Systemic Analysis of Internet Domain Vulnerabilities and Multi Layered Mitigation Strategies

Mihail DUMITRACHE[1,3], Ionut SANDU[1], Carmen ROTUNĂ[1,2], Monica TODERAȘCU[1]
[1]National Institute for Research & Development in Informatics - ICI Bucharest
[2] Politehnica University of Bucharest
[3]University of Bucharest, Faculty of Letters
mihail.dumitrache@ici.ro, ionut.sandu@ici.ro, carmen.rotuna@ici.ro, monica.toderascu@ici.ro

Abstract: Internet domain names constitute a critical component of global digital infrastructure, supporting resource identification and trust establishment across environments. Their security is therefore essential to the resilience and reliability of digital systems nowadays. This paper analyses the main vulnerabilities affecting Internet domains within 2022-2025 timeframe, with a focus on developments and assesses their implications for future defensive strategies. The findings indicate a shift from protocol based attacks toward exploitation of administrative control ecosystems, lifecycle management failures and domain trust mechanism issues. Identified vulnerabilities affect domain owners, registrars, registries and all internet ecosystem. These include DNS records, denial-of-service, cache poisoning, homograph attacks, certificate mis-issuance DNS-based amplification attacks and DNSSEC-related. This research paper integrates academic research with institutional and operational sources, including ICANN, RIPE NCC and national CERT reporting. It highlights the systemic nature of domain name security, driven by governance gaps, inconsistent enforcement and increasing attacker automation. In response, a multi-layered mitigation framework is proposed, emphasizing lifecycle governance, control-plane security, resolver resilience, identity protection and availability engineering. The results suggest that effective domain security in 2026 requires continuous monitoring, automated detection and coordinated ecosystem-level governance to ensure the trustworthiness of domain-based digital identity.

Keywords: Domain name, DNS, security, threat, vulnerabilities, incident, defense resilience, mitigation.

INTRODUCTION

Internet domains represent an important part of the global digital infrastructure, facilitating the identification of relevant online resources, the delivery of interconnected digital services, and the implementation of trust across the Internet ecosystem (Banciu, Petre și Dumitrache, 2019). Domains, which are key elements of digital identity, they support critical services such as web access,

https://doi.org/10.54851/v8i1y202607

electronic mail, authentication mechanisms, and cryptographic certificate validation. As a result, the security of Internet domains is directly associated with the reliability, availability, and trustworthiness of contemporary digital systems (Dumitrache et al., 2024; Smada et al., 2024; Rotună et al., 2019; Gheorghiță et al., 2023).

In recent years, Internet domains have become targets for cyber threat actors due to their important role in the digital trust chain. Recent attacks frequently exploit administrative vulnerabilities and misconfigurations within the Domain Name System (DNS) and deficiencies in domain lifecycle management, rather than focusing on attacks directed at the network layer. Incidents like domain hijacking, subdomain takeover, DNS abuse, and reputation manipulation have demonstrated that the breach of a single domain can lead to massive service disruption, financial loss, and deterioration of end-user confidence (Kuerbis and Mueller, 2023; Herzberg et al., 2024).

Between 2022-2025, persistent systemic vulnerabilities and new risks that continue to emerge were highlighted, both generated by automation and artificial intelligence. Attackers used more and more automated scanning, credential-based attacks against domain registrars, and large-scale domain generation techniques to exploit weaknesses in DNS configurations and governance processes. These developments demonstrated the constraints of traditional security models, which usually focus on isolated technical controls rather than systemic risk analysis (Liu et al., 2024).

As the threat environment is evolving, 2026 is bringing new challenges for the security of Internet domains, especially on the centralization of infrastructure and the dependency on third party services. An analysis of vulnerabilities during the previous two years is critical and shows the attacker behaviour, identifying failure patterns that are repeated and reinforcing preventive security measures. Such retrospective analysis not only supports effective mitigation of known threats but also increases the ability to prevent novel attack vectors before they are widely exploited.

Therefore, this research paper intends to analyse the most important vulnerabilities affecting Internet domains during the 2022-2025 period, evaluate their implications for the wider Internet ecosystem, and emphasize associated security considerations relevant to mitigating and preventing emerging attacks in 2026. This work seeks to contribute to improving the resilience and trustworthiness of the global domain name infrastructure by deriving future defensive strategies using empirical analysis of recent incidents.

STATE OF THE ART

Since 2022, the research on domain name security has dynamically changed from mainly protocol-centric views (e.g., “classic” DNS spoofing and cache poisoning) to a broader socio-technical view that treats domains as digital assets incorporated in an ecosystem of registries, registrars, hosting, CDNs, and detection/abuse management processes. This change is given in two directions. The empirical analyses of how abuse is reported, sustained, and processed in the DNS ecosystem and measurement and detection studies that outline malicious domains and DNS-based attack patterns using machine learning and traffic analytics (Cheng et al., 2022).

A significant amount of research has investigated how effectively different internet entities handle abuse reports and how these processes influence the persistence of harmful domains. Cheng et al. (2022) offer an empirical evaluation of the mechanisms for receiving and handling abusive domain reports across multiple entities in the DNS ecosystem, emphasising the practical “operational gap” between enforcement and reporting. This work is important because there are incidents involving domain infrastructure and they persist due to processes that are not consistent, jurisdictional differences, and variation in incentives across providers - factors that significantly influence mitigation timelines for abusive registrations, not due to a newly identified exploit. (Cheng et al., 2022).

An important research thread in 2022-2025 regards the identification of algorithmically

generated domains (AGDs) produced by domain generation algorithms (DGAs), usually used for botnet resilience of command-and-control. Address detection of malicious AGDs, showing the limitations of simpler filters when they are confronted with dictionary-based DGAs that seem like good lexical structures.

Also, research has progressively examined hostile robustness of DGA detectors - i.e., how attackers can manipulate training or inference behaviour. Zhai et al. (2023) study backdoor style threats against LSTM based domain classifiers, showing that high baseline accuracy may not translate to reliable detection under hostile conditions (Zhai et al., 2023).

These studies inform a prospective outlook for 2026 indicates that domain reputation and lexical detection must be approached as adaptive security challenges, where attackers iterate on naming strategies to evade models.

