Authentic Web

Empowering Teams for DNS Security, Compliance and Performance

A CISO Briefing

Why Your Enterprise Is Exposed on the External DNS?

What will happen if not addressed?

What are the Business and Customer Impacts?

What to prioritize and action?

Contents

"In every organization where we run our external DNS network audits, we uncover glaring deficiencies in DNS hygiene and security. These gaps expose the business and its customers to cyber risk. This condition coincides with increasing frequency of external DNS incidents. It's time for a CISO directive."

Peter LaMantia, CEO, Authentic Web Inc.

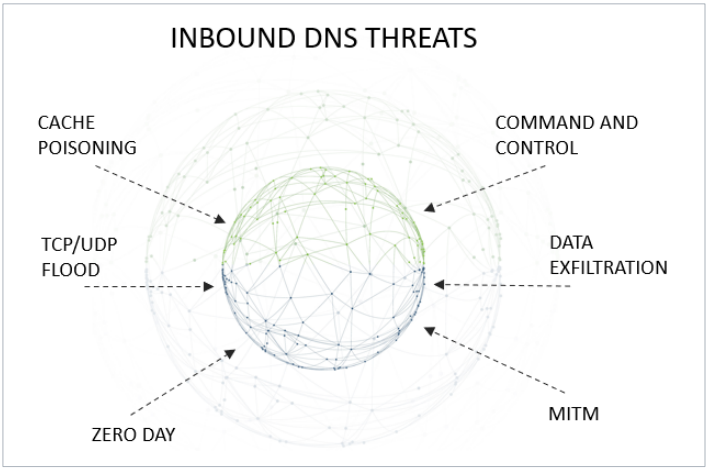
Introduction: DNS Threat Vectors

First let's clarify the focus of this brief. DNS threat vectors exist in two primary buckets.

1. INBOUND DNS THREATS TO INTERNAL NETWORKS

Threats related to inbound DNS traffic are designed to attack the business through data exfiltration, establish command and control, compromise systems or make DNS inoperable.

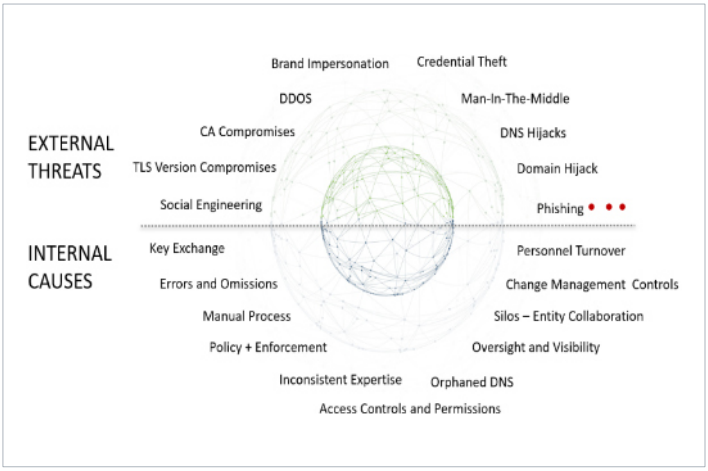
These threats can be addressed by various types of blocking and traffic analysis services to identify abnormal traffic patterns in the DNS and then prevent traffic from penetrating and compromising internal systems.



2. EXTERNAL DNS NETWORK THREATS and CAUSES

Threats related to an organization's external DNS network can include DNS hijacking, social engineering, or phishing as first strike vectors to execute any sequence of subsequent cybercrimes.

These threats exist due to management gaps in DNS system change controls and security policy enforcement. It persists due to a lack of visibility, controls, and automation to ensure DNS hygiene. These threats can be mitigated by service providers who provide control systems to empower IT to Get and Keep control.



In this brief, we discuss the external DNS Network threats and causes that will impact the enterprise, supporting third party research and a conclusion summary with a recommended CISO Directive to keep your company and customers safe.

WHY ENTERPRISES ARE EXPOSED | WHAT WILL HAPPEN | WHAT ARE THE IMPACTS

© 2022 Authentic Web Inc. All rights reserved.

1.855.436.8853 | info@authenticweb.com

Domain and External DNS Network Management Risk

Two factors over all others place the enterprise and its customers at risk.

