RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: ZT-R01

# Protective DNS, DNS Encryption, & Zero-Trust: Tackling NSA Guidance

**Steve Staden, CISSP**

Senior Director, Product Management
DNSFilter

# Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA® Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

# Is your DNS leaking?

RSAConference2022

# Understanding DNS

# DNS (Domain Name System)

**Recursive DNS Resolver**

- Middleman between client and DNS infrastructure
- Caches information received during DNS lookups
- Typically provided by ISP

**Root Nameserver**

- There are 13 root nameservers [a-m].root-servers.net
- Multiple nodes using anycast
- Hosted by Verisign, USC, NASA, DoD, US Army, ICANN

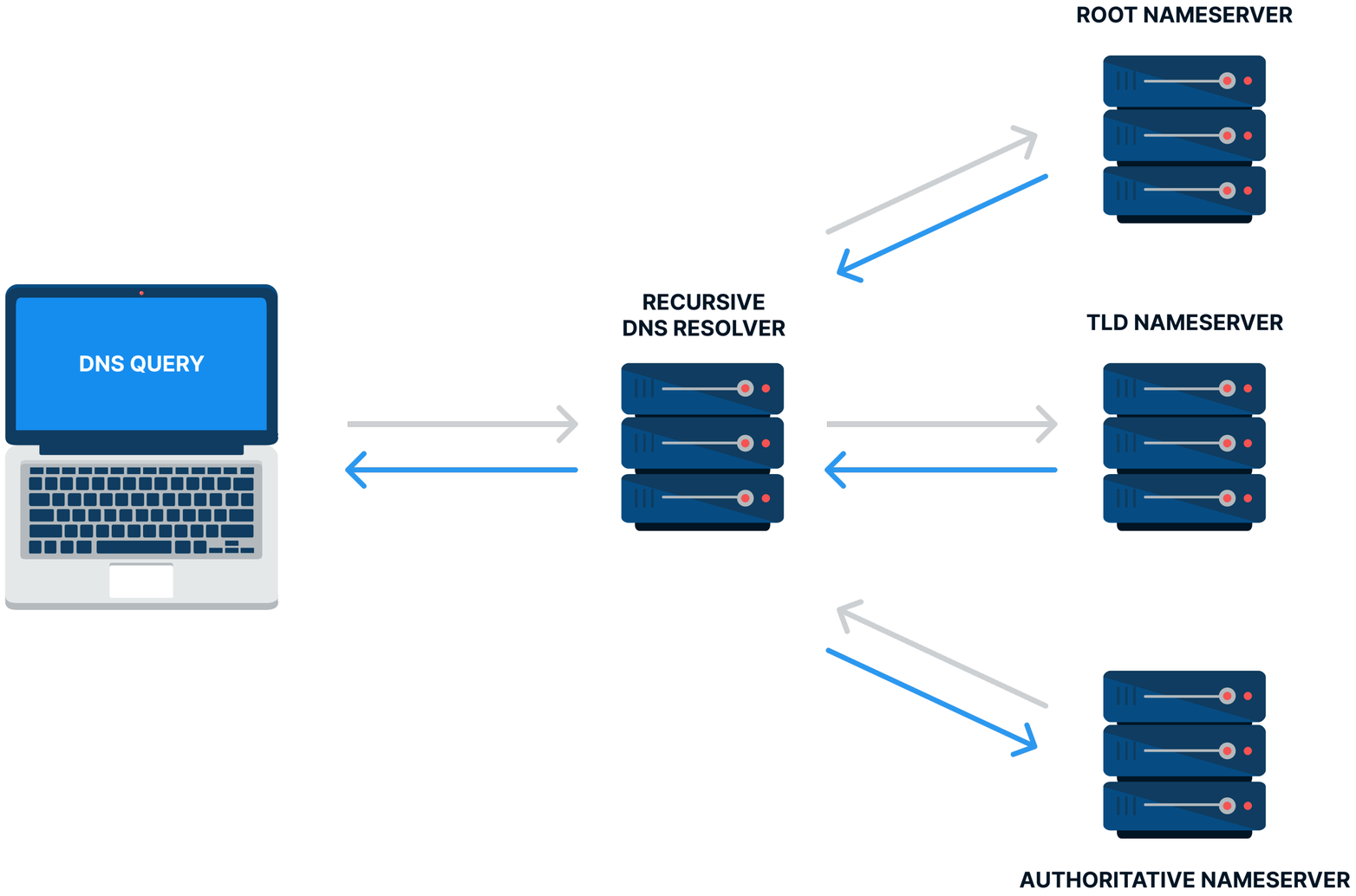
**TLD Nameserver**

- Stores info for all domains that share an extension
- Hosted by Internet Assigned Numbers Authority (IANA)
- gTLD (generic), sTLD (sponsored), ccTLD (country code)

