Quantifying the Impact of Encrypted DNS for Network Defenders

Blake Anderson, Principal Engineer, blake.anderson@cisco.com

David McGrew, Cisco Fellow, mcgrew@cisco.com

Overview

- Motivation
- Real-World Examples
- Moving Forward

Motivation

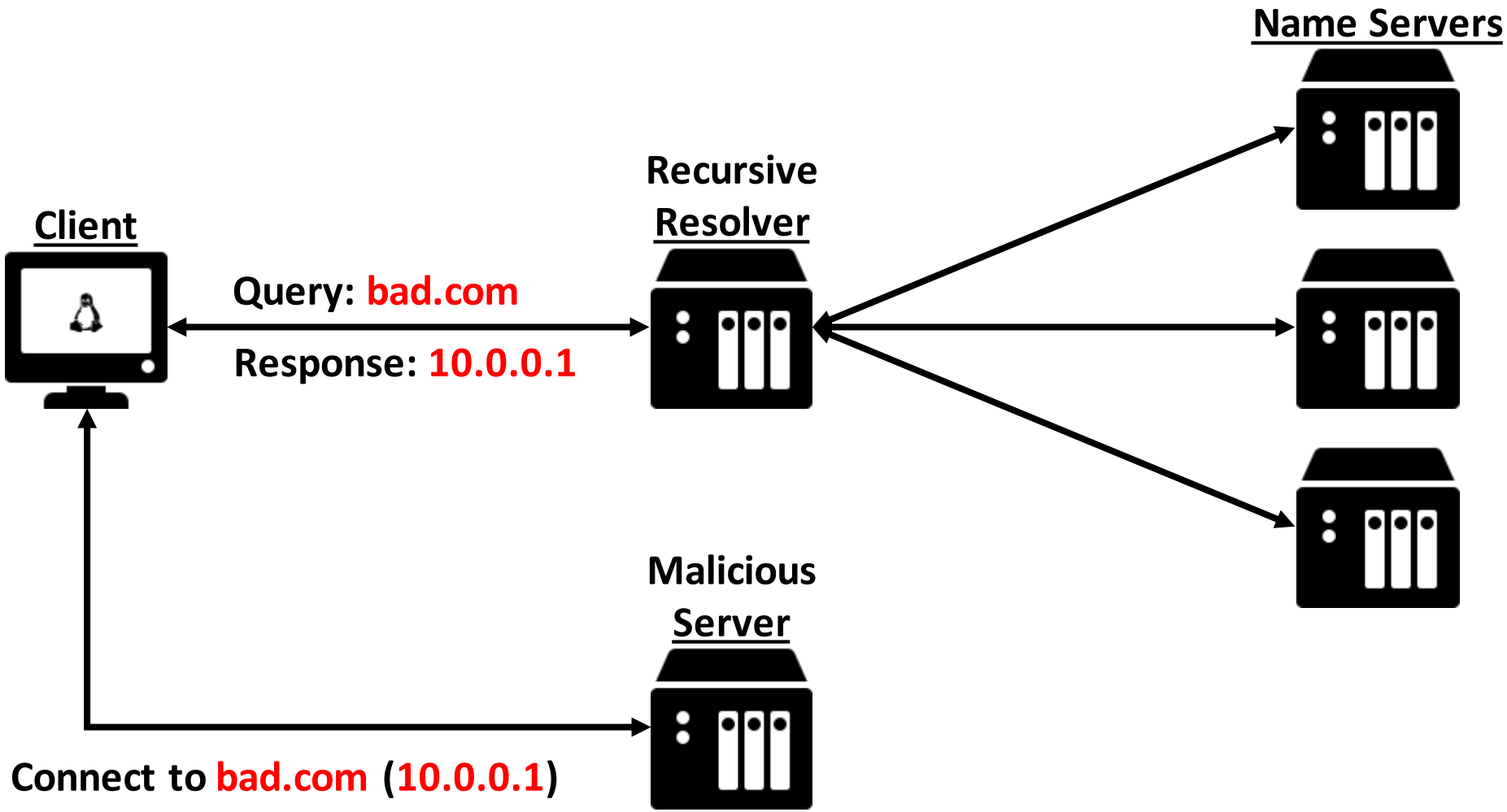
Motivation

- DNS-layer visibility and enforcement is an efficient means to securing your enterprise...

