DNS Ecosystem Security Training

Patrick Jones

17 February 2020 – Internet.EE, Tallinn, Estonia

ICANN

Patrick Jones
Senior Director, Global Stakeholder Engagement
ICANN

Overview for today – 17 February 2020, Tallinn

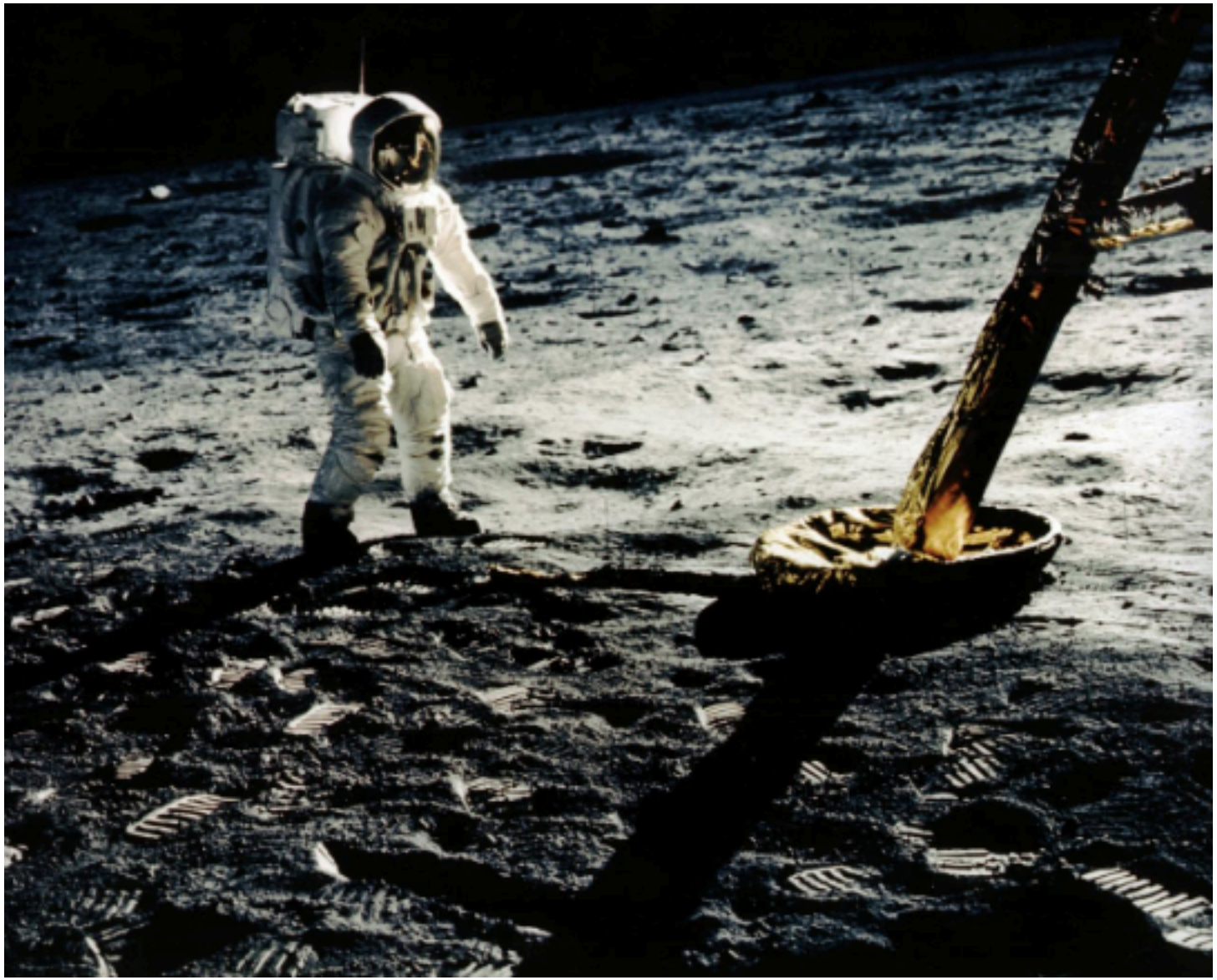
- Block 1 0930/1000-1100 (Break around 1100 or 1130)
  - Intro/Marking 50 Years of Milestones
  - Definitions
  - ICANN's Technical Functions & Current Projects
  - Why data is an attractive target
- Block 2 (1.5 hours)
  - Why data is an attractive target
  - Evolving Threat Landscape
  - DNS Security & DNS Abuse
  - Recent DNS Attacks and Mitigations
  - Securing DNS Infrastructure
  - Email Security

Overview for today

- Block 3
  - DNSSEC Developments
  - DNS Privacy
  - DNS over applications (DoT and DoH)
  - New Technologies & Emerging Issues
    - DNS & Internet of Things
    - Future KSK Rollover
  - Upcoming: GDD Summit & DNS Symposium in Paris

Marking 50 years of milestones

50th anniversary of the Moon Landing



(Source: NASA, Apollo 11, July 1969)

Computing Power

The latest USB-C chargers are apparently more powerful than Apollo 11's computer

Fly me to the Moon, and let me... charge... among the stars

By Jon Porter | @JonPorty | Feb 11, 2020, 11:45am EST

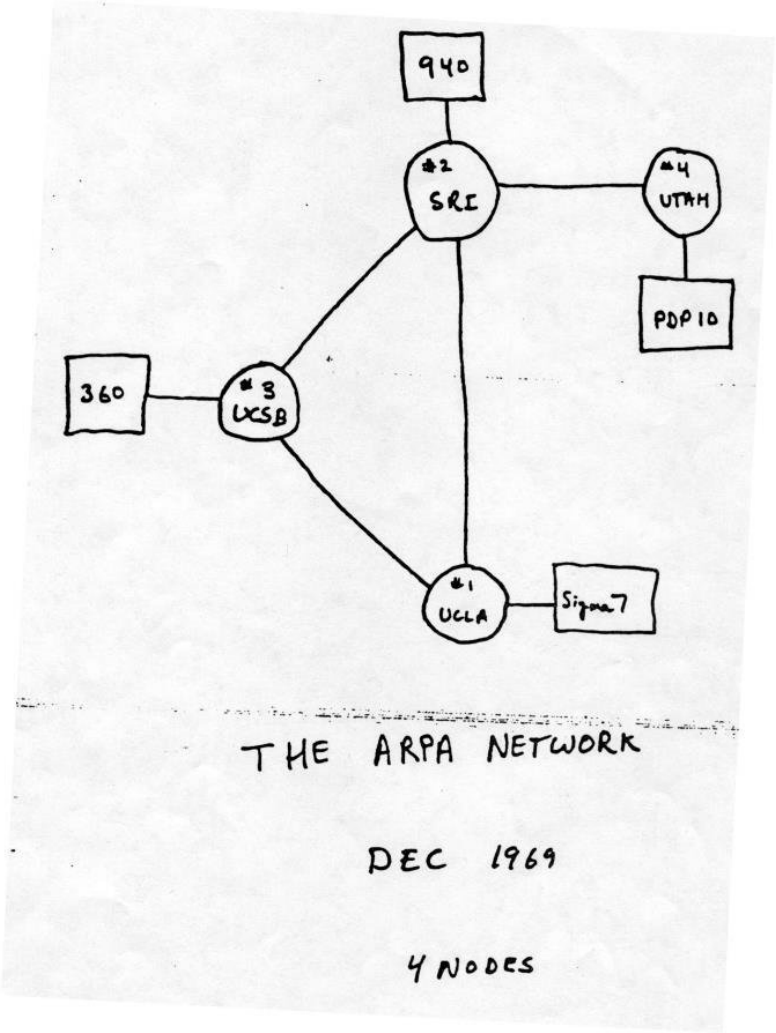
SHARE

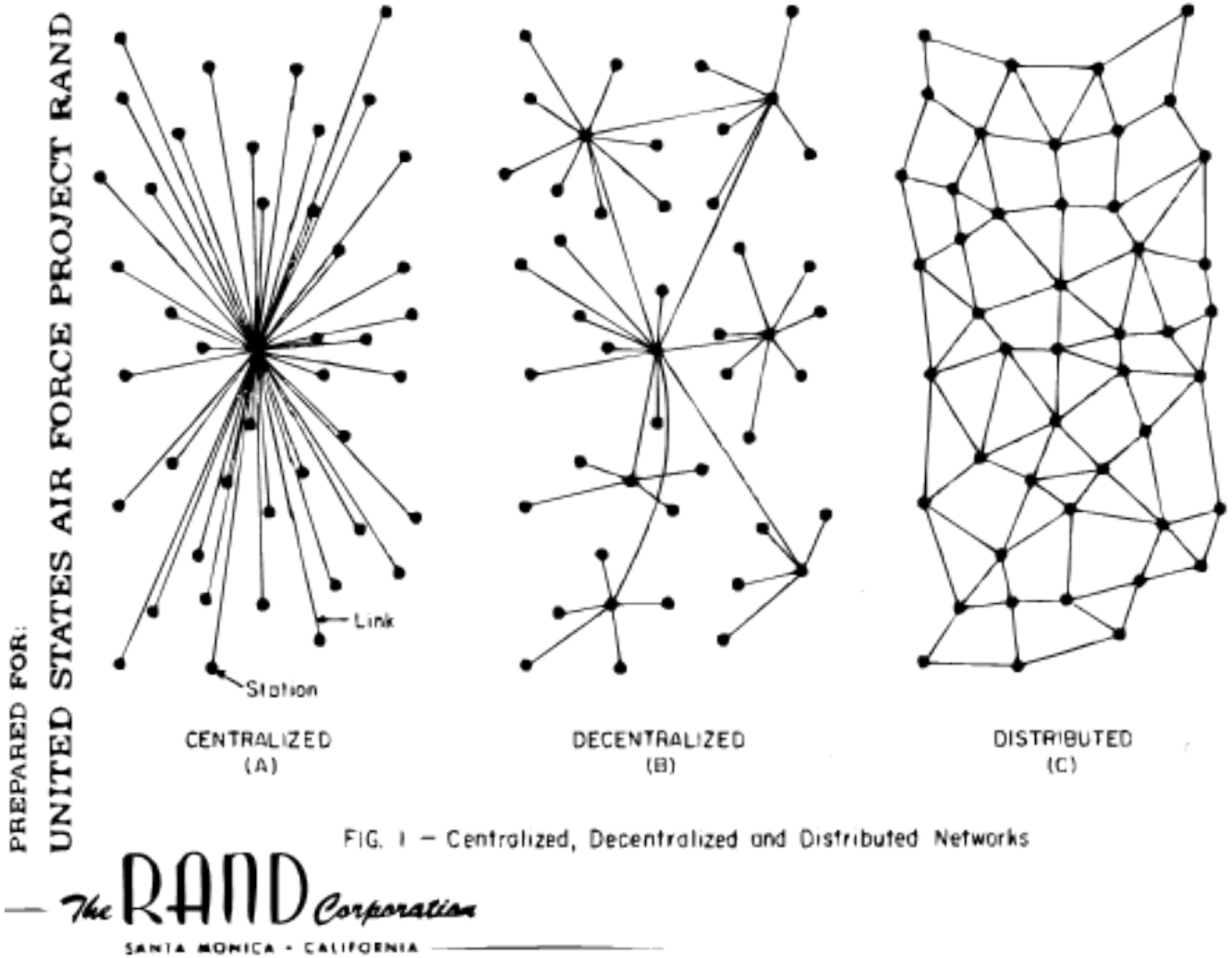
Here are

- If interested in the technical details, read: https://forrestheller.com/Apollo-11-Computer-vs-USB-C-chargers.html

(Source: The Verge, 11 Feb 2020)

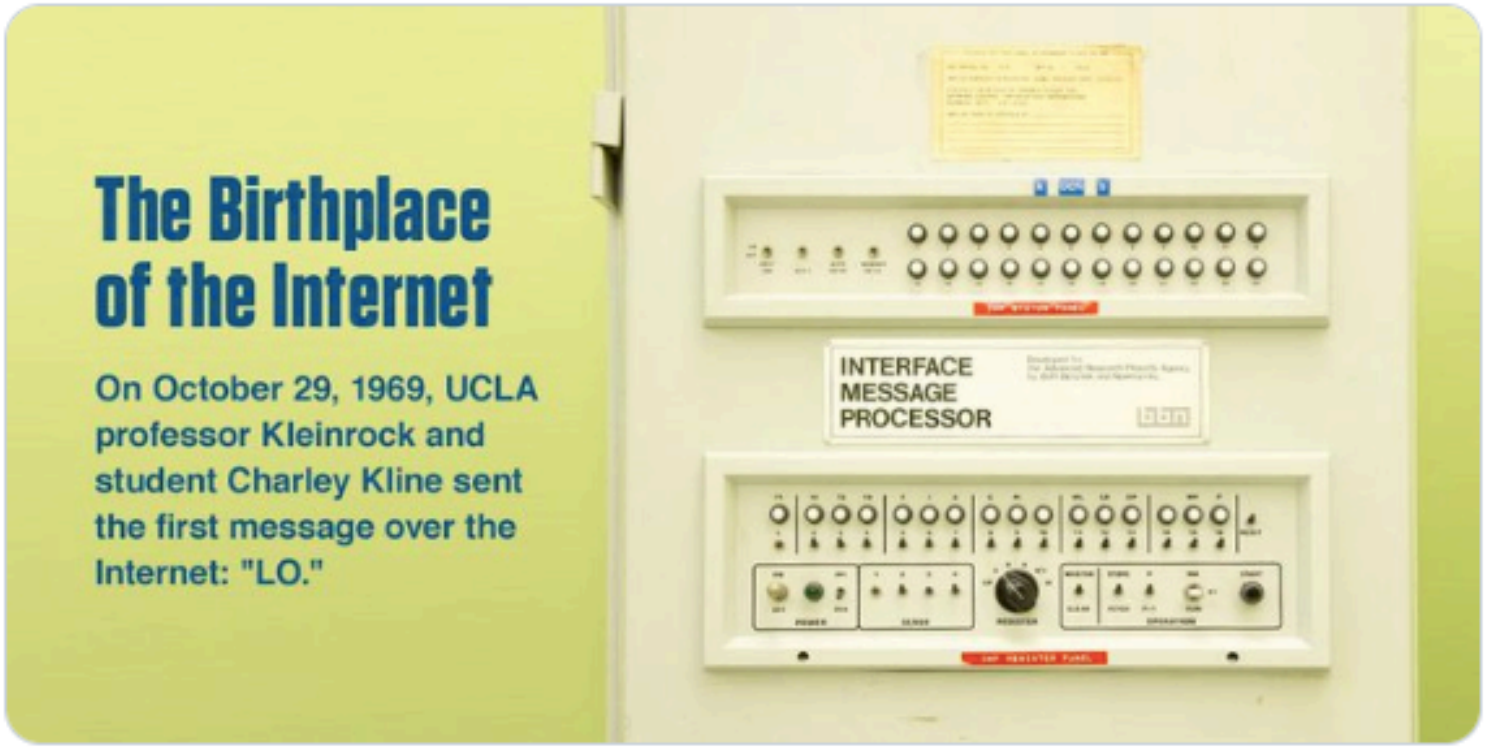
Internet at 50





Internet at 50

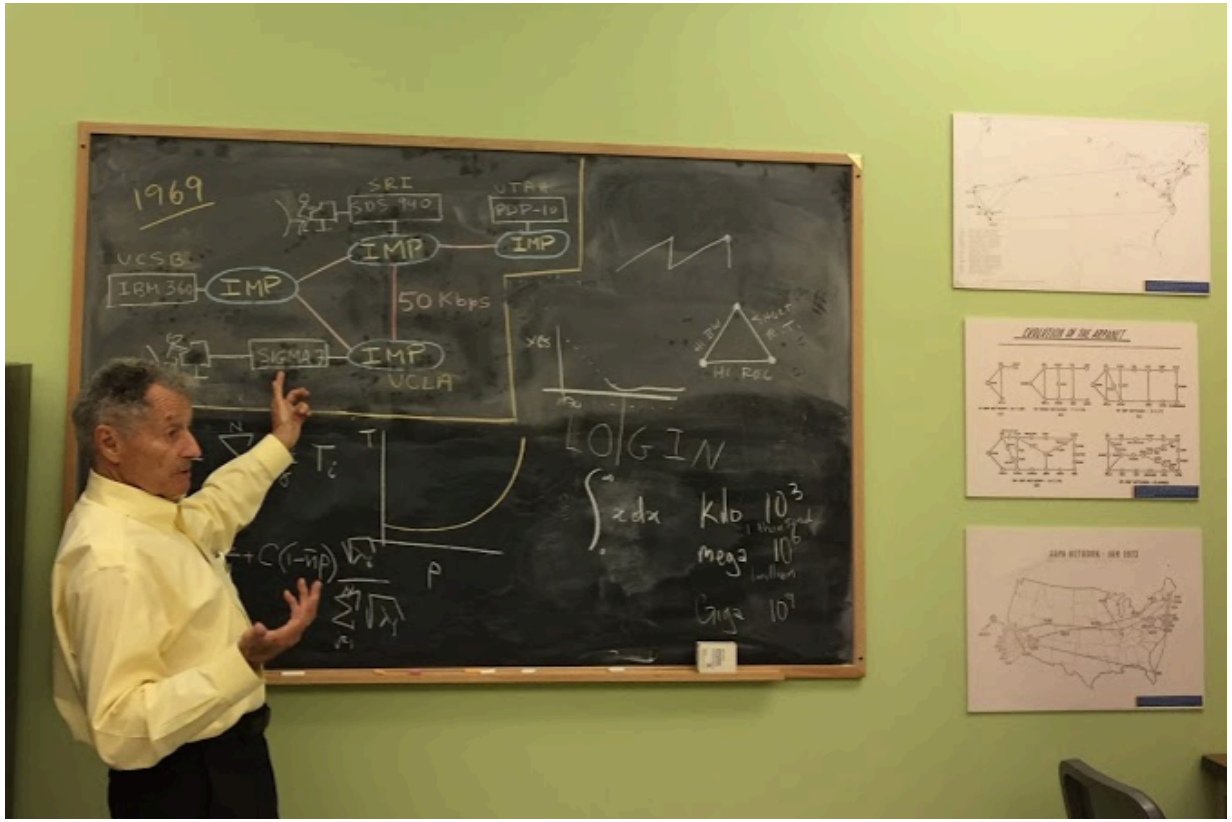
#Internet50 #UCLA100 #InternetDay
@UCLAengineering