1. LACK OF OWNERSHIP

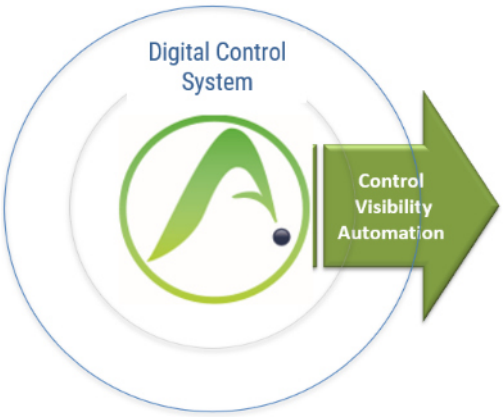
When domains and DNS zone files are ungoverned without end-to-end ownership and enforced security policies, you are likely exposed. Functional teams may all be stakeholders; however, domains and DNS are often managed in silos without clear oversight and ownership. Since the DNS underpins the entire digital footprint and service delivery network, it is critical to have clear ownership inside the organization.

WITHOUT CLEAR OWNERSHIP ...

- x Individuals put in no effort
- x Frustrate | Demotivate
- x Environment of blame
- x Increase business risk

2. LACK OF DIGITAL CONTROL SYSTEMS

Where domains and DNS zones are not managed under a centralized control system, your business is likely exposed. DNS network security exposure and change management compliance gaps are generally unaddressed. This is recognized by security experts as a material risk, necessitating action to Get and Keep control over the long-term.



Lack of clear internal ownership and digital control systems combine to represent a material risk to the enterprise.

At the same time, exploits targeting enterprise external DNS are escalating.

These threat vectors call for a CISO Directive to network & IT security leaders to prioritize external DNS security risk & change management

© 2022 Authentic Web Inc. All rights reserved.

1.855.436.8853 | info@authenticweb.com

Exposures: Why Your Enterprise is Exposed | What Will Happen

The exposures below are based on real-life DNS audit data Authentic Web has audited on large enterprise external DNS networks. To learn more about the audit findings, watch the webinar: Enterprise DNS Audit Results Revealed

WHY EXPOSED	WHAT WILL HAPPEN
Lack of clear internal ownership, governance, and digital control systems.	DIGITAL OUTAGE | BRAND IMPERSONATION RANSOMWARE | THEFT OF PERSONAL IDENTIFIABLE INFORMATION | CREDENTIAL THEFT | DDOS

Exposure Type	Why Your Enterprise is Exposed	What Will Happen
DNS Hijack aka Man-in-the-Middle (MITM)	**DNSSEC FAILURES / NOT ENABLED** DNSSEC records may exist however, compliance checks show very few or none of the DNSSEC records to be properly configured and hence, not functioning. Many companies fail to enable DNSSEC at all.	Without DNSSEC, domains can be hijacked with a DNS cache poisoning attack to redirect users to a malicious website. Multiple types of compromises can then be executed by the attacker. Malicious actors have proven the ability to redirect traffic through their servers, harvesting data, then passing traffic to the destination. Neither the enterprise nor the customer would know data is being harvested for use in subsequent attacks. A recent example is the Sea Turtle Attack.
Social Engineering	**MULTIPLE LIVE DNS SERVICES** Most enterprises have several live DNS services, largely due to a legacy of untended DNS accounts. Access permissions are unclear and visibility to change management controls are incomplete or absent. Without governance they are subject to takeover.	Ungoverned DNS accounts are vulnerable to social engineering exploits in which parties can take control of the DNS. Perpetrators can harvest data to further attack enterprise targets, customers and/or commit crimes. At Risk: → Customer Login Credentials → Internal Credentials, i.e., VPN → Customer Personal Identifiable Information (PII) → Ransomware

© 2022 Authentic Web Inc. All rights reserved.