More recent work is proposing moving "left of boom", detecting domains most likely associated with abusive activity before full exploitation. Rotună (2025) frames proactive domain name security around adaptive analysis of domain characteristics and attacker behaviours (including typo squatting/ homoglyph patterns and rapid domain churn). This line of work reflects a broader trend toward the development of predictive domain risk assessment models, where lexical, registration, and infrastructure signals are combined to reduce attacker dwell time and limit campaign scale (Rotună, 2025).

There is another ongoing research direction that is using DNS traffic as a measurement lens. Moure-Garrido et al. (2024) analyse DNS traffic generated by IoT devices and show that queried domains could be very different, offering device identification and eventually facilitating targeted exploitation. This privacy study is critical to domain security as it demonstrates how DNS domain patterns can leak sensitive information and support data acquisition and adversarial planning (Moure-Garrido et al., 2024).

DNS integrity attacks remain as important, but recent work tends to emphasize operational detection and real-time monitoring rather than solely protocol fixes. Yu et al. (2025) propose a distributed "DNS cache sensor" architecture to detect anomalies by comparing cached records against authoritative data - an approach aligned with defensive observability. This supports the broader state of the art perspective that practical DNS defense increasingly depends on ongoing measurement and anomaly detection alongside cryptographic mechanisms (Yu et al., 2025).

Encrypted DNS (e.g., DoH) enhances confidentiality, but it introduces enterprise visibility challenges and can be abused for covert channels. Talabani et al. (2025) propose a DoH tunneling detection system based on statistical feature extraction from traffic, reflecting a broader trend of classifying encrypted DNS behaviours using flow-level and session-level features rather than payload inspection (Talabani et al., 2025).

De Bernardi et al. (2025) propose an approach based on explainability to DNS leveraging autoencoder models, tunnelling detection, and explainable artificial intelligence (XAI) techniques to optimize transparency. Their work aims to strengthen analyst trust and support more effective operational responses by offering clear justifications for flagged traffic, a capability that is becoming important as detection systems based on machine learning gain widespread adoption. (De Bernardi et al., 2025).

Between 2022-2025, the literature unifies on three practical conclusions for 2026:

- Domain abuse is ecosystem-driven (reporting, enforcement, incentives) and technical (Cheng et al., 2022).
- Detection need be robust to adaptive adversaries, especially for DGAs, typo squatting, and model-targeting attacks (Zhai et al., 2023; Rotună, 2025).
- Operational visibility is furthering measurement and anomaly detection, particularly for cache integrity and encrypted DNS covert channels (Yu et al., 2025; Talabani et al., 2025; De Bernardi et al., 2025).

These lines of work are motivated by analyzing vulnerabilities detected in the early three years as

a base line for preventing emergent attacks in 2026, because attacker tradecraft is increasingly using automation, ML evasion, and the unevenness of real-world DNS governance processes.

INSTITUTIONAL AND OPERATIONAL PERSPECTIVES

Recent work on vulnerabilities of domain names and DNS abuse (2022-2025) has been complemented increasingly by institutional and operational work produced by governance bodies (e.g., ICANN/SSAC), regional Internet registries (e.g., RIPE NCC), and national/sectoral CERTs. This "state of the art" layer matters because, in practice, numerous domain compromises are facilitated less by novel protocol-level breaches and more by weaknesses in the control plane, inconsistent abuse handling, and insufficient operational hardening of resolvers and authoritative infrastructure.

DNS abuse on domain names

Recent outputs from ICANN frame DNS abuse and domain-name misuse not only as a technical issue but also as a contractual and ecosystem enforcement challenge. Through its DNS Abuse Mitigation Program, ICANN consolidates definitions, community resources, and reporting channels focused on the name of the domain abuse categories typically associated with DNS (e.g., malware, phishing, botnets, pharming) and on improving mitigation practices by contracted parties (registries/registrars) (ICANN Progress and Next Steps in Enforcing DNS Abuse Mitigation, 2024)

Since April 2024, an important development is the publication of regular compliance reporting for DNS abuse, including monthly reporting and more contextual "six-month" reporting intended to improve transparency around enforcement actions and complaints processing (ICANN Progress and Next Steps in Enforcing DNS Abuse Mitigation, 2024).

In 2025, ICANN documented progress and next steps in enforcing DNS abuse mitigation requirements, including quantified investigation activity and audits. (ICANN DNS Abuse Mitigation Program, 2025)

From a "state of the art" perspective, these materials support two research points that are relevant:

- Mitigation capacity is partly institutional: "who is responsible" and "what is enforceable" affects real world outcomes for abusive domains. (ICANN Generic Names Supporting Organization, 2025)
- Abuse policy overlaps with technical side effects ICANN SSAC reports (e.g., on DNS blocking) highlight that operational interventions at the DNS level can have inadvertent consequences, which need to be taken into consideration when designing mitigation strategies. (ICANN SSAC, 2025)

RIPE NCC best current practices

RIPE NCC contributions are particularly important for domain security because they address the recursive resolver as a major security control point and because they provide measurement infrastructure used broadly in DNS studies.

RIPE-823 (DNS Resolver Recommendations), published in 2024, provides the best recent practices for operating DNS resolvers (public and private), covering resilience, privacy, and security guidance. This operational baseline has seen a rise in citations because resolver misconfiguration and weak operational controls intensify the blast radius of both abuse and software vulnerabilities (e.g., cache poisoning, validation DoS).

In parallel, the RIPE Atlas platform continues to serve as a key measurement substrate for DNS research and monitoring. RIPE NCC documentation on DNS measurements with RIPE Atlas (RIPE NCC DNS Measurements with RIPE Atlas, 2024) shows how global vantage points can be used to detect DNS behaviour, misconfigurations, and ecosystem-level phenomena. (RIPE 2024a; RIPE, 2024b) Recent synthesis work evaluating RIPE Atlas operations

also highlights the breadth of DNS-related measurement topics (including DNSSEC, caching, fragmentation, and delegation issues), reinforcing measurement as a state of the art pillar for DNS security analytics (Nosyc, 2024).

