Fingerprinting Malicious Tunnels in DNS over QUIC

Hafiz Farooq
Senior Cyber Security Architect, **Aramco**
ICANN – Member RSSAC Caucus, GNSO BC

Disclaimer

This presentation and its contents are NOT based on Aramco network data and instead based on lab-simulated and research data available from different online resources. All slides are solely those of the presenter and not necessarily reveal the Aramco's Security Policies and Standards.

Whoami

Hafiz Farooq

Education

MSc Next Gen Networks, **Aston University**, United Kingdom

BE Computer Engineering, **NUST**, Pakistan

Experience

Nationwide Network Engineer, **Pakistan Telcos** - 9 years

Network & Security Architect, **DELL** - 2 years

Professional Services Architect, **Juniper Networks** - 1 year

Senior Cyber Security Architect , **Aramco** – 6 years

ICANN Fellow – Routing, Switching & IDN Workgroups

Internet Society (ISOC)

Research

15+ Research papers in Network & Cyber Security

2 US Patents (Sep 2022), **ML/AI Book** being published by Packtr

Speaker at GITEX, GISEC, FLOCON, Cambridge, CMU

Professional Certificates

CISSP, CISM, Data Science Architect

SANS Forensic Examiner, SANS Exploit Researcher

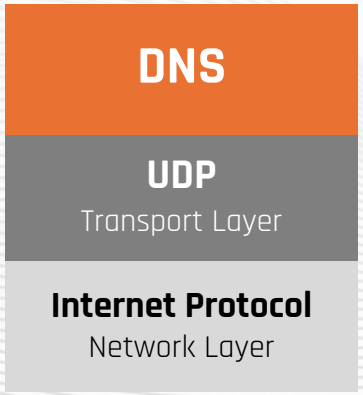
Splunk Big Data Architect, Qradar Deployment Professional

Juniper Networks – JNCIE Security and JNCIP-Service Provider Routing

DNS Privacy Protocols

Do53

Port 853

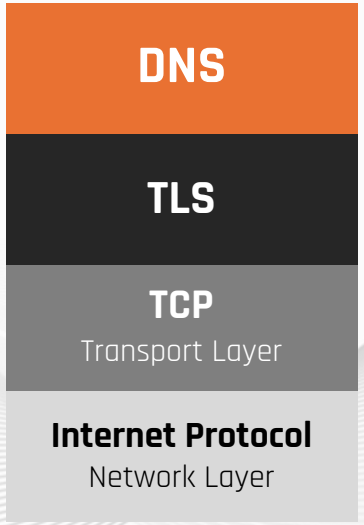


DNS

Easy-2-Block

DoT

Port 853



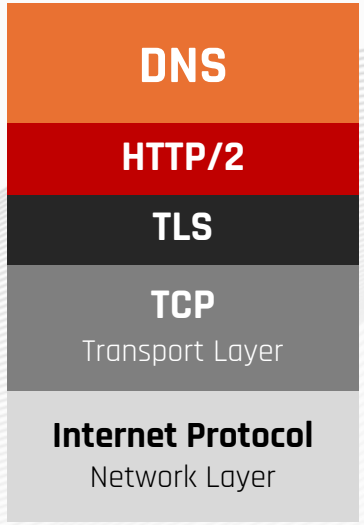
DNS over TLS

2016 / RFC 7858

Slow / Non-API / Easy-2-Block

DoH

Port 443



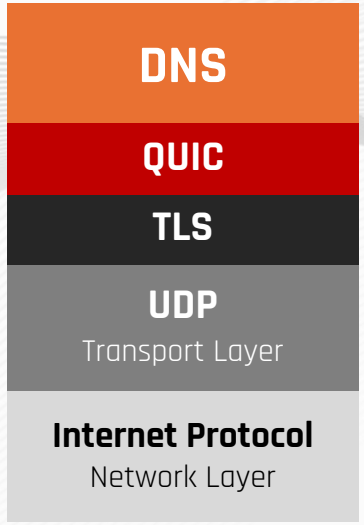
DNS over HTTP

2016 / RFC 8484

Slow / API / Difficult-2-Block

DoQ

Port 443



DNS over QUIC

2022 / RFC 9250

Fastest / API / Difficult-2-Block

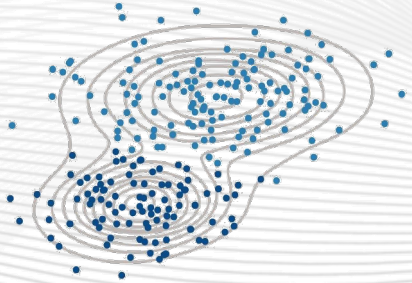
USC University of Southern California

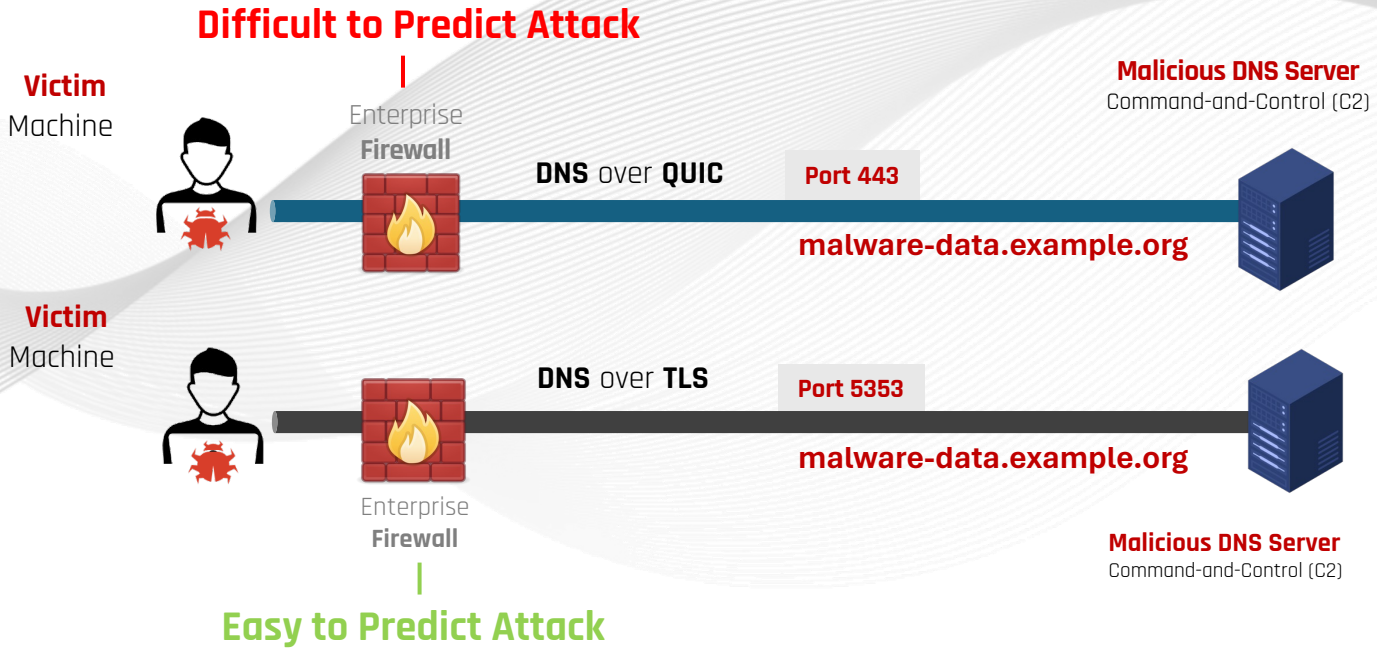
aramco

Upstream Digital Center
Leading Digital Excellence

DNS Tunneling Attack

- DNS is always vulnerable to C2 Tunneling Attacks
- DNS-over-HTTP due to inherent obfuscation, is now more lucrative for attackers





USC University of Southern California

aramco

Upstream Digital Center
Leading Digital Excellence

Protections against DNS Tunnels

- **Active**
  - DNS Query Logs (Shannon Entropy, Top Talkers)
  - **Disable DNS**
    - DoT (port 853)
    - Disable Well-Known DOH Providers (Google, Quad9, Cloudflare, Xfinity, OpenDNS, AdGuard)
    - Disable Well-Known DOQ Providers (AdGuard)

This approach is not going to scale in future

- **Passive**
  - Deploy DNS Proxy: dnsdist, dnscrypt/doh-server, sinkhole
  - DNS Capturing: Zeek, NetFlow & Lock-less DNSTAPs

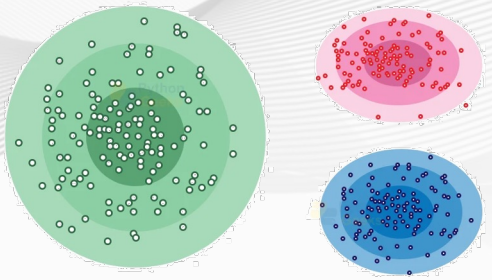
Attack Detection & Response

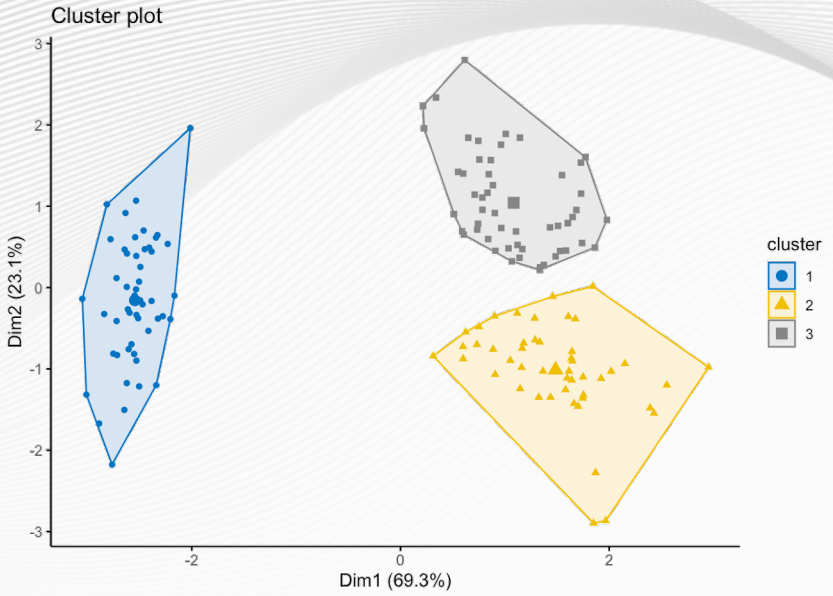
- Possible Analytics / Machine Learning Approaches
  - Numerical Clustering using **K-Means / DBSCAN**
  - JA3 or JA4 **Fingerprinting**

$$a_k = \frac{\sum_{i=1}^{n} z_{ik} x_{ij}}{\sum_{i=1}^{n} z_{ik}}$$

$$z_{ik} = \begin{cases} 1 \; if \; \|x_i - a_k\|^2 = \min\limits_{1 \le k \le c} \|x_i - a_k\|^2 \\ 0, \quad otherwise \end{cases}$$

K-Means I Euclidean Distance Formula





Cyber Security
is a key towards
excellence

Questions
& Answers

Thank Your

DINR 2024

USC University of Southern California

aramco

Upstream
Digital Center
Leading Digital Excellence