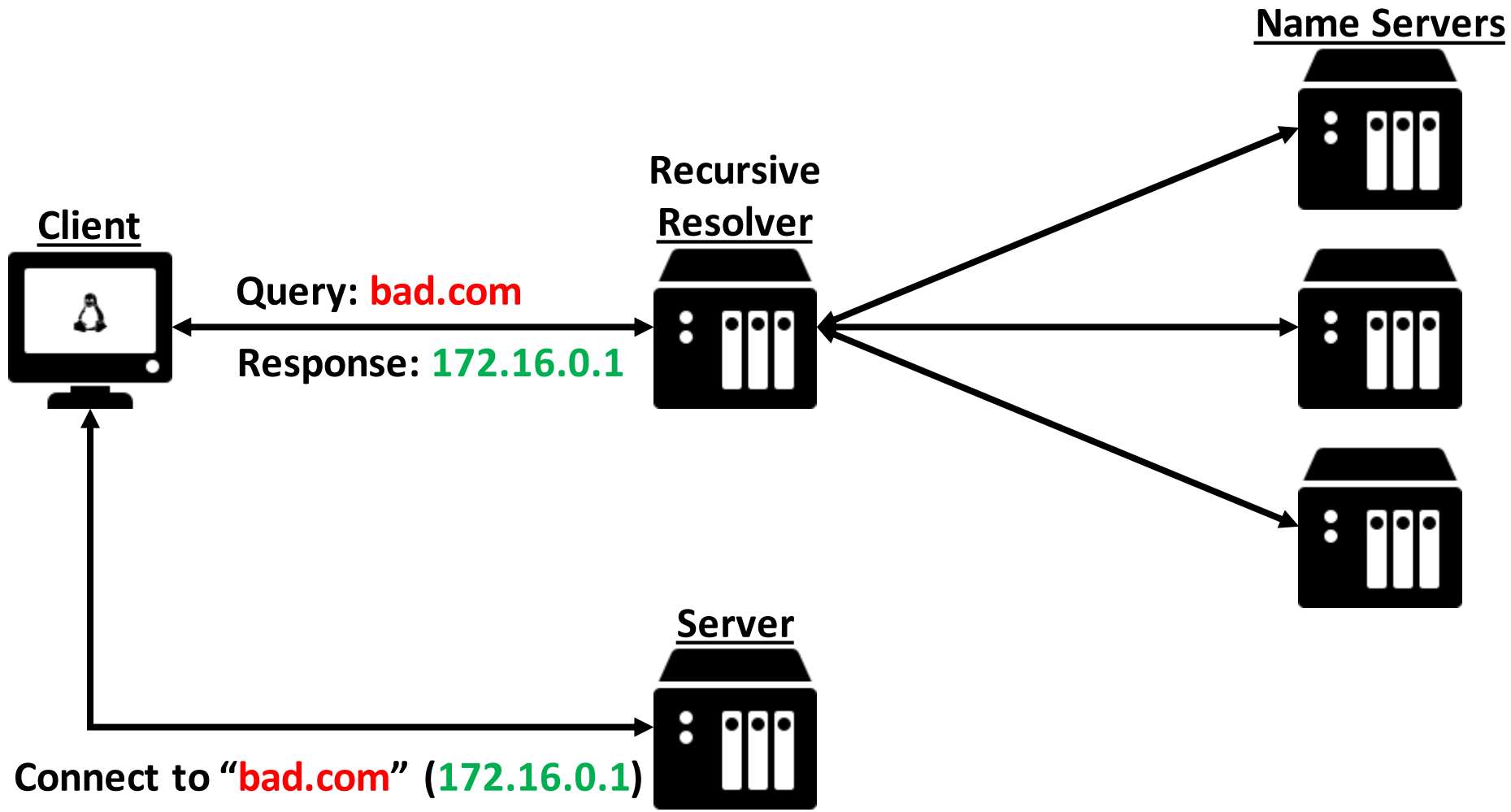
- ... but it isn't perfect:
  - Unsanctioned DNS servers restrict enforcement
  - Encrypted DNS restricts visibility

- "For enterprise networks, however, NSA recommends using only designated enterprise DNS resolvers in order to properly leverage essential enterprise cybersecurity defenses, facilitate access to local network resources, and protect internal network information."
  - https://media.defense.gov/2021/Jan/14/2002564889/-1/-1/0/CSI_ADOPTING_ENCRYPTED_DNS_U_OO_102904_21.PDF