8:00 AM · Oct 29, 2019 · Khoros

(Source: Twitter/UCLA)

Internet at 50



(Photos from 3420 Boelter Hall, UCLA, 25 Sept 2017)

2020 - Connected devices, connected everything

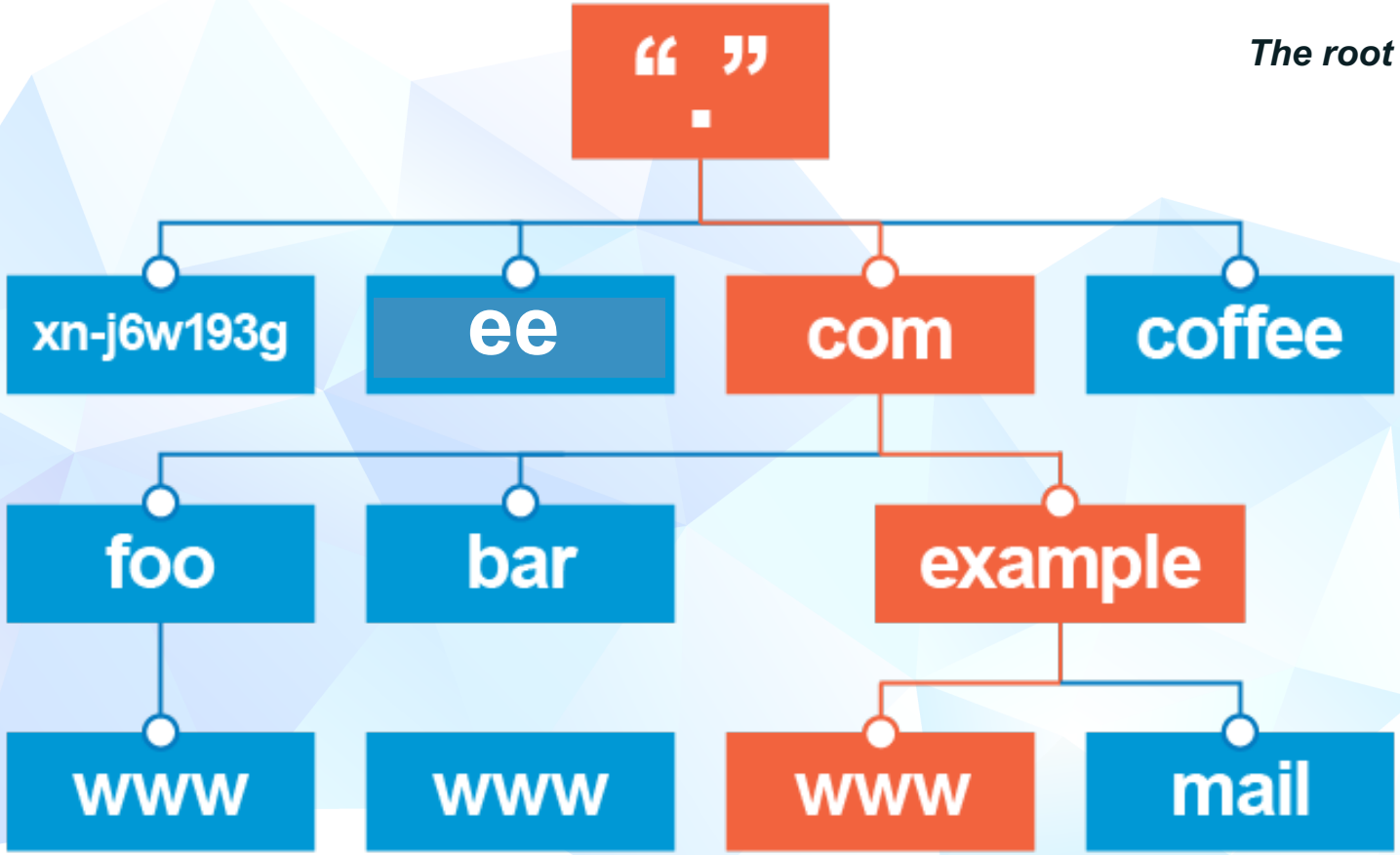
Definitions

What is the DNS?

- No single consistent definition – considered a combination of:
- **A commonly used naming scheme for objects on the Internet**
- **A distributed database representing the names & certain properties of these objects**
- **An architecture providing distributed maintenance, resilience & loose coherency for the database**
- **A simple query and response protocol implementing this architecture**

(Source: IETF BCP 219, https://tools.ietf.org/html/bcp219)

The Domain Name System (DNS)



The root

Top-level nodes

Second-level nodes

Third-level nodes

Root

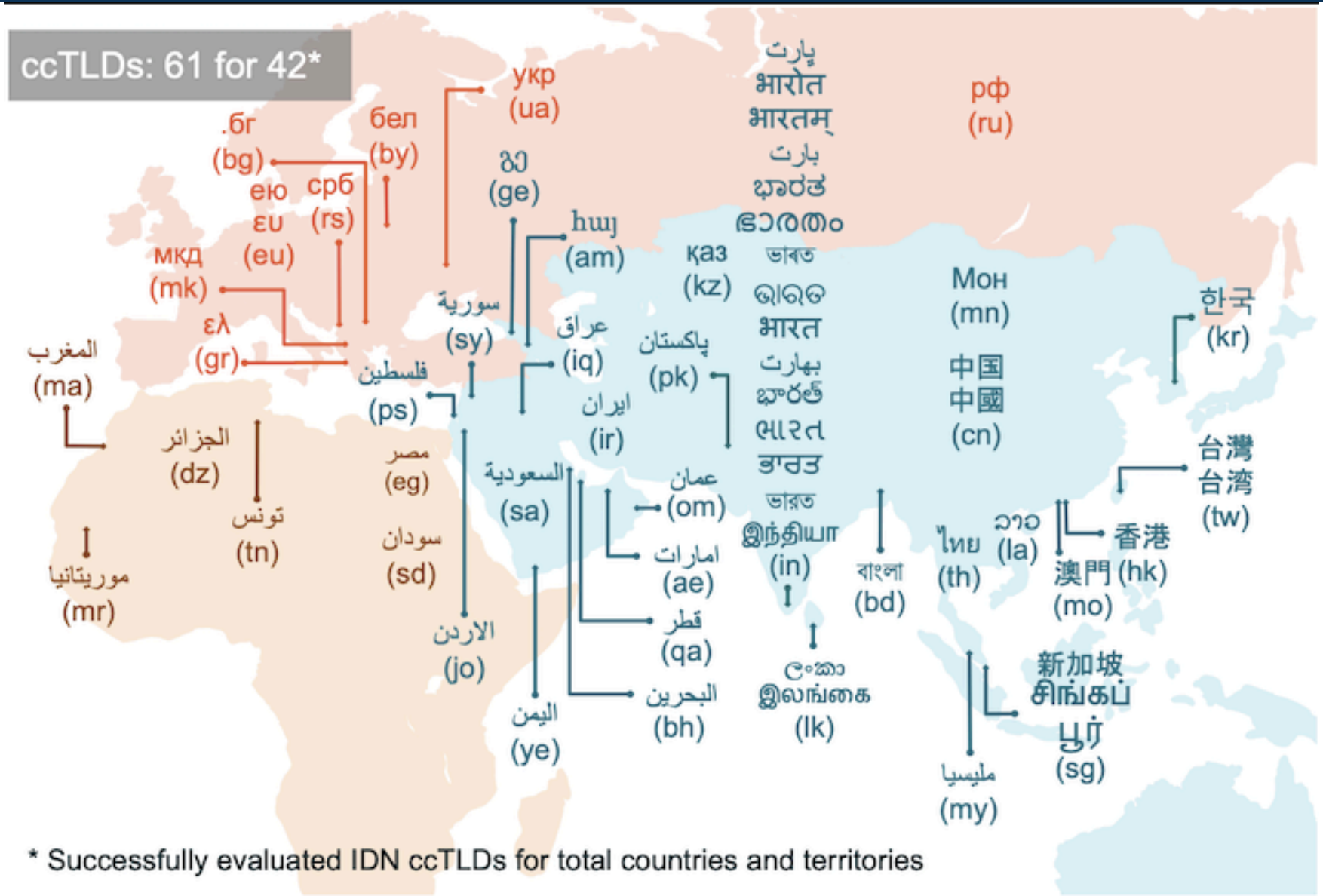
Top-level

Second level

www.example.com.

FQDN = **F**ully **Q**ualified **D**omain **N**ame

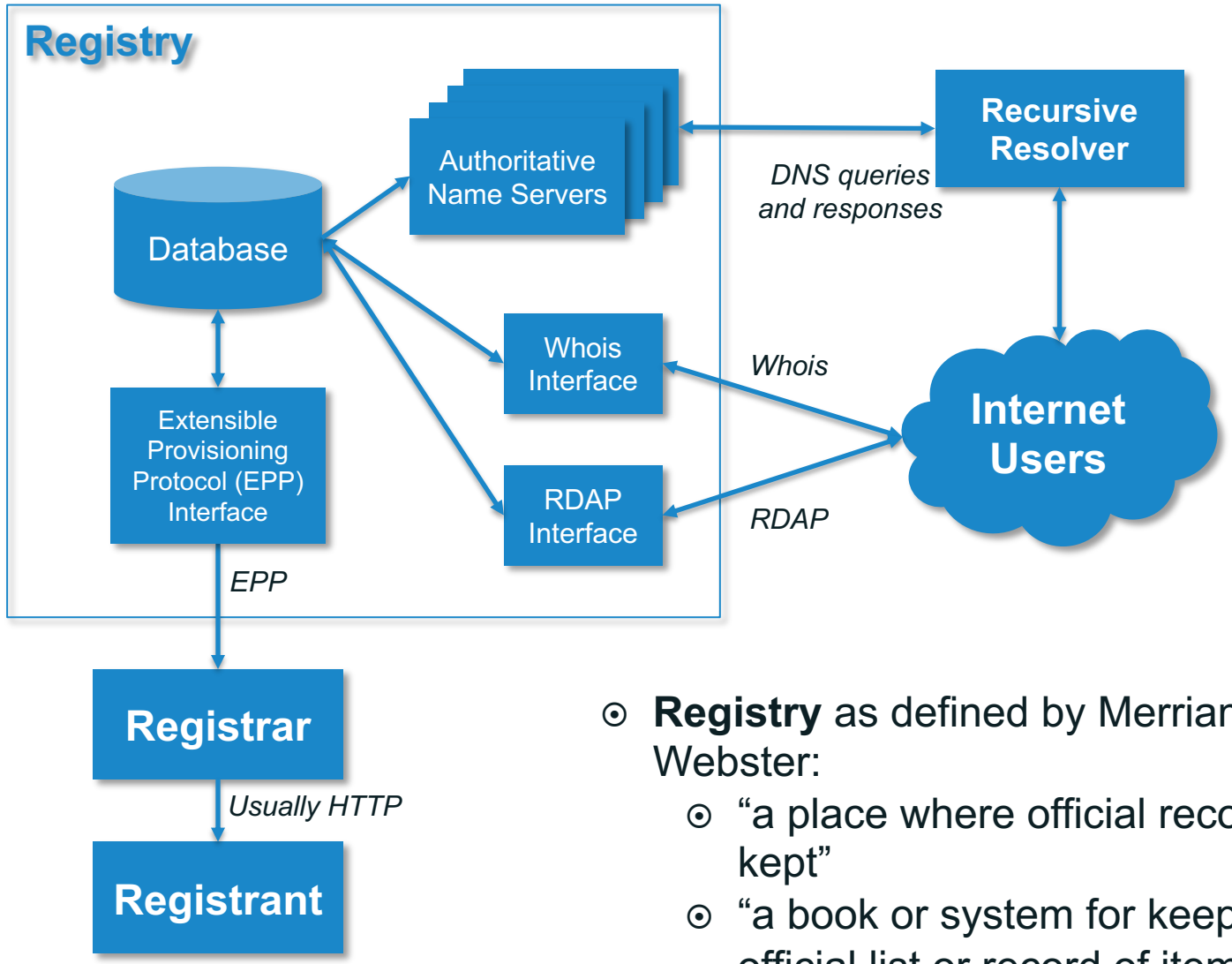
Internationalized Domains



* Successfully evaluated IDN ccTLDs for total countries and territories

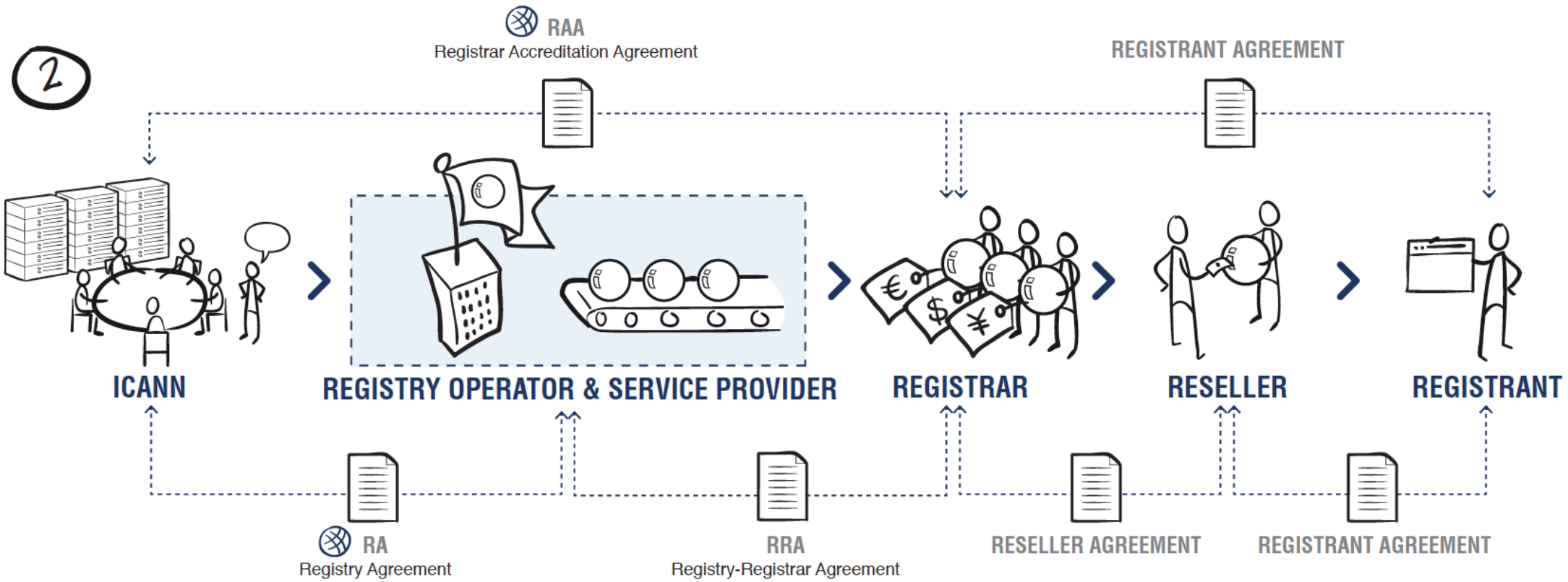
(Source: ICANN - https://www.icann.org/resources/pages/fast-track-2012-02-25-en.)

