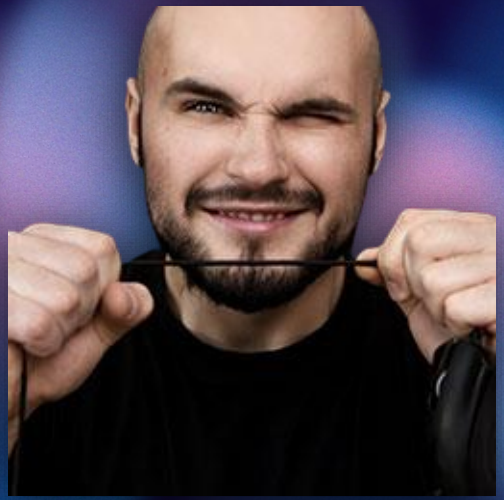
Protecting the Digital World

OWASP

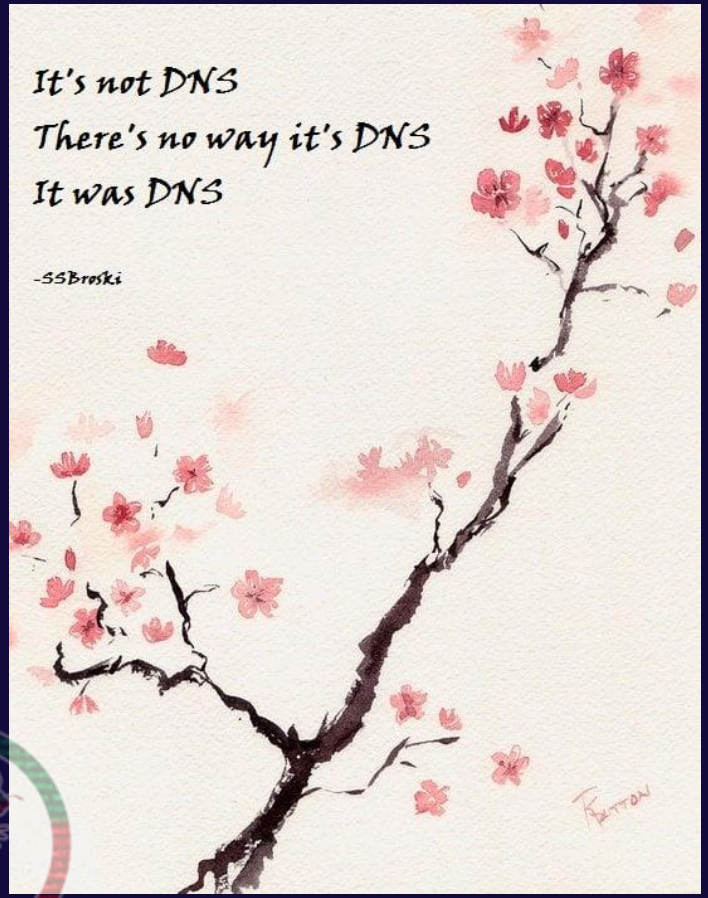
SOFIA, BULGARIA

owasp.org/www-chapter-sofia/

CENTIO
#CYBERSECURITY



BASELINE
CyberSecurity



Cloudflare 1.1.1.1 incident on July 14, 2025

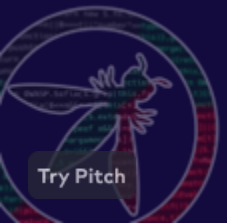
2025-07-15

Google services were down in Turkey, parts of Europe

By **Reuters**

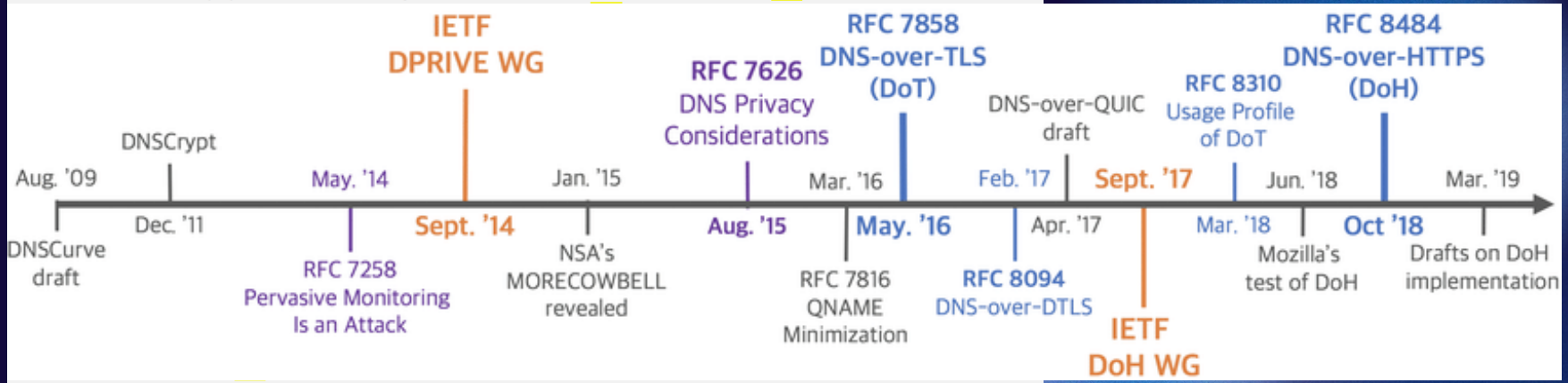
September 4, 2025 12:25 PM GMT+3 · Updated September 4, 2025

- History of DNS
- Anatomy of DNS
- Abusing DNS
- Defending DNS



DNS History Timeline

- 1969-09-25 The telnet access to a serving host connects using an official site name, such as SRI, UCLA, UCSB, or UTAH. RFC 15
- 1973-02-07 The Stanford Research Institute's Augmentation Research Center (SRI-ARC) is considering to offer a Network Information Center to implement and maintain identification files for all network users and sites and make these files available via the network. RFC 453
- 1973-03-08 The SRI NIC will provide standard addresses of mail recipients. RFC 469
- 1973-06-13 FTP MAIL proposes that a mail user may be a combination of a host name and mailbox name. RFC 524



- 1984 The SRI-NIC runs a centralized name server answering queries for all hosts from all systems. (Zhou, S., The Design and Implementation of the Berkeley Internet Name Domain (BIND) Servers. UCB/CSD 84/177)
- 1984 Graduate students at University of California at Berkeley design and implement the Berkeley Internet Name Domain (BIND) servers and database on 4.2BSD Unix for distributed name service. This was developed in parallel with USC-ISI's different system running on a TOPS-20.
