

DNS Ecosystem Threats & Challenges

At Large Capacity Development – ICANN 65

26 June 2019





Patrick Jones

Senior Director, Global Stakeholder Engagement
ICANN

GARRETT M. GRAFF SECURITY 12.13.17 03:55 PM

HOW A DORM ROOM *MINECRAFT* SCAM BROUGHT DOWN THE INTERNET



NASA Lab Hacked Using A \$25 Raspberry Pi Computer

By **Manisha Priyadarshini** - June 21, 2019



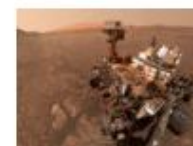
Images: [Shutterstock](#)

Latest Articles



**Raspberry Pi 4
LPDDR4 RAM A**

June 24, 2019



**NASA Rover Fir
Mars Hinting At**

June 24, 2019



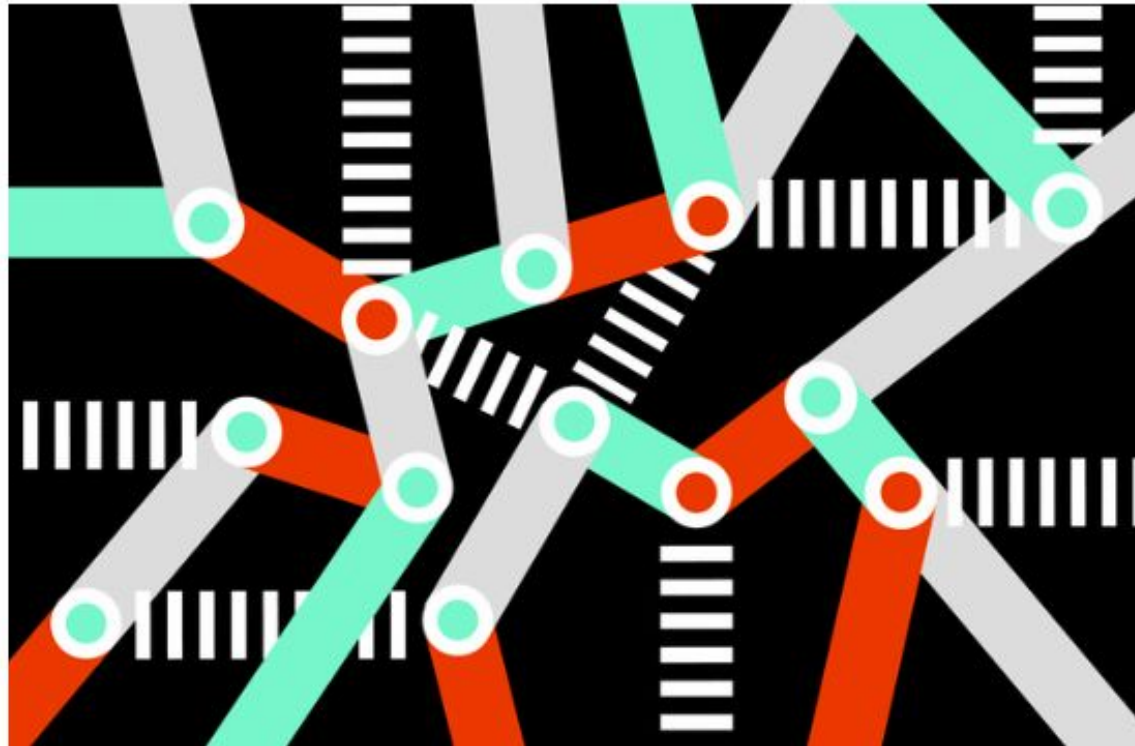
**Intel Is Working
Parallel C++ Pr
Language**

June 24, 2019



**Google Calend:
Phishing: How
From...**

A WORLDWIDE HACKING SPREE USES DNS TRICKERY TO NAB DATA



DECIIPHER

Security news that informs and inspires

Feb 26, 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

- E-mail
- Calendaring
- Contacts

Database servers

- Asset data
- Customer data
- Employee data

File servers

- Financial information
- Design documents
- 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