**Authoritative Nameserver**

- Usually the last step in finding an IP address
- Configured by the domain owner
- Provides the officially answer for a DNS query

# How DNS Works?



RSAConference2022

# DNS Encryption

# DoH (DNS-over-HTTPS)

- Runs on port 443
- Traffic is hidden from network admin
- Larger packet sizes
- Higher latency, more coding
- Good for privacy

# DoT (DNS-over-TLS)

- Runs on port 853
- Traffic is visible to network admin
- Smaller packet sizes
- Lower latency, less coding
- Not great for privacy

# DNSSEC (Domain Name System Security Extensions)

- DNSSEC extends the DNS protocol by adding cryptographic authentication for responses received from authoritative DNS servers.
- DNSSEC is the only protocol with protects against cache poisoning.

# DDR (Discovery of Designated Resolvers)

- Clients connecting to a new network don't have any way of automatically finding encrypted DNS servers that might be available.
- DDR creates special, new, DNS records that point to servers using DoT or DoH.

RSAConference2022

# Is DNS security discussed at your organization?

RSAConference2022

# NSA and CISA Release Cybersecurity Information on Protective DNS

# Protective DNS: March 2021

- DNS lookups were unencrypted
- DoH is fine for home or mobile users
- Only use designated enterprise resolvers, disable others
- Balance of DNS security, privacy and governance

# PDNS Guidance Outlined from NSA and CISA

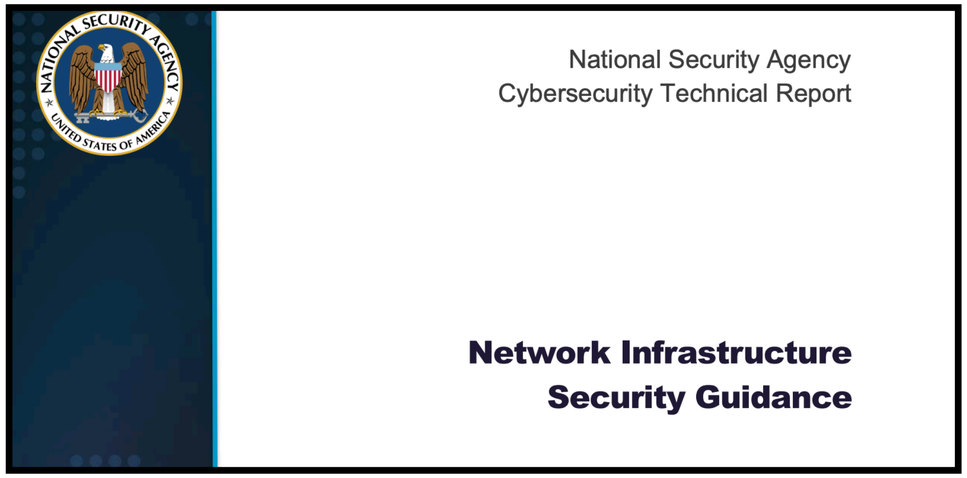
- Block:
  - Malware domains
  - Phishing domains
  - Malware DGA
- Supports:
  - Content filtering
  - SIEM integration
  - DNSSEC validation
  - DoH/DoT
  - Customizable policies
  - Hybrid architectures

# Why Protective DNS?

- DNS is ubiquitous
- DNS was not built with security in mind
- Bad actors use domain names
- Malicious domain names are often knowable

# Fast Forward: March 2022

- Zero Trust
- Multiple Defensive Layers
- Encryption and Secure Protocols



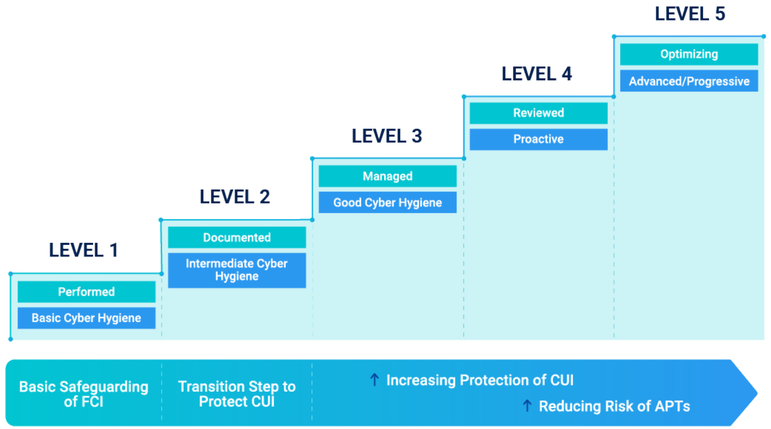

# CISA's Shields Up Program

- Reduce the likelihood of damaging cyber intrusion
- Take steps to quickly detect a potential intrusion
- Ensure the organization is prepared to respond
- Maximize the organization's resilience to a destructive cyber incident