CERT advisories

CERT publications function as a bridge between disclosure and operational defense by translating CVEs into actionable remediation guidance, often with clear impact framing.

For example, the 2024 "KeyTrap" class of vulnerabilities affecting DNSSEC, validating resolvers (DoS via CPU exhaustion) was very quickly reflected in national CERT advisories such as CERT-In's advisory explicitly referencing DNS server DoS risk associated with KeyTrap/NSEC3, related weaknesses that help organizations focus on patching and validation hardening.

Complementary entries from other CERT ecosystems (e.g., INCIBE-CERT) further disseminated technical summaries and risk context, contributing to broader and faster mitigation across jurisdictions (INCIBE-CERT, 2024).

This "CERT layer" is important in domain security research because it provides evidence of time to awareness and the practical framing defenders receive (DoS vs. takeover, exploitability assumptions, affected software) (NIST, 2024).

DNSC threat trend reporting

At the national level, Romania's Directorate for National Cyber Security (DNSC) fulfills a role analogous to a CERT/CSIRT function, publishing situational and trend analyses that are important to domain abuse and DNS-enabled attack patterns (e.g., phishing, malware delivery, campaign-scale indicators).

The annual activity reporting of DNSC and periodic reports on indicators/statistics/tendencies provide a structured view of the threat landscape that is evolving at the regional level, which can be exploited as contextual data for domain security studies (e.g., correlating domain abuse spikes with campaign narratives or identifying dominant social engineering themes linked to malicious domains).

These materials are not "domain-only" research papers, and they contribute to the state of the art by providing empirically grounded threat context that academic studies often lack. (DNSC, 2024)

Integrating institutional outputs into a domain vulnerability research lens

A practical way to incorporate the sources into the present article, in the comparative analysis, is to treat them as complementary evidence streams:

- ICANN/SSAC addresses governance definitions, compliance mechanisms, and side-effect analysis of mitigation interventions (e.g., blocking) (ICANN SAC, 2025).
- RIPE NCC deals with operational best practices for resolvers and globally scalable measurement methodologies for DNS behaviour and misconfiguration detection (RIPE, 2024b).
- CERTs addresses rapid operational guidance and "defender framing" of newly disclosed DNS/DNSSEC vulnerabilities.
- DNSC describes national threat trend baselines and situational awareness to contextualize domain abuse campaigns and prioritization (DNSC, 2024).

In 2026, focused work, this integration supports a more defensible argument that preventing new attacks requires identifying technical vulnerabilities and understanding operational adoption, enforcement capacity, and measurement visibility across the DNS/domain ecosystem.

VULNERABILITY LANDSCAPE AND RECENT INCIDENTS 2022-2025

In the past four years, the global cybersecurity landscape has been marked by an important increase in the discovery and exploitation of software and infrastructure vulnerabilities. These trends show the complexity that is growing and the linkage of the digital systems, the rise of complex attack techniques, and the expansion of attack surfaces across cloud services and critical infrastructure (Shet and Alsmadi, 2025; Thiyagarajan, Bist, and Nayak, 2025). In the same time, national cybersecurity authorities including the DNSC report that these international trends are aligned at the national level, with a growing number of incidents, evolving threat tactics and increasing impact on important services (DNSC, 2025; Agerpres, 2025a).

International Vulnerability Trends

At a global level, public vulnerability repositories and academic analyses report tens of thousands of recently reported software flaws and vulnerabilities each year, with a significant part representing high-risk exposures (Shet and Alsmadi, 2025). Of particular concern is the growing frequency of zero day vulnerabilities, which are exploited before the official mitigation is available. This type of vulnerabilities have been observed in adopted enterprise software and infrastructure services, significantly increasing their potential impact.

A critical example is the 2023 MOVEit Transfer breach, which is the result of a critical zero-day SQL injection vulnerability (CVE-2023-34362) that was actively exploited, leading to data theft across thousands of organizations worldwide. This incident shows how software dependencies and third party components can spread risk outside a single vendor or user community.

In the same time, attacks targeting the software supply chain, in which adversaries violate development pipelines or update mechanisms, have become systemic threats that are problematic for traditional defensive models (Kshetri and Voas, 2023). Usually, these attacks bypass perimeter defences and abuse the trust relationships between software producers and consumers.

Incidents and Structural Vulnerabilities in Romania

Romanian cybersecurity authorities have documented an important escalation in cyber threats at the national level. According to the DNSC's 2024 activity report, in Romania, cyber fraud incidents have grown by 40.2 % and malware incidents amplified by 286.8 % in regards to the previous year (Agerpres, 2025a; CECCAR Business Magazine, 2025). The DNSC also notes that the next sectors, healthcare, public administration and energy are among the most targeted by cyber threats, showing the wide economic impact of vulnerabilities on important services.

Also, the DNSC has reported many cyberattack activities, including ransomware targeting critical infrastructure. Near the end of 2025, an important ransomware attack affected the Romanian national water management authority, compromising around 1,000 systems and prompting national incident response coordination. This is a critical example of how exploited vulnerabilities can disrupt operational networks and services (DNSC, 2025).

Prior, coordinated distributed denial of service (DDoS) attacks (including those attributed to foreign threat actors) attempted to disrupt Romanian public sector websites, highlighting persistent network level vulnerabilities against volumetric attacks (Agerpres, 2022). Also, DNSC advisories show persistently phishing and malware distribution campaigns that target Romanian users, then illustrating the diversity and persistence of threats across different exploitation vectors (Agerpres, 2025b).

Institutional and Regulatory Context

The cyber threat landscape in Romania is developing, and it has also defined the regulatory environment. Emergency Ordinance no. 155/2024 designates DNSC as the national authority responsible for managing

cybersecurity risks and incident reporting obligations, showing the state's approach to integrating vulnerability governance (Portal legislativ, 2024). This regulatory shift is aligning to European Union frameworks such as the NIS2 Directive, which seeks to enhance network capabilities and information security across member states by imposing harmonized security and incident reporting requirements (European Commission, 2024; DNSC, 2025).

Notably, DNSC's role includes technical incident management and strategic threat monitoring, allowing Romania to align national defensive measures with increasing threat patterns. Reports from DNSC underline technical exploits and the increasing complexity and sophistication of attacks, signalling the need for multi-level resilience strategies.