1.855.436.8853 | info@authenticweb.com

Exposure Type	Why Your Enterprise is Exposed	What Will Happen
Phishing	**SPF AND DMARC IMPLEMENTATION** SPF and DMARC records are typically set on only a handful of domains. Without these security resource records your domains can be used against you for phishing. If you own it, you must manage and secure it.	Nefarious actors can send emails from a domain that is owned by your enterprise to a target list, or as a spear phish to an internally targeted individual. This tactic is effective since the phishing email appears to be authentic from an enterprise-owned domain. Phishing can result in any number of attack outcomes.
Session Compromise and MITM	**END-TO-END ENCRYPTION GAPS** Redirects are often not set with HTTPS on redirect servers. This is a common vulnerability. DNS audits typically show hundreds of insecure redirects, each representing an attack vector.	Malicious actors compromise a HTTPS session left open by HTTP only redirects. This permits session eavesdropping to harvest data or enable the ability to redirect (MITM) users to a malicious website. Additional implications include browser warnings which are becoming increasingly strict. This will negatively impact consumer trust. Lastly, SEO will be affected since search engines openly reward end-to-end HTTPS.
Dangling DNS	**ORPHANED DNS RECORDS** Subdomain ARecords and CNAMEs to host resources are set and forgotten over time. IT does not have adequate tools to ensure all endpoints provisioned on the DNS are known and governed by InfoSec defined security policies.	Dangling subdomains with A Records pointing to a cloud provider IP pose risk. Malicious actors target IP control by cycling through IPs until they gain service control over the orphaned IP. Similarly, bad actors hunt down dangling CNAMEs where the host destination resource is no longer live. Attackers can take control by setting up their own resource with the same name, set up a malicious site and carry out attacks. This is a particular risk if the CName destination name is in use by other enterprise services. A webinar on Dangling DNS can be watched here. The Zone File Mess

© 2022 Authentic Web Inc. All rights reserved.

1.855.436.8853 | info@authenticweb.com

Exposure Type	Why Your Enterprise is Exposed	What Will Happen
Internal Actor Malicious/Error	**CHANGE CONTROL GAPS** Lack of DNS network visibility and change management controls allows internal employees to make any change without oversight and governance.	**ANYTHING CAN BE DONE INTENTIONALLY OR IN ERROR!** Without change management, change history records, internal personnel can maliciously or inadvertently configure DNS to create security gaps
DNS Network Reconnaissance *DNS Hygiene*	**PUBLICLY VISIBLE VULNERABILITY MAP** The external DNS is insecure by design. It provides a globally accessible map for external parties to discover your network and vulnerabilities. Potential attackers can discover DNS security gaps and identify servers which may not be covered by InfoSec security policies and governance. Poor DNS hygiene exposes the fact that your organization may not have controls in place, thereby highlighting the organization as an attractive target.	Most cybersecurity incidents start with an external DNS scan by unauthorized parties. They use the DNS to map enterprise networks, inspect endpoints, and look for gaps in server software updates or configurations. Complicating matters, the digital attack surface continues to expand to the cloud. By leaving DNS ungoverned without control systems, you are exposing the lack of control to prospective attackers. Conversely, good DNS hygiene indicates that your organization is not an easy target.

© 2022 Authentic Web Inc. All rights reserved.

1.855.436.8853 | info@authenticweb.com

Business and Customer Impacts and Costs

DIGITAL OUTAGE | BRAND IMPERSONATION | RANSOMWARE | THEFT OF PERSONAL IDENTIFIABLE INFORMATION (RECORDS) | CREDENTIAL THEFT | DDOS

The full extent of a DNS network breach or compromise can be irreparably damaging and far-reaching to the enterprise. Fallout can impact budgets & costs, brand reputation, consumer trust, careers and livelihoods, team morale, and impact business plan execution. Common cost areas are summarized below.

- Calculate outage impact by the hour for business impact on revenue and/or service delivery interruptions.
- Costs to manage Client Services teams addressing customer needs during an incident.
- Costs to IT/Infrastructure/InfoSec managing the incident. Resolution | Containment | Productivity
- Postmortem responsibility and work effort required to prevent future incidents.
- Reactive vs Proactive: Cost are orders of magnitude higher in reactive postures. ie: Internal and Vendors
- Brand Damage: Consumer Trust: Impact to new customer acquisition, retention and upsell business goals.
- Brand Damage: Investor: Market value and outlook.
- Brand Damage: Partner: Reputational and deal conditions.
- Regulatory Consequences and Management Costs.

The cost of a cybersecurity incident can be far reaching beyond dollars and short-term quantifiable attribution.

AVERAGE COST OF A COMPROMISE (USD) IN 2021

IDC DNS THREAT REPORT (2021)

DIRECT DNS SPECIFICALLY / INCIDENT

$950,000

IBM COST OF A DATA BREACH (2021)

GLOBAL AVERAGE TOTAL COST OF A BREACH

$4,240,000

Other research reports show similar increasing probability and rising impacts and costs.

© 2022 Authentic Web Inc. All rights reserved.