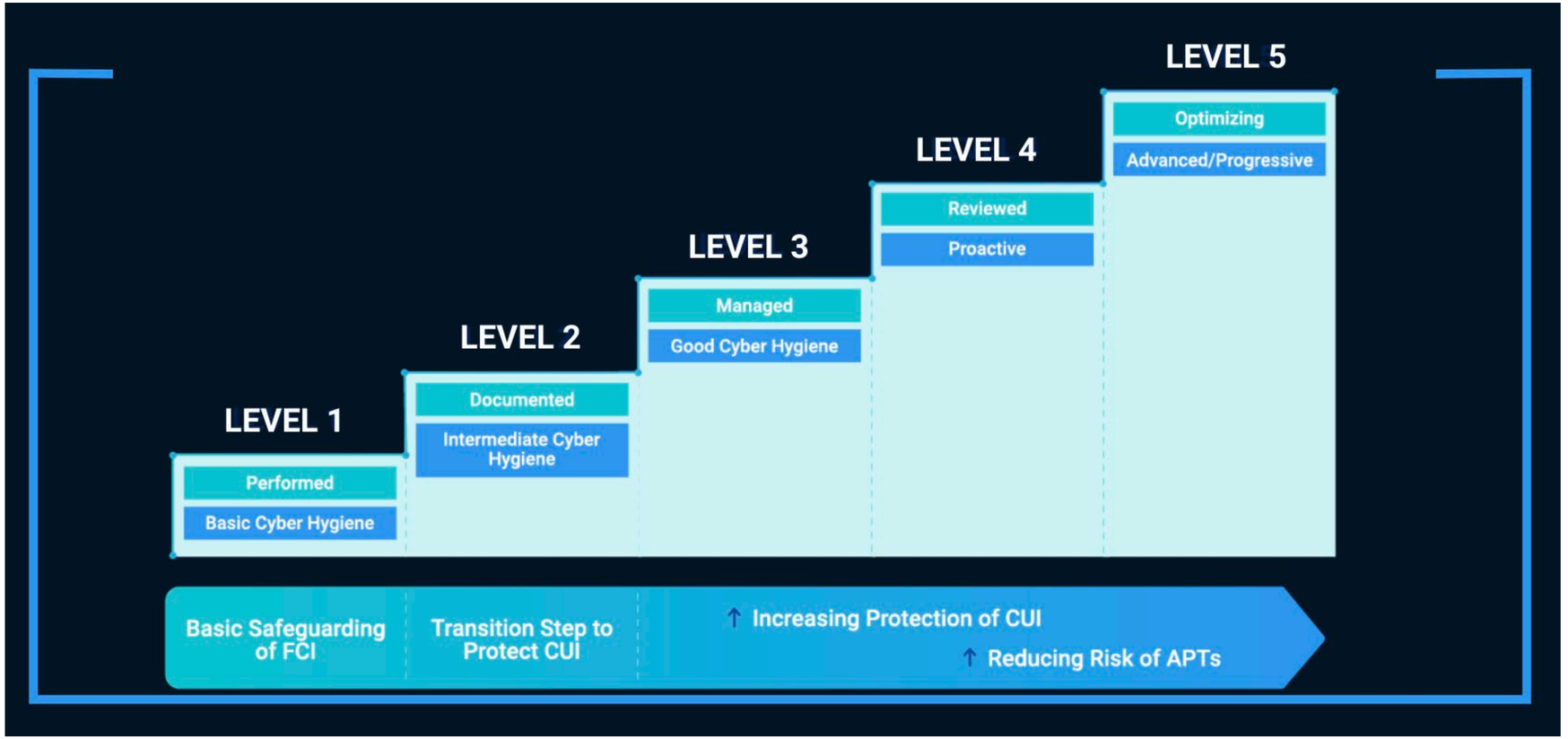
*"90% of successful cyber-attacks start with a phishing email"*

# Driving further interest of PDNS & DNS Encryption

CISA
CYBER+INFRASTRUCTURE

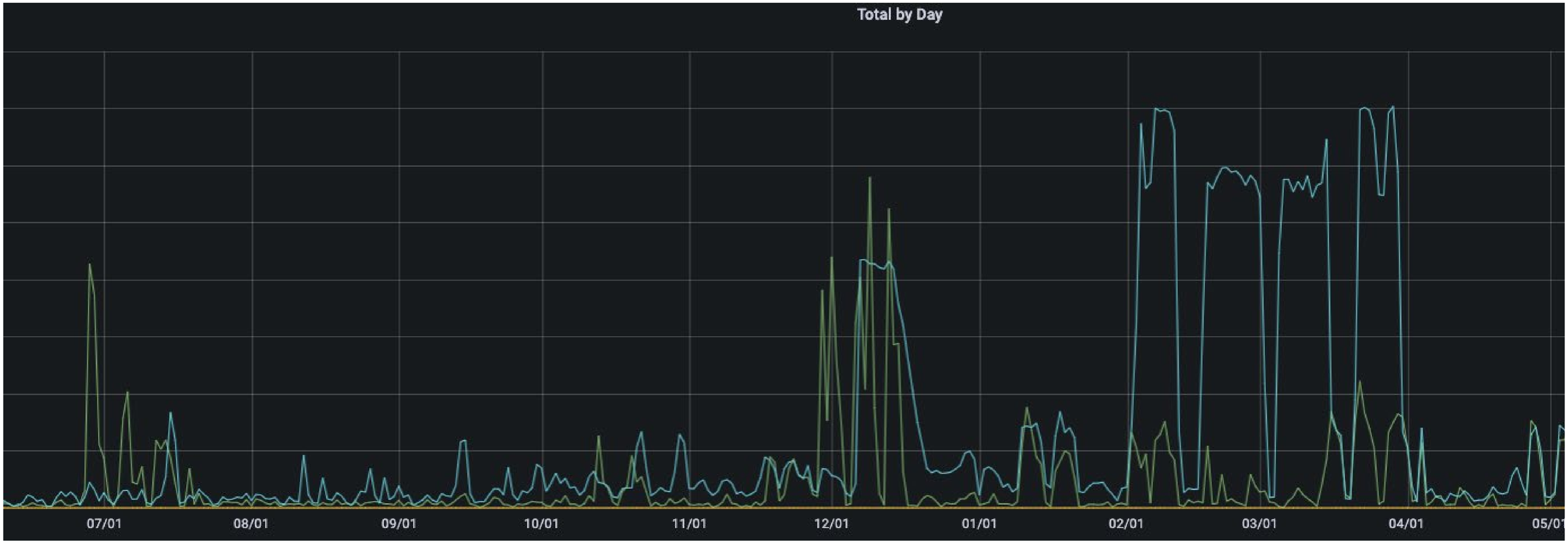


# CMMC 1.0 and CMMC 2.0 (coming soon)




CMMC 2.0 to include aspects of protective DNS

# Malicious Sites containing “gov”




Almost 500% increase in .gov domains seen in traffic over one year

RSAConference2022

# Zero Trust

# Defining Zero Trust

| | | |
|---|---|---|
| **Zero** Trust | → | Trust **Nothing** |
| Zero Trust **Access** | → | Who (and What) Needs **Access** |
| Zero Trust **Network** Access | → | Which **Applications** You Should Allow |

# Now What? How to Apply - Part 1

- **Next week** ask how does your DNS work:
  - How is your DNS configured and who is managing your DNS?
  - When and why were settings configured?
- Over the next **three months:**
  - What DNS are you using for authoritative and recursive? (Public, private, independent?)
  - Do you have encryption, filtering, VPNs, firewalls that are relying on DNS?
  - Are you using tools like AD, Hyper-V, specific hardware, etc. that will impact DNS settings?

# Now What? How to Apply - Part 2

- Within **six months** you should:
  - Regularly audit and review your DNS security settings at least quarterly
  - Defining roles and responsibilities around DNS
  - Consider tools supporting protective DNS:
    - Enabling DoT and/or DoH in your environment
    - Blocking malware/phishing/ransomeware at DNS
    - Aggregating your DNS queries with your SIEM

# In Summary

- DNS is critical infrastructure
- DNS has become a major attack vector for bad actors
- DNS best practices are heading towards protective DNS
- Patch your leaks!

Contact: sstaden@dnsfilter.com

RSAConference2022

# Protective DNS, DNS Encryption, & Zero Trust

## Tackling NSA Guidance

## Q&A