What's Going on in the World of DNS

Current Topics in the DNS Operations Community

David Huberman
ICANN's Office of the CTO

DD Month 2017

Topics

- Applications Doing DNS
- Public DNS & Resolver Centrality
- DNS as an Attack Vector
- Update on the KSK Rollover

Applications Doing DNS

DNS Resolution's Traditional Model

Recursive resolvers are typically run by the service provider:

- The ISP
- The University
- The Company

And when the service provider controls the recursive, many of the *needs* of the service provider are met. For example:

- Regulatory compliance
  - Searches for certain key words that the government requires be logged and/or not responded to
- Malware Protection
  - Service providers know to block access to certain sites that seek to harm the end users

It Works in Public DNS, too!

Increasingly, recursive resolvers are operated by public DNS providers:

- Google: 8.8.8.8
- Cloudflare: 1.1.1.1
- TWNIC: 101.101.101.101
- … and many, many others

The same goals can still be met:

- Regulatory compliance
  - Governments serve legal process on public DNS operators to respect their local laws
- Malware Protection
  - Some public DNS providers (like Quad9: 9.9.9.9) block access to bad sites as part of their value proposition

But These Resolution Models have Security Concerns

“The DNS is one of the most significant leaks of data about an individual’s activity on the Internet.”
– Sara Dickinson, Sinodun

- DNS queries are sent in cleartext (UDP or TCP) which means anyone doing passive monitoring of our DNS learns everything we are asking
- Queries contain the domain names being asked about, but also contain *metadata* about domains for things like the chat services we are using and the domains of our email contacts
- Some VPNs don't include the resolvers the user might have chosen, and in that case the DNS traffic will be exposed in unencrypted channels
- DNS responses from the recursive to the stub are the most vulnerable to being censored or re-written

One Solution is to Encrypt

- Encryption provides assurances:
  - Queries cannot be surveilled
  - Eliminates man-in-the-middle attacks
- In 2017 and 2018, the IETF standardized two encryption technologies for DNS:
  - DNS-over-TLS (DoT)
  - DNS-over-HTTP (DoH)

DNS-over-TLS (DoT)

- DoT (RFC 7858) takes advantage of Transport Layer Security (TLS) to encrypt DNS traffic between the stub resolver and the recursive resolver, giving users authentication and confidentiality for their DNS queries
- Runs on TCP/853 instead on UDP/53 (making it easy to discover and filter)
- Useable by any application taking advantage of TLS
  - Email
  - Mobile apps

DNS-over-HTTPS (DoH)

Protocol Goals (RFC 8484)

- Who do you trust?
  - “I trust my bank to give them my money.”
  - “I trust my bank enough to do online banking with them.”
  - “Maybe my bank is the most trusted vendor I should use for recursive resolver service.”
- The user decides who she trusts the most with her DNS traffic, and she configures the DoH application to use a trusted DoH resolver
- Runs on TCP/443 and is co-mingled with *web traffic* in a single HTTPS connection, making it much harder to discover and filter

But This New Model Prompts Some Concerns

Service providers have a new paradigm to negotiate:

- No longer able to rely only on DNS to meet regulatory compliance and filtering goals
- What happens if it does not work?
  - The user configures her web browser to use a DoH resolver. For whatever reason, DNS resolution stops working properly. A major concern for service providers is that the user now calls them and asks for help.
- ISPs do significant business working with parents on parental controls. When applications do their own DNS, a lot of these parental controls no longer work.
- ISPs often receive court orders to block certain sites. DoH/DoT resolvers do not know about these court orders, and still resolve these sites.