Domain Name Registries



- **Registry** as defined by Merriam-Webster:
  - "a place where official records are kept"
  - "a book or system for keeping an official list or record of items"

Relationships based on contracts



Security Stability & Resiliency

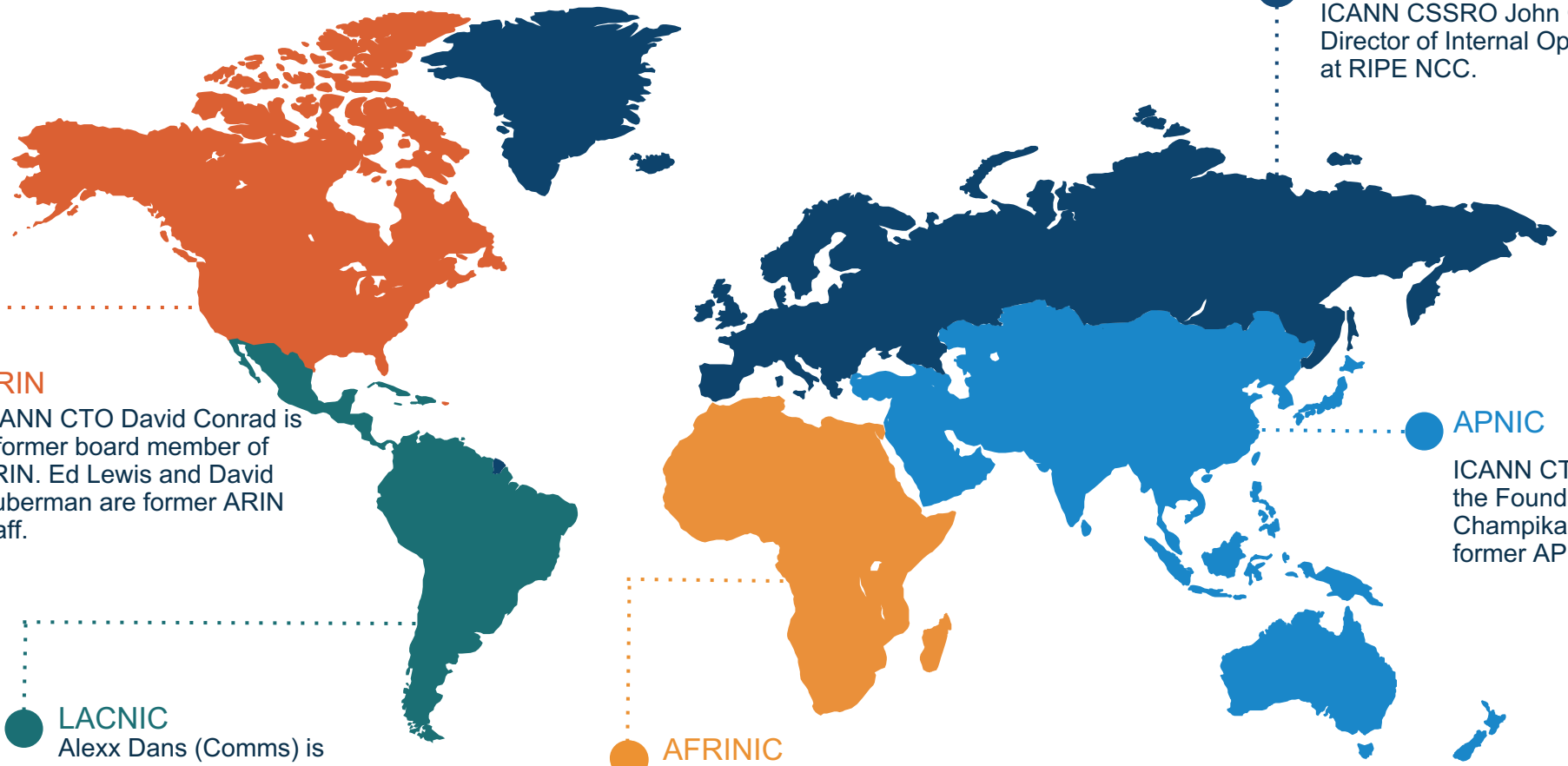
- **Security** - Within ICANN's remit, "security" means the capacity to protect and prevent misuse of Internet unique identifiers.

- **Stability** - means the capacity to ensure that the system operates as expected, and that users of the unique identifiers have confidence that the system operates as expected.

- **Resiliency** - means the capacity of the unique identifier system to effectively withstand/tolerate/survive malicious attacks and other disruptive events without disruption or cessation of service.

ICANN’s Technical Functions & Current Projects

Did You Know?



RIPE NCC

ICANN CSSRO John Crain was Director of Internal Operations at RIPE NCC.

ARIN

ICANN CTO David Conrad is a former board member of ARIN. Ed Lewis and David Huberman are former ARIN staff.

APNIC

ICANN CTO David Conrad was the Founding CEO of APNIC & Champika Wijayatunga was former APNIC staff.

LACNIC

Alexx Dans (Comms) is former LACNIC staff.

AFRINIC

ICANN VP of Technical Engagement Adiel Akplogan was the Founding CEO of AFRINIC

ICANN's Technical Work

Technology @ ICANN

As a technical coordinating body, ICANN performs a variety of activities related to the Internet's unique identifiers. These include operational activities, collaboration, coordination and engagement.

Internet Identifier System Research and Security, Stability, and Resiliency

Office of the Chief Technology Officer supports improving the Security, Stability, and Resiliency of Internet's system of unique identifiers; researches issues related to those identifiers; provides capacity building training for DNS, DNSSEC, and Security; participates in technical and security community groups (IETF, regional TLDs, AntiPhishing)

Internet Assigned Numbers Authority Functions

Part of ICANN Operational functions include the maintenance or key Global Registries (Protocol Parameters, Top level IP number Prefixes and Top level Domain name delegation) under the IANA functions, and the Time Zone Database which contains the code and data that represents local time around the globe

Information Systems, Corporate Security, IT and DNS Engineering

Office of the Chief Information Officer monitors and maintains ICANN systems and technical operations, corporate security, and Information Technology. The DNS Engineering Team administers ICANN's DNS network services and the global L-root constellation.

Global Domain Division Technical Services

The Global Domains Division supports gTLD Registries and Registrars under contract with ICANN. This includes contracting for Emergency Backend Registry Operator, Registry and Registrar Data Escrow, operating the CZDS, and Registry Services Evaluation Process. Also supports IDNs, ccTLD Fast Track Process, Root Zone Label Generation Ruleset...

Bylaws

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"*

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**

(https://www.icann.org/en/system/files/files/revised-strategic-plan-2021-2025-draft-23may19-en.pdf)

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

(https://pti.icann.org/)

Identifier Operations: IANA's Role in DNSSEC

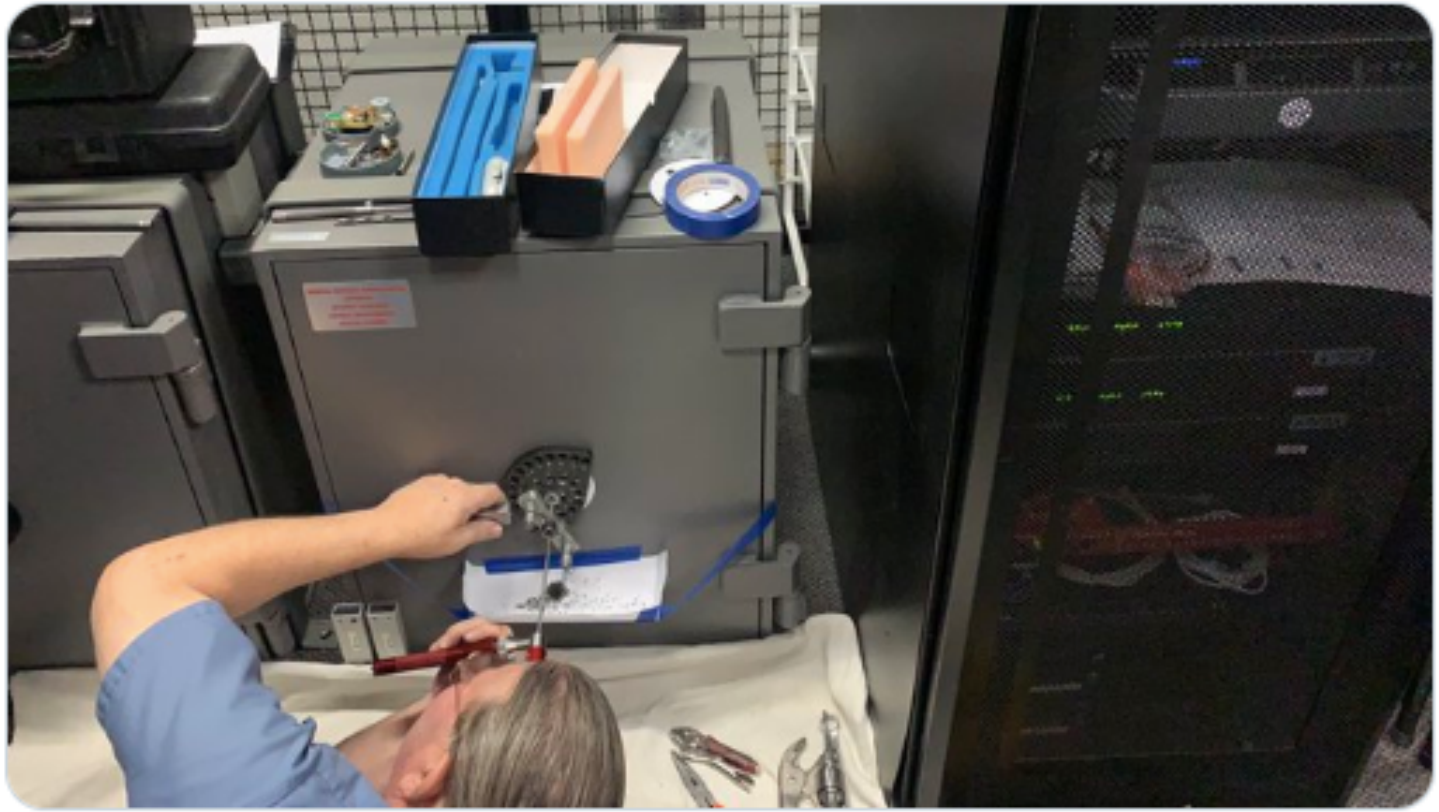
IANA is entrusted by the Internet Community to:

- Issue, manage, change, and distribute DNS keys
- Sign the keyset
- Follow cryptography best practices developed by the Internet Engineering Task Force (IETF)

DNSSEC Key Ceremonies

joao_damas @joao_damas · Feb 14

Sometimes the process of signing the root needs unusual action



(Source: Joao Damas, 14 Feb 2020)

Policy Development: Communities

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

Capacity Development

ICANN staff and community regularly participate in efforts to train and inform organizations worldwide on matters relating to the unique identifier system and cybersecurity to increase knowledge and awareness

- Webinars
- “How it Works” at ICANN meetings
- Technical workshops
- Global law enforcement trainings
- . . . and many other types of capacity building

Key SSR Projects & Initiatives

- Domain Abuse Activity Reporting (DAAR), measures abuse activity and generates reports
  - **Current Status:**
    - Monthly report is published online for the community. The report does not make attribution neither does it draw conclusion about the measurements. ccTLDs invited to participate (19 Nov 2019)
  - **Next Steps:**
    - Data publication into the Open Data Program
    - Improving the system based on comments and reviews
    - New metrics and analytics based on DAAR
    - Discussion with registries who are interested in viewing their own data

Office of the CTO Publications

- IETF Year in Review for 2019 (Jan 2020)
- 5G Technology (Jan 2020)
- Local & Internet Policy Implications of Encrypted DNS (Oct 2019)
- Digital Object Architecture & the Handle System (Oct 2019)
- Security in the Spotlight: A recap of IDS 2019 (Jun 2019)
- See also: Name Collision Analysis Project Study 1 (out for public comment now through 31 March 2020)

(Source: https://www.icann.org/resources/pages/octo-publications-2019-05-24-en)

ICANN OCTO Research

Like many organizations, several ICANN departments do different types of research

- **Global IPv6 deployment**
- **Conversations with root server operators**
- **Root server instance placement**
- **Examining how browsers interact with the DNS**
- **Exploring DNS magnitude ('how popular is this domain')**
- **Domain Abuse Activity Reporting**
- **Identifier Technology Health Indicators**

(Source https://www.icann.org/octo and Paul Hoffman's presentation at IDS 2019)

ITHI – October 2019 snapshot

Home Metrics Participate About

ITHI by ICANN		Full table
Identifier Technology Health Indicator		**As of Oct 2019**
% No Such Domain queries seen by root servers		**74.21%**
% of resolvers that perform DNSSEC validation		**0.00%**
%requests to top name at the root	.LOCAL	**3.51%**
%requests to top name at resolvers	.MAIL	**0.45%**
Number of resolvers accounting for 50% of eyeballs		Coming soon
Phishing Domains per 10,000 registered names		**2.08**

In 2017, ICANN started a project to monitor the health of the registered identifiers ecosystem, through a set of Identifier Technology Health Indicators (ITHI), or ITHI Metrics. There are eight detailed metrics for which data can be seen on this site. The metrics are computed using data captured from various sources including data collected by ICANN projects and traces obtained from participating root DNS servers, authoritative DNS servers, and recursive DNS resolvers. Our first data collection partners are:

- National University of La Plata (UNLP), Argentina ,
- University of Cape Coast, Ghana,
- DNS Nawala, Indonesia,
- KazNIC Organization, Kazakhstan, and
- Taiwan Network Information Center (TWNIC).

(Source https://ithi.research.icann.org/)

ITHI – February 2020 snapshot

Home Metrics Participate About

ITHI by ICANN		Full table
Identifier Technology Health Indicator		As of Feb 2020
% No Such Domain queries seen by root servers		72.68%
% of resolvers that perform DNSSEC validation		33.25%
%requests to top name at the root	.LOCAL	3.12%
%requests to top name at resolvers	.UNIFI	0.05%
Number of resolvers seeing 50% of first queries		242
Phishing Domains per 10,000 registered names		2.08

In 2017, ICANN started a project to monitor the health of the registered identifiers ecosystem, through a set of Identifier Technology Health Indicators (ITHI), or ITHI Metrics. There are eight detailed metrics for which data can be seen on this site. The metrics are computed using data captured from various sources including data collected by ICANN projects and traces obtained from participating root DNS servers, authoritative DNS servers, and recursive DNS resolvers. Our first data collection partners are:

- National University of La Plata (UNLP), Argentina ,
- University of Cape Coast, Ghana,
- DNS Nawala, Indonesia,
- KazNIC Organization, Kazakhstan, and
- Taiwan Network Information Center (TWNIC).

(Source https://ithi.research.icann.org/)

ITHI – Oct 2019

ITHI by ICANN	Identifier Technology Health Indicator		As of Oct 2019	Past 3 months	Historic Low	Historic High
Root Server Health	% No Such Domain queries seen by root servers		74.21%	74.37%	62.95%	74.93%
DNSSEC Deployment	% of resolvers that perform DNSSEC validation		0.00%	31.97%	23.43%	32.26%
Name collision	%requests to top 3 names at the root	.LOCAL	3.51%	3.06%	2.36%	4.47%
		.HOME	2.58%	2.61%	2.53%	3.67%
		.LAN	0.91%	0.95%	0.47%	0.98%
	%requests to top 3 names at resolvers	.MAIL	0.45%	2.72%	0.00%	6.80%
		.UNIFI	0.05%	0.07%	0.03%	0.09%
		.DNS	0.02%	0.02%	0.00%	0.03%
Resolver Concentration	Number of resolvers accounting for 50% of eyeballs		Coming soon			
	Number of resolvers accounting for 90% of eyeballs		Coming soon			
	Abuse Domains per 10,000 registered names	Phishing	2.08	2.72	1.79	4.13
		Malware	1.16	1.11	1.08	2.00
		Botnets C&C	0.53	0.37	0.11	1.48
		Spam	16.27	14.70	8.65	61.89

(Source https://ithi.research.icann.org/)

ITHI – Feb 2020

ITHI by ICANN	Identifier Technology Health Indicator		As of Feb 2020	Past 3 months	Historic Low	Historic High
Root Server Health	% No Such Domain queries seen by root servers		72.68%	72.65%	62.95%	75.10%
DNSSEC Deployment	% of resolvers that perform DNSSEC validation		33.25%	33.83%	23.43%	34.45%
Name collision	%requests to top 3 names at the root	.LOCAL	3.12%	3.41%	2.36%	4.47%
		.HOME	3.01%	2.96%	2.48%	3.67%
		.DHCP	1.22%	0.79%	0.21%	1.00%
	%requests to top 3 names at resolvers	.UNIFI	0.05%	0.07%	0.03%	0.09%
		.DNS	0.03%	0.02%	0.00%	0.03%
		.INTERNAL	0.01%	0.01%	0.00%	0.02%
Resolver Concentration	Number of resolvers seeing 50% of first queries		242	225.81	205.50	234.55
	Number of resolvers seeing 90% of first queries		2185	2221.12	2036.90	2231.86
	Abuse Domains per 10,000 registered names	Phishing	2.08	2.72	2.43	4.13
		Malware	1.16	1.11	1.10	2.00
		Botnets C&C	0.53	0.37	0.54	1.48
		Spam	16.27	14.70	56.56	61.89

(Source https://ithi.research.icann.org/)

ITHI – Feb 2020

M2: Domain Name Abuse

2019/08

The domain name abuses are tracked by measuring the number of registered domain names used in four kinds of abuse: phishing, malware distribution, command and control of botnets, and spam. The number of abusive domains are tabulated either based on the TLD in which they are registered (Measures M2.1.*.*) or based on the registrar that registered them (Measures M2.2.*.*). The values measured each way differ. One reason for the difference is the inclusion of "parked" domains in the TLD counts. These domains are known to be used for abuse, have been taken over by law enforcement or by other regulation systems, and are "parked" in specialized registrars. These specialized registrars are not included in the metrics "per registrar".