Implications for Defensive Strategies

The international and national noted incident trends show the limitations of defensive reactive approaches that focus on patching known vulnerabilities. The frequency of zero day exploits, ransomware campaigns and multi vector attacks underlines the need for proactive threat hunting, anomaly detection, and coordinated response frameworks.

From Romania's perspective, national data show that the public and the private sector are subject to exposure to cyber threats, emphasizing the importance of cross sector information sharing, risk vulnerability management, and multi-stakeholder defensive cooperation.

These developments provide the foundation for subsequent sections that focus on reinforcing detection mechanisms, improving mitigation times and strengthening resilience to adaptive threats.

DOMAIN NAME VULNERABILITIES 2022-2025

Between 2022 and 2025, the security status of the names for Internet domains was defined by a convergence of technical, operational and governance-related weaknesses. As domain names function as anchors for DNS resolution, cryptographic trust, email authentication and cloud service integration, vulnerabilities have materialized primarily at control plane interfaces and lifecycle boundaries rather than within DNS protocol semantics alone. This chapter systematically identifies and classifies the dominant vulnerability classes identified between 2022-2025.

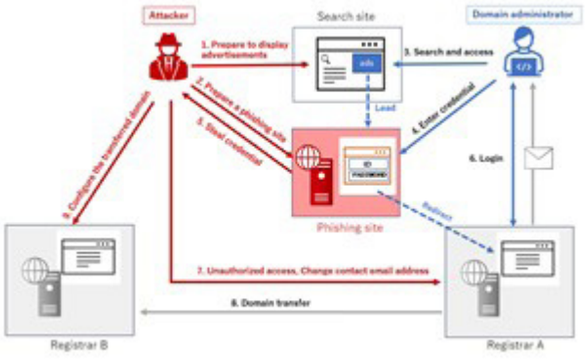

Figure 1. *High-level view of domain name vulnerabilities(Source: own)*

Lifecycle induced vulnerabilities

One of the most important vulnerabilities that affects domain names across 2022-2025 unlinked DNS records, particularly CNAME, NS and TXT records referencing decommissioned or not claimed third party services. Attackers can reclaim the abandoned infrastructure and inherit trust associated with legitimate subdomains when cloud resources or external platforms are retired without corresponding DNS cleanup.

Data driven analyses and incident reports demonstrate that these types of vulnerabilities remain exploitable for extended periods, usually not noticed due to the absence of functional service interruption. This vulnerability class is very tied to modern operational practices, for example, continuous deployment and cloud outsourcing, which systematically increase DNS dependency complexity while reducing

centralized control. Therefore, lifecycle induced weaknesses are a key driver of subdomain takeover and long term abuse campaigns.

Registrar and DNS provider control plane weaknesses

Control plane weaknesses at registrars and DNS hosting providers represented another category with significant impact during the analysed period. Authentication weaknesses, limited ownership verification and inconsistent change control procedures permitted unauthorized alteration of nameserver records, delegations and domain transfers without exploiting DNS resolution mechanisms.

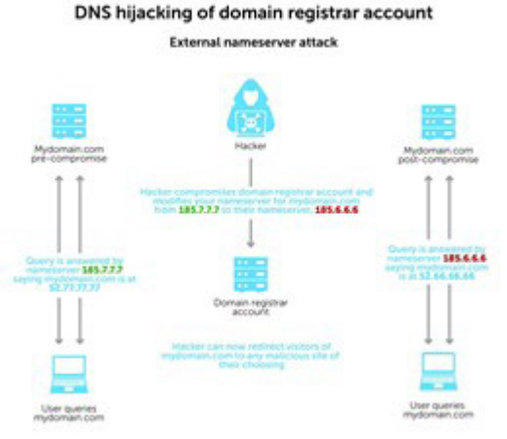

Figure 2. *DNS hijacking of the domain registrar account*

Attackers obtain the ability to redirect traffic, obtain valid TLS certificates, and manipulate email routing once control over authoritative functions is compromised. This class of vulnerability overrides many downstream security controls and shows that administrative weaknesses can undermine the integrity of the entire domain trust chain. Studies and governance reports from ICANN stress that such incidents are often amplified by variable security practices across registrars and DNS providers.

DNSSEC validation denial of service

The disclosure of vulnerabilities for DNSSEC related denial of service in 2024 identified an important weakness at the recursive resolution tier. Specifically, maliciously constructed DNS responses that exploit validation complexity can consume resolver CPU resources, culminating in distributed resolution failures affecting domains that are otherwise properly configured.

This vulnerability category is substantial because its impact propagates across individual domain owners, affecting all domains resolved through vulnerable infrastructure. The findings stress the shared-risk nature of recursive resolvers and demonstrate how cryptographic protections, when erroneously bounded, can introduce structural fragility rather than resilience.

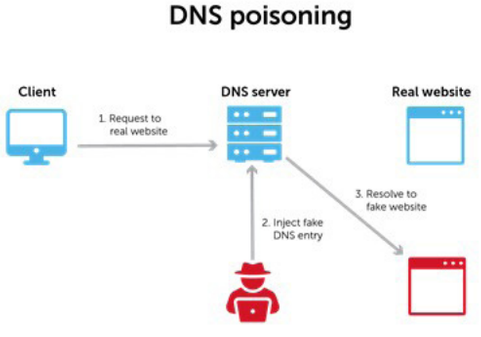

Figure 3. *DNS poisoning attack*

Resolver integrity vulnerabilities

In 2025, the attention was designed to address cache poisoning vulnerabilities, especially in widely deployed DNS software. These weaknesses exploit not enough randomness in query identifiers or flawed response validation logic, allowing attackers to introduce malicious records into resolver caches.

These integrity violations allow redirection of domain traffic at scale and diminish user trust

even when authoritative domain configurations remain with no modification. The continued persistence of cache poisoning vulnerabilities underlines the long term challenges of securing shared resolver infrastructure and consolidates the importance of layered security approaches such as DNSSEC and cache integrity monitoring.