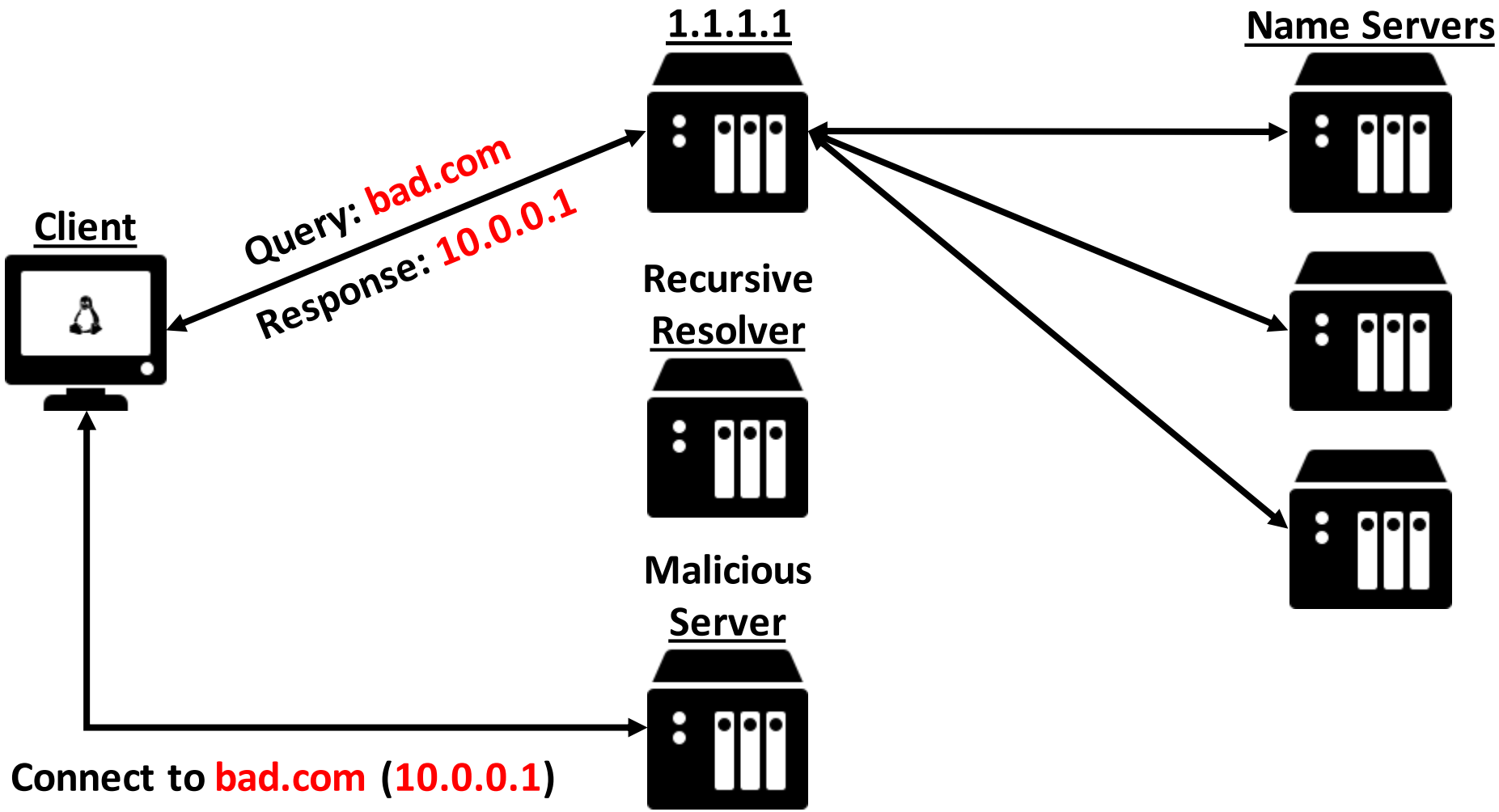
Traditional DNS



Traditional DNS Enforcement



Unsanctioned DNS



New Standards

DNS-over-TLS (DoT)

- RFC 7858
- Published May 2016
- Default port: TCP/853
- alpn: -

- Detection: easy

DNS-over-HTTPS (DoH)

- RFC 8484
- Published Oct 2018
- Default port: TCP/443
- alpn: `h2` / `http/1.1`

