Authentic Web

Enterprise Domain Management for the New TLD Era

External DNS Attack Surface Compromises and Insights

This briefing paper provides context and evidence-based research on the material risks that medium and large enterprises face when proactive DNS security controls are not prioritized.

"DNS trust relationships frequently outlive infrastructure lifecycle management. Now, with automated AI-driven discovery and exploitability at scale, addressing DNS attack surface gaps has become urgent."

Peter LaMantia, CEO, Authentic Web Inc.

The purpose is to inform information security, infrastructure, and compliance executives. The extent of material reliance on, and the depth of, external DNS is often not fully understood, even by technically strong leaders.

This paper is designed to help them understand the broad reach and use of DNS by threat actors, a foundational upstream dependency leveraged in many modern attack chains. It is intended to provide senior leadership with the background needed to play their role to ensure the enterprise adopts a proactive DNS security posture that will materially reduce exposures and resulting compromises.

Contents

1.855.436.8853 | info@authenticweb.com

1 Executive Summary Takeaways and Recommendations

Enterprises are increasingly exposed due to fragmented DNS governance, incomplete visibility, and insufficient DNS hygiene controls. DNS hygiene refers to the operational practices used to inventory, validate, secure, monitor, and retire domains, DNS records, delegations, cloud references, and trust relationships throughout their lifecycle. Effective programs use centralized monitoring and a unified change-control model to identify exposures, remediate issues, and measure posture over time.

External DNS attacks are not theoretical.

→ Surveys show most organizations experienced DNS-related attacks with significant financial impact.
→ Customer-facing outages can lead to multi-million-dollar losses.
→ Phishing and credential attacks exploits in domain impersonation or weak email authentication remain among the costliest enterprise breach vectors.
→ Brand trust erosion and downstream customer compromise are recurring outcomes.

How to know if your enterprise has DNS exposures?

These questions indicate DNS governance maturity.

× Does the company have clear governance and oversight (GRC) over domains and DNS?
× Does any team have full visibility and change control across the entire external DNS attack surface?
× Do you monitor DNS vulnerabilities across all domains, including brand protection and parked domains?
× Do you utilize multiple registrars and DNS providers without centralized visibility and control?
× Is least-privilege access enforced with full auditability?
× After M&A, has domain and DNS consolidation been executed?
× Does the company rely on retail/SMB-grade registrars with high social-engineering exposure?
× Are DNS controls part of cybersecurity, infrastructure, and compliance programs?

Recommendations

Establish a proactive DNS security posture to reduce operational risk, incident exposure and reputation harm.

1. Prioritize external DNS attack surface governance in cybersecurity programs.
2. Consolidate domains/DNS to an enterprise-grade provider with visibility, vulnerability detection, and a unified change-control plane
3. Establish reporting cadence to maintain DNS security posture maturity.

1.855.436.8853 | info@authenticweb.com

2 Hidden DNS Risk Exposure: The Attribution Mirage

Many DNS-related compromises are misattributed to downstream systems. The incidents referenced in this paper have been DNS-attributed and represent a small sample of publicly disclosed events. Many more incidents involve DNS as a root cause but are never attributed to it.

Here is why. DNS is an enabler of attacks, not the system identified in the final incident report. Attackers exploit DNS hygiene gaps such as orphaned subdomains, dangling CNAMEs, forgotten cloud resources, and incomplete SPF/DMARC coverage. These create hidden trust paths enabling phishing, malware delivery, and credential harvesting. As a result, incidents often appear as application, cloud, or identity failures, masking DNS as the initiating exposure point.

This **Attribution Mirage** materially limits prevention. If proper DNS hygiene and lifecycle controls were in place, the exposed endpoint or trust relationship would likely have been reduced or eliminated. Since DNS underpins public-facing services, DNS hygiene must be addressed as a foundational component of attack surface management, security governance, and digital identity protection, not merely an operational networking function.

The Attribution Mirage

Attackers use DNS for:	The breach is then attributed as:
Reconnaissance	An email compromise
Infrastructure discovery	Cloud compromise
Phishing domain impersonation	SaaS breach
Command-and-control routing	Web application vulnerability, or
Subdomain takeover, and TLS trust exploitation	Identity compromise

DNS operates upstream of many traditional security visibility controls, including those focused on endpoints, applications, IAM, SIEM telemetry, and network traffic.