UNDER ATTACK

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”

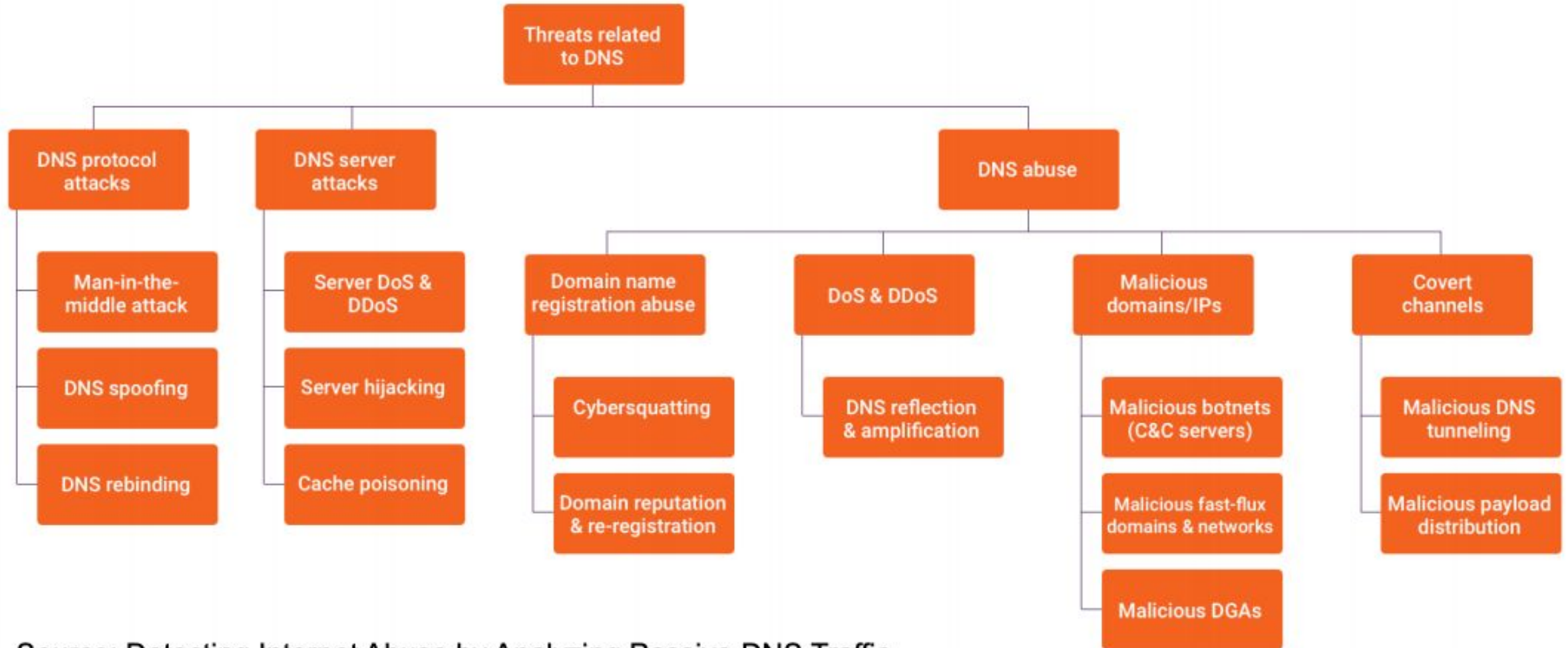
What is DNS abuse?