Domain based identity abuse

An important part of domain abuse between the years 2022 and 2025 utilized identity and trust services anchored in domain names. Internationalized Domain Name (IDN) homograph attacks used Unicode character similarity to misdirect users and avoid superficial validation. Concurrently, weaknesses in automated TLS certificate issuance enabled attackers to obtain valid certificates during brief windows of domain or subdomain misconfiguration.

Email authentication is lacking, especially absent or permissive SPF, DKIM and DMARC policies, supported impersonation and phishing campaigns using valid domain identities. All these vulnerabilities show that domain security extends outside DNS resolution into the wider ecosystem of trust services.

Information exposure through DNS misconfiguration

Misconfigured DNS zone transfers and excessively permissive query responses continued to expose internal domain structure, facilitating reconnaissance and targeted exploitation. While such exposures do not compromise domain integrity directly, they reduce a lot of the effort of the attacker by revealing subdomains, service naming conventions, and legacy infrastructure.

This vulnerability class highlights DNS's role as a resolution system and an information disclosure surface, needing rigorous configuration and continuous auditing.

DNS amplification and authoritative infrastructure exhaustion

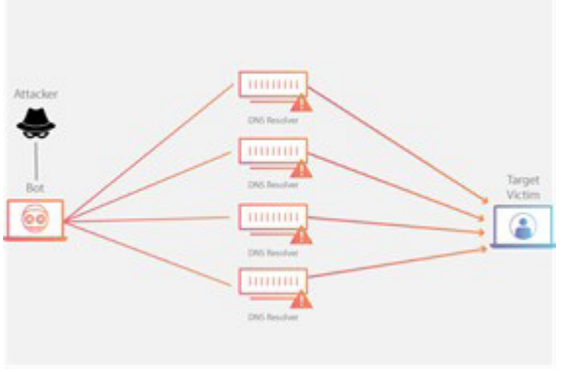

Figure 4. *Amplification of denial of service attacks*

Amplification driven by denial of service attacks against authoritative DNS servers remained an important threat throughout all periods. By exploiting the stateless and open nature of DNS, attackers were able to overload authoritative infrastructure, leading to entire domains not being reachable.

Although amplification attacks are not new, their impact has expanded due to growing reliance on DNS for application delivery and security validation. This vulnerability class underlines that availability must be considered a critical property of domain security rather than a secondary operational concern.

Synthesis aligned with the unified vulnerability framework

The vulnerabilities identified between 2022 and 2025 align with the categories presented in Table 1 and show that domain name security failures are interdependent and systemic. The following interact to create amplified risk Lifecycle drift, control plane exposure, resolver vulnerability, trust service abuse, and availability threats.

This synthesis underlines the need for the multi-layered mitigation strategies developed in the next chapter, and it supports the conclusion that effective domain security in 2026 requires action coordinated across multiple domains, such as technical, administrative, and governance.

EXTENDED MITIGATION MEASURES FOR DOMAIN VULNERABILITIES

The system weaknesses identified in the previous chapter show that domain security is no longer limited to the precision of DNS protocol implementations. Rather, it results from the interaction of technical controls, operational discipline, and ecosystem governance mechanisms. Effective mitigation strategies need to be composed of multiple layers, always enforced, and capable of adapting to evolving attacker behaviour.

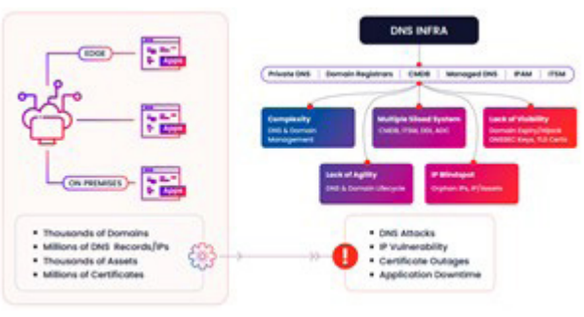

Figure 5. *DNS Infrastructure*

This chapter extends previous mitigation discourse by examining defensive measures across five complementary protection layers: lifecycle governance, control plane security, resolver and availability resilience, identity and trust protection.

Lifecycle governance and DNS mitigation measures

The persistence of vulnerabilities caused by orphaned DNS artifacts is a repeated theme during 2022-2025 incidents, with records that remain active long after the associated service or ownership context has changed. Mitigation begins with recognizing DNS data as live security dependencies, not with static configuration elements.

Organizations should implement DNS hygiene through many asset inventories, where each domain and subdomain is mapped to an owner, a purpose, and a lifecycle state. Automated detection of dangling DNS records, obsolete delegations, and inactive validation tokens enables early remediation before leveraging. Lifecycle governance must extend to mergers, cloud migrations, and vendor transitions, where domain dependencies are frequently ignored, which is an important aspect.

Lifecycle governance transforms DNS from a reactive operational component into a proactive security control.

Strengthening domain control plane security

Control plane vulnerabilities, which involve registrar access, DNS provider accounts and delegation authority, have proven to be the most important risks. Mitigation requires a transition from convenience management to assurance driven domain administration.

At least, domain operators should apply multi factor authentication for all registrar and DNS-hosting interfaces, restrict authorized actions to secured accounts, and, if available, enable registry lock mechanisms. These measures raise the cost of unauthorized delegation changes and domain transfers.

Procedural assurance is important as well. Regular audits of registrar data, name server assignments, and contact information help detect not authorized or accidental changes. Implementing formal change control procedures for delegation modifications further reduces exposure to malicious and unintended configuration errors.

Resolver side resilience

Even if domain owners do not operate directly with recursive resolvers, resolver side weaknesses may affect a lot the domain availability and integrity. The DNSSEC validation

denial of service vulnerabilities and cache poisoning issues disclosed in 2024 - 2025 show how shared infrastructure fragility propagates risk across unrelated domains.

At this layer, mitigation efforts emphasize resilient resolver operations, including software updates, validation complexity controls, and diversified resolver deployments. Monitoring resolver behaviour for atypical CPU usage, validation failures, or cache inconsistencies provides early warning of exploitation attempts.

From an ecosystem perspective, collaboration between resolver operators, software vendors, and coordination bodies such as RIPE NCC enhances collective resilience, thereby reducing systemic exposure to single implementation flaws.