Here are some examples of how DNS issues are often misclassified in postmortems.

1. A Dangling CNAME takeover, categorized as a “cloud infrastructure/application compromise.”
2. SPF and DMARC gaps, categorized as “email fraud.”
3. Malicious redirect through abandoned infrastructure, categorized as a “web application vulnerability.”

The Reality: DNS governance and lifecycle weaknesses materially contributed to the compromise.

1.855.436.8853 | info@authenticweb.com

3 Real-world External DNS/Domain Compromise Incidents

These cases demonstrate that DNS trust failures are actively exploited across sectors and often do not require compromising internal infrastructure.

Brazilian Bank DNS Hijack (Full Digital Takeover)

ATTACK TYPE

Large-scale DNS hijacking + phishing

WHAT HAPPENED

Attackers altered DNS for 36 domains, redirecting to fake banking sites

IMPACT

- × Full interception of customer logins, cards, and credentials
- × Entire online banking presence hijacked for ~5 hours
- × Attackers served valid HTTPS, increasing user trust in the fraudulent site
- × Financial theft and fraud exposure (exact losses publicly undisclosed)
- × Significant reputational and customer trust impact (credentials to attacker infrastructure)
- × Regulatory exposure (banking sector)

Source: Wired

“Sea Turtle” Campaign (Nation-State DNS Hijacking)

ATTACK TYPE

Registrar and DNS infrastructure hijacking

TARGETS

40 organizations, including ISPs, government and registrars

IMPACT

- × Interception of sensitive communications: Email + web traffic
- × Long-term espionage and credential theft
- × Demonstrated systemic registrar/provider compromise risk

STRATEGIC INSIGHT

DNS infrastructure and registrars are a key part of the supply chain attack surface.

Source: Wired / Cisco

1.855.436.8853 | info@authenticweb.com

MyEtherWallet

ATTACK TYPE

BGP/DNS hijack combined with phishing

WHAT HAPPENED

Users were redirected to a fake wallet site

IMPACT

- × ~$150,000 stolen directly from users
- × Severe trust damage in crypto ecosystem
- × Immediate ecosystem-wide trust impact

Source: Indusface

“Sitting Ducks” DNS Vulnerability

ATTACK TYPE

DNS misconfiguration exploitation due to DNS delegation weakness

WHAT HAPPENED

According to research, 30,000+ hijacked domains, many from large companies.

IMPACT

- × Domains reused for scams and malware

Source: CSO Online

Microsoft Subdomain Takeover Exposure Research

(Not an exploitation)

ATTACK TYPE

Dangling DNS / subdomain takeover exposure

WHAT HAPPENED

Researchers identified hundreds of Microsoft-owned subdomains as vulnerable because of dangling DNS records that point to decommissioned resources.

IMPACT

- × Potential phishing from trusted Microsoft subdomains
- × Malware hosting under trusted Microsoft domains
- × Credential harvesting risk
- × Abuse of browser and enterprise trust relationships
- × Affected properties of: microsoft.com, skype.com, windows.com, visualstudio.com

STRATEGIC INSIGHT

Researchers identified hundreds of Microsoft-owned subdomains as vulnerable because of dangling DNS records that point to decommissioned resources.

Source: Sophos / Security Affairs / Microsoft Guidance

1.855.436.8853 | info@authenticweb.com

GoDaddy Dormant DNS Delegation Exploitation

ATTACK TYPE

Orphaned or Lame Delegation

WHAT HAPPENED

→ Attackers reportedly exploited dormant domains still delegated to GoDaddy nameservers
→ Domains reportedly lacked properly maintained authoritative DNS configurations, including unresolved or incomplete zone configurations
→ Weak DNS provisioning allowed malicious entries on delegated but unmaintained domains

IMPACT

× Included compromises for many companies including Mozilla, Expedia, Yelp and many more
× Hijacked trusted domains used for spam and malware campaigns
× Abuse of legitimate enterprise domain reputation
× Phishing and malicious redirect infrastructure using established domains
× Email trust exploitation and reputational damage

STRATEGIC INSIGHT

This incident demonstrated how orphaned DNS or LAME delegations and incomplete lifecycle governance can create exploitable trust relationships without directly compromising enterprise infrastructure. This also stresses the importance of the domain owners, to ensure their own DNS hygiene visibility and controls.