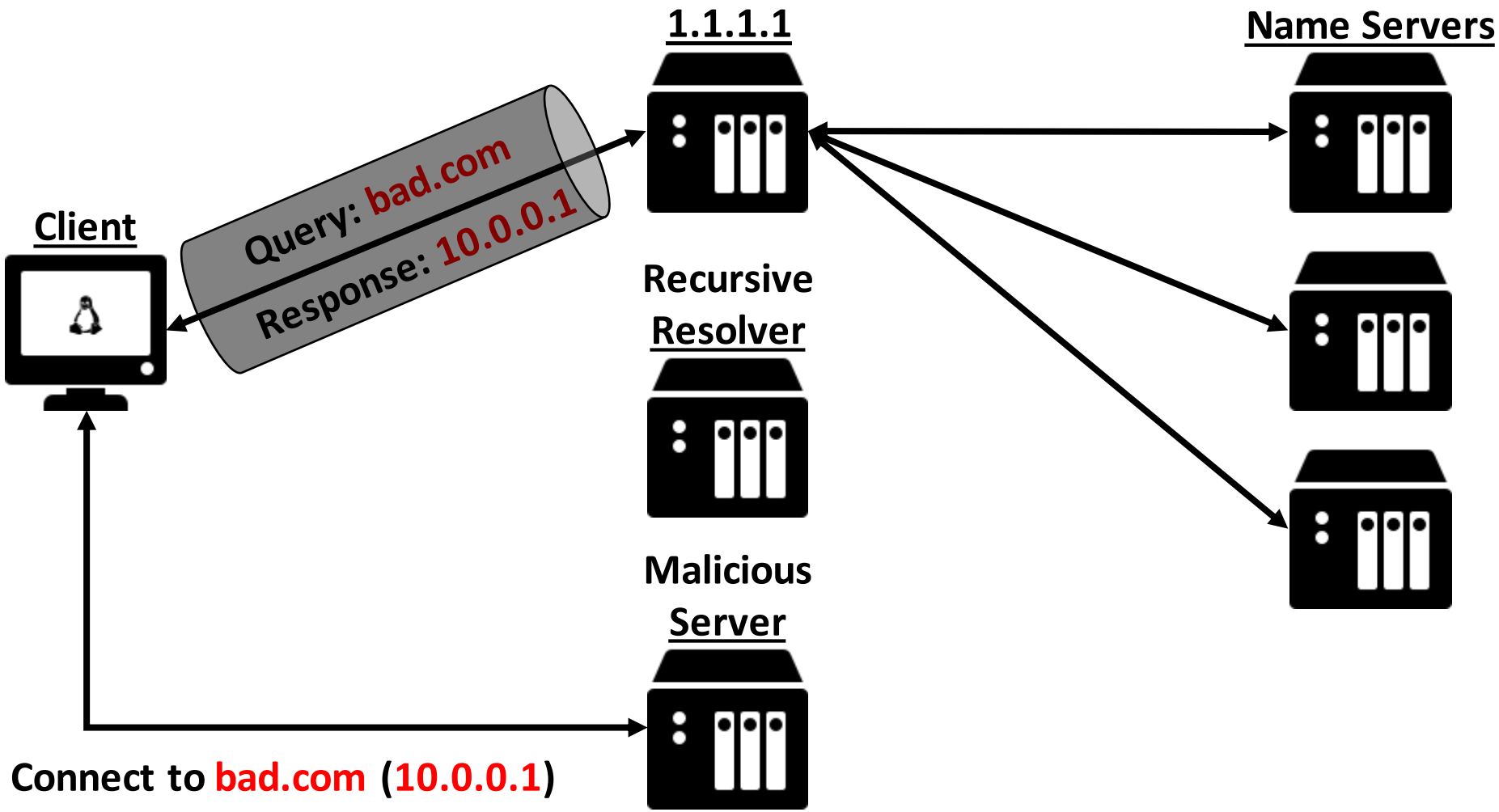
- Detection: hard

DNS-over-QUIC (DoQ)

- draft-ietf-dprive-dnsoquic-07
- Published Dec 2021
  - draft
- Default port: UDP/443
- alpn: `doq`