Taking a Further Step Back: Policy Concerns

Stepping back from the service provider concerns, ADD introduces all new challenges for broader public policy:

- Which laws apply?
  - In the traditional model, the recursive resolver providing the answers to the end user device is generally found in the same country as the user. Applications doing their own DNS will often mean that the recursive resolver is in a different country, which means a different legal jurisdiction.
  - Very important when you think about complex topics like content filtering laws and end user data privacy regulations

Taking a Further Step Back: Policy Concerns

Stepping back from the service provider concerns, ADD introduces all new challenges for broader public policy:

- Who gets to determine the resolver?
  - The DoH protocol was designed to allow the end user to decide who they trust most for recursive DNS service. But nothing stops the application maker from deciding *for the user* what resolver will be used.
  - What if the application maker is not honest and is purposely using a resolver which steers queries away from their intended sites and instead, provides DNS answers to sites that the application maker can profit from?
  - What if the resolver operator is monetizing DNS data without the user's consent?
  - Bad or dishonest implementations of ADD *disempower* end users, and do so in a context that most end users know nothing about: recursive DNS resolution

Taking a Further Step Back: Policy Concerns

Stepping back from the service provider concerns, ADD introduces all new challenges for broader public policy:

- Where do we discuss these broad public policy issues?
  - ICANN?
  - CENTR?
  - Network operator forums?
  - IETF?
  - CAB Forum?
  - Regulators?
- The answer is probably all of the above. Through community consultation and collaboration we can identify issues and find resolutions.

Parting Thoughts on Applications Doing DNS

- Applications doing their own DNS with DoH is new, but ADD in general is already being implemented in web browsers and mobile applications
- DNS privacy – especially end user DNS data privacy – is a major regulatory and societal concern
- Encrypting DNS data with TLS or HTTPS is good for addressing privacy concerns
- But implementation details matter, and there are a lot of public policy concerns for how ADD could be implemented in a way that has negative effects for end users, for service providers, and for regulators

Public DNS & Resolver Centrality

Public DNS

APNIC recently conducted some measurements into resolver centrality

- They asked: “How many recursive resolver operators does it take to cover 50% of Internet users?”
- Their answer was: “About 8 or 9”
- Google Public DNS (8.8.8.8) answered about 33% of the queries
- Other big global resolvers included China Unicom, China Mobile, DNSpai, Comcast, and OpenDNS (Cisco Umbrella)

Centrality at ORG

The CTO of PIR recently publicly stated:

> *"Two dozen resolver systems are responsible for some 80% of all traffic seen at ORG servers, today. Somewhere between 15 and 20% of all end-user systems use Google Public DNS for resolution."*

The Centrality Dilemma

- The popularity of public DNS can be a good thing for a lot of network operators. But we have to keep in mind that centrality of recursive resolvers could mean that a relatively small number of organizations could make decisions that affect a lot of people.
  - e.g., supporting or not supporting a particular DNS protocol enhancement or a feature
    - DNSSEC might be a good example: Google DNS is responsible for a huge amount of DNSSEC validation happening.

- ”Over-centralized” recursive service prompts numerous concerns about the content being resolved:
  - What if a central resolver operator decides to do content filtering?
    - A nation-state with authority over a central resolver operator might exert control
    - Twitter, Facebook, and other mass media have tried in the past to implement automated content filtering. Arguably, that hasn’t worked so well. Now think about doing that at the DNS level, and you’re affecting a lot of people!
  - Or what if an operator decides to augment the namespace by adding their own TLD?