- 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
(Sadeqh Torabi, Amine Boukhtouta, Chad Assi, and Mourad Debbabi)

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

DNSSpionage (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

Primary and secondary victims



DN Sespionage 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
4. US DHS Emergency Directive 22 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:

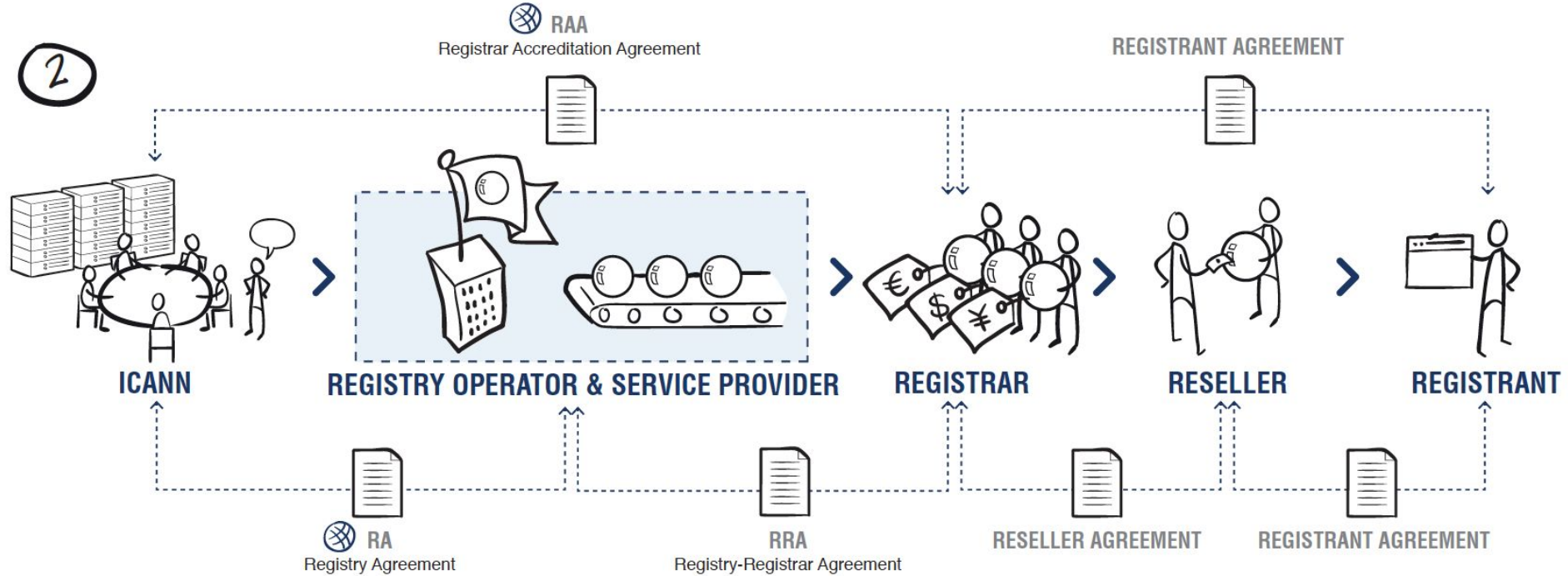
*“Preserve and enhance the administration of the DNS and the operational **stability**, reliability, **security**, global interoperability, **resilience**, and openness of the DNS and the Internet”*

- **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



Identifier Operations: PTI

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

Identifier Operations: What is DNSSEC?

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

Major Actors During a Cyberattack

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










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

TLD		Description	DS Date
mc.			20-JUN-2019
gy.		University of Guyana	8-MAY-2019
sk.		SK-NIC, a.s.	19-APR-2019
dz.		CERIST	19-APR-2019
kw.		Communications and Information Technology Regulatory Authority	27-MAR-2019
md.		MoldData S.E.	14-MAR-2019
inc.		Intercap Holdings Inc.	18-JUL-2018
ελ		ICS-FORTH GR	30-JUN-2018
vc.		Ministry of Telecommunications, Science, Technology and Industry	15-JUN-2018

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, MENO
- 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

Conclusion

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

Takeaway: ICANN Recommendations

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

See: <https://www.icann.org/news/announcement-2019-02-15-en>

Questions and Answers

Please ask questions!



Engage with ICANN – Thank You and Questions



One World, One Internet

Visit us at icann.org



[@icann](https://twitter.com/icann)



facebook.com/icannorg



youtube.com/icannnews



flickr.com/icann



linkedin/company/icann



slideshare/icannpresentations



soundcloud/icann