- Detection: easy*

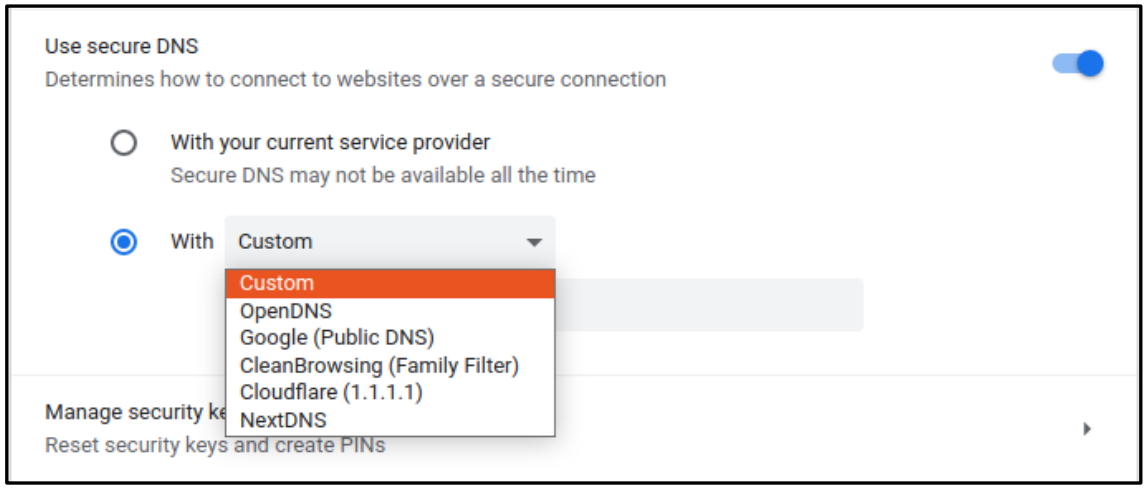
Encrypted DNS



Widespread Support for Encrypted DNS

Firefox

Chrome

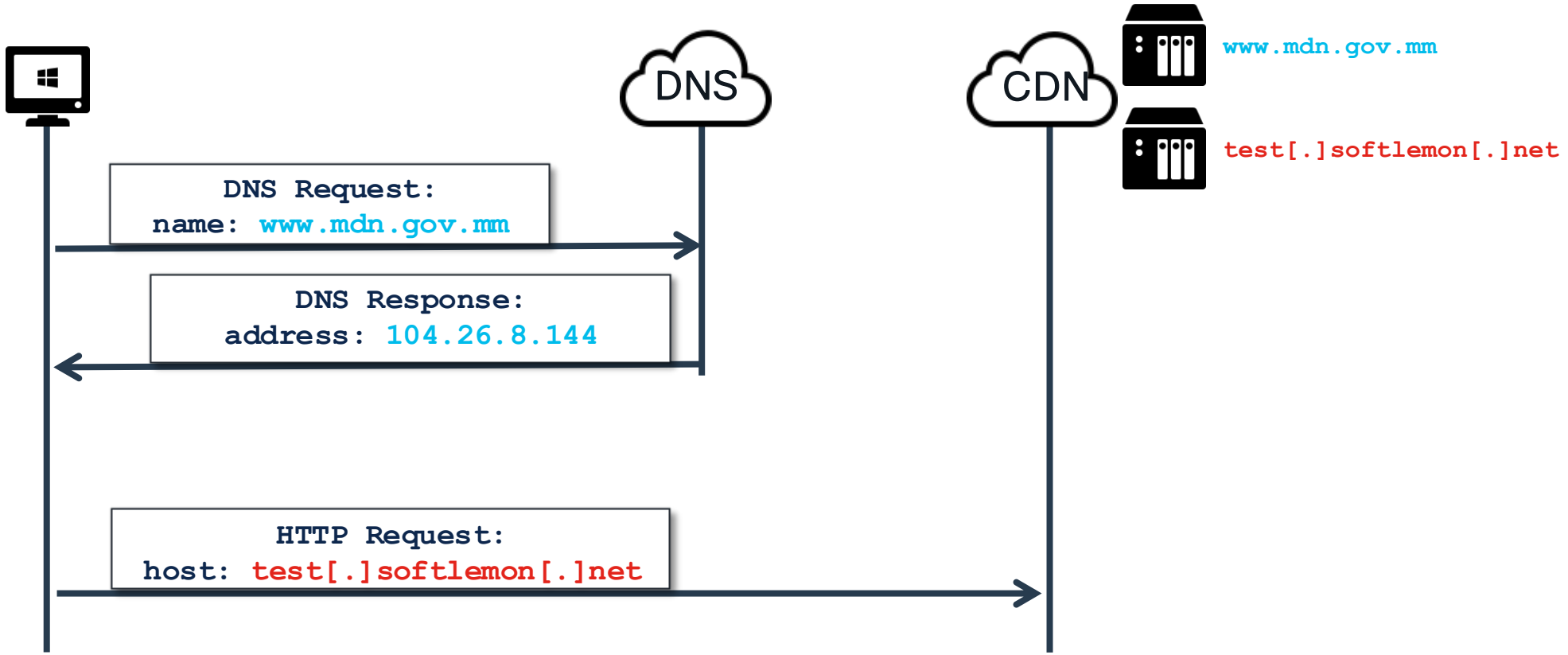


Real-World Examples

Using DNS-over-HTTPS to Evade Detection

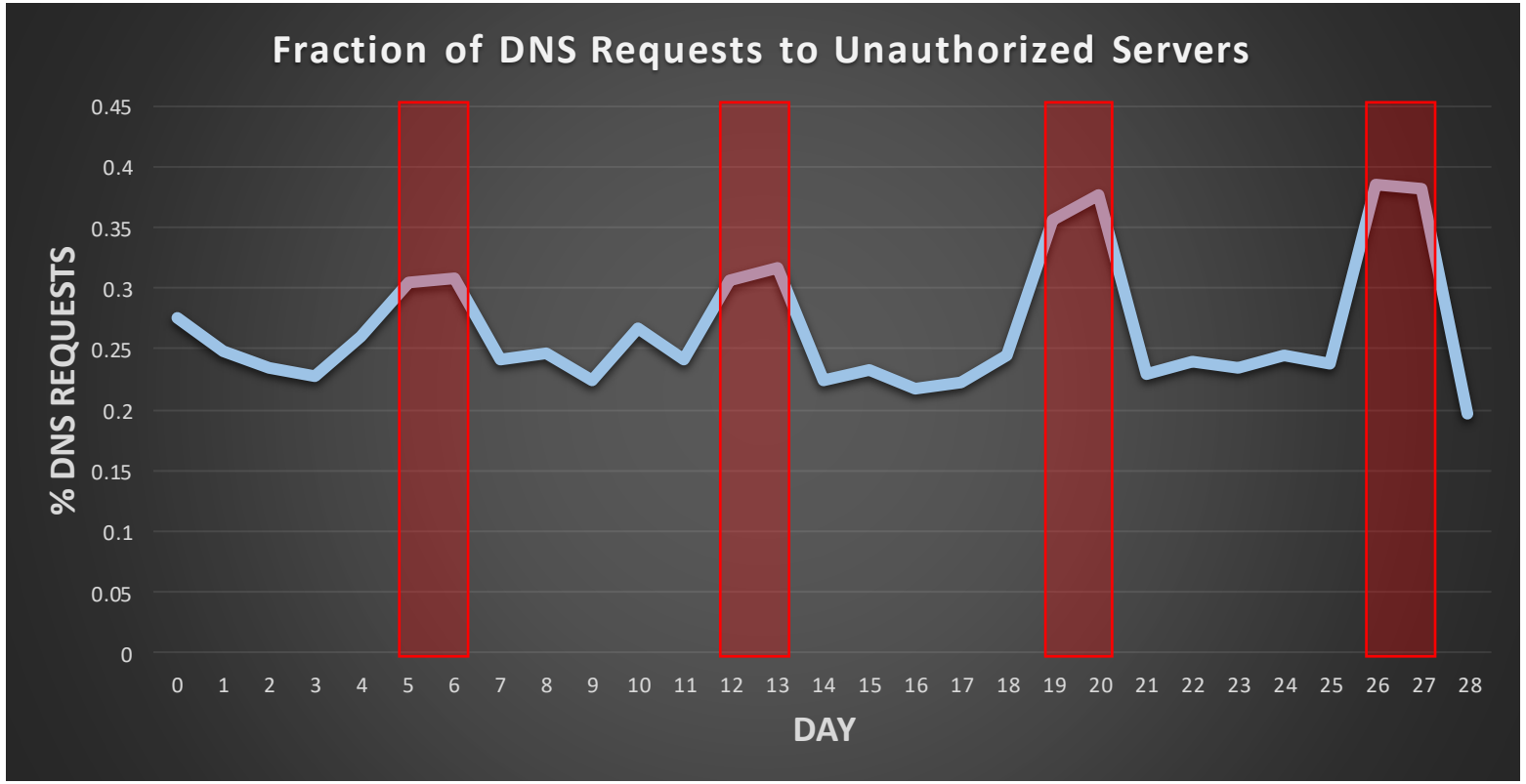
- https://github.com/nicehash/NiceHashMiner
  - “an advanced auto-miner that supports the latest algorithms and miners.”
  - Hard codes 1.1.1.1 / cloudflare-dns.com
- https://github.com/AdguardTeam/AdGuardHome
  - “powerful network-wide ads & trackers blocking DNS server.”
  - Hard codes 94.140.15.16 / dns-family.adguard.com (among others)
- https://ultrasurf.us/
  - “enables internet users to bypass internet censorship, and is free to users.”
  - Hard codes 9.9.9.11 / dns11.quad9.net