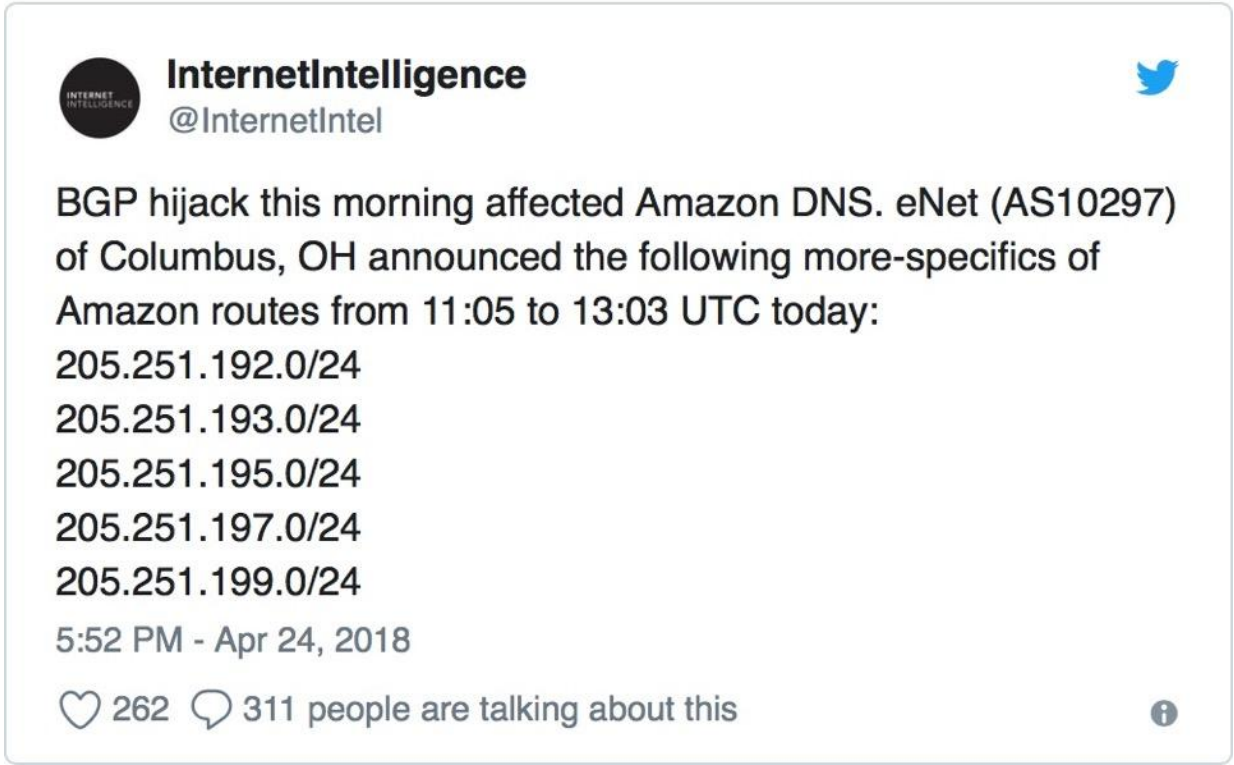
Centrality and Privacy

- If data privacy is the goal of efforts like DoH and DoT, then perhaps we should be worried that a large percentage of query traffic is resolved by the most popular recursive resolver providers
- Some of the most popular public DNS resolvers are homed in countries where there are either weak data privacy laws, or there are laws that allow the home government to demand query data from the providers

DNS as an Attack Vector

MyEtherWallet.com

- Route hijacking of AWS auth DNS addresses to re-direct user queries to a name server the criminals control
- NS now gives out IP address to a fake MyEtherWallet.com website
- Users input login credentials into the fake site
- Attackers steal ~USD21,000,000 of cryptocurrency from the real MyEtherWallet.com using the harvested login credentials