Domain based identity and trust mechanisms

Numerous of the high impact domain abuses do not requiring full takeover of the domain. Instead, attackers exploit identity and trust mechanisms linked with domains. Mitigation strategies need to evolve beyond DNS resolution to encompass certificate issuance and email authentication.

Protective measures will include monitoring certificate transparency logs to be able to detect unauthorized TLS certificates, restricting domain validation tokens to strictly controlled DNS zones, and enforcing strict DMARC policies for email. For Internationalized Domain Names, registries and brand owners benefit from script restriction policies and ongoing monitoring for visually confusable registrations.

In conjunction, these measures are protecting the semantic trust users associate with domain names, which attackers continuously seek to exploit.

Mitigation for DNS-based denial of service

Availability remains a core security property for domain names. Amplification based DDoS attacks against authoritative DNS infrastructure persist in presenting a risk, especially for organizations relying on a single provider or deployments geographically centralized.

Mitigation requires an architectural resilience: Anycast based authoritative DNS, response rate limiting, and integration with upstream DDoS mitigation services are reducing the performance of volumetric attacks. Regular stress testing and incident response exercises ensure that mitigation mechanisms function under real-world conditions.

What is also important is that the availability mitigation need be treated as a domain security condition but also as a network operations concern.

Toward integrated domain security in 2026

The mitigation measures presented here show that no single control can address the full spectrum of domain vulnerabilities identified between 2022 and 2025. But effective defence materializes from integration across layers, putting together technical hardening with governance, monitoring, and coordination.

As domain infrastructures develop into integrated with DNS, TLS, email and cloud services, tightly coupled mitigation strategies must evolve accordingly. For 2026, an approach could be that the domain security prioritizes visibility, accountability, and resilience, ensuring that domain names remain trustworthy anchors of digital identity.

Table 1. *Domain vulnerabilities mapping to mitigation measures*

Vulnerability	Mitigation Measures
Dangling DNS records and abandoned services	Continuous DNS inventory, automated dangling-record detection, lifecycle governance
Domain hijacking via delegation or account compromise	Registry lock, role separation, and delegation audits
DNSSEC validation denial of service	Resolver patching, validation limits, anomaly monitoring
Resolver cache poisoning	Strong randomness, DNSSEC, and cache integrity verification
IDN homograph abuse	Script restriction, punycode display, and monitoring
Unauthorized TLS certificate issuance	Certificate transparency monitoring, controlled DNS validation
Exposed DNS zone transfers	Restricted AXFR/IXFR, configuration audits. AXFR (Full Zone Transfer) and IXFR (Incremental Zone Transfer) are DNS protocols used to synchronize zone files between primary and secondary name servers.
DNS amplification DDoS	Rate limiting, anycast deployment, upstream mitigation
Email spoofing via SPF/DKIM/DMARC misconfiguration	Strict DMARC enforcement, authentication alignment

Integrated Framework for Domain Vulnerabilities and Mitigation

The figure below illustrates the multi layered nature of domain security, underlining how vulnerabilities become apparent at the intersection of lifecycle governance, administrative control planes, resolver infrastructure, identity services, and availability engineering. The figure summarizes the analyses developed in Chapters 4 and 5 and provides a holistic view of domain security as an ecosystem property rather than an isolated technical function.

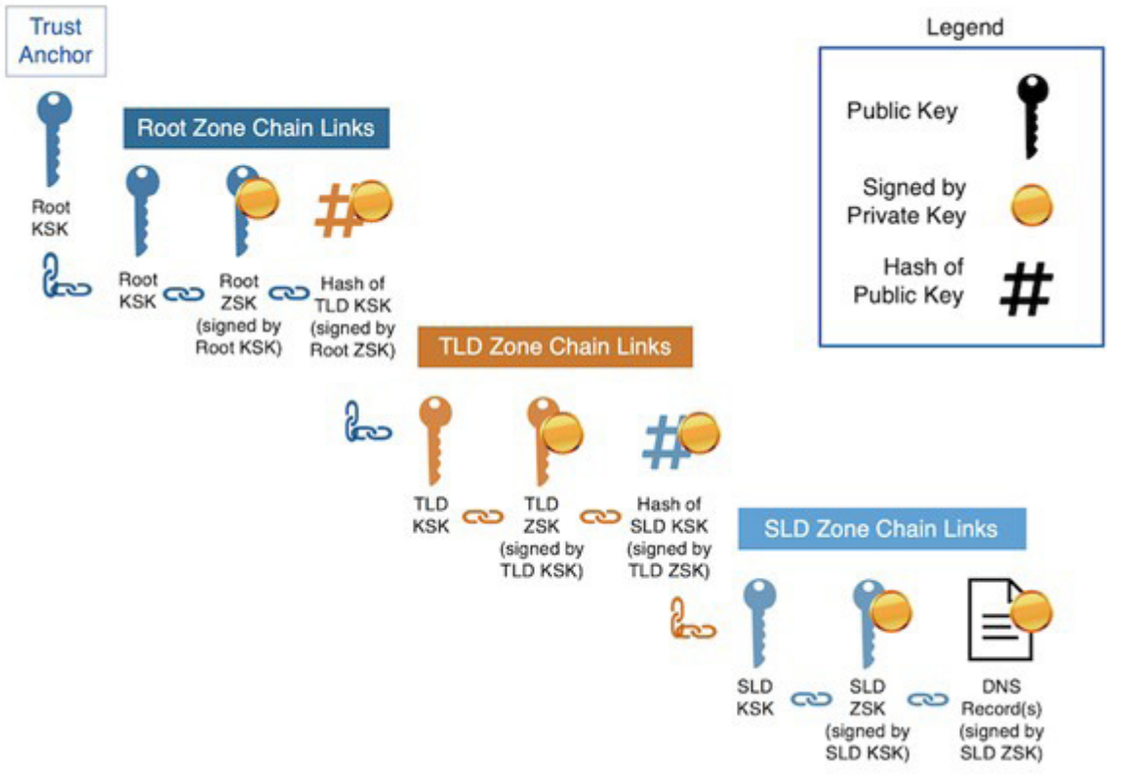

Figure 6. *Domain security ecosystem*

Table 2. *Unified vulnerability-mitigation-stakeholder matrix*

Vulnerability class	**Primary impact**	**Key mitigation measures**	**Responsible stakeholders**
Dangling DNS records and abandoned dependencies	Subdomain takeover, trust abuse	Continuous DNS inventory; lifecycle governance, automated dangling-record detection	Domain owners, cloud providers
Registrar and DNS provider Control plane weaknesses	Full domain hijacking	MFA, registry lock, role separation, and delegation audits	Registrars, DNS providers, domain owners
DNSSEC validation denial of service	Resolution unavailability	Resolver patching, validation complexity limits, and load distribution	Resolver operators, software vendors
Resolver cache poisoning	Traffic redirection, integrity loss	Strong randomness, DNSSEC, and cache integrity monitoring	Resolver operators

