How Can We Raise the Bar for DNS Administration?

Sean Thorne
Director Engineering, DNSi

DNS OARC 45 Stockholm
Oct 7/8

DNS Touches *Everything*

User experience

Services and applications

Brands

Web presence

Privacy

The Good

Phishing

Bot C&C

DDoS

Cache poisoning

Email fraud

Brand abuse

Authoritative compromise

Malware distribution

DGAs

The Bad

Availability · Trust · Security

DNS Configuration Matters More Than Ever

Operations has well defined practices. Long term management is evolving….

Investigating DNS Configuration

What

Evaluate the DNS security & certificate posture of **over 19,000 domains of financial institutions**

How

DNS Scanner

Continuous monitoring tool detecting CAA/SPF/DKIM/DMARC/Registry Lock, and many other DNS record types

Akamai's Global DNS Telemetry

Trillions of DNS Queries per day

Why

Illustrate **DNS security and certificate exposure**

Discuss importance of development and adherence to best practices that incorporates continuous monitoring, with automated guidance and enforcement

Key Findings

Inconsistent adoption across even high-profile financial brands

Misconfigured or partially configured records

Absence of DNS hygiene practices (e.g., stale zones, legacy entries)

Lack of tools in DNS Posture....

Email Lapses

😬 *ruh roh*

Email Spoofing Risk

52% of domains in the financial sector lack DKIM authentication, making them vulnerable to email spoofing attacks.

DMARC Visibility Gap

28% of financial domains do not have DMARC records configured, leaving them exposed to impersonation and brand abuse.

SPF Misconfigurations

11% of financial sector domains have missing or inadequate Sender Policy Framework (SPF) records, allowing for unauthorized email sending.

Phishing Threat Vector

Without strong email authentication controls, financial institutions face an increased risk of successful phishing campaigns targeting their customers and employees.

Email needs DNS....

Legacy Settings

😳 *ugh*

Registry Lock OFF in 25%

Unprotected domain registrations make it easy for attackers to hijack or transfer your critical domains.

93% missing CAA records

Lack of CAA increases the risk of unauthorized SSL/TLS certificate issuance.

5% Single Name Server

Relying on a single DNS nameserver introduces a single point of failure, increasing the risk of outages and downtime.

11% Wildcard DNS

Uncontrolled wildcard DNS configurations can lead to rogue subdomain takeovers and data leaks.

TLS needs DNS....

Akamai

Forgotten Records

come on

Real World Example…

A world class financial institution accidentally typo'd a CNAME record, leading to over 100,000 daily DNS queries being misdirected.

Invisible Attack Surface

The DNS misconfiguration went unnoticed for an extended period, leaving its systems and customer data exposed.

Costly Consequences

The DNS incident resulted in potential data leaks, compliance violations, and reputational damage, costing the bank significantly.

Welcome Mat for Attackers

The uncontrolled DNS entries created a prime opportunity for cybercriminals to exploit and launch further attacks against the bank.

The Internet needs DNS….

Akamai

DNS Administration is Difficult Today

Environmental Complexity

What was that company we acquired last year....

Expanding Threat Landscape

They did what???

Organization Silos & Ownership Confusion

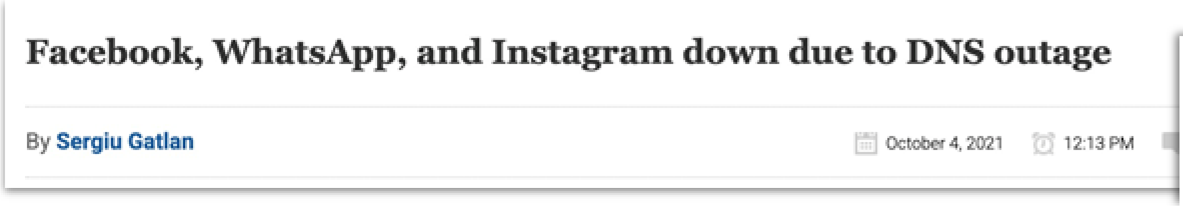
The marketing team said....

Lack of Visibility & Automation

I don't even know who built that thing...

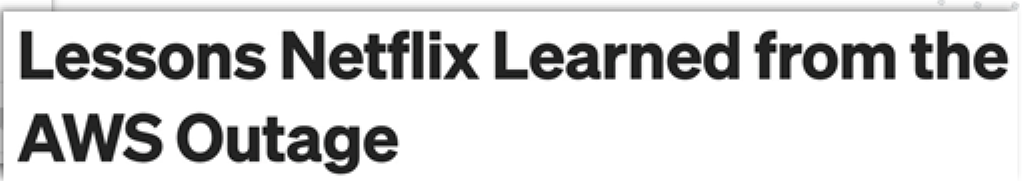
Akamai

Why Arbitrary or Inconsistent DNS Configuration Matters

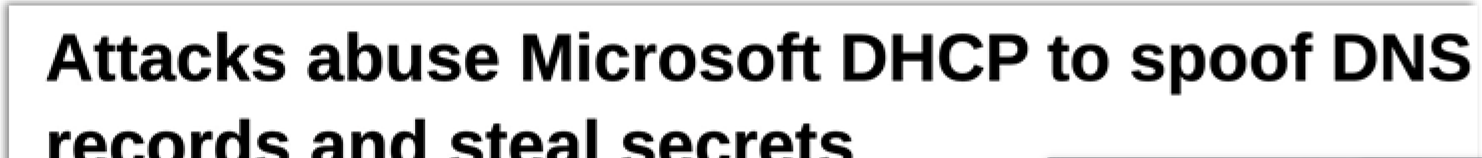


Facebook, WhatsApp, and Instagram down due to DNS outage

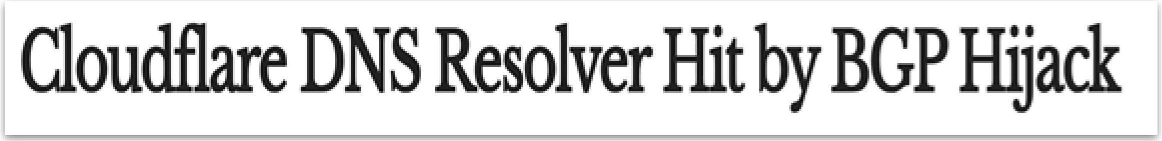
By Sergiu Gatlan October 4, 2021 12:13 PM



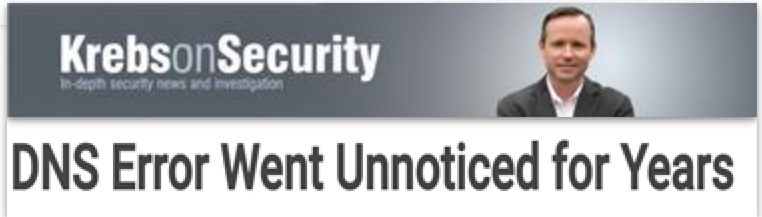
Lessons Netflix Learned from the AWS Outage



Attacks abuse Microsoft DHCP to spoof DNS records and steal secrets



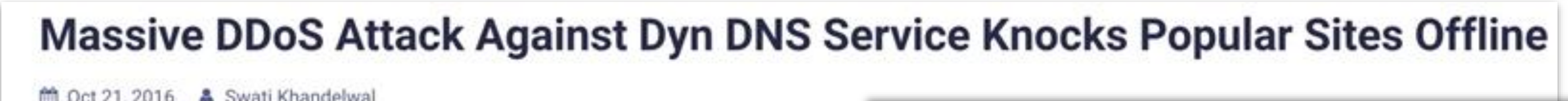
Cloudflare DNS Resolver Hit by BGP Hijack



KrebsonSecurity

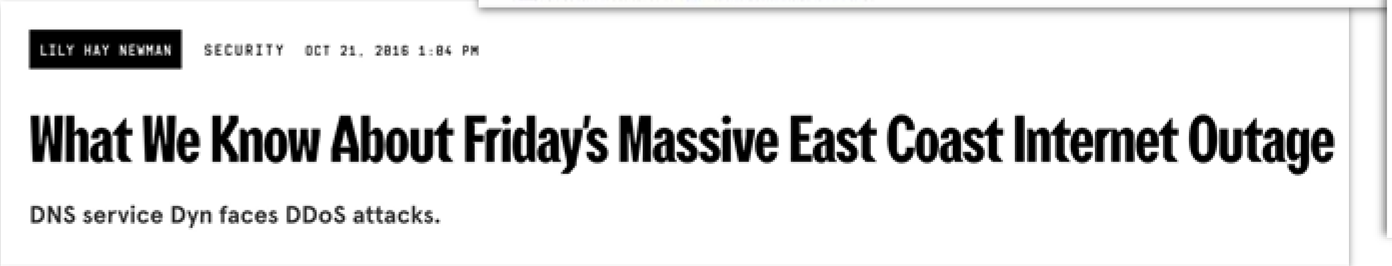
In-depth security news and investigation

DNS Error Went Unnoticed for Years



Massive DDoS Attack Against Dyn DNS Service Knocks Popular Sites Offline

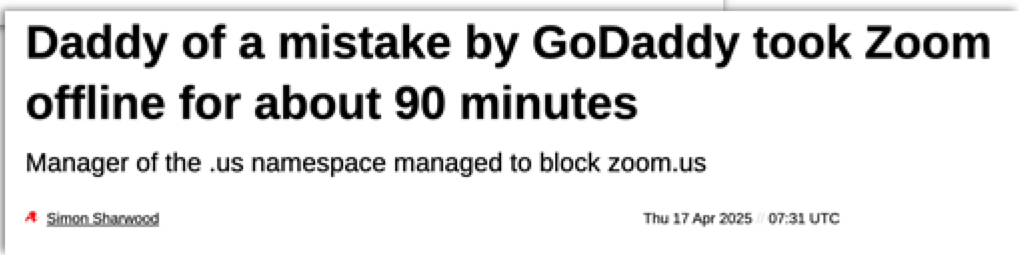
Oct 21, 2016 Swati Khandelwal



LILY HAY NEWMAN SECURITY OCT 21, 2016 1:04 PM

What We Know About Friday's Massive East Coast Internet Outage

DNS service Dyn faces DDoS attacks.



Daddy of a mistake by GoDaddy took Zoom offline for about 90 minutes

Manager of the .us namespace managed to block zoom.us

Simon Sharwood Thu 17 Apr 2025 // 07:31 UTC

Reputation is Capital...

Raising the Bar: What Can Change?

Principles for modern DNS hygiene:

- Consistent record validation & renewal
- Cross-team coordination (SecOps, NetOps, DevOps)
- Threat-informed configuration baselines

Opportunities for community & stds:

- Open frameworks for posture evaluation
- Better alerting/reporting pipelines
- Shared registries or transparency models

We need to bring the recursive threat management to authoritative….

DNS is a Strategic Asset, Not Just Plumbing

Managing DNS Configuration is Challenging

How Can we Make it Better?

What's Stale? What's Broken? What's wrong? What am I missing?

Questions?