.

[37] M. Marx and Team, *Bogusbazaar: A criminal network of webshop fraudsters*, Security Research Labs Blog, Retrieved: Jun. 2025, May 2024. [Online]. Available: https://www.srlabs.de/blog-post/bogusbazaar.

[38] PortSwigger, *How expired web domains help criminal hackers unlock enterprise defenses*, https://portswigger.net/daily-swig/how-expired-web-domains-help-criminal-hackers-unlock-enterprise-defenses, Retrieved: Jun. 2025.

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org