Using Shared Hosting to Evade Detection

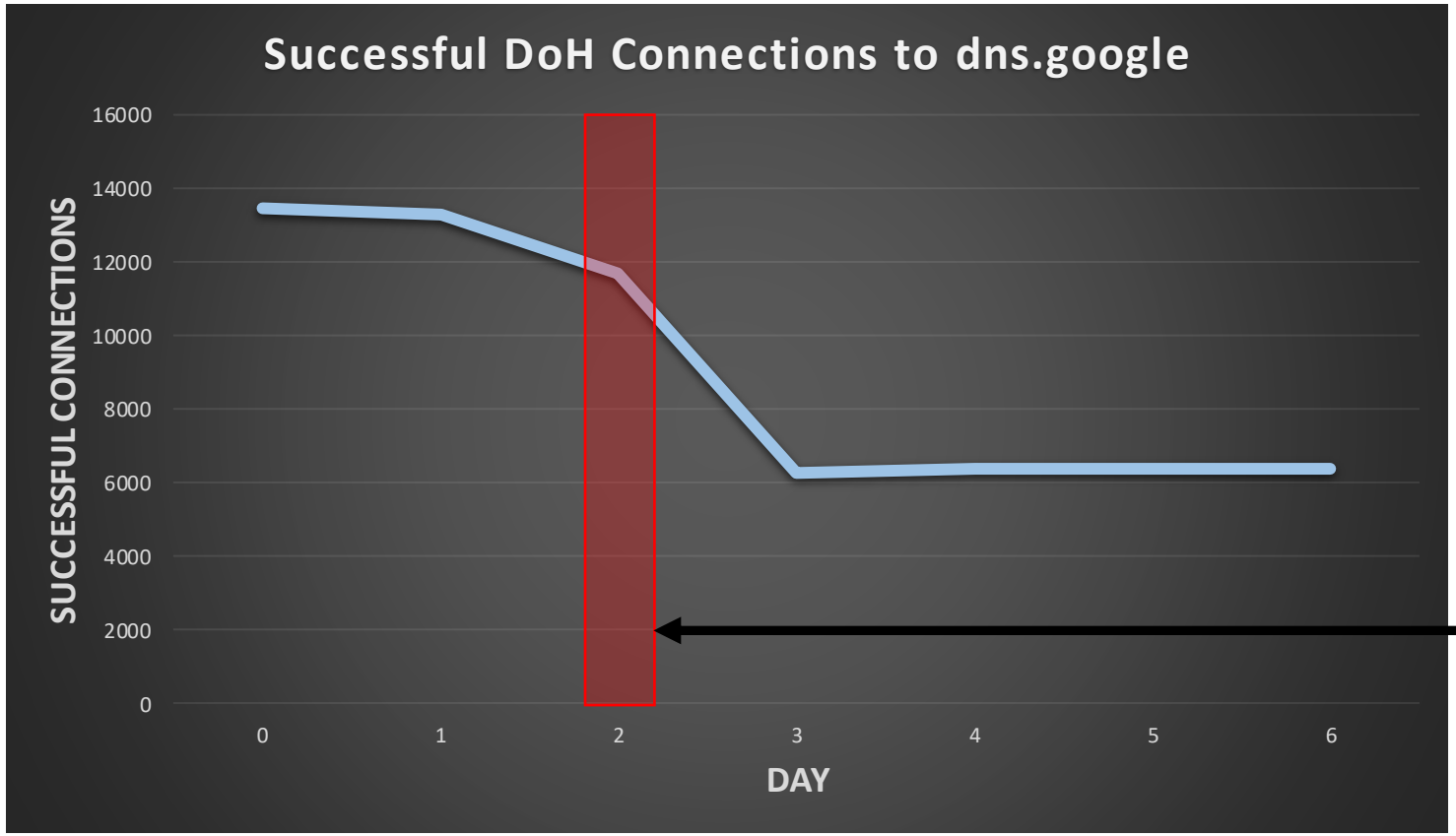


https://blog.talosintelligence.com/2021/11/attackers-use-domain-fronting-technique.html