Each subset of M2 comprises 4 different sub metrics, one for each type of abuse. For each of these abuse, the first metric (M2.*.*.1) is defined as the number of domains engaged in that type of abuse for 10000 domains. The second and third metric measure the "shape" of the distribution of abuse with two key values: the minimum number of agents (TLD or registrars) that account for 50% of this type of abuse, and the minimum number that account for 90% of the abuse.

The metrics incorporate data from **1193 GTLD and 1793 registrars.**

The following table provides the value observed for the "abuse per 10,000 domains" metric in the current month, as well as the average value over the 3 previous months, and the "historical" minimum and maximum observed since the beginning of the measurements.

Metric			As of Aug 2019	Past 3 months	Historic Low	Historic High
Abuse Domains per 10,000 names registered in GTLDs	Phishing	M2111 (?)	4.15	5.79	4.28	7.10
	Malware	M2121 (?)	1.85	1.99	1.86	4.10
	Botnets C&C	M2131 (?)	1.84	1.60	0.35	3.97
	Spam	M2141 (?)	30.08	47.82	34.10	112.68
Number of GTLDs to account for 50% of abuses	Phishing	M2112 (?)	1	1.67	1	3
	Malware	M2122 (?)	1	1.00	1	3
	Botnets C&C	M2132 (?)	3	2.33	1	3

(Source https://ithi.research.icann.org/)

ICANN Security Incident Reporting

ICANN Cybersecurity Incident Log

This cybersecurity incident log is part of the ICANN organization's commitment to transparency.

Reporting Guidelines

These guidelines describe how the ICANN org handles vulnerabilities that have the potential to exploit or threaten the security, stability, or resiliency of the ICANN org systems and services. These principles apply whether the vulnerabilities are discovered by the ICANN org or are reported by a third party.

- Cybersecurity Transparency Guidelines [PDF, 17 KB]. In general, we will disclose major security vulnerabilities and resulting incidents that cause significant risk to the security of ICANN's systems, or to the rights and interests of data subjects, or otherwise require disclosure under applicable legal requirements.

Cybersecurity Incident Log

Announcement Date	Issue or Incident	Status	Related Information
16 July 2019	SAP Concur Incident	Closed	An external party reported a misconfiguration in the SAP Concur Travel Application related to the delegation and autocomplete features, which could lead to personal information disclosure in certain limited circumstances, such as name, title, phone number and email address. No legal risk was determined. Mitigations were put in place and confirmed

(Source https://www.icann.org/cybersecurityincidentlog)

Why is this work important to the ICANN community?

- Many parts of the DNS ecosystem can be attacked to cause end users to receive false answers
- Attackers may try to infiltrate systems that manage or host the DNS, or will try to intercede in the communication between those systems, in order to change the data users see
- There are methods to prevent these attackers from succeeding, some of which can be considered ***recommended good practices*** while others may offer limited protection
- ICANN wants to promote those practices for protecting the integrity of the DNS and alert the community why they are so important

Transitioning Registration Data Services from WHOIS to RDAP

ICANN

Registration Data Access Protocol (RDAP)

- Developed through the IETF as replacement for WHOIS
- Like WHOIS but better
  - Standardized data for improved machine to machine communication
  - Support for internationalized registration data
  - More secure than WHOIS
  - Enables differentiated access
- How it is defined
  - Protocol defined by RFCs
  - Output defined by “Profile”

RDAP – Recent Activities

- As of 26 August 2019 all ICANN Accredited Registrars and gTLDs must provide an RDAP service in addition to the WHOIS service.
- GDD starting the contract amendment process to the 2013 RAA & Base Registry Agreement to:
  - Incorporate more robust requirements for RDAP
  - Define a Sunset Plan for WHOIS

Timing

- **WHOIS Sunset Timing: Est. 18-36 months from now**
  - Contractual Amendment Process expected to take roughly a year
  - WHOIS Sunset parameters not yet defined with Contracted Parties
    - Unlikely to be less than 6 months, more likely 12-24 months after amendment effective date
- **Public comment on plan will be available**

WHOIS to RDAP

- **Transitioning will require significant outreach to user communities**
  - Law Enforcement & Government
  - Security Community
  - Software & Applications
  - Domain Industry
  - General Users

RDAP Resources

- ICANN's RDAP Site: icann.org/rdap
  - Information for Implementers (Contracted Parties)
    - IETF RFC's
    - RDAP Profile
  - Information for Users – ICANN's lookup tool
    - Lookup.icann.org

For more information

Registration Data Access Protocol (RDAP)

RDAP Overview
Resources for RDAP Implementers
gTLD RDAP Profile
RDAP Pilot Program
FAQs
RDAP Timeline
Information for Users

RDAP Overview

The Registration Data Access Protocol (RDAP) enables users to access current registration data and was created as an eventual replacement for the WHOIS protocol. RDAP was developed by the technical community in the Internet Engineering Task Force (IETF).

RDAP is a protocol that delivers registration data like WHOIS, but its implementation will change and standardize data access and query response formats. RDAP has several advantages over the WHOIS protocol, including support for internationalization, secure access to data, and the ability to provide differentiated access to registration data.

(Source: icann.org/RDAP, 7 Oct 2019)

ICANN Lookup Tool

ICANN | LOOKUP

ABOUT WHOIS | POLICIES | GET INVOLVED | WHOIS COMPLAINTS | KNOWLEDGE CENTER

Domain Name Registration Data Lookup

Enter a domain name

Frequently Asked Questions (FAQ)

Enter a domain

Lookup

By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN Privacy Policy, and agree to abide by the website Terms of Service and the Domain Name Registration Data Lookup Terms of Use.

About ICANN's Domain Name Registration Data Lookup

This tool gives you the ability to look up the registration data for domain names.
More information about this tool and how it works can be found here: https://lookup.icann.org/faq.

DOMAIN NAME REGISTRATION DATA LOOKUP TERMS OF USE

The Domain Name Registration Data Lookup conducts Registration Data Access Protocol (RDAP) queries. RDAP enables users to access current registration data and was created as an eventual replacement for the WHOIS protocol. The results displayed come directly from registry operators and/or registrars in real-time. ICANN does not generate, collect, retain, or store any data associated with an RDAP compliant lookup. If the queried information is not available in RDAP, the query will be redirected to whois.icann.org (WHOIS failover lookup). In cases of WHOIS failover lookups, ICANN may generate, collect, retain or store the domain name queried and the results for the transitory duration necessary to show results in response to real-time queries.

(Source: https://lookup.icann.org/)

Overview and Status of Universal Acceptance (UA)

Universal Acceptance Initiative

Vision

All domain names and all email addresses work in all software applications

Mission

To mobilize the software application developers to get their products UA Ready by providing encouragement, documentation, case studies, tools and measures to deliver the right user experience to the end user

Impact

Promote consumer choice, improve competition and provide broader access to end users

Categories Affected by UA Issues

- **Domain Names**
  1. **Newer** top-level domain names: example.sky
  2. **Longer** top-level domain names: example.global
  3. **Internationalized** domain names البحرين.مثال
     - Display is another problem, in addition to above

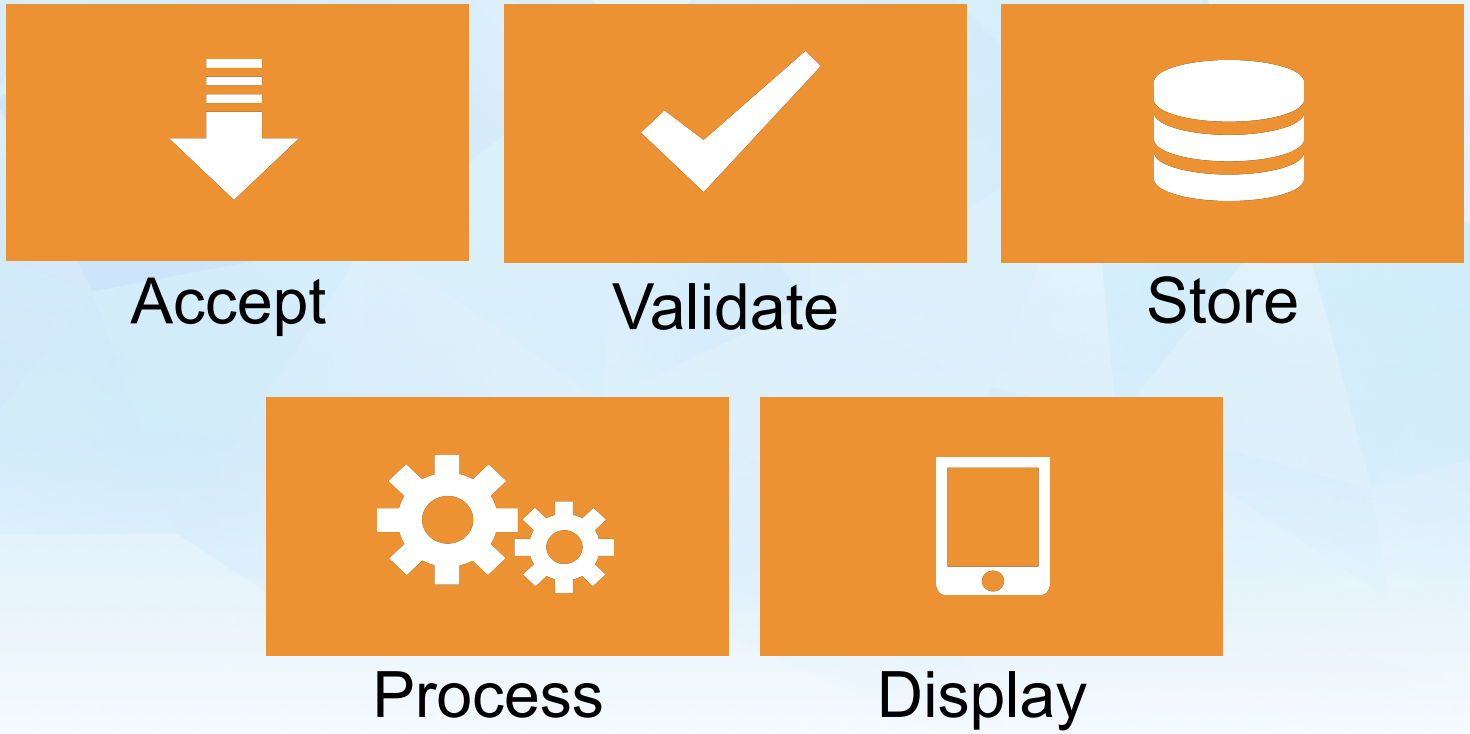
       Should not be as A-label: xn--mgbh0fb.xn--mgbcpq6gpa15g

       Should be correct for right-to-left scripts: مثال.البحرين

- **Internationalized email addresses (EAI)**: अजय@डाटा.भारत (email address in Hindi language)
  4. Available standards not implemented by all email software and service providers making email delivery unreliable
     - Test if your email is compliant: https://uasg.tech/eai-check/

Five Actions for UA Readiness

Applications should be able to do the following for all domain names and email addresses:



Universal Acceptance Steering Group (UASG)

- UASG is a community-based group supported by ICANN org
  - **Leadership Team:** Chair and two to three Vice-chairs elected by the community
  - **Coordination Group:** UASG Leadership and chairs of all working groups
  - **Working Groups:** UASG community can opt for focused working groups
  - **Community:** General UASG community, interacting on UA-discuss email list
- UASG has produced documentation to define, address the challenges and share progress, posted at https://UASG.tech, e.g.:
  - Quick Guide to Universal Acceptance
  - Quick Guide to Email Address Internationalization
  - UA Case Study: Government of Rajasthan, India
  - Quick Guide to Tendering and Contractual Documents
- UASG is actively engaged in disseminating the information to relevant stakeholders

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

TLD		Description	DS Date	% Signed
cpa.			21-SEP-2019	-
eu			12-SEP-2019	-
ve.		Comisin Nacional de Telecomunicaciones (CONATEL)	1-SEP-2019	
ss.		National Communication Authority (NCA)	1-SEP-2019	-
gay.		Top Level Design, LLC	10-AUG-2019	-
срб		Serbian National Internet Domain Registry (RNIDS)	26-JUL-2019	-
rs.		Serbian National Internet Domain Registry (RNIDS)	24-JUL-2019	-
mc.		Gouvernement de MonacoDirection des Communications Electroniques	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	-

(Source: rick.eng.br/dnssecstat)

Recent DNS Trainings (FY19 & FY20)

ccTLD and local community trainings

- Lithuania, Latvia, Finland, Iceland, Hungary
- Ghana, Saudi Arabia
- Uzbekistan, Bahamas

Regional DNSSEC trainings

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

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

Living in an Insecure World

Attacks in the news

COMPUTERS

Equifax, Words with Friends and beyond: Every major security breach and data hack

We've started a running list, and the results are sobering.

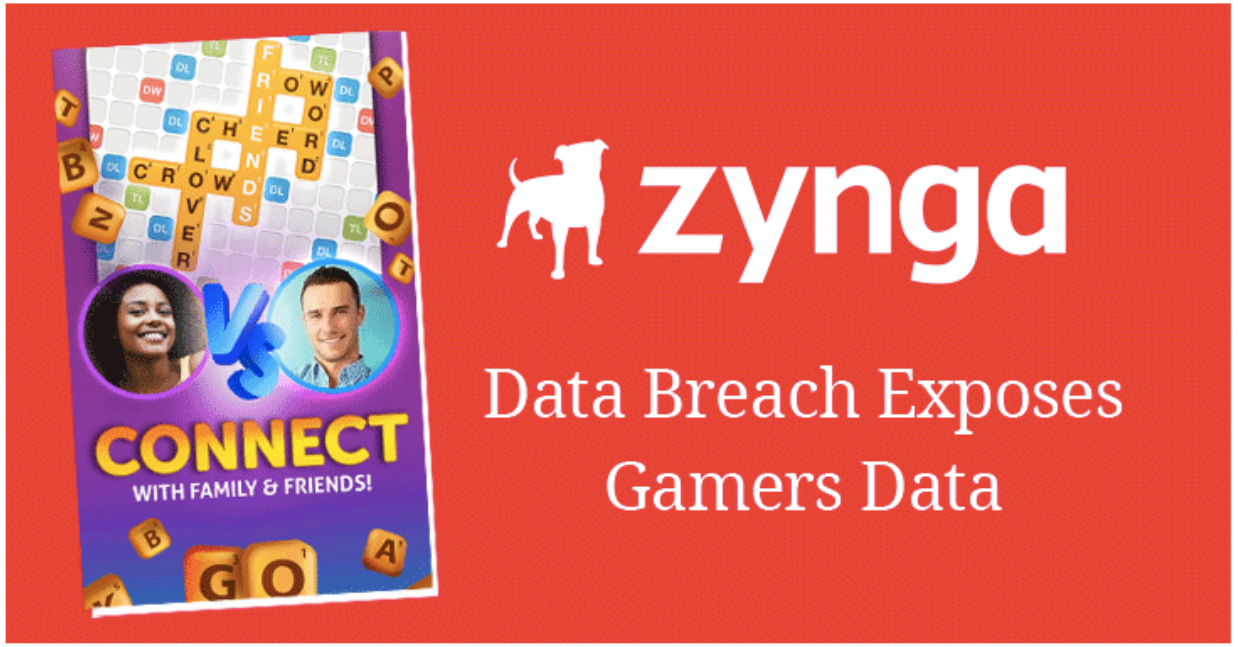
BY SHELBY BROWN | OCTOBER 1, 2019 12:45 PM PDT

(Source: Cnet, 1 Oct 2019)

Do you have Words with Friends on your phone?

Exclusive — Hacker Steals Over 218 Million Zynga 'Words with Friends' Gamers Data

September 29, 2019 Swati Khandelwal



A Pakistani hacker who previously made headlines earlier this year for selling almost a billion user records stolen from nearly 45 popular online services has now claimed to have hacked the popular mobile social game company **Zynga Inc**.

With a current market capitalization of over $5 billion, Zynga is one of the world's most successful

(Source: Hacker News, 29 Sept 2019)

Starting off 2020 with more attacks

threat post

Cloud Security / Malware / Vulnerabilities / InfoSec Insider / Podcasts

Author:
Tara Seals

January 7, 2020
/ 12:04 pm

Researchers suspect the cybercriminals attacked using an unpatched critical vulnerability in the company's seven Pulse Secure VPN servers.

The Sodinokibi ransomware strain is apparently behind the New Year's Eve attack on foreign currency-exchange giant Travelex, which has left its customers and banking partners stranded without its services.

(Source: Threatpost, 7 Jan 2020)

Starting off 2020 with more attacks

Oscar Nominated Movies Featured in Phishing, Malware Attacks

By Sergiu Gatlan February 6, 2020 11:33 AM 0

Attackers are exploiting the hype surrounding this year's Oscar Best Picture nominated movies to infect fans with malware and to bait them to phishing websites designed to steal sensitive info such as credit card details and personal information.

This method is the perfect way to get around movie fans' defenses seeing that many of them are willing to take down their defenses for a chance to get a free preview, especially given that the 92nd Academy Awards ceremonies are just around the corner on February 9th.