1.855.436.8853 | info@authenticweb.com

DNS Security Research: Frequency and Business Impacts

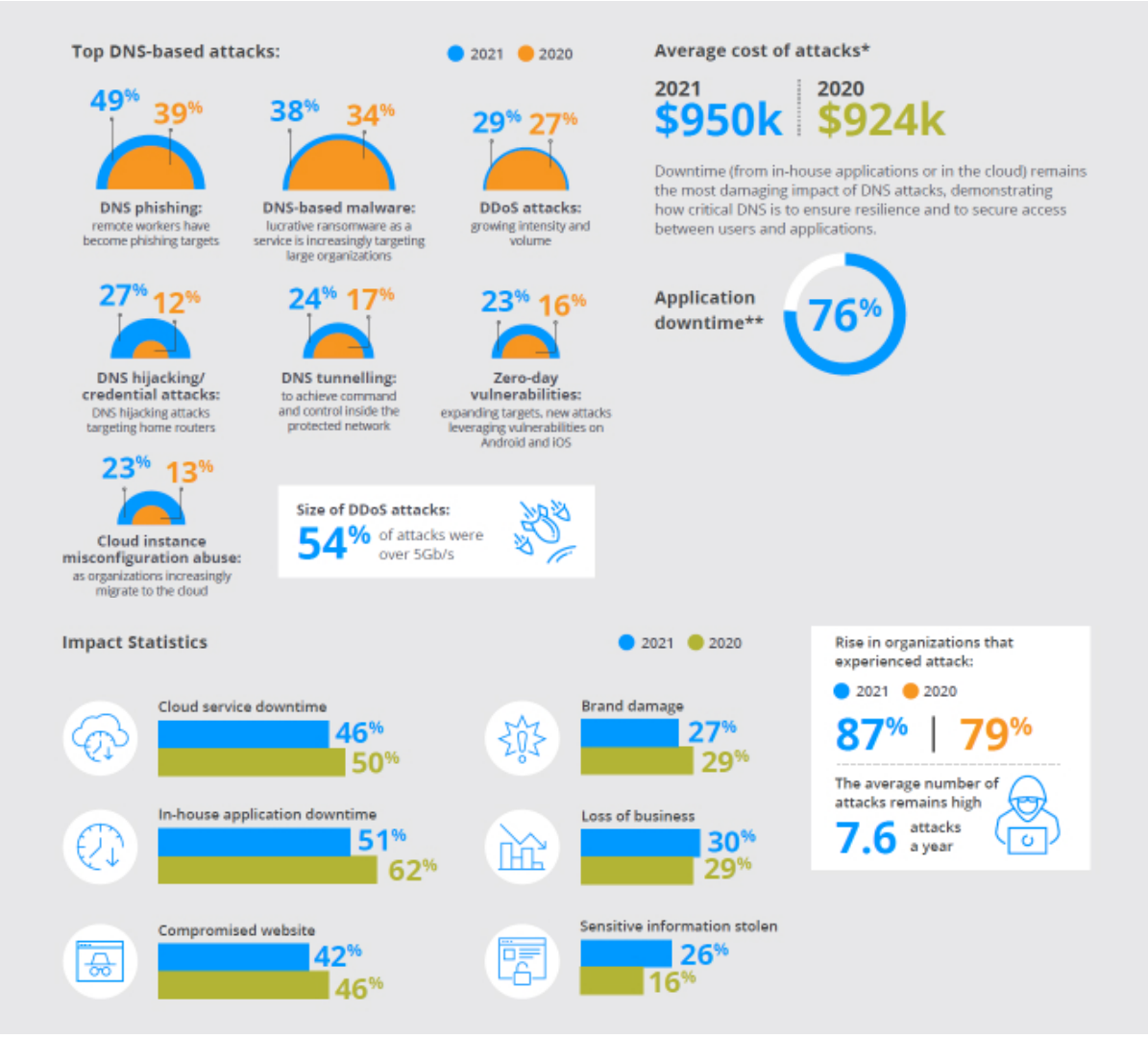
External DNS networks are becoming a more common attack vector. Recent industry research confirms this trend. Two key data points are raising the need to prioritize ownership and modernization of systems to Get and Keep control.

1. **FREQUENCY**: Increasing DNS Related Incidents
2. **COST**: Increasing Business Impacts

IDC 2021 Global DNS Threat Report (June 2021)

Source: https://www.efficientip.com/resources/idc-dns-threat-report-2021/

This is an excellent report with easy-to-understand data summaries showing the increasing frequency and cost of a DNS attack. It covers both inbound and external DNS network management threats. It is recommended reading for any practitioner working to improve security and any enterprise leader building a business case for modernization.