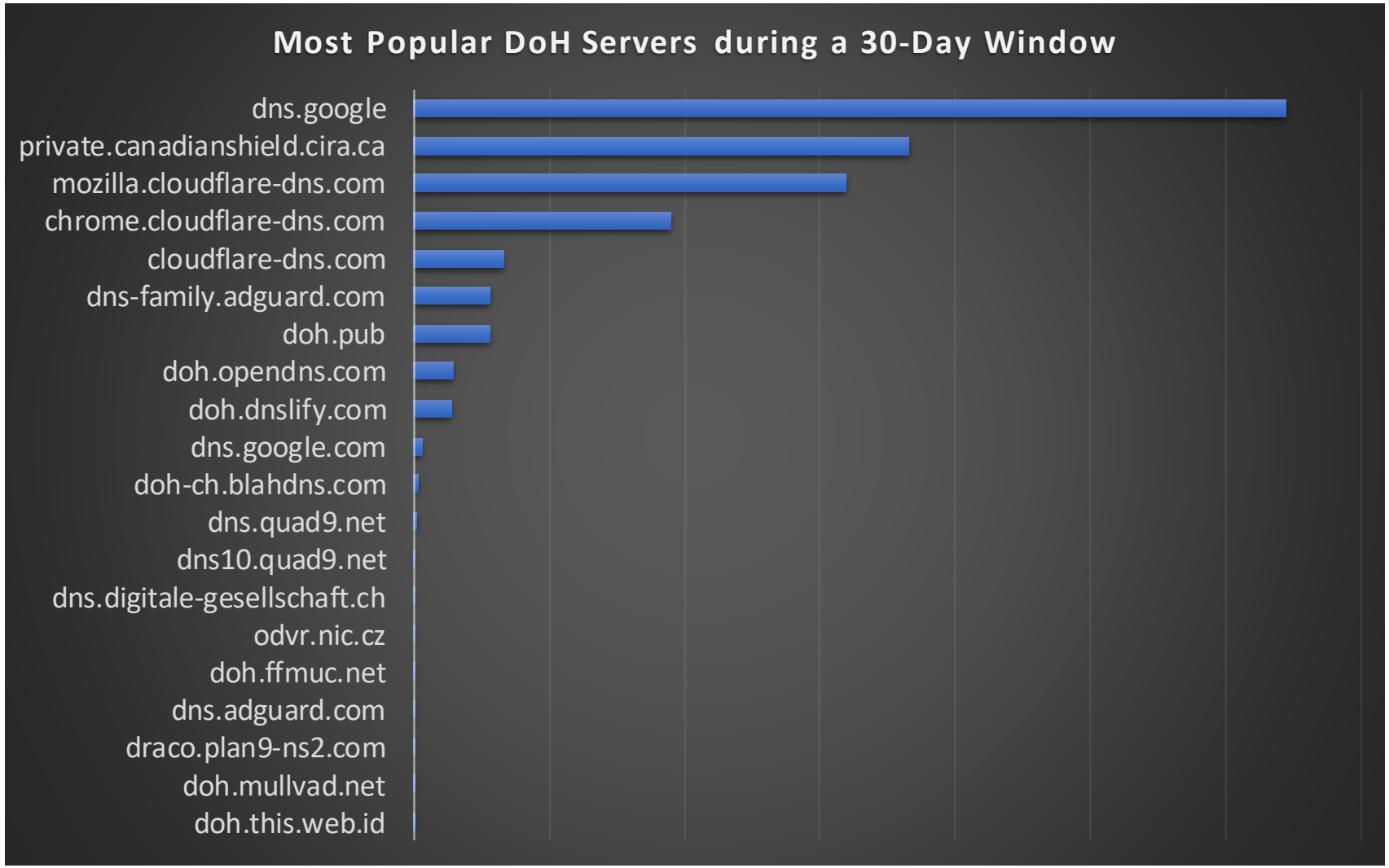
DNS Requests to Unauthorized Servers



DNS Enforcement in the Real-World



Diversity of DNS-over-HTTPS Servers



Maintaining Visibility

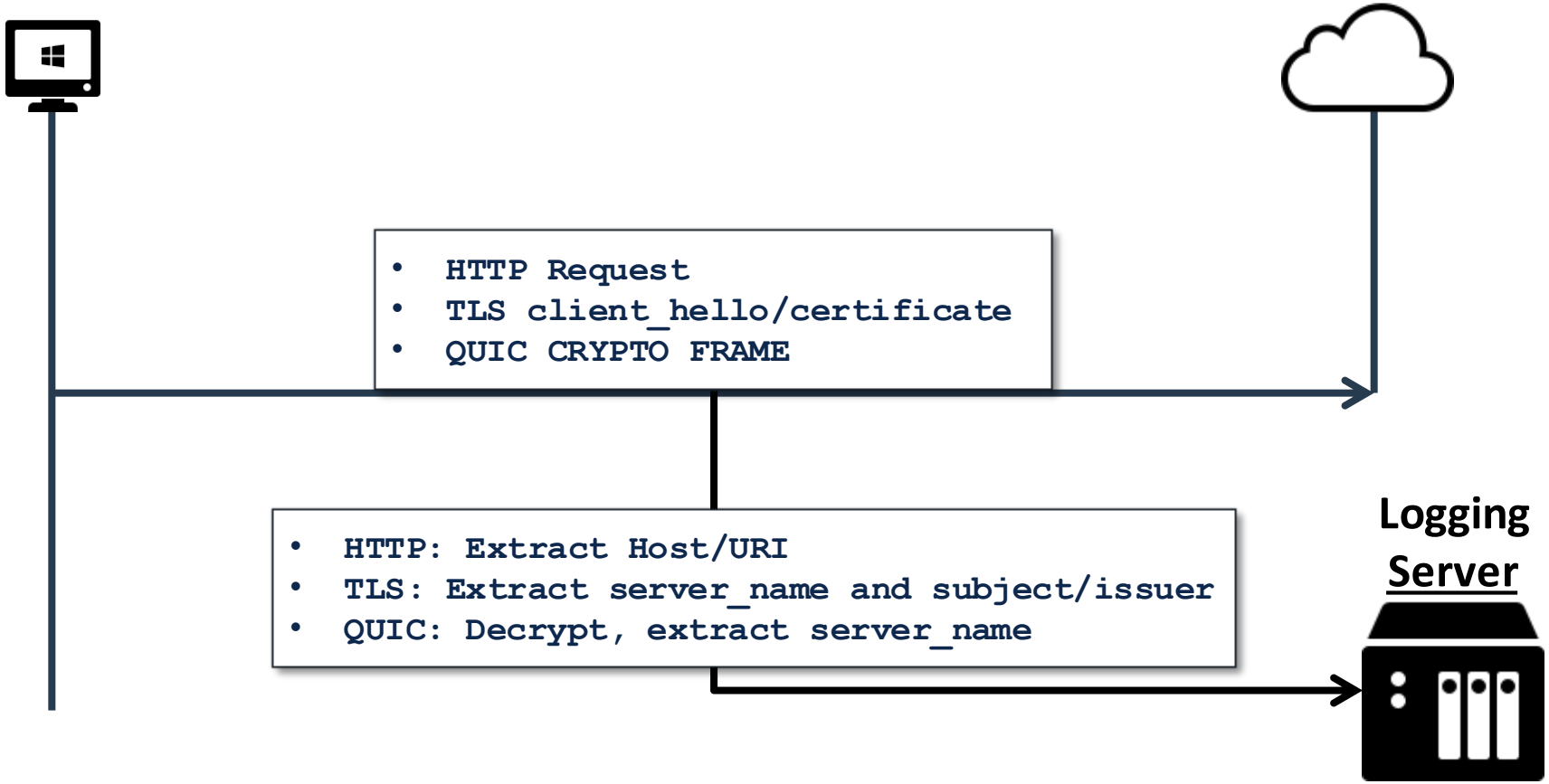
Detecting Encrypted DNS

- Network Traffic Analysis
  - Privacy of DNS-over-HTTPS: Requiem for a Dream?
- Network Traffic Tells
  - port: TCP/853
  - TLS extension alpn: “dot” (DNS-over-TLS) or “doq” (DNS-over-QUIC)
- Internet-Wide Scan Data
  - `re.findall('https://(.*?)/dns-query', line)`

Encrypted DNS Server Verification

- Detection techniques only need high recall and reasonable precision
- mercury
  - opensource
  - provides a utility program, tls_scanner
  - straightforward to verify if a domain or IP address is providing Encrypted DNS
- Currently identify 200-300 potential Encrypted DNS servers each week
  - Verify 5-6 Encrypted DNS servers

Expanded Domain Name Monitoring



- Other protocols: FTP/SMTP/IMAP/POP3/IRC

Conclusions

- DNS-layer visibility and enforcement is an efficient means to securing your enterprise
- But networks operators need to additionally:
  - Minimize unsanctioned DNS
  - Ensure all encrypted DNS is to authorized providers
  - Maintain active intelligence on encrypted DNS domain names and IP addresses
  - Augment visibility gaps by extracting and analyzing domain names in HTTP/TLS/QUIC/etc.

References

- https://github.com/cisco/mercury
- RFCs/drafts:
  - RFC 7858 (DNS-over-TLS)
  - RFC 8484 (DNS-over-HTTPS)
  - draft-ietf-dprive-dnsoquic-06 (DNS-over-QUIC)
- https://blog.talosintelligence.com/2021/11/attackers-use-domain-fronting-technique.html
- Privacy of DNS-over-HTTPS: Requiem for a Dream?
- Adopting Encrypted DNS:
  https://media.defense.gov/2021/Jan/14/2002564889/-1/-1/0/CSI_ADOPTING_ENCRYPTED_DNS_U_OO_102904_21.PDF


DNS
Thank You