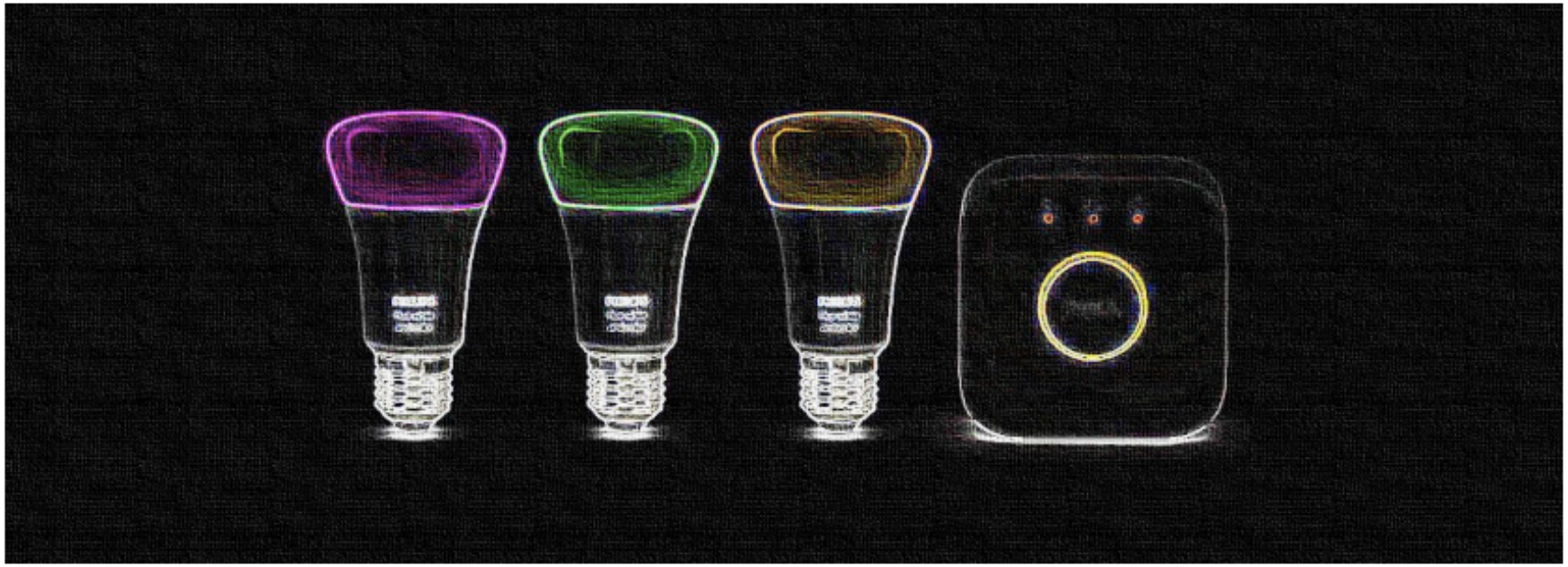
(Source: BleepingComputer, 6 Feb 2020)

And more threats

Bug in Philips Smart Light Allows Hopping to Devices on the Network

By Ionut Ilascu

February 6, 2020 12:03 AM 1



Security researchers taking a closer look at the Philips Hue smart bulbs and the bridge device that connects them discovered a vulnerability that helped them compromise more meaningful systems on the local network.

(Source: BleepingComputer, 6 Feb 2020)

And more threats

App Used by Netanyahu's Likud Leaks Israel's Entire Voter Registry

Names, identification numbers and addresses of over 6 million voters were leaked through the unsecured Elector app

Ran Bar-Zik Feb 09, 2020 9:40 PM

3132 Tweet 3 Zen Subscribe now

(Source: Haaretz, 9 Feb 2020)

Have you stayed at a Starwood hotel?

The New York Times

Marriott Hacking Exposes Data of Up to 500 Million Guests

Marriott International acknowledged on Friday that an "unauthorized party had copied and encrypted information" belonging to about 500 million customers on its Starwood reservations system. Mauritz Antin/EPA, via Shutterstock

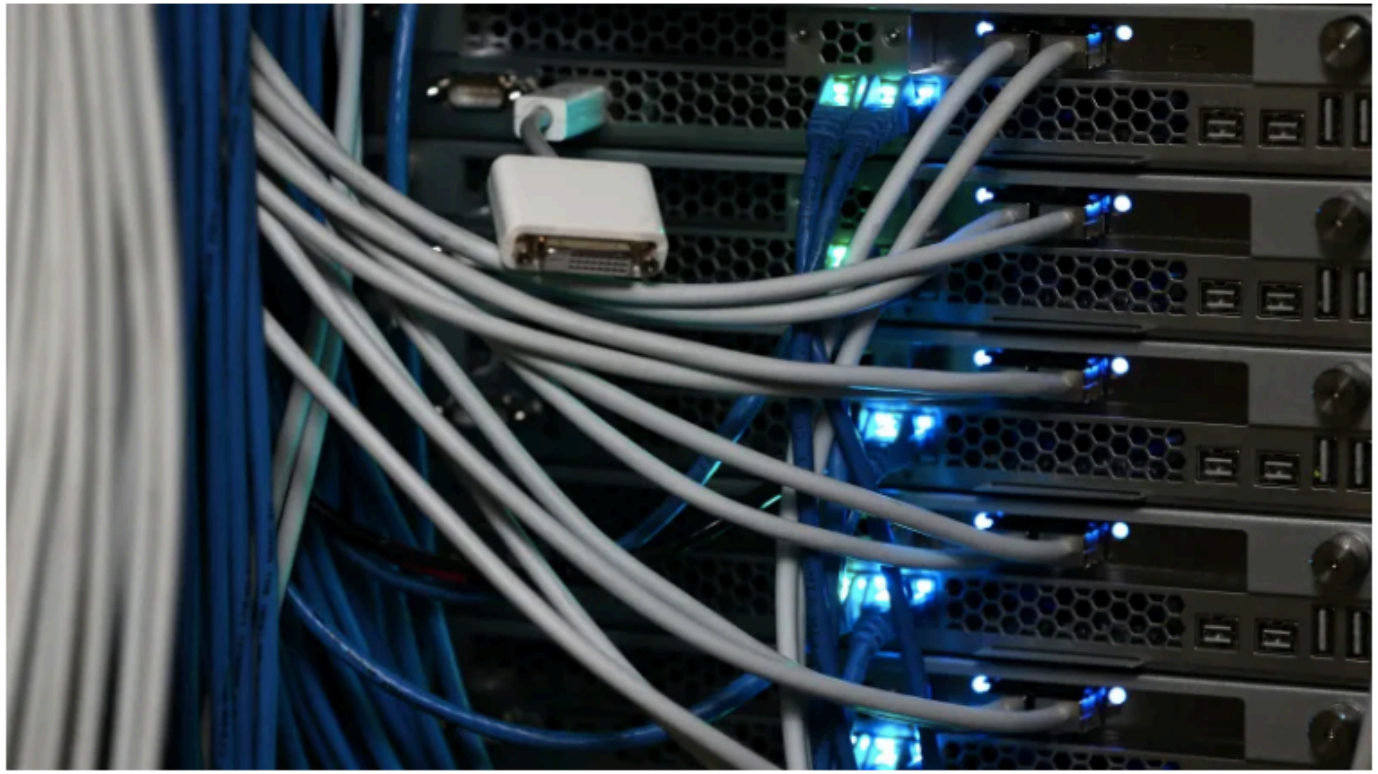
FBI warns of ransomware attacks

PRIVACY AND SECURITY

Alabama Hospitals Pay Out in Ransomware Attack Amid FBI Warning of More to Come

Tom McKay
Yesterday 3:20pm • Filed to: RANSOMWARE

11.9K 34 1



(Source: Gizmodo, 6 Oct 2019)

Even NASA hit by an attack

FOSSBYTES NEWS GEEK SECURITY HOW TO TOP X REVIEWS VIDEOS

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 A
June 24, 2019

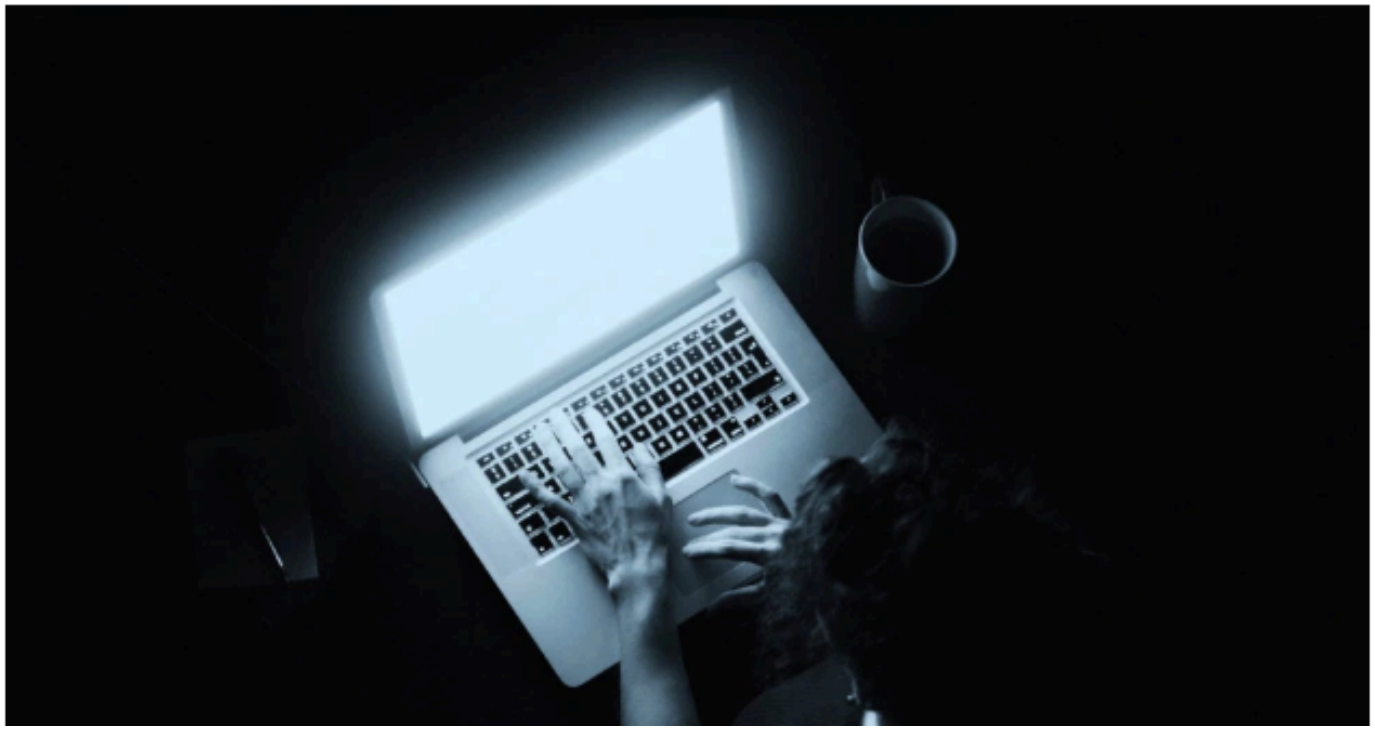
Intel Is Working
Parallel C++' Pr
Language
June 24, 2019

Google Calenda
Phishing: How
From...

Common web conferencing tools attacked

A flaw in Webex and Zoom let researchers snoop on users' video calls

Zack Whittaker @zackwhittaker / 6:00 am EDT • October 1, 2019 Comment

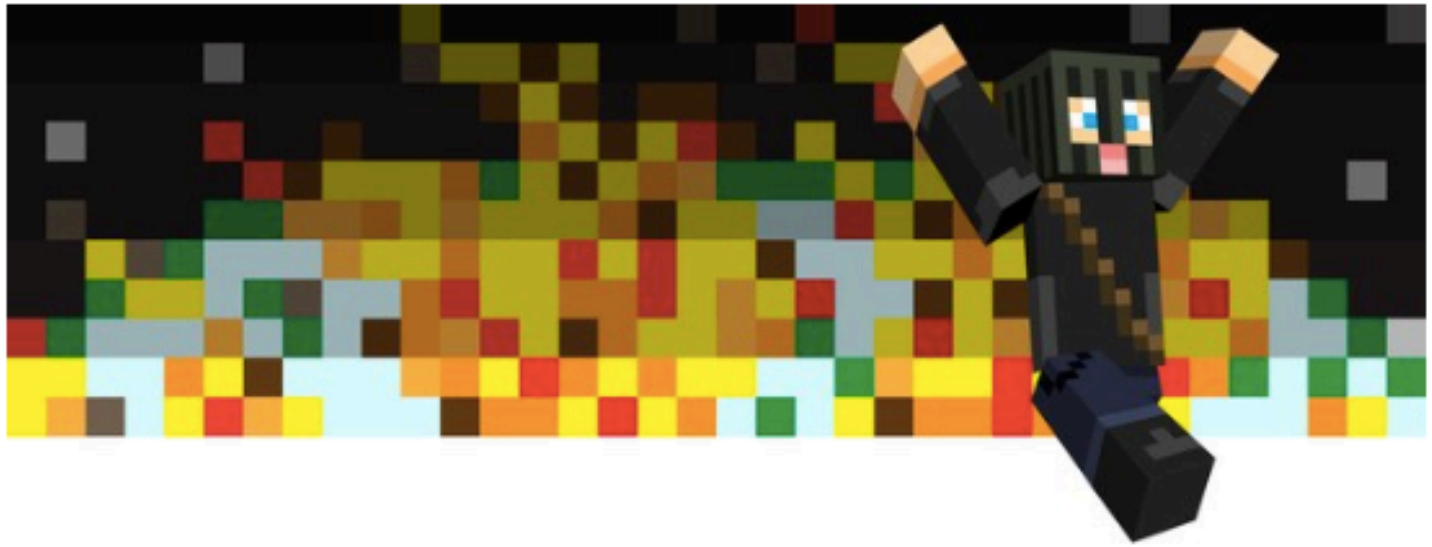


(Source: TechCrunch, 1 Oct 2019)

Popular streaming games

GARRETT M. GRAFF SECURITY 12.13.17 03:55 PM

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



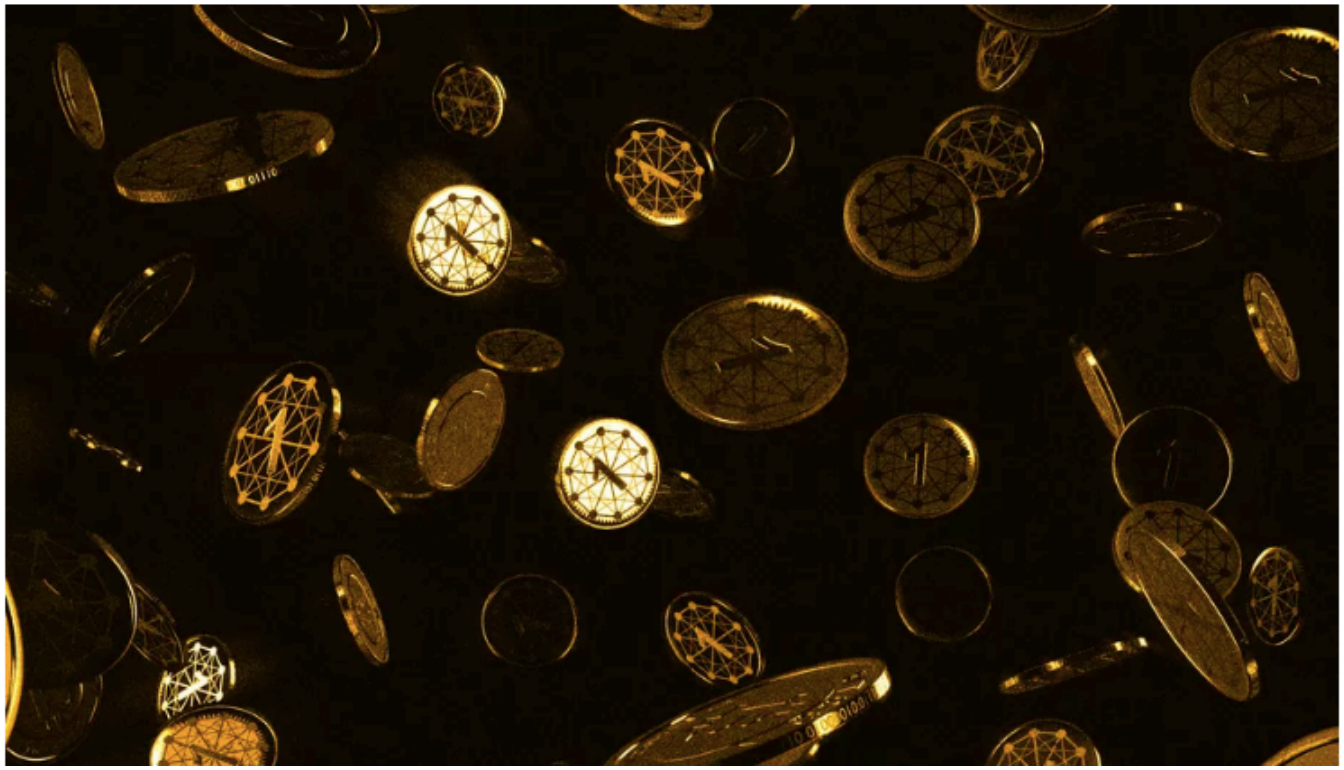
(Source: Wired, Dec 2017)

Web-based crypto-lockers

Hackers emptied Ethereum wallets by breaking the basic infrastructure of the internet