© 2022 Authentic Web Inc. All rights reserved.

1.855.436.8853 | info@authenticweb.com

Domain Security: A Critical Component of Enterprise Risk Management (June 2021)

Source: http://interisle.net/DomainSecurity2021.pdf

This report from Interisle Consulting Group describes in plain language the real risks that expose enterprise and best practices to address the exposure.

"Incidents and responses attract public attention, there is an overemphasis on attack response and underemphasis on pro-active, preventative measures to detect, identify, and mitigate threats before an attack can occur."

"Because cyber investigators actively look for malicious domain registration indicators such as look-alike domains, many attackers prefer to exploit legitimately registered domain names. ... the domain hijacking is an enabling attack."

DNS Hijacking | Enabling Attacks

Direct attacks against domain account holder	Possible consequences to domain holder	Direct attacks against others	Possible consequences to others
Mail redirection	Correspondence or sensitive data disclosure, transaction, or CEO fraud	Domain is used to distribute spam	Spam, malware distribution, phishing, or business email compromise (BEC)
Web server redirection	Disruption of online presence or merchant transactions	Redirection to fake sites, data leak, traffic interception, malicious content hosted	Phishing attack, Malware distribution, credential harvesting
Web site compromise	Reputational harm, Service disruption	Defacement, malicious content insertion, redirection	Loss of confidence in organization
Extortion or domain takeover	Financial loss, online presence disrupted, protracted dispute resolution		Supply chain disruption, necessary service disruption
Data, media, or streaming server redirection	Disruption or critical operations, passive surveillance, data disclosure, alteration, or destruction		Disclosure of personal data or activities

© 2022 Authentic Web Inc. All rights reserved.

1.855.436.8853 | info@authenticweb.com

CONCLUSION | THE CISO DIRECTIVE

A. Domains and External DNS networks are vulnerable to compromise. WHY?

- **OPERATING SILOS:** Lack of clear end-to-end functional team ownership inside the enterprise.
- **SYSTEM SILOS**: Lack of unified control system to enforce security policies and change management.

B. It is Extremely Hard for IT to Get and Keep Control

- **ACCOUNTABILITY:** Lack of clear ownership has left this area lacking in accountability.
- **LEGACY SYSTEMS:** Teams do not have modern systems to efficiently see the risk, much less address the risk.

C. Business impact and cost risk of legacy reactive postures are no longer an option

- **COST:** The cost of incidents to the enterprise continues to climb year over year.
- **PROBABILITY:** The probability of an incident approaches 100%. Not IF but WHEN.

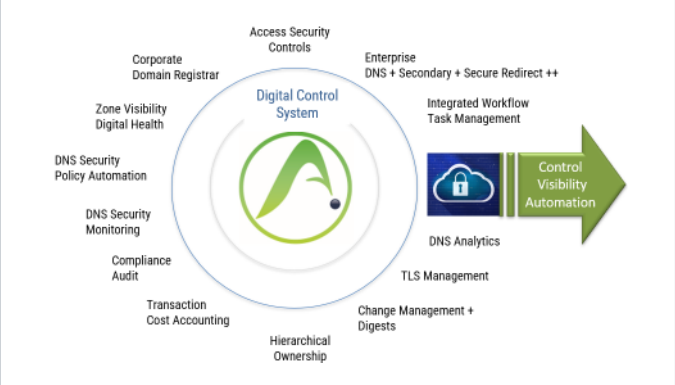
THE CISO DIRECTIVE >> GET PROACTIVE | PRIORITIZE ACTION

Assign ownership and prioritize systems modernization to empower teams

A Domain, External DNS, and TLS Control System

Authentic Web reengineered DNS management processes with systems solutions that empower Digital and IT teams with CONTROL, VISIBILITY, and AUTOMATION tools to improve SECURITY, COMPLIANCE, and PERFORMANCE.

- Mitigate Domain and DNS security risk to keep the company and customers safe.
- Ensure change management compliance controls over your digital footprint.
- Reduce Total Cost of Ownership managing Domains, DNS, and TLS Certificates.



Make it ***EASY*** for Your Teams and **Reduce Cost**

Learn more

Contact us to learn how easy DNS security can be with a control system to keep your brand secure and customers safe.

authenticweb.com

info@authenticweb.com | NA: 1-855-436-8853 | INT: +1-416-583-3770

©Authentic Web Inc. 2022. All rights reserved