IDN homograph abuse	User deception, phishing	Script restriction, punycode display, and confusable-domain monitoring	Registries, brand owners
TLS certificate mis-issuance	Trusted impersonation	Certificate transparency monitoring, controlled DNS validation	Domain owners, Competent Authorities
Email authentication misconfiguration	Domain spoofing, phishing	Strict DMARC enforcement, SPF/DKIM alignment	Domain owners, mail providers
DNS zone transfer exposure	Reconnaissance enablement	AXFR/IXFR restriction, configuration audits	DNS operators
DNS amplification and DDoS	Domain unavailability	Anycast deployment, rate limiting, upstream mitigation	DNS operators, ISPs

This matrix shows that no single stakeholder can fully mitigate domain risk in isolation, supporting the need for coordinated ecosystem level security practices.

CONCLUSIONS AND FUTURE WORK

This study did the analysis for the security of Internet domain names through an examination of vulnerabilities observed between 2022 and 2025, underlining a clear attacker behaviour's evolution and failure conditions. Rather than exploiting DNS protocol mechanics alone, adversaries increasingly targeted administrative control planes, lifecycle inconsistencies and trust dependencies that develop from the central role of domains in the digital ecosystem.

The results show that domain vulnerabilities are structural and persistent, but also influenced by growing infrastructure complexity, decentralized ownership and uneven governance practices across registrars, DNS providers and cloud platforms. High impact incidents are frequently resulted from the interaction of multiple weaknesses, for example the lifecycle drift combined with weak Control plane security, rather than from isolated technical flaws.

The analysis of mitigation strategies is confirming that effective domain security requires integrated, multi layered defences, putting together technical hardening with continuous monitoring, governance enforcement and cross-organizational coordination. In 2026, the domain security needs to be understood as a resilience problem spanning DNS, TLS, email and cloud service ecosystems.

Implications for domain security in 2026

Looking forward, several implications emerge. First, automation and scale will continue to favour attackers unless defenders adopt likewise automated governance and monitoring mechanisms for DNS and domain assets.

Second, shared infrastructure risk especially at recursive resolvers and authoritative DNS providers will remain an important concern, intensifying the impact of software vulnerabilities and misconfigurations.

Third, identity centric attacks that exploit domain infrastructures (certificates, email, visually deceptive names) are likely to escalate, requiring closer integration between domain security and broader digital identity frameworks.

Implications for domain security in 2026

Future work should focus on:

- Quantitative measurement of DNS lifecycle drift and its correlation with compromise probability

- Detection of anomalous delegation and certificate issuance patterns assisted by machine learning
- Evaluation of registry and registrar level policy interventions on abuse reduction
- Cross-layer simulation of propagating failures involving DNS, TLS and email infrastructure

These types of research directions can support evidence based policy and technical improvements, contributing to a better resilient domain ecosystem.

In conclusion, securing Internet domains in 2026 requires moving beyond reactive patching toward continuous, ecosystem aware governance. By integrating vulnerability analysis with structured mitigation strategies and stakeholder accountability, this work is contributing to strengthening the foundations of trust upon which the modern Internet depends.

REFERENCE LIST

Agerpres (2022) *DNSC: Atacurile cibernetice produse vineri în România revend*icate de Killnet. Available at: https://agerpres.ro/economic/2022/04/29/dnsc-atacurile-cibernetice-produse-vineri-in-romania-revendicate-de-gruparea-killnet--909733 [Accessed: 23rd January 2026]

Agerpres (2025a) *Cyberfraud in Romania up over 40% in 2024, malware attacks up 286.8% - report.* Available at: https://agerpres.ro/english/2025/08/27/cyberfraud-in-romania-up-over-40pct-in-2024-malware-attacks-up-286-8pct-official-report--1478992[Accessed: 23rd January 2026]

Agerpres (2025b) *DNSC avertizează asupra unor tentative de phishing asupra utilizatorilor din România.* Available at: https://agerpres.ro/economic/2025/12/11/dnsc-avertizeaza-asupra-unor-tentative-de-phishing-asupra-utilizatorilor-din-romania-ai-platformei-t--1511123 [Accessed: 23rd January 2026]

Banciu, D., Petre, I., Dumitrache, M. (2019) Electronic system for assessing and analysing digital competences in the context of Knowledge Society, *ECAI 2019 – International Conference – 11th Edition, Electronics, Computers and Artificial Intelligence, Pitești, România, 27–29 June.* Vol. 11(1), ISBN 978-1-7281-1624-2.

CECCAR Business Magazine (2025) *Raport DNSC: Fraudele informatice au crescut în România cu peste 40% în 2024, atacurile malware majorare cu 286.8%.* https://www.ceccarbusinessmagazine.ro/raport-dnsc-fraudele-informatice-au-crescut-in-romania-cu-peste-40-in-2024-atacurile-malware-majorare-cu-2868/a/MTmKnyloHRUQemOjrJSY [Accessed: 27th January 2026]

Cheng, Y., et al. (2022) Evaluating the Effectiveness of Handling Abusive Domain Reports in the DNS Ecosystem. *Electronics*, 11(8), 1172.

De Bernardi, G., et al. (2025) Rule-Based eXplainable Autoencoder for DNS Tunneling Detection. *Computers*, 14(9), 375.

DNSC. (2024) Raport anual de activitate 2024. https://www.dnsc.ro/vezi/document/dnsc-raport-anual-2024.