By Russell Brandom | Apr 24, 2018, 1:40pm EDT

SHARE

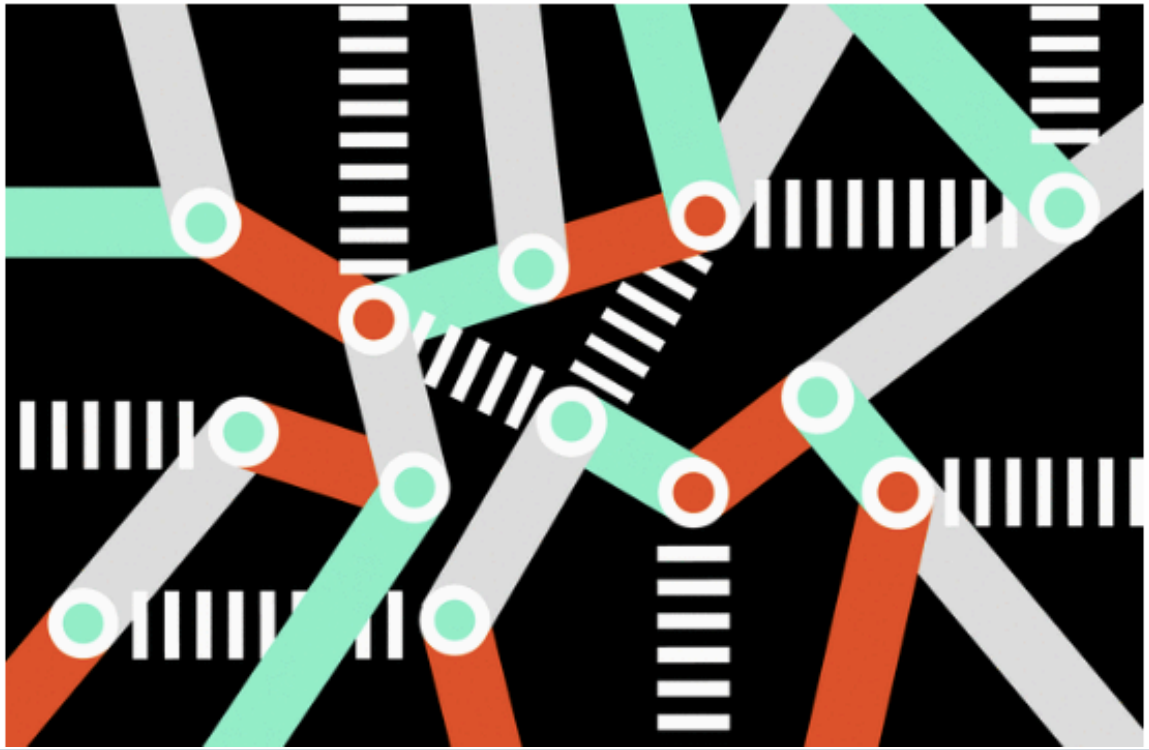


GOOD DEALS

(Source: The Verge, Apr 2018)

Attacks in the news

A WORLDWIDE HACKING SPREE USES DNS TRICKERY TO NAB DATA



(Source: Wired, Feb 2019)

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

Evolving Threat Landscape

Cyber Incident & Breach Trends

- Number of data breaches and exposed records were reported down
- Ransomware & DDoS reported down overall
- Financial impact of ransomware rose by 60%
- 5 billion records exposed in 2018
- 12% rise in business-targeted ransomware

(Source Internet Society OTA Cyber Incident & Breach Trends Report, 9 July 2019)

Cyber Incident & Breach Trends

- Increase in public attribution by governments through indictments
- Attackers following data to cloud services
- Advanced Persistent Threat groups (state-sponsored)

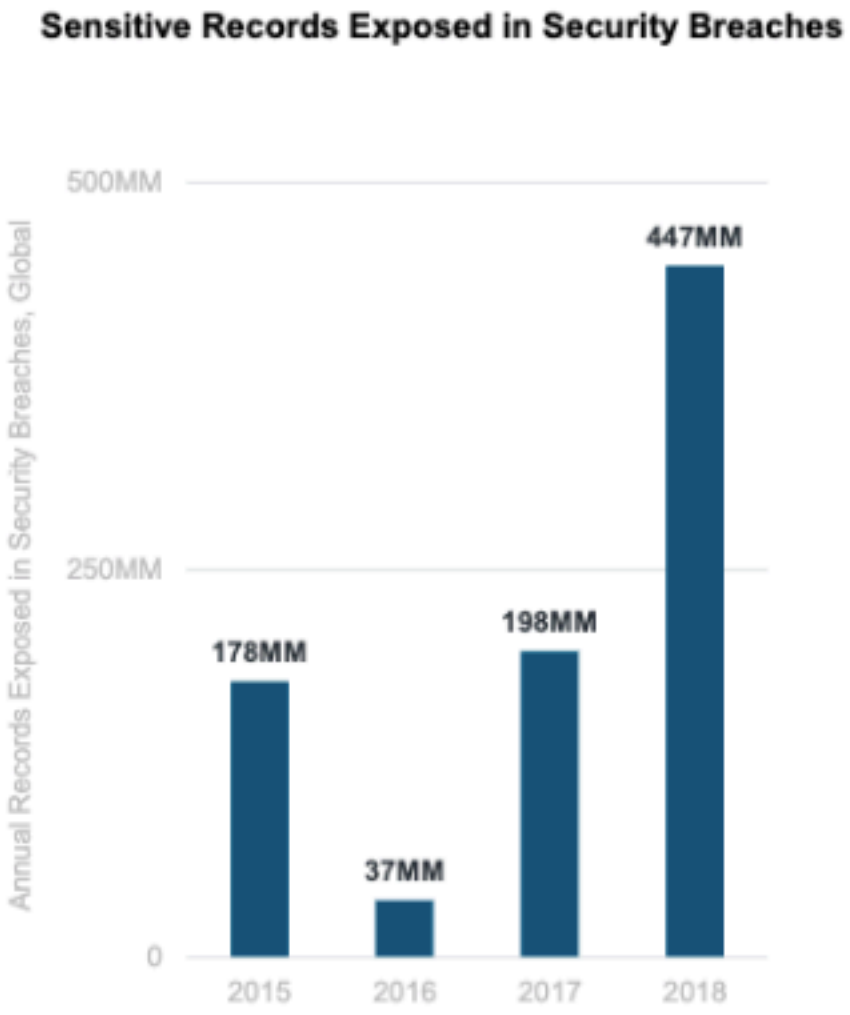
(Source Fireeye M-Trends Report, 2019)

Attackers focus on sensitive data

As more & more customers move to software as a service & cloud, attackers are following data.

Attacks against cloud providers, telecoms & other organizations with access to large amounts of data… increased in 2018.

FireEye M-Trends Report 2018



(Source https://www.bondcap.com/#view/210)

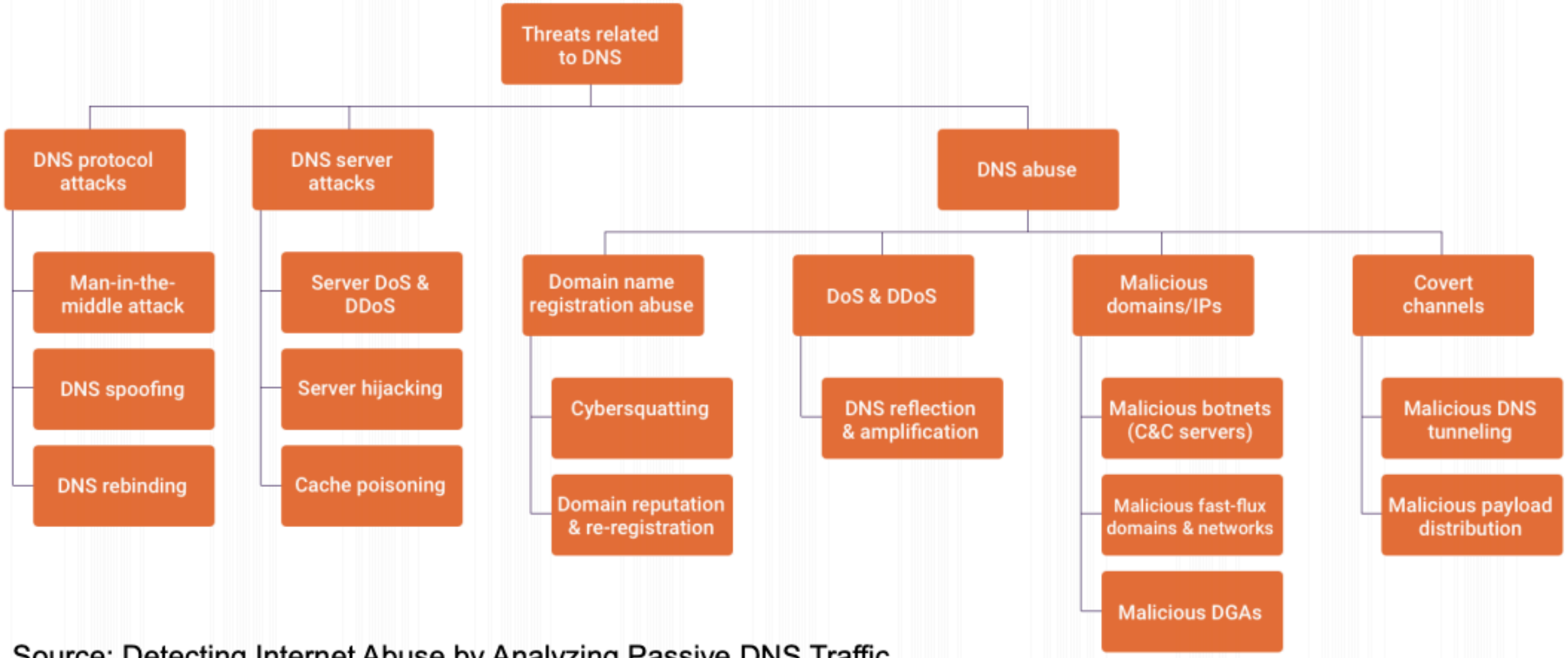
Trends (from May 2019 IDS in Bangkok)

- Some level of malicious activity almost everywhere
- Some new gTLDs do a good job policing malicious activity
- Some don't…
- Analysis being done to explore the threat types across different TLDs (DAAR, security research community)
- Looking at common characteristics among TLDs with high levels of malicious activity

Why is the DNS a target for attacks?

- Everyone uses the DNS to resolve user friendly names to Internet Protocol addresses
- Disrupt the DNS and you disrupt merchant transactions, government services, social networks
- Exploit the DNS and you can trick, defraud or deceive users
- Vectors for exploitation:
  - Maliciously register domain names
  - Hijack name resolution or registration services
  - Corrupt DNS data, zone files

DNS Ecosystem Technical Threats



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

(Source: Merike Kaeo presentation at FIRST, June 2019)

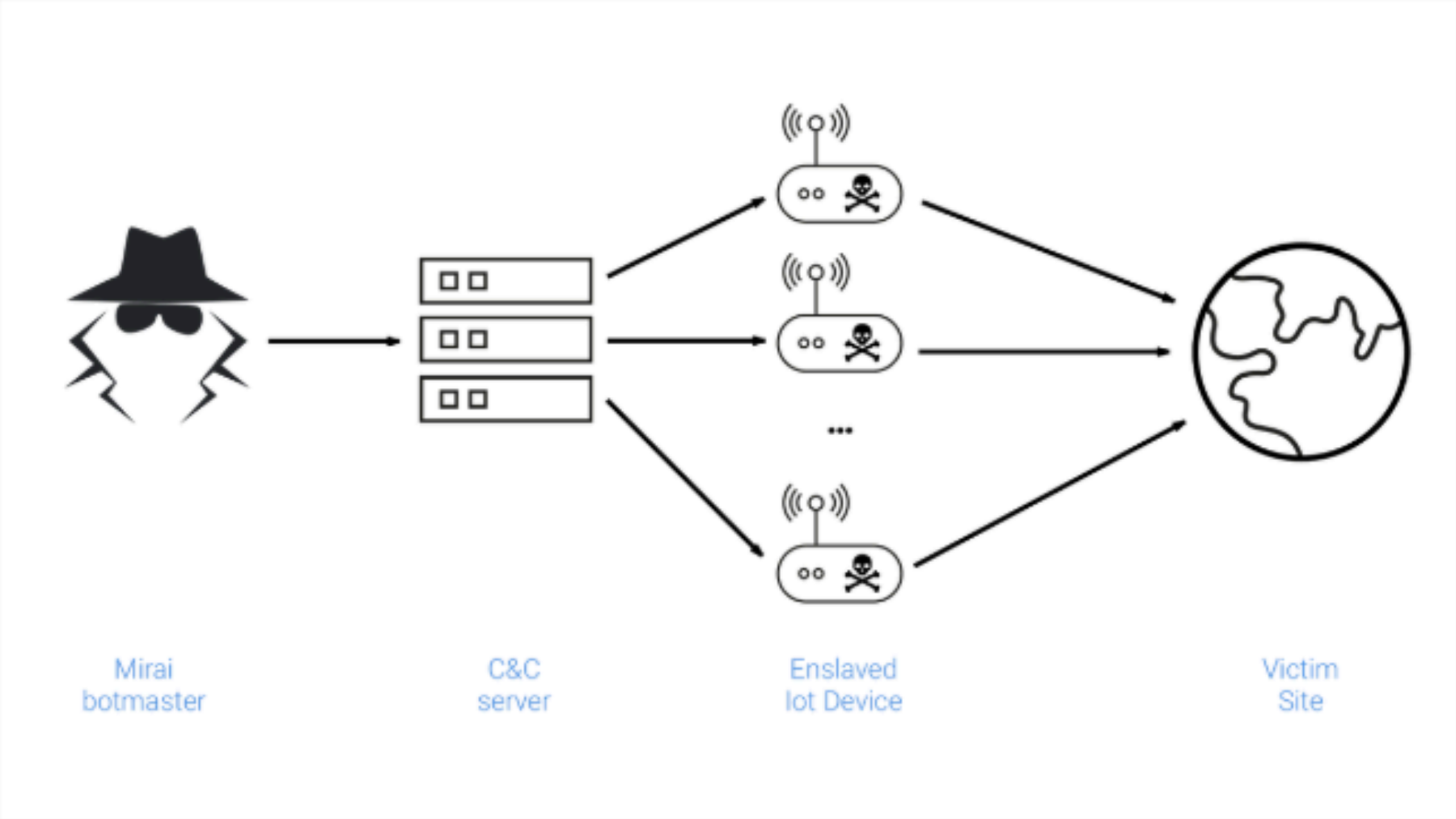
Avalanche Malware

- Criminal malware and DNS hosting infrastructure
  - Evolved from botnet to malware delivery service
  - Bulletproof hosting used double fast-flux
  - Predominantly used for financial fraud attacks
- Avalanche offered a “cloud customer experience”
  - Criminal domain registrations
  - Access to a C2 server and service assets (bots)
  - Choice of Malware: 20 families available

Andromeda	Nymaim	Carberp	KBot / Bolek	Panda Banker
CoreBot	Ranbyus (.tw)	Doc-Downloader	Rovnix	Dofoil
Slempo	GOZI2	Teslacrypt	GozNym	Trusteer App
KINS	URLZone	Marcher	VawtrakMatsnu	Xswkit

Avalanche Outcome

Mirai botnet attack



Mirai botnet

- Attack on Brian Krebs & OVH (July & Sept 2016)
- Attack on Dyn (Oct 2016), affected services on hundreds of domains across the DNS
- Attack on Lonestar (Liberian telco)
- Attack on Deutsche Telekom (Nov 2016)

Warning bells Mirai rings for us all

- Mirai characteristics expose many IoT security issues
  - A botnet that is largely comprised of IoT devices
  - The compromised devices use plain text channels that have long been regarded as unsecured and removed from use in previous waves of technology
  - The default credentials for these services are known and shared
  - The devices can be re-purposed for many kinds of attacks

- An IoT-populated botnet: DDOS as a service to a new level

A view on the root

The RIPE NCC DNS Monitoring Service (DNSMON) provides a comprehensive, objective and up-to-date overview of the quality of the service offered by high-level Domain Name System (DNS) servers. It is an active measurement service. It uses our RIPE Atlas active measurement network to provide an up-to-date service overview of all DNS root and many Top-Level Domain (TLD) name servers. An important feature is the ability to view historical data. This allows quick analysis of both past and present DNS issues. [Read more]

DNS responses for . (root) Go

Protocol: UDP Servers: IPv4 and IPv6 Show RIPE Atlas measurements

(Source: RIPE DNSmon, 7 Oct 2019)

Major Actors During a DNS attack

Responding to an ongoing attack requires coordinated responses from:

- Network operators
- Global law enforcement agencies
- National or Regional Computer Incident Response Teams (CIRTs)
- Registries

Attribution

One of the most important activities during an attack is proper attribution

- Who is the registrant of the IP addresses used in the attack?
- Who is the registrant of the domain names used in the attack?

Attribution requires data sources which is the primary role of registration data

- Registration records for IP addresses and AS numbers (RIRs)
- Registration data for domain names

ICANN's Role?