Source: Ars Technica, Spamhaus

Hazy Hawk Dangling DNS Campaign

ATTACK TYPE

Dangling DNS / abandoned cloud resource takeover

WHAT HAPPENED

→ Threat actors exploited dangling DNS records tied to abandoned cloud infrastructure
→ Trusted subdomains of major organizations were hijacked and repurposed for malware and scams
→ Attackers abused forgotten CNAMEs to cloud resources no longer controlled by the organization
→ Affected organizations reportedly included: Panasonic, Bose, CDC, Deloitte

IMPACT

× Malware distribution from legitimate enterprise subdomains
× Browser trust exploitation
× Scam delivery through trusted enterprise infrastructure
× Persistent phishing and malicious redirect capability

STRATEGIC INSIGHT

Demonstrates how DNS lifecycle gaps create exploitable trust relationships without compromising enterprise networks.

Source: TechRadar / Infoblox / SecurityWeek

1.855.436.8853 | info@authenticweb.com

Azure DevOps Subdomain Takeover

ATTACK TYPE

Dangling DNS / cloud service takeover

WHAT HAPPENED

→ Researchers demonstrated takeover of abandoned Azure DevOps-linked subdomains
→ DNS records continued pointing to decommissioned cloud resources
→ Attackers could potentially abuse the trusted subdomain relationship for phishing or account compromise workflows

IMPACT

× Potential credential theft
× Abuse of trusted Microsoft infrastructure relationships
× Potential downstream compromise of CI/CD and DevOps trust chains

STRATEGIC INSIGHT

Highlights the operational risk when DNS records outlive the lifecycle of cloud apps and DevOps infrastructure.

Source: Binary Security

Windows Live Tiles Azure Takeover

(Research PoC Report - Not an exploitation)

ATTACK TYPE

Dangling DNS / cloud resource hijack

WHAT HAPPENED

→ A researcher demonstrated the takeover of a Microsoft-owned Windows Live Tiles subdomain through an Azure cloud service weakness
→ The attack leveraged DNS references to unclaimed cloud infrastructure

IMPACT

× Ability to serve attacker-controlled content from a trusted Microsoft property
× Potential phishing and malware delivery risk
× Abuse of trusted Microsoft branding and browser trust

STRATEGIC INSIGHT

Demonstrated how cloud resource lifecycle failures combined with DNS trust relationships can create enterprise exposure without direct infrastructure compromise.

Source: The Hacker News

1.855.436.8853 | info@authenticweb.com

4 What These Cases Prove

1. This is happening to mature, sophisticated Tier-1 brands

→Brazilian Bank
→Microsoft, Mozilla, Expedia, Yelp
→Deloitte / PwC / EY / CDC / Panasonic / Bose
→Additional enterprise domains were reportedly affected across these campaigns

Even highly mature organizations accumulate DNS lifecycle gaps that expose trusted domains and subdomains.

2. Many DNS attacks do not require compromise of infrastructure or applications

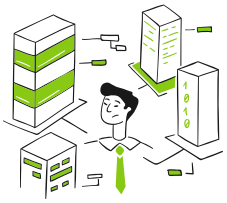
Key recurring root causes include:

→Orphaned DNS records
→Missing DNS security records such as SPF/DMARC
→Registrar and DNS provider exposure
→Lack of monitoring, visibility and controls
→Unmanaged third-party or supply chain dependencies
→DNS is the foundational trust and routing layer for digital identity and external communications

3. Brand trust and reputational impacts

Across these real incidents, brand trust was degraded.

→Customers gave credentials to attackers
→Malware distributed under trusted domains
→Global reputational exposure
→Direct financial theft (crypto, banking)



4. DNS is upstream of most enterprise program systems:

DNS manipulation routes users to attacker infrastructure before IAM, EDR, WAF, or Zero Trust controls activate. DNS governance should be treated as a foundational layer of external attack surface management, supply chain risk management, and digital identity assurance.