Dumitrache, M., Rotună, C.I., Gheorghiță, A., Vevera, A.V., Sandu, I. și Smada, D. (2024) A domain reputation system architecture description using TOGAF, *Studies in Informatics and Control*, 33(1), pp. 61–72.

European Commission (2024) NIS2 Directive: cybersecurity standards for critical sectors in the EU. Available at: https://digital-strategy.ec.europa.eu/ro/policies/nis2-directive [Accessed: 23rd January 2026]

Gheorghiță, C.-A., Smada, D., Vevera, A.-V., Dumitrache, M., Sandu, I.-E. și Rotună, C.-I. (2023) Listele negre și listele albe în cadrul unui sistem de reputație a domeniilor, *Revista Română de Informatică și Automatică* (Romanian Journal of Information Technology and Automatic Control), 33(4), pp. 33–46.

Herzberg, A., Shulman, H. and Waidner, M. (2024) DNS Security: From DNSSEC to Modern Threats. *IEEE Security & Privacy*, 22(1), pp. 45-53.

ICANN Generic Names Supporting Organization(GNSO) (2025). Available at: https://gnso.icann.org

ICANN SAC. (2025) *SAC127: DNS Blocking Revisited, 16 May*. Available at: ICANN SSAC reports (PDF). https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac127-dns-blocking-revisited-16-05-2025-en.pdf

ICANN. (2024) CANN's Enforcement of DNS Abuse Mitigation Requirements, 8 November. *ICANN announcements.* https://www.icann.org/en/announcements/details/new-report-icanns-enforcement-of-dns-abuse-mitigation-requirements-08-11-2024-en

ICANN. (2025) *DNS Abuse Mitigation Program.* https://www.icann.org/dnsabuse

ICANN. (2025) *ICANN's Progress and Next Steps in Enforcing DNS Abuse Mitigation Requirements, 20 October*. https://www.icann.org/en/blogs/details/icanns-progress-and-next-steps-in-enforcing-dns-abuse-mitigation-requirements-20-10-2025-en

INCIBE-CERT (2024) *CVE-2023-50387 (KeyTrap) vulnerability note.* https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2023-50387

Kshetri, N. and Voas, J. (2023) Supply Chain Cybersecurity and Risk, *Journal of Cybersecurity.* [Accessed: 28th January 2026]

Kuerbis, B. and Mueller, M. (2023) Governance, Security and Stability of the Domain Name System. *Telecommunications Policy*, 47(2), 102465.

Liu, Y., Li, Z. and Chen, X. (2024) Automated Abuse of Internet Infrastructure: DNS and Domain-Based Attacks. *Computers & Security,* 131, 103270.

Moure-Garrido, M., et al. (2024) Reducing DNS Traffic to Enhance Home IoT Device Privacy. *Sensors*, 24(9), 2690.

NIST (2024) *NVD: CVE-2023-50387 Detail.* Available at: National Vulnerability Database. https://nvd.nist.gov/vuln/detail/cve-2023-50387

Nosyk, Y. (2025) Day in the Life of RIPE Atlas: Operational Insights and Applications in Network Measurements (PDF). arXiv:2511.22474v1 [cs.NI] 27 Nov 2025. https://arxiv.org/pdf/2511.22474 [Accessed: 15th January 2026]

Portal Legislativ (2024) *Ordonanța de Urgență 155/2024 privind securitatea cibernetică.* https://legislatie.just.ro/public/DetaliiDocument/293121 [Accessed: 23rd January 2026]

RIPE NCC (2024a) *RIPE-823: DNS Resolver Recommendations, 1 May.* Available at: RIPE NCC publications. https://www.ripe.net/publications/docs/ripe-823

RIPE NCC (2024b) *DNS Measurements with RIPE Atlas (PDF)*. Available at: RIPE NCC documents. https://www.ripe.net/media/documents/DNS-Measurements-with-RIPE-Atlas.pdf [Accessed: 16 January 2026]

Rotună, C. I., Sacală, I. Ș., & Alexandru, A. (2025). Towards Proactive Domain Name Security: An Adaptive System for .ro domains Reputation Analysis. *Future Internet*, 17(10), 478. doi: 10.3390/fi17100478.

Rotună, C., Cohl, A., Sandu, I. și Dumitrache, M. (2019) Noi tendințe în predicția liniară a evenimentelor, *Revista Română de Informatică și Automatică (Romanian Journal of Information Technology and Automatic Control)*, 29(3), pp. 19–30.

Shet, A. and Alsmadi, I. (2025) An empirical analysis of zero-day vulnerabilities disclosed by the Zero Day Initiative. *arXiv.* https://arxiv.org/abs/2512.15803 [Accessed: 23rd January 2026]

Shulman, H. (2023) The Security of the Domain Name System. *ACM Computing Surveys*, 55(6), pp. 1-36.

Smada, D., Dumitrache, M., Rotună, C.-I. și Gheorghiță, C.-A. (2024) 'Impactul statusului numelor de domenii internet asupra reputației acestora', *Revista Română de Informatică și Automatică (Romanian Journal of Information Technology and Automatic Control)*, 34(1), pp. 31–44.

Talabani, H. S., Abdul, Z. K., & Mohammed Saleh, H. M. (2025). DNS over HTTPS Tunneling Detection System Based on Selected Features via Ant Colony Optimization. *Future Internet,* 17(5), 211. doi: 10.3390/fi17050211.

Thiyagarajan, G., Bist, V. and Nayak, P. (2025) The hidden dangers of outdated software: a cybersecurity perspective. *arxiv.* https://arxiv.org/abs/2505.13922 [Accessed: 23rd January 2026]

Yu, H., Yuchi, X., Yang, X., Li, H., Yang, X., & Wang, W. (2025). DNS-Sensor: A Sensor-Driven Architecture for Real-Time DNS Cache Poisoning Detection and Mitigation. *Sensors,* 25(22), 6884. https://doi.org/10.3390/s25226884.

Zhai, Y., et al. (2023) BadDGA: Backdoor Attack on LSTM-Based Domain Generation Algorithm Detection, *Electronics,* 12(3), 736.