- Large scale attacks appear to be growing, and because of their surface area, involve:
  - Governments
  - Multi-national companies
  - International law enforcement
  - Widespread news coverage
- Other (smaller scale) DNS security incidents happen daily
- The ICANN Community and members of the ICANN Org have a role before, during, and after these types of security incidents

ICANN's Coordination Role

ICANN has a team inside the Office of the CTO (OCTO) that works with organizations during an attack to coordinate responses

- Deep understanding of cybercrime from both perspectives (attackers and responders)
- Strong connections to global law enforcement and the Internet's OpSec community
- The team uses their deep understanding and their strong community connections to bring all the parties together during takedown efforts

ICANN has a Coordinated Disclosure Process that security researchers, registries, registrars, and others in the community can use to report vulnerabilities and bugs to ICANN

Case Studies: IDN Based Abuse & Emojis

IDN-based Abuse

Script Commingling: It's A Problem

- The mixing of different scripts at effective second-level domain
- (Basic Latin + Cyrillic)
  - xn--pypal-4ve.com. --> paypal.com.

а а

U+0430 U+0061

Credit: Mike Schiffman, Farsight Security

IDN confusability

IDNs: Homoglyphs and Homographs

- **Homoglyph** One of two or more glyphs with shapes that appear identical or very similar

a ã

- **Homograph** One of two or more strings that appear identical or very similar

facebook
fãcebook

IDN confusability

ASCII Look-alikes vs IDN Homographs

- ASCII Look-alike: One of two or more **ASCII** strings that appear identical or very similar
- Solutions exist for detecting some ASCII look-alikes that do not exist for IDN Homographs

acme.example

acrne.example

IDN confusability

Real Site	Homograph	A-label
easyjet.com.	easyjet.com.	xn--easyje-n17b.com.
delta.com.	de|ta.com.	xn--deta-1kb.com.
ryanair.com.	ryanair.com.	xn--ryanai-1x7b.com.
poloniex.com.	poloniex.com.	xn--polonex-3ya.com.
bittrex.com.	bittrex.com.	xn--btrex-m3a12b.com.
linkedin.com.	linkedin.com.	xn--lnkedin-zya.com.

Courtesy of
Mike Schiffman,
Farsight Security

IDN confusability

Observed via Passive DNS

ƒacebook.com. ƒacebọọk.com.
ƒacebook.tk. ƒacebook.com.
facebook.com. fácebook.com.
fàcebook.com. fâcebook.com.
fácebook.com. fäcebook.com.
fãcebook.com. fåcebook.com.
fącebook.com. fācebook.com.
fącebook.com. fącebook.com.
fàćebook.com. fačebook.com.
fačebook.com. fačebook.com.
façebook.com. facebook.com.
facébook.com.

apple.com. applė.com.
âpplê.cf. ápple.com.
ăpple.com. åpple.com.
äpple.com. ąpple.com.
applе.com. applе.com.
applé.com. applè.com.
àpplè.com. applĕ.com.
ăpplĕ.com. ápplê.com.
àpplê.com. âpplê.com.
applĕ.com. applë.com.
äpplë.com. applė.com.
åpplė.com.

ñetflix.com.
ṇetflix.com.
nétflix.com.
nėtflix.com.
neṭflix.com.
netflíx.com.
netflìx.com.
netflîx.com.
netflïx.com.
netflix.com.
netflix.com.
netƒlix.com.

ǵoogle.xyz. goôgle.com.
ǵoogle.com. google.com.
gọọglē.com. googlè.tk.
googlę.com. googlè.com.
googlé.com. ǵoogle.com.
google.com. googlè.com.
googlé.com. google.com.
gooǵle.com. gooǵle.com.
gooǵle.com. gooǵle.com.
gooǵle.com. gooǵle.com.
gooǵle.com. gooǵle.com.
gooǵle.com.

bankofamerica.com. baŋkofamerica.com.
baŋkofamerica.net. bąnkofamerica.com.
bankôfamerica.com. banköfamerica.com.
bankofamerîca.com. bänkofämericä.com.
bankofamerica.com. bankofamerica.net.
bankofamerica.com.

wellsfargo.com.
wellsfargo.com.
wellsfárgo.com.
wellsfârgo.com.
wellsfargó.com.
wellsfargọ.com.
wellsfargo.com.

çhase.com.
chàse.com.
chäse.com.
chasé.com.
chasë.com.
chase.com.
chase.com.

Courtesy of
Mike Schiffman,
Farsight Security

World Emoji Day – 17 July 2019

Al Jazeera English @AJEnglish · 2h

It's #WorldEmojiDay🎭 💃 🧞‍♀️ 🙌

What emoji do you use most? Share with us your most used emoji 👇

Emojis in Domain Names Create a Security Risk

The ambiguity and confusion the emojis cause in domains can lead to a denial of service or misconnections, possibly exposing users to phishing and other social engineering attacks

The current IDNA 2008 standard for IDNs prohibits emojis. Therefore, applications that follow the standard may not support emojis at all; others may process them inconsistently

An advisory by Security and Stability Advisory Committee of ICANN points out that emojis in domain names create a number of problems from an end-user standpoint, as explained below

Emojis Can Be Visually Too Similar to Distinguish

Emojis can be visually too similar to distinguish especially when displayed in smaller fonts or by different applications.

Users could easily confuse the "Grinning face" emoji (left) and "Grinning face with smiling eyes" emoji (right).

Emoji Unicode Labels

№	Code	Browser	Appl	Goog	Twtr	One	FB	Sams.	Wind.	GMail	SB	DCM	KDDI	CLDR Short Name
1	U+1F600	😀	😀	😀	😀	😀	😀	😀	😀	😁	—	—	—	grinning face
2	U+1F601	😁	😁	😁	😁	😁	😁	😁	😁	😁	😁	😁	😁	beaming face with smiling eyes
3	U+1F602	😂	😂	😂	😂	😂	😂	😂	😂	😂	😂	—	😂	face with tears of joy
4	U+1F923	🤣	🤣	🤣	🤣	🤣	🤣	🤣	🤣	—	—	—	—	rolling on the floor laughing
5	U+1F603	😃	😃	😃	😃	😃	😃	😃	😃	😃	😃	😃	😃	grinning face with big eyes
6	U+1F604	😄	😄	😄	😄	😄	😄	😄	😄	😄	😄	—	—	grinning face with smiling eyes

Full list at https://unicode.org/emoji/charts/full-emoji-list.html

Emojis Can Be Visually Too Similar to Distinguish

Some emoji allow users to apply one of five skin tone modifiers. These can make emojis difficult to distinguish and are subject to interpretation.

https://  .example

https://  .example

Users could easily confuse the "Detective-medium light skin" emoji (left) with the "Detective-medium skin" emoji (right).

Emoji Skin Tone Unicode Points

№	Code	Browser	Appl	Goog	Twtr	One	FB	Sams.	Wind.	GMail	SB	DCM	KDDI	CLDR Short Name
1	U+1F3FB									—	—	—	—	light skin tone
2	U+1F3FC									—	—	—	—	medium-light skin tone
3	U+1F3FD									—	—	—	—	medium skin tone
4	U+1F3FE									—	—	—	—	medium-dark skin tone
5	U+1F3FF									—	—	—	—	dark skin tone

Reference at https://unicode.org/emoji/charts/full-emoji-modifiers.html

Combining Emoji is Unreliable

Some emojis can be combined (or “glued”) using a joining character to display them as a single symbol, but:

- Systems that do not support combining will render “glued together” emojis as a sequence of separate emojis.
- To the user, a single unmodified emoji may appear to be “glued together” when it is not.

Single: 👪
Unicode: 1F46A

Combined: 👩 + 👨 + 👦
Unicode: 1F468$_{200D}$1F469$_{200D}$1F466

Both displayed as:

https:// 👪 .example

Emojis Are Not Displayed Uniformly

Emojis are not displayed uniformly across all platforms because there is currently no standard specifying how they should look.

"Dizzy face" emoji (Unicode: 1F635) as displayed by:

Apple	https:// 😵 .example
Google	https:// 😵 .example
Windows	https:// 😵 .example

Recent Domain Registration Hijacking

Attacks in the news

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

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
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

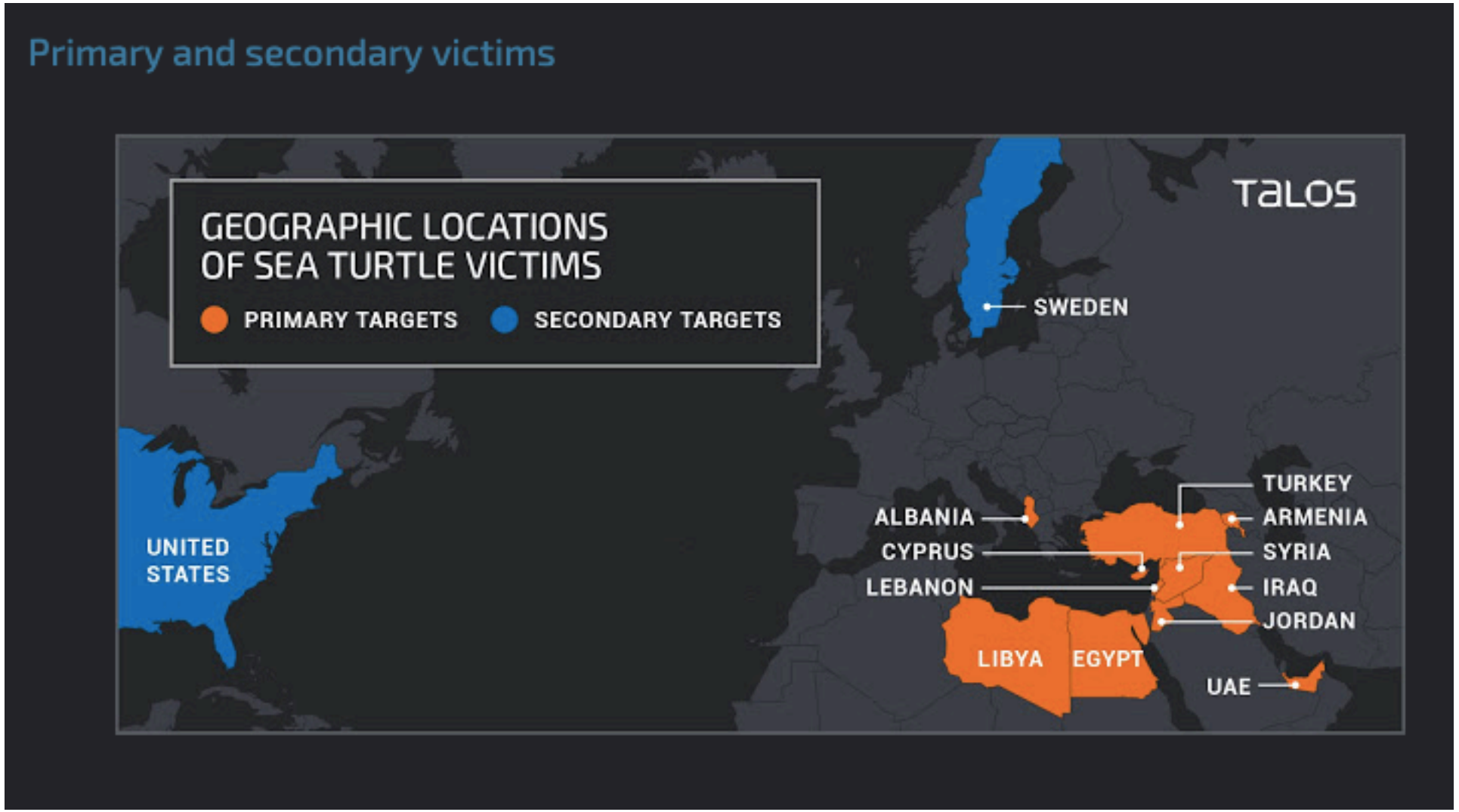
Domain Registration Hijacking Background

1. Attackers had the ability to modify registration records at the registry, typically by compromising login credentials
2. Attackers changed DNS delegations (NS) pointing the zones to the attackers' DNS servers. A and MX records also modified.
3. Once zones were redirected, attackers impersonated services hosted by the victims (eg: e-mail, websites)
4. Attackers could Man-In-The-Middle (MITM) user traffic

Methodologies

- 10-minute attacks to avoid detection
- Compromised EPP credentials
- Re-write authoritative nameservers
- Obtain easy-to-get certs from Let’s Encrypt or Comodo
- Harvesting data to build credentials repository
- Re-write Internet Message Access Protocol info
- Capture email credentials
- Capture email, calendaring, vcards

Sea Turtle – Initial Victims (late 2018)



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

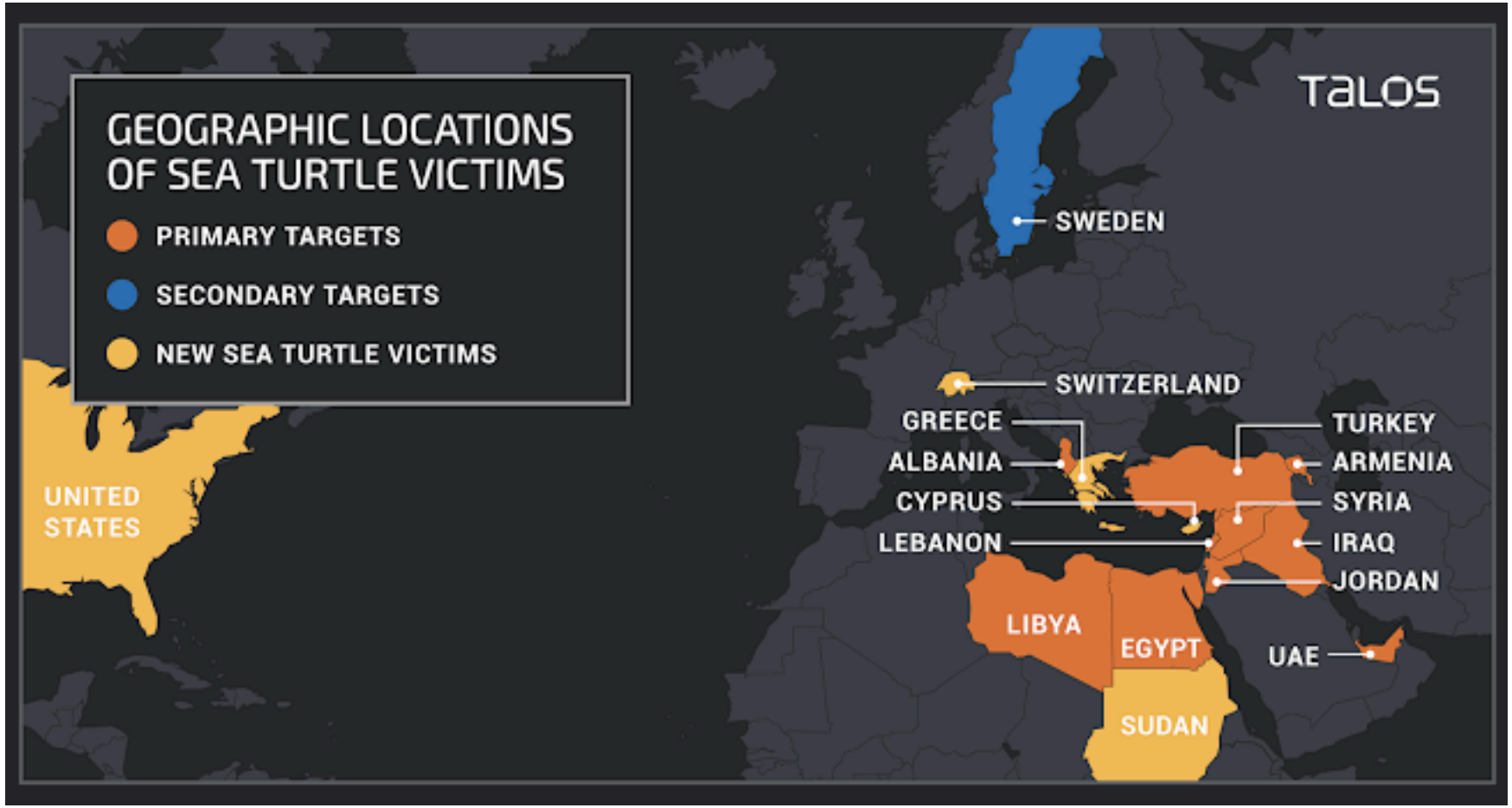
Sea Turtle

TUESDAY, JULY 9, 2019

Sea Turtle keeps on swimming, finds new victims, DNS hijacking techniques

(Source https://blog.talosintelligence.com/2019/07/sea-turtle-keeps-on-swimming.html)

Sea Turtle Updated Victims (through mid 2019)



(Source https://blog.talosintelligence.com/2019/07/sea-turtle-keeps-on-swimming.html)

It’s time to move away from SHA-1 (January 2020)

SHA-1 is a Shambles (see https://sha-mbles.github.io/)

- New attack that makes it easier to fool DNS zone administrators into creating hash values (trusted signatures over DNS records) they don’t intend to sign.
- Attack makes it much faster for malicious actor to create chosen-prefix collisions.
- This creates serious consequences for parts of the Internet using SHA-1.
- **Action:** Stop using SHA-1 and change to algorithms using stronger hashes.

