DNS Ecosystem Security: We’re all in this together

Session: “DNS SECURITY: PROMOTING SECURITY AS A STATE OF MIND”

David Conrad
Chief Technology Officer, ICANN
EEDNS Forum
11 October 2019
It Takes a Village… (for the DNS to exist)

- **ICANN Community**: Defines the policies by which top-level names are created/managed
- **ICANN Org**: Implements the policies defined by the community, including updates to TLDs
- **Registries**: Responsible for the definition and proper operation of their part of the namespace
- **Registry Back End Operators**: Implements the operational requirements of the registries
- **Registrars**: Acts as the interface to the registries for registrants
- **Authoritative Server Operators**: Runs the servers that publish domain names on the Internet
- **Hosting Providers**: Runs the servers pointed to by registrant’s domain names
- **Registrants**: Obtains the domain names and points those names at servers
- **Resolver Operators**: Provides the service that translates names into addresses
- **Network Operators**: Allows packets to flow to/from the services end users want
- **End users**: Look up domain names to gain access to services
- **Internet Engineering Task Force (IETF)**: defines/modifies the DNS protocol
- **Software Developers**: Implements DNS standards into DNS servers
- **Software Distributors**: Distributes DNS software to various operators
- **Governments**: Provides the regulatory environment in which network services operate
- **Et cetera, et cetera**: People I’m forgetting…
And Sometimes the Village is Under Attack…

- The DNS is a wonderful target for attackers
  - Core part of the Internet infrastructure
  - The first service nearly all Internet transactions start with
  - Rarely filtered or even monitored
    - “It just works”

- Compromise the DNS and the attackers can gain control of pretty much **everything**

- Block the DNS and attackers can block pretty much **any** service

- Make use of the DNS and attackers can bypass filters, controls, and other mitigations
Some of the Potential Target Points of the DNS Ecosystem

- **Man in the middle and information exfiltration**
- **Cache poisoning**
- **Modified Data**
- **Secondary**
- **Spoofing**
- **Corrupted data**
Implications of those vulnerable points

http://www.gmail.com/

Peak Attack Sizes Through March 2018

Ransomware attacks

Imperva 2019 Cyberthreat Defense Report

A More Secure DNS Ecosystem

Encryption (DoT & DoH)
DNSSEC
Internal Security Hygiene
Registrant Security Hygiene
It Takes a Village… (for the DNS and Internet to be secure)

- **ICANN Community**: Defines the policies by which top-level names are created/managed
- **ICANN Org**: Implements the policies defined by the community, including updates to TLDs
- **Registries**: Responsible for the definition and proper operation of their part of the namespace
- **Registry Back End Operators**: Implements the operational requirements of the registries
- **Registrars**: Acts as the interface to the registries for registrants
- **Authoritative Server Operators**: Runs the servers that publish domain names on the Internet
- **Hosting Providers**: Runs the servers pointed to by registrant’s domain names
- **Registrants**: Obtains the domain names and points those names at servers
- **Resolver Operators**: Provides the service that translates names into addresses
- **Network Operators**: Allows packets to flow to/from the services end users want
- **End users**: Look up domain names to gain access to services
- **Internet Engineering Task Force (IETF)**: defines/modifies the DNS protocol
- **Software Developers**: Implements DNS standards into DNS servers
- **Software Distributors**: Distributes DNS software to various operators
- **Governments**: Provides the regulatory environment in which network services operate
- **Et cetera, et cetera**: People I’m forgetting…
We’re All in This Together

- Vulnerabilities in the DNS ecosystem can impact everyone
  - Compromising domain names to gain control over entire organizations (or countries!) is currently an attack of choice

- Securing the DNS ecosystem requires cooperation among a wide array of actors and stakeholders.
  - Some actions are easy, but require diligence, e.g., basic cyber hygiene
  - Some actions should be easy, but turn out not to be, e.g., deploying DNSSEC
  - Some actions are hard, e.g., changing behavior

- We need to work together to make progress
Thank You and Questions

Visit us at icann.org
octo@icann.org

@icann
facebook.com/icannorg
youtube.com/icannnews
flickr.com/icann
linkedin/company/icann
slideshare/icannpresentations
soundcloud/icann