- 1984-10 A limited set of top level domains is introduced: GOV, EDU, COM, MIL, ORG; and two-letter country code top-level domains are proposed (based on ISO-3166). RFC 920
- 1985 Digital Equipment funded further development and maintenance of BIND, further integrating the nameserver into a real working environment.
- 1985 The name server lookup program nslookup was released to the Unix community.
- 1989 Security researcher Steven M. Bellovin's ``Security Problems in the TCP/IP Protocol Suite'' paper published in 1989 clearly identified a sequence number attack.
- 1993 Christoph Schuba's 1993 ``Addressing Weaknesses in the Domain Name System Protocol'' thesis outlined problems with predictable IDs, spoofing referrals, cache poisoning, and documented a mechanism to use signatures and public keys stored in DNS.
- 1994-02 The first DNS Protocol Security Extensions IETF draft specification proposed using digital signatures and authentication keys added as

a.b om

✅ **253 characters** (in practice) — according to DNS standards.

Here's the breakdown:

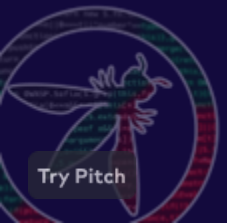
- **Per-label limit:** Each label (the parts between dots, e.g., `example` in `example.com`) can be **up to 63 characters** long.
  → Defined in RFC 1035, section 2.3.4 ↗
- **Total FQDN length:** The entire domain name, including dots separating labels, can be **at most 255 bytes**, including the trailing null byte used internally in DNS messages.
  → So, the **maximum usable length** in textual form is **253 characters** (since 255 − 1 for null terminator − 1 because the last label doesn't end with a dot).