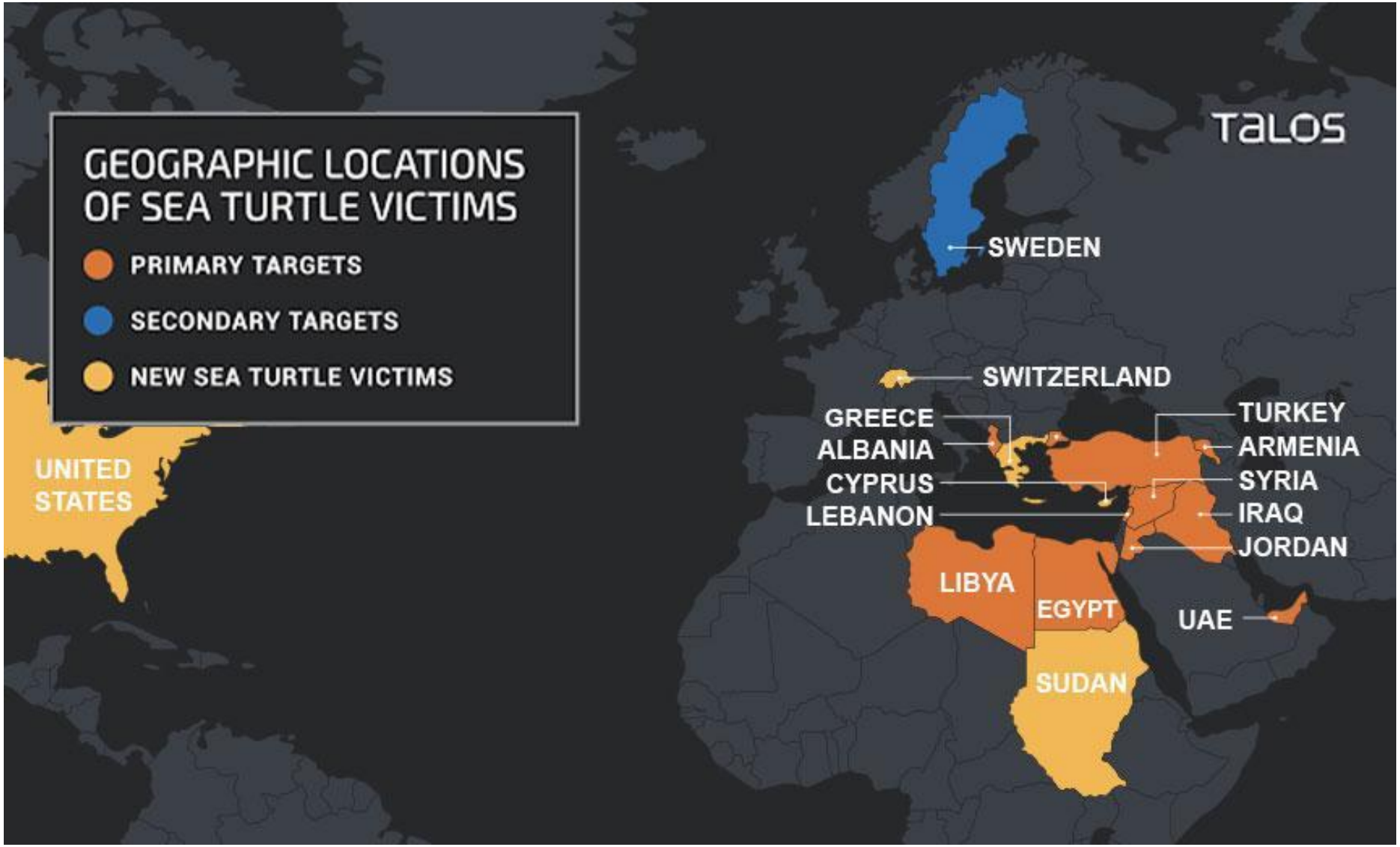


DNSpionage & Sea Turtle

“Military cyber-offense prepositioning” – gathering the intelligence needed to launch military cyber attacks

- Apparently targeting ~40 organizations in 13 countries in North Africa and the Middle East
- Apparently targeting:
  - National security organizations
  - Ministries of foreign affairs
  - Energy companies

Cisco Talos's View of Sea Turtle



Methodologies

- 10-minute attacks to avoid detection
- Compromised EPP credentials
- Re-write authoritative NS
- Obtain easy-to-get certs from Let’s Encrypt or Comodo
- Keep harvesting data to build credentials repository
- Re-write IMAP info
- Capture email credentials
- Capture email, calendaring, vcards

Improvements

- RPKI
- Consider making IMAP accessible only from within a trusted LAN
- Registry Lock
- DNSSEC as a path to DANE

Update on the KSK Roll

The KSK Rollover

- 11 October 2018 ICANN changed the KSK
- The multi-year process to get to 11 October taught us that we don't fully understand the effects of rolling the KSK
  - We saw evidence a small number of operators experienced downtime. But they're not participating in DNS technical community forums, so we don't know why they went down.
  - DNSKEY queries greatly increased until KSK-2010 was removed from the root zone
- Next steps:
  - The IANA owns the decision making on this and will propose a strategy for public comment in the near future. Some considerations include:
    - Roll it yearly? 2 years? 5 years?
    - Oh and by the way, at some point in the future we need to consider rolling the algorithm used to compute the key signatures

Engage with ICANN – Thank You and Questions

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann