DNS Ecosystem Threats & Challenges

At Large Capacity Development – ICANN 65

26 June 2019
Patrick Jones
Senior Director, Global Stakeholder Engagement
ICANN
Attacks in the news

(Source: Wired, Dec 2017)
Attacks in the news

NASA Lab Hacked Using A $25 Raspberry Pi Computer

By Manisha Priyadarshini - June 21, 2019
Attacks in the news

A WORLDWIDE HACKING SPREE USES DNS TRICKERY TO NAB DATA

(Source: Wired, Feb 2019)
ICANN WARNS OF ‘ONGOING AND SIGNIFICANT’ THREAT TO DNS
Attacks in the news (5 June 2019)

ICANN @ICANN · 7h
Beware of Phishing Schemes
There’s a recent attempt to harvest your email address using a website and URL that looks like go.icann.org/wWVOw8. Double-check URLs before clicking. Get tips on how to protect yourself and report phishing attempts here >>
go.icann.org/2JZLOX9
Connected devices, Internet of Everything
Data is an attractive target
Common Elements Inside a Network

Mail servers
  o E-mail
  o Calendaring
  o Contacts

Database servers
  o Asset data
  o Customer data
  o Employee data

File servers
  o Financial information
  o Design documents
  o Organizational processes and procedures
What Underpins These Elements?

- **Identity Management**
  - Authorization
  - Authentication
  - Key Management

- **Systems Engineering**
  - Hardware
  - Software
  - Patching

- **Routing Infrastructure**
  - External & Internal Connectivity
  - IP addressing
  - DNS

- **Governance**
  - Security Policy
  - Data Storage
  - Data Retention
Common Types of Cybercrime

Phishing
“The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.”

Malware
“Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system”
- e.g., ransomware, key loggers, root kits, viruses

Botnets
“A network of private computers infected with malicious software and controlled as a group without the owners' knowledge”
What is DNS abuse?

- No globally accepted definition, variants include
  - Cyber crime
  - Hacking
  - Malicious conduct

- Threats to the DNS often fall under three categories:
  - Data corruption, denial of service, & privacy violations
DNS abuse and misuse

- DNS abuse refers to anything that **attacks** or **abuses** the DNS infrastructure, or

- DNS misuse refers to **exploiting** the DNS protocol or domain name registration processes for **malicious purposes**
DNS Ecosystem Technical Threats

Source: Detecting Internet Abuse by Analyzing Passive DNS Traffic (Sadegh Torabi, Amine Boukhouta, Chad Assi, and Mourad Debbabi)

(Source: Merike Kaeo presentation at FIRST, June 2019)
ICANN’s Role?

- Large scale attacks appear to be growing, and because of their surface area, involve:
  - Sovereign governments
  - Multi-national companies
  - International law enforcement
  - Widespread news coverage

- Other (smaller scale) cybersecurity incidents happen daily

- The ICANN Community and members of the ICANN Org have a role before, during, and after cybersecurity incidents
Recent Domain Registration Hijacking
Increased level of targeted attacks

DNSpionage (2018) & Sea Turtle (present day)

- “Military cyber-offense prepositioning” – gathering all the intelligence needed to launch military (or very well-organized) cyber attacks

- Initially 40 organizations in 13 countries in North Africa and the Middle East

- Targeting primarily:
  - National security organizations
  - Ministries of foreign affairs
  - Energy companies

- Infiltrating DNS and e-mail and certificate authorities
  - With all these elements under control, the attackers can obtain and decrypt documents
Sea Turtle

(Source https://blog.talosintelligence.com/2019/04/seaturtle.html)
DNSespionage timeline

1. November 2018 – Cisco Talos identifies campaign targeting Lebanon & UAE domains, businesses
2. Attackers compromised users with infected websites & malware
3. Fireeye report January 2019
5. Netnod Statement 5 February 2019
6. ICANN Alert 15 February 2019
7. Sessions at ICANN 64 in Kobe, March 2019
ICANN’s Role: Before a Cybersecurity Incident
ICANN’s Bylaws place a strong emphasis on cybersecurity

“The mission of the Internet Corporation for Assigned Names and Numbers ("ICANN") is to ensure the stable and secure operation of the Internet's unique identifier systems”

Our bylaws include many commitments, including:

“Preserve and enhance the administration of the DNS and the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet”
Revised ICANN Strategic Plan 2021-2025

• 1) Strengthen security of the Domain Name System and the DNS root server system

• 3) Evolve the unique identifier systems in coordination and collaboration with relevant parties to continue to serve the needs of the global Internet user base

Throughout the ICANN ecosystem there are numerous **communities** developing policies and procedures to improve SSR:

- **GAC’s Public Safety Working Group (PSWG)**
  - PSWG “focuses on aspects of ICANN’s policies and procedures that implicate the safety of the public” including developing the “DNS Abuse and Cybercrime mitigation capabilities of the ICANN and Law Enforcement communities”

- **Security and Stability Advisory Committee (SSAC)**
  - SSAC engages in ongoing threat assessment and risk analysis of the unique identifier system to assess where the principal threats to stability and security lie

- **Root Server System Advisory Committee (RSSAC)**
  - Advises the ICANN Board and community on matters relating to the operation, administration, security, and integrity of the Root Server System
Relationships based on contracts
ICANN subsidiary **Public Technical Identifiers (PTI)** is responsible for the operational aspects of coordinating the Internet’s system of unique identifiers

- **Number Resources**
  - Allocate IPv4, IPv6, and AS numbers to the RIRs

- **DNS Operations**
  - Maintain the root zone for forward DNS
  - Administer the .ARPA zone for reverse DNS
  - Maintain the trust anchor for **DNSSEC**

- **Protocol Parameter Registries**
  - Coordinate over 3,000 registries for IETF protocols
Domain Name System Security Extensions (DNSSEC)

- To help prevent DNS abuse, DNSSEC introduces cryptography that provides assurances to users that DNS data they are seeing is valid and true
- Domain name registrants **SIGN** their DNS data
- DNS operators **VALIDATE** all DNS data passing through DNS resolvers
ICANN’s Role: During a Cybersecurity Incident
Stopping an ongoing cyberattack requires coordinated responses from:

- Network operators
- Global law enforcement agencies
- National Computer Incident Response Teams (CIRTs)
- Registries
Capacity Development
PTA & ICANN Hold a Workshop on DNS Abuse and Misuse

Posted 5 months ago by Press Release

(Source: https://propakistani.pk/2019/02/07/pta-icann-hold-a-workshop-on-dns-abuse-and-misuse/)
ICANN-supported DNSSEC Trainings in the regions

- DNSSEC for regulators/decision-makers and businesses
- Hands-on training
- Train-the-trainer program
- Supporting local deployment by TLD managers, registrars and encouraging validation by ISPs, network operators
# Impact of Trainings

<table>
<thead>
<tr>
<th>TLD</th>
<th>Description</th>
<th>DS Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>mc.</td>
<td></td>
<td>20-JUN-2019</td>
</tr>
<tr>
<td>gy.</td>
<td>University of Guyana</td>
<td>8-MAY-2019</td>
</tr>
<tr>
<td>sk.</td>
<td>SK-NIC, a.s.</td>
<td>19-APR-2019</td>
</tr>
<tr>
<td>dz.</td>
<td>CERIST</td>
<td>19-APR-2019</td>
</tr>
<tr>
<td>kw.</td>
<td>Communications and Information Technology Regulatory Authority</td>
<td>27-MAR-2019</td>
</tr>
<tr>
<td>md.</td>
<td>MoldData S.E.</td>
<td>14-MAR-2019</td>
</tr>
<tr>
<td>inc.</td>
<td>Intercap Holdings Inc.</td>
<td>18-JUL-2018</td>
</tr>
<tr>
<td>eA.</td>
<td>ICS-FORTH GR</td>
<td>30-JUN-2018</td>
</tr>
</tbody>
</table>

(Source: rick.eng.br/dnssecstat)
DNS Trainings

ccTLD and local community trainings
- Lithuania, Latvia
- Finland, Ghana
- Uzbekistan, Bahamas

Regional DNSSEC trainings
- Kuwait, India, Pakistan, Tonga, Vanuatu
- Mongolia, Philippines, Lesotho (with NSRC), Nigeria (with NSRC)
- Myanmar, Malaysia, Uzbekistan, Georgia, Morocco

Network Operator Group, Regional Internet Registry Meetings, Regional TLD Orgs
- TWNOG
- LKNOG
- LACNIC/LACNOG, GTER Brazil
- CaribNOG, MENOG
- CENTR, APRICOT
Showing impact of DNS abuse trainings

- Community collaboration related to Conficker
- Avalanche and Andromeda DGAs
- Registries using Expedited Registry Security Requests for a contractual waiver for actions taken to mitigate a security incident
- ICANN Coordinated Vulnerability Disclosure process
- Better coordination between LEAs and registries/registrars
- Or more informed decision makers on proper points of contact during an attack or incident
ICANN’s Role: After a Cybersecurity Incident
Post Mortem Activities

- Conferences to understand what happened and identify vulnerabilities
  - ICANN DNS Symposium
  - DNS-OARC (DNS Operations, Analysis & Research Center)
  - Network Operator Groups

- Adjust the ecosystem to *harden* the Internet against these attacks
  - Policy updates?
  - Contract updates?
  - Protocol (re-)development?

- Community capacity building
  - Network operators
  - Global law enforcement
Takeaway: the DNS Really Matters

- The DNS is no longer just a technical function of the network run by system administrators.
- The DNS is now a critical infrastructure used in every day communications (e-mail, web browsing, mobile applications) and is a gateway to all your internal systems.
- It is critical that policy makers and organization decision makers pay attention to their DNS infrastructure.

*If your DNS is compromised, all of your systems and networks are at serious risk.*
ICANN **strongly recommends** a set of cybersecurity measures to harden your local DNS infrastructure against attacks.

Steps include implementing strong cybersecurity practices for:

- Authorization
- Authentication
- Encryption
- Patching
- E-mail Security

One of the most important recommendations is to implement DNSSEC.

Please ask questions!
Engage with ICANN – Thank You and Questions

Visit us at icann.org

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