Example of a maximal FQDN:

Copy code

```
63charslabel.63charslabel.63charslabel.61charslabel
```

(Total = 63 + 1 + 63 + 1 + 63 + 1 + 61 = 253 characters)



DNS

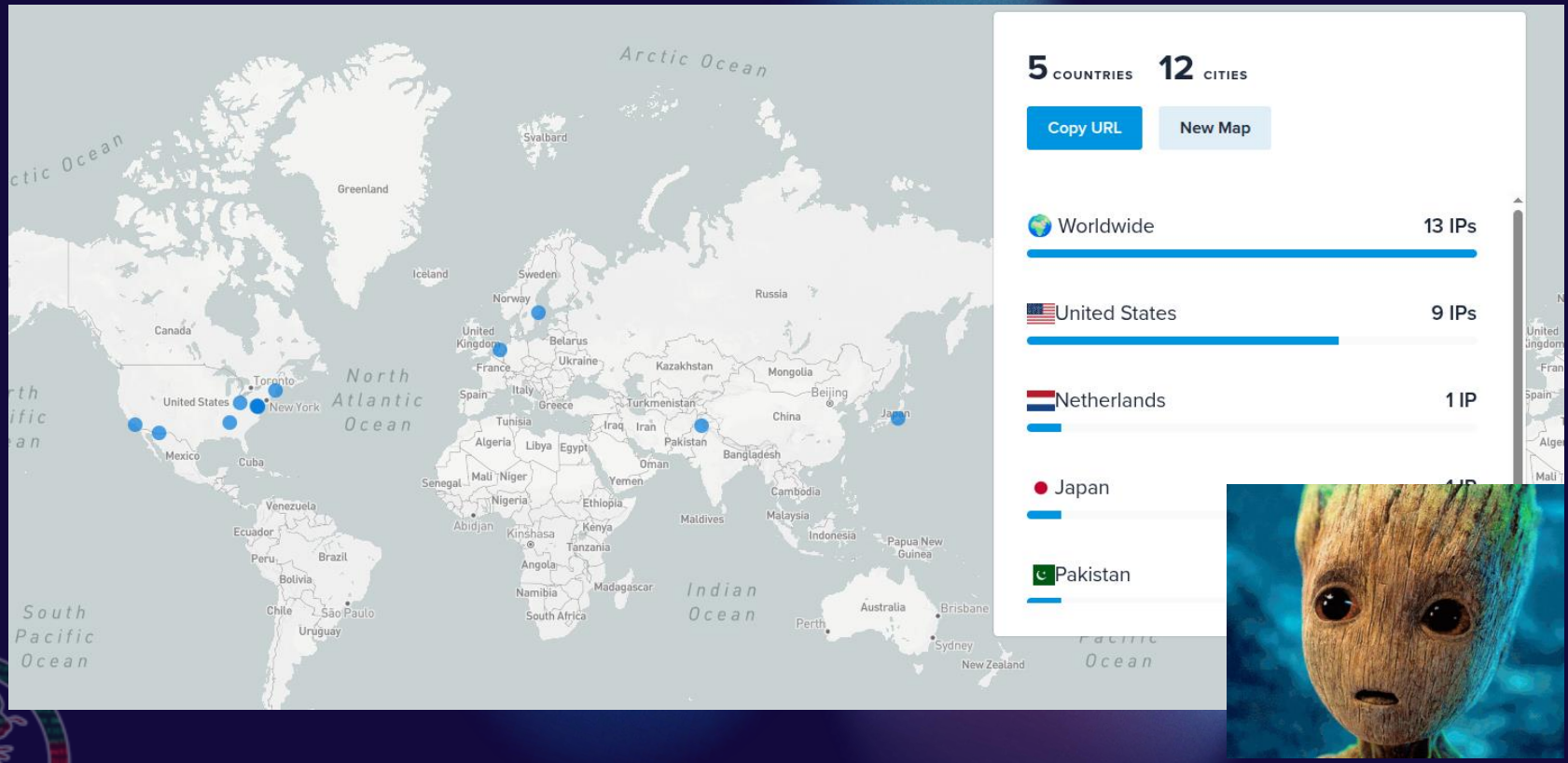
This is the full list of all DNS/DNSSEC-related articles on my blog, starting from the basics to more details such as key rollover and NSEC3.

Basic DNS and DNSSEC Validation

- It's Always DNS – **Poster**
- It's Always DNS! @ SharkFest'23 EU (90 min. YouTube session)
- [DE] Das Domain Name System (c't Artikel)
- Basic **BIND** Installation
- **BIND** DNSSEC Validation
- DNSSEC Validation with **Unbound** on a Raspberry
- **Pi-hole** Installation Guide
- DNS **Capture**: UDP, IP-Fragmentation, TCP, EDNS, ECS, Cookie
- Single DNS Query – Hundreds of Packets

DNSSEC Signing

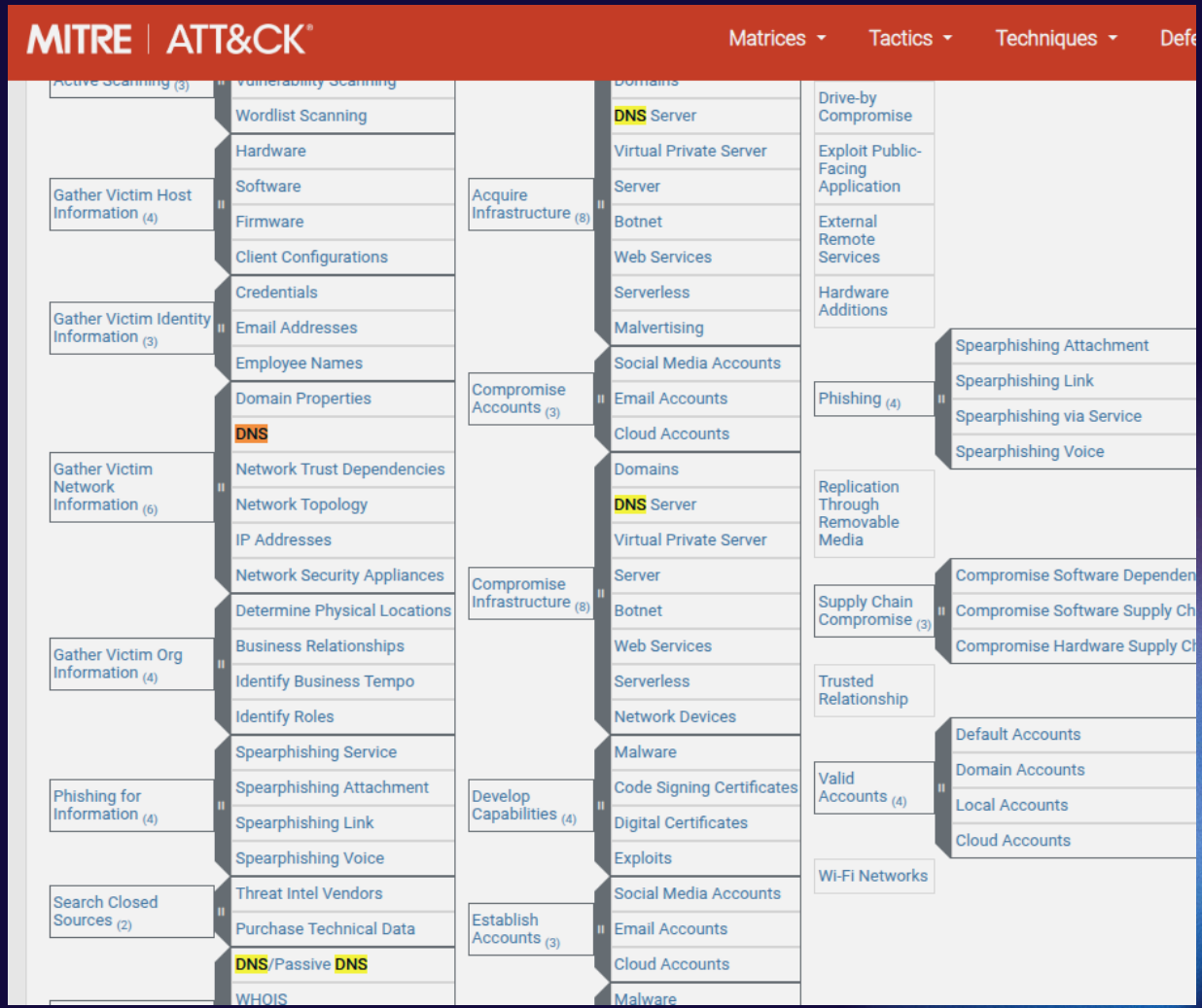
OWASP Sofia

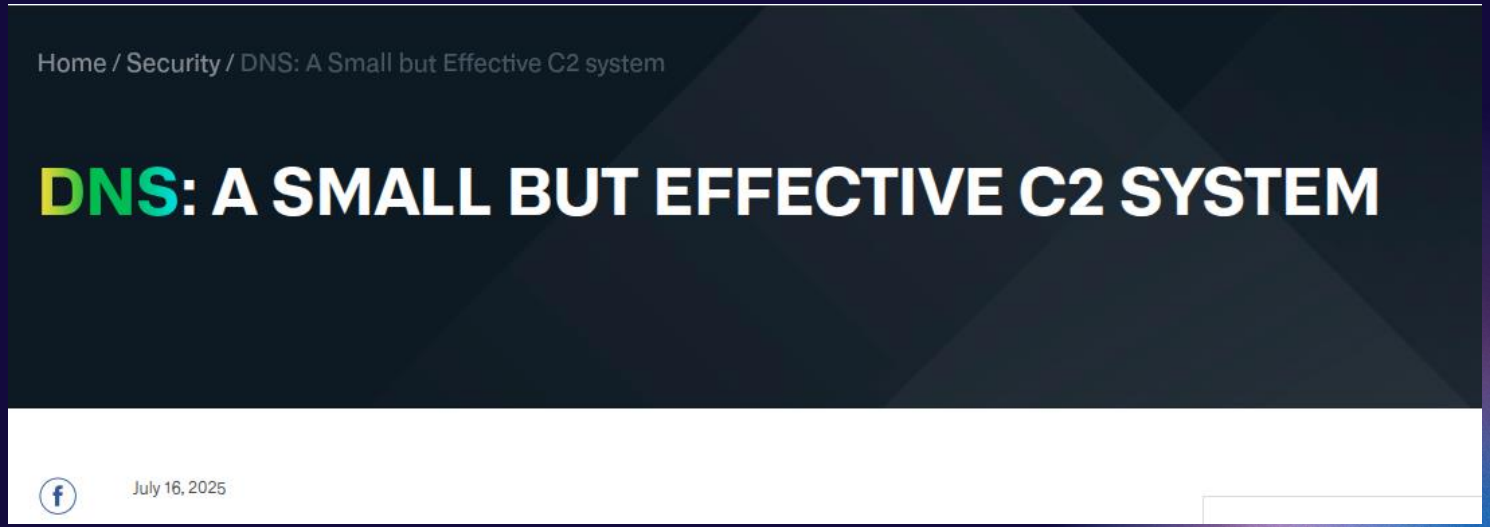


Try Pitch

OWASP Sofia

Try Pitch

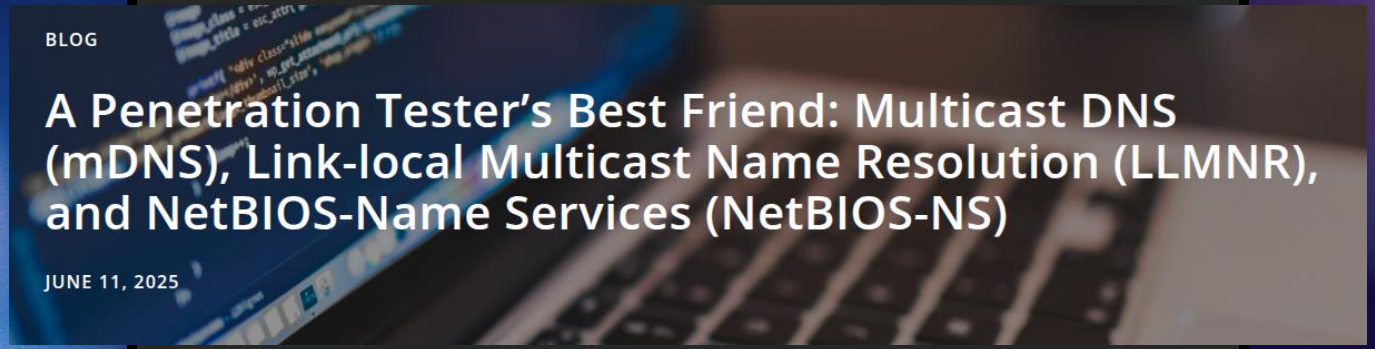

MITRE | ATT&CK
Matrices
Tactics
Techniques
Wordlist Scanning
Gather Victim Host Information (4)
Hardware
Software
Firmware
Client Configurations
Gather Victim Identity Information (3)
Credentials
Email Addresses
Employee Names
Gather Victim Network Information (6)
Domain Properties
DNS
Network Trust Dependencies
Network Topology
IP Addresses
Network Security Appliances
Gather Victim Org Information (4)
Determine Physical Locations
Business Relationships
Identify Business Tempo
Identify Roles
Phishing for Information (4)
Spearphishing Service
Spearphishing Attachment
Spearphishing Link
Spearphishing Voice
Search Closed Sources (2)
Threat Intel Vendors
Purchase Technical Data
DNS/Passive DNS
WHOIS
Acquire Infrastructure (8)
DNS Server
Virtual Private Server
Server
Botnet
Web Services
Serverless
Malvertising
Compromise Accounts (3)
Social Media Accounts
Email Accounts
Cloud Accounts
Compromise Infrastructure (8)
Domains
DNS Server
Virtual Private Server
Server
Botnet
Web Services
Serverless
Network Devices
Develop Capabilities (4)
Malware
Code Signing Certificates
Digital Certificates
Exploits
Establish Accounts (3)
Social Media Accounts
Email Accounts
Cloud Accounts
Malware
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (4)
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Spearphishing Voice
Replication Through Removable Media
Supply Chain Compromise (3)
Compromise Software Dependen
Compromise Software Supply Ch
Compromise Hardware Supply Ch
Trusted Relationship
Valid Accounts (4)
Default Accounts
Domain Accounts
Local Accounts
Cloud Accounts
Wi-Fi Networks


Home / Security / DNS: A Small but Effective C2 system
DNS: A SMALL BUT EFFECTIVE C2 SYSTEM
July 16, 2025