1.855.436.8853 | info@authenticweb.com

5 Why DNS Governance Gaps Persist in Large Enterprises

Enterprises do not intentionally neglect DNS security. The problem is structural. These sophisticated modern organizations accumulate DNS risk over time through the weight of complexity.

That complexity includes:

- × Merger and acquisition activity
- × Cloud migrations
- × Decentralized SaaS adoption
- × Shadow IT
- × Multiple registrars and DNS providers
- × Legacy applications
- × Expired projects and abandoned infrastructure
- × Siloed operations and systems
- × No centralized DNS visibility and control plane across the enterprise
- × External agencies and vendors

Over time, DNS sprawl accumulates across the enterprise.

→ DNS records outlive applications
→ Delegations outlive ownership
→ Cloud resources are retired without DNS cleanup
→ Subdomains remain trusted long after operational oversight
→ DNS records are added freely and rarely removed
→ Knowledge loss through team turnover

Siloed ownership and tooling prevent unified DNS visibility.

→ No single team owns the entire external DNS attack surface
→ DNS visibility is fragmented across infrastructure, networking, cloud, security, and application teams
→ Security tooling focuses primarily on endpoints, identities, applications, and internal telemetry rather than external DNS trust relationships
→ External DNS is considered infrastructure only, rather than an attack surface
→ Internal teams do not universally understand the risks that exist on the external DNS
→ Domain/DNS management is viewed as overhead rather than strategic security infrastructure

As a result, organizations accumulate unmanaged risk across the external DNS attack surface, including:

→ Orphaned DNS records and Dangling CNAMEs
→ Lame Delegations
→ Insecure trust relationships (e.g., HTTP-only transport or weak TLS trust configurations)
→ Expired Cloud resource connections
→ Weak registrar and DNS change controls
→ Incomplete email authentication and reporting (SPF/DMARC)

This is why organizations with mature security programs are exposed to hidden DNS-enabled compromises.

1.855.436.8853 | info@authenticweb.com

6 Closing Insights, Summary and Statement

Insights

These cases demonstrate that compromise paths can originate upstream of applications and downstream security controls through DNS, registrar, or infrastructure trust weaknesses. As enterprises become increasingly dependent on cloud services, SaaS platforms, and digital identity trust relationships, DNS governance is becoming a material concern for operational resilience and compliance. In these cases, attackers exploited DNS trust paths, registrar exposure, or lifecycle failures upstream of the application layer.

Organizations lacking the following capabilities face material DNS-enabled risk:

→ Complete domain + DNS inventory
→ Verified ownership and change-control
→ Automated detection of orphaned/dangling assets
→ Continuous DNS/web monitoring
→ Enforced DNS lifecycle policy

Without these controls, attackers can compromise your brand identity without accessing internal systems.

DNS is the very foundation of your brand's digital identity. When you implement mature DNS hygiene practices to establish a proactive DNS security posture, your external attack surface risk is materially reduced.

Summary

DNS is the enterprise's public identity layer, yet remains one of the least governed and least visible parts of the attack surface. Organizations that lack ...

→ Centralized governance
→ Lifecycle management
→ Visibility and controls
→ Continuous security monitoring

... face materially increased external attack surface exposure.

Organizations that do implement these capabilities can materially reduce DNS-related exposure risk.

Closing Statement

As regulators, insurers, and enterprise customers increasingly evaluate operational resilience and third-party security governance, unmanaged DNS attack surface exposure is becoming a material concern for governance and accountability.

Enterprises need to prioritize external DNS attack surface management by implementing centralized visibility, control-plane systems, and lifecycle management practices to achieve a mature DNS security posture.

1.855.436.8853 | info@authenticweb.com

Appendix

Domain Hijacking and Registrar Compromise
(Enterprise Risk)

Board Domain Hijacking via Social Engineering at registrars through large call center operations

Outcomes and Impacts

- × Domain transfers and ownership
- × DNS record modification
- × Email interception (MX changes)
- × Phishing hosted on a legitimate domain
- × Financial loss + regulatory exposure

Dangling DNS / Subdomain Takeover
(Orphaned Assets)

Abandoned SaaS /cloud resources taken over to serve malicious content under a trusted domain

Outcomes and Impacts

- × Phishing on legitimate subdomains
- × Malware hosting under trusted brands
- × Trust exploitation at scale

Email Interception via DNS
(MX Manipulation)

Attackers modify MX records
→ receive corporate email

Outcomes and Impacts

- × BEC fraud
- × Invoice redirection
- × Insider impersonation

Third-Party DNS / Registrar Compromise Risk

Domain and DNS compromise increasingly involve vendors, SaaS providers, registrars, or DNS providers

Outcomes and Impacts

- × Traffic redirection
- × Credential harvesting
- × Supply chain compromise
- × Long-term brand erosion

Man-in-the-Middle via DNS Control

DNS hijack → traffic interception without direct compromise of the application layer.

Outcomes and Impacts

- × Credential harvesting
- × Session hijacking
- × SSL certificate abuse (as seen in bank case)

DNS-Enabled Phishing
(SPF/DMARC Failures)

Phishing via Domain Abuse, where SPF and DMARC records are not globally in place

Outcomes and Impacts

- × Spoofed email domains to enable phishing
- × Customer credential theft and/or malware infection
- × Business email compromise (BEC)
- × DNS misconfiguration to allow attacker-controlled mail routing
- × Average phishing-related breach cost: $4.76M (Source: IBM)
- × Drives majority of cyber insurance claims (billions total losses)
- × Long-term loss of brand trust in communications

1.855.436.8853 | info@authenticweb.com

Domain and DNS Compromises: Source References

NIST: Secure Domain Name System
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81r3.pdf

CISA DNS Security Guidance
https://www.cisa.gov/news-events/alerts/2021/03/04/joint-nsa-and-cisa-guidance-strengthening-cyber-defense-through-protective-dns

Microsoft
https://learn.microsoft.com/en-us/azure/security/fundamentals/subdomain-takeover

Cisco Talos Report
https://blog.talosintelligence.com/sea-turtle/

OWASP Subdomain Takeover
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/10-Test_for_Subdomain_Takeover

Infoblox Research
https://blogs.infoblox.com/threat-intelligence/sitting-ducks-domain-hijacking-technique

IBM
https://www.ibm.com/reports/data-breach?

KrebsonSecurity
https://krebsonsecurity.com/2019/01/bomb-threat-sextortion-spammers-abused-weakness-at-godaddy-com

SecurityScorecard
https://securityscorecard.com/blog/top-strategies-for-preventing-domain-hijacking/

ArsTechnica
https://arstechnica.com/information-technology/2019/01/godaddy-weakness-let-bomb-threat-scammers-hijack-thousands-of-big-name-domains

TechRadar
https://www.techradar.com/pro/security/criminals-hijacking-subdomains-of-popular-websites-such-as-bose-or-panasonic-to-infect-victims-with-malware-heres-how-to-stay-safe

CenterforCybersecurityPolicy
https://www.centerforcybersecuritypolicy.org/insights-and-research/what-is-dns---a-dns-security-primer

EfficientIP DNS Threat Reports
https://efficientip.com/resources/idc-global-dns-threat-report/

Atlassian
https://www.atlassian.com/incident-management/kpis/cost-of-downtime

Sophos
https://www.sophos.com/en-us/blog/researcher-finds-670-microsoft-subdomains-vulnerable-to-takeover

Security Affairs
https://securityaffairs.com/98981/hacking/microsoft-sub-domains-hijacking.html

The HackerNews
https://thehackernews.com/2025/06/why-dns-security-is-your-first-defense.html

Security Week
https://www.securityweek.com/dangling-dns-used-to-hijack-subdomains-of-major-organizations

Binary Security
https://www.binarysecurity.no/posts/2022/11/azure-devops-takeover

The HackerNews
https://thehackernews.com/2019/04/subdomain-microsoft-azure.html

Spamhaus
https://www.spamhaus.org/resource-hub/domain-reputation/the-current-state-of-domain-hijacking-and-a-specific-look-at-the-ongoing-issues-at-godaddy

AuthenticWeb: 4 Board Mandates
https://authenticweb.com/wp-content/uploads/2026/02/Whitepaper-2026-Board-Mandates_Proving-Digital-Identity-Control.pdf