Hunting Lazarus: Expanding Indicators with Historic DNS

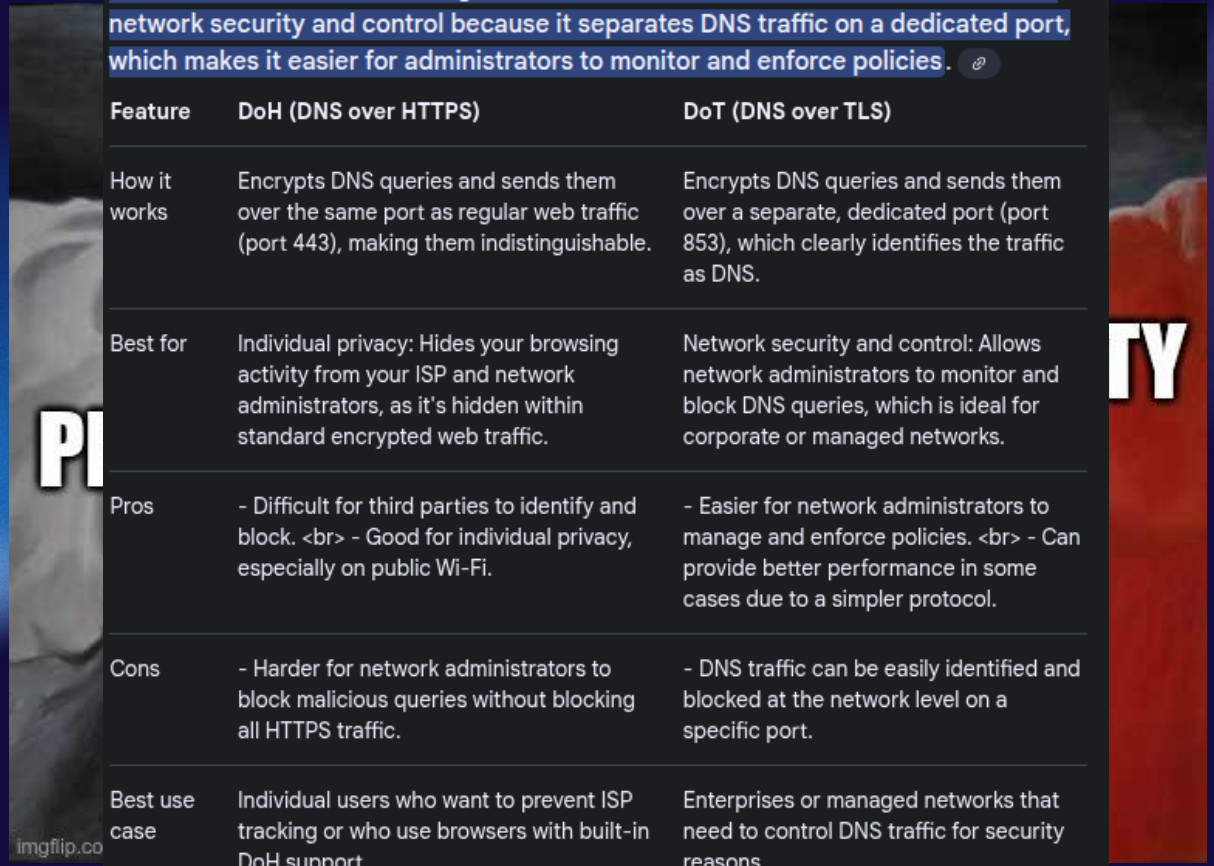
By: Kenneth Kinion	2024-07-15	general

LLMNR and mDNS are both protocols for name resolution on a local network without a DNS server, but they differ in origin, use, and specifications. LLMNR (Link-Local Multicast Name Resolution) is a Microsoft-developed protocol for Windows, while mDNS (Multicast DNS) is a more universal, multi-platform protocol that is part of a broader zero-configuration network standard. LLMNR uses a DNS-like packet format over link-local multicast addresses, whereas mDNS uses UDP port 5353 and specific multicast addresses for both IPv4 and IPv6.



Feature	LLMNR	mDNS
Multicast Address	Uses a link-scope multicast address.	Uses specific IPv4 address `224.0.0.251` or IPv6 address `ff02::fb`.
Query/Response	Queries are sent to a link-local multicast address; responses are unicast.	Queries and responses are both sent via multicast to specific addresses.
Security	Vulnerable to poisoning attacks, like mDNS.	Vulnerable to poisoning attacks.

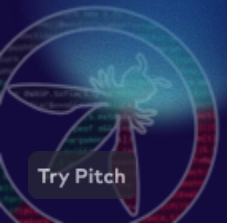

DNS Packet
Inspection
for
Network Threat
Hunters
ACTIVE COUNTERMEASURES



Neither DoH nor DoT is universally "better"; the best choice depends on your needs. DoH is generally better for individual privacy because it hides DNS requests within standard HTTPS traffic, making them harder to block, while DoT is often better for network security and control because it separates DNS traffic on a dedicated port, which makes it easier for administrators to monitor and enforce policies.

Feature	DoH (DNS over HTTPS)	DoT (DNS over TLS)
How it works	Encrypts DNS queries and sends them over the same port as regular web traffic (port 443), making them indistinguishable.	Encrypts DNS queries and sends them over a separate, dedicated port (port 853), which clearly identifies the traffic as DNS.
Best for	Individual privacy: Hides your browsing activity from your ISP and network administrators, as it's hidden within standard encrypted web traffic.	Network security and control: Allows network administrators to monitor and block DNS queries, which is ideal for corporate or managed networks.
Pros	- Difficult for third parties to identify and block. - Good for individual privacy, especially on public Wi-Fi.	- Easier for network administrators to manage and enforce policies. - Can provide better performance in some cases due to a simpler protocol.
Cons	- Harder for network administrators to block malicious queries without blocking all HTTPS traffic.	- DNS traffic can be easily identified and blocked at the network level on a specific port.
Best use case	Individual users who want to prevent ISP tracking or who use browsers with built-in DoH support.	Enterprises or managed networks that need to control DNS traffic for security reasons.

- Self hosted DNS server (DC forwerders)
- DNS traffic rules and policies
- What is encrypted SNI? - asked the poor NGFW
- Use of split-horizon DNS for internal/external separation
- Regularly audit **cloud DNS configurations & records**
- Log all DNS queries and perform anomaly detection



THE INTERNET WAS NEVER DESIGNED TO BE SECURE !

Pitch

Want to make a presentation like this one?

Start with a fully customizable template, create a beautiful deck in minutes, then easily share it with anyone.

Create a presentation (It's free)