(Source: https://www.icann.org/news/blog/it-s-time-to-move-away-from-using-sha-1-in-the-dns)

Recent guidance on phishing

Attacks in the news (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

Reporting suspicious email

- If you receive a suspicious email appearing to come from ICANN
  - Avoid clicking links or opening the attached file
  - FORWARD the entire message to globalsupport@icann.org
  - Do not alter the subject line or forward message as attachment
  - Delete the suspicious email from your inbox
  - If you opened an attached file or clicked a link, contact your IT support staff

Protecting yourself from phishing

- Carefully review every email you receive
- Phishing emails and websites often mirror familiar visuals and language, may include the logos and branding of the organization and appear that the organization is the sender
- Be suspicious of any email or webpage from ICANN that offers domain renewals or registration services.
- ICANN org does not process domain renewals or send WHOIS data privacy notices.

Protecting yourself from phishing

- Email attachments may contain malware
- Hyperlinks may direct you to malicious websites or forms
- Never enter your password into a page you arrived at by following a link in an email
- Phishing emails often contain a false sense of urgency (such as legal scams, expiring domain renewals)

DNS Security & DNS Abuse

Domain Name System (DNS) - Abuse vs. Misuse

DNS misuse is different from DNS abuse

- **DNS abuse** refers to anything that attacks or abuses the DNS infrastructure
- **DNS misuse** refers to exploiting the DNS protocol or the domain name registration processes for malicious purposes

What Constitutes DNS Abuse or Misuse?

There is no globally accepted definition, but some definitions include:

- Cybercrime
- Hacking
- Malicious conduct

Categories within threats to the DNS:

- Data corruption
- Denial of service
- Privacy

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." – legal threats, targeted/spear phishing

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"

Maliciously Registered Domain Names

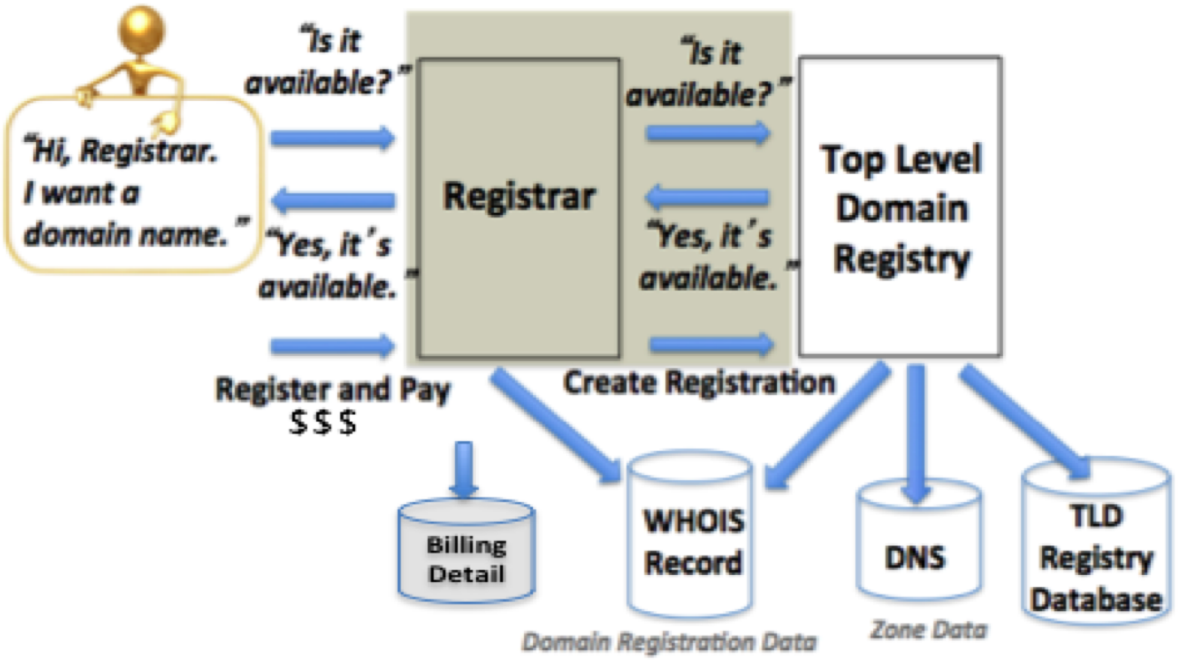
- Domains registered by criminals for
  - Counterfeit goods
  - Data exfiltration
  - Exploit attacks
  - Illegal pharma
  - Infrastructure (ecrime name resolution)
  - Malware C&C
  - Malware distribution, ransomware
  - Phishing, Business Email Compromise
  - Scams (419, reshipping, stranded traveler…)

Misused Domain Registrations

- Domains compromised or hijacked by criminals or state-sponsored actors
- Host criminal DNS infrastructure
- Domain, NS, or MX Hijacking
- Hacktivism (e.g., defacement)
- Tunneling (covert communications)
- Data Exfiltration
  - Methods
- Infection (Malware)
- Configuration change (DNSChanger)
- Poisoning (resolver/ISP)
- Man in the Middle attacks

Domain name registrations are attractive targets for attacks

- Process is automated and rapidly provisioned
- Registrar correspondence with registrants is largely email
- Registrant is responsible for registration data accuracy
- Inexpensive registrations are plentiful…
  Good for consumers, good for attackers, too



Criminals exploit registrar email correspondence (Phishing)

Please verify your email address for [redacted]om

GoDaddy <info@godaddy.com-verify.name>

Dear GoDaddy Customer,
ICANN has implemented a new Transfer Policy which affects all ICANN-accredited r
email is in response to ICANN's requirement that registrars ask their customers to c
can read more about this requirement on ICANN's site at http://www.icann.org/who
You have registered one or more domains from Godaddy Inc. and verification of the
to remain active. Please click the link below to verify the email address. If you don't
website on hold u
Please cut-and-pa
http://www.godad
Please remember
domain name reg
Thanks for your at
Thanks for being
Copyright (C)1999

Account Notice : Error number :6678 Spam x

GoDaddy.com <Renewals@i.godaddy.com>
to me

Why is this message in Spam? It contains content that's typically used in spam messages. Learn more

Dear Valued GoDaddy Customer: Cristian Badea

more than 7852 directo

Reply Reply All Forward More

Domain [redacted].COM Suspension Notice
From: LIQUIDNET Ltd. Add to Contacts
Sent: Mon, Nov 2, 2015 at 9:50 pm
To: [redacted]@thexyz.com

Dear Sir/Madam,

The following domain names have been suspended for violation of the LIQUIDNET Ltd. Abuse Policy:

Domain Name: [redacted].COM
Registrar: LIQUIDNET Ltd.
Registrant Name: [redacted]

Multiple warnings were sent by LIQUIDNET Ltd. Spam and Abuse Department to give you an opportunity to address the complaints we have received.

We did not receive a reply from you to these email warnings so we then attempted to contact you via telephone.

We had no choice but to suspend your domain name when you did not respond to our attempts to contact you.

Click here and download a copy of complaints we have received.

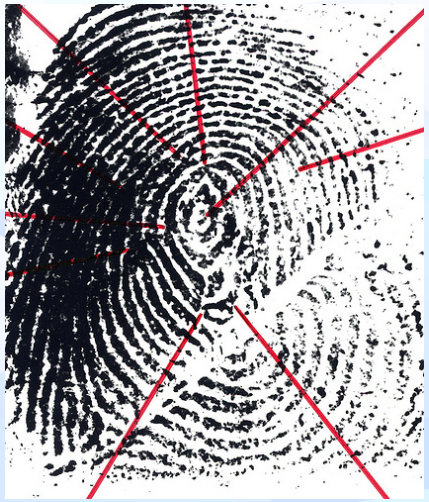
Please contact us for additional information regarding this notification.

Sincerely,
LIQUIDNET Ltd.
Spam and Abuse Department
Abuse Department Hotline: 480-324-4655

How many domain registrants are victims of compromised email accounts?

How many use compromised account credentials from Yahoo! or Equifax breaches?

Collecting Evidence of DNS Abuse/Misuse



Analogs:
- Number of matching minutiae
- Body of evidence

- ✓ Recent domain registration creation date
- ✓ Questionable Whois contact data
- ✓ Privacy protection service
- ✓ Suspicious values in DNS Zone data (e.g., TTL)
- ✓ Spoofing or confusing use of a brand
- ✓ Known DGA or malware control point
- ✓ Hosted on suspicious/notorious name servers
- ✓ High frequency/volume of name errors
- ✓ Suspicious (notorious) hosting location
- ✓ Suspicious (notorious) service operator
- ✓ Base site content is non-existent or bad
- ✓ Linked content is suspicious or bad
- ✓ Suspicious mail headers, sender, or content

Not always easy to identify badness

- Criminals Use Obfuscation
  - Redirection: hacked sites use URL shorteners
  - Recursion: Shortened URLs are shortened
  - One-time use URLs
  - Add subdomains to zone at a hacked DNS server
  - Country- or script-specific content; non-visible content
  - Privacy-protected domain registrations
  - Whois Point of Contact information culled from obituaries
- Criminals use impersonation
- Criminals hide in plain sight
  - They operate from legitimate or compromised resources

Governmental Advisory Committee

Beijing GAC communique, April 2013

- Mitigating abusive activity—Registry operators will ensure that terms of use for registrants include prohibitions against the distribution of malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law.
  https://www.icann.org/en/system/files/correspondence/gac-to-board-18apr13-en.pdf

Hyderabad GAC communique, November 2016

- The GAC would like to remind ICANN that the list of Security Threats in the New gTLD Safeguards is not meant to be exhaustive. In fact, the Security checks Safeguard applicable to all New gTLDs refers to "security threats such as phishing, pharming, malware, and botnets" (emphasis added), which does not exclude other relevant threats. Please describe what analysis and reporting is conducted regarding other relevant threats not listed above, including **spam**?
  https://www.icann.org/en/system/files/correspondence/gac-to-icann-08nov16-en.pdf

Governmental Advisory Committee

- **GAC Public Safety Working Group (PSWG)**

The GAC PSWG continued the discussion with the GAC on abuse mitigation measures. In line with its previous communiqués, the GAC noted that DNS abuse threatens the security and stability of the DNS, the universal acceptance of TLDs and consumer trust. This is also reflected in the recommendations of the Consumer Trust, Consumer Choice and Competition Review Team (CCT RT) whose importance the GAC highlighted in its Kobe Communiqué. The GAC agreed to engage with the ICANN community on a more effective approach to abuse mitigation, also with a view to the adoption of effective abuse mitigation policies for subsequent rounds of new gTLDs. The PSWG indicated that next steps should include the renewed engagement with the ICANN organisation to obtain further clarifications on a number of implementation questions contained in the annex to the Hyderabad Communiqué; the follow-up on the CCT RT recommendations; and a cross-community session at ICANN66 in Montreal.

(Source GAC Marrakech Communique, 27 June 2019)

Public Safety Entities

Roles of Law Enforcement

Top-level domain (TLD).com

Based on an official request the TLD refers to a law enforcement nameserver replacing the criminals' nameserver

Law Enforcement Name Server

"Sinkhole"

- Secure Information Exchange
- In-Depth Analysis and Digital Forensics
- Operational Coordination and De-confliction
- Bridge between LE and Private Sector
- 24/7 Command Post
- Financial support
- Public Awareness Raising

Public Safety Working Group

- Working Group reports to & advises GAC on matters of abuse, public safety or public interest policy
- Includes law enforcement & invited cybersecurity SMEs
- Considers:
  - General Data Protection Regulation
  - Carrier Grade Network Address Translation
  - Fast Flux
  - DNS Abuse

Consideration of DNS abuse in ICANN agreements

Registry base agreement

Specification 6 (4):

- Abuse PoC, malicious use of orphan glue records

Specification 11 (3):

- Registry Operator agrees to perform the following specific public interest commitments…

https://www.icann.org/resources/pages/registries/registries-agreements-en

Registrar Accreditation Agreement (RAA13)

Section 3.18:

- Abuse Point of Contact,
- Duty to investigate reports of abuse: "reasonable and prompt steps to investigate and respond appropriately to any reports of abuse"
- Publish procedures for receipt, handling, and tracking of abuse reports

Section 2.2:

- Abuse/Infringement Point of Contact for Privacy/Proxy Provider
- Publish process or facilities to report abuse of a domain name registration managed by the P/P Provider

- https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

Investigating Hosting Sites and Hosted contents

Identifying Bad Neighborhoods

An ASN is like a neighborhood on the Internet

Crime activity often concentrates in neighborhoods

These neighborhoods earn poor reputations from researchers or investigators

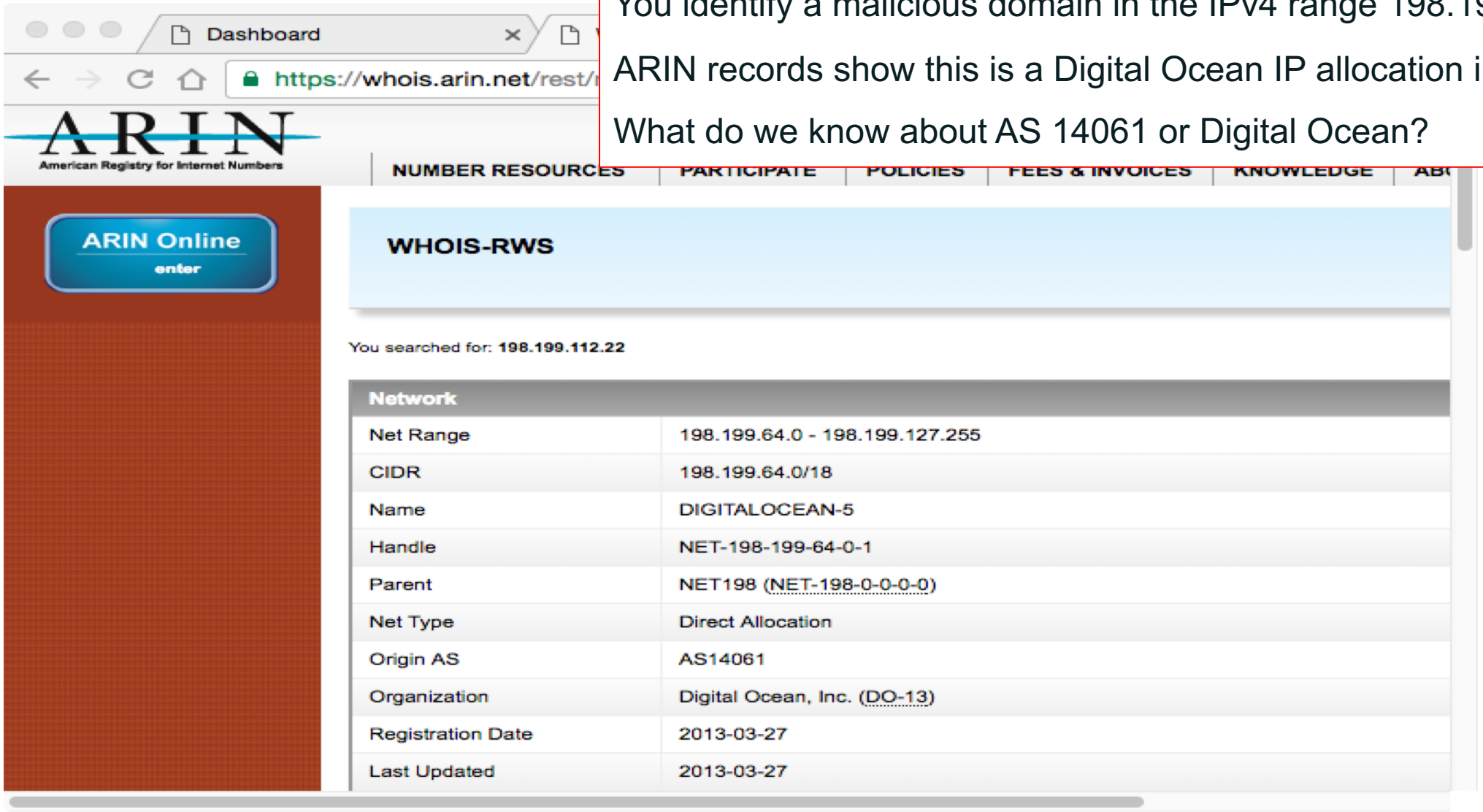
https://www.flickr.com/photos/tagthis/

Use Case: Checking the reputation of an ASN

You identify a malicious domain in the IPv4 range 198.199.64.0/18

ARIN records show this is a Digital Ocean IP allocation in AS 14061

What do we know about AS 14061 or Digital Ocean?



Enumerate ASNs Using Seclytics Threat Intelligence

https://dashboard.seclytics.com

SECLYTICS

HOME STATS API DOCS BLOG MY ACCOUNT

digital ocean | Look up

ASNs

We found 10 ASNs that match your query.

Search our threat data for these ASNs.

14061	DIGITALOCEAN-ASN - Digital Ocean, Inc.
62567	DIGITALOCEAN-ASN-NY2 - Digital Ocean, Inc.
133165	DIGITALOCEAN-AS-AP Digital Ocean, Inc.
200130	DIGITALOCEAN-ASN-1
201229	DIGITALOCEAN-GERMANY
202018	DIGITALOCEAN-ASN-3
202109	DIGITALOCEAN-ASN-2
393406	DIGITALOCEAN-ASN-NY3 - Digital Ocean, Inc.
394362	DIGITALOCEAN-ASN-CA1 - Digital Ocean, Inc.
135340	DIGITALOCEAN-AS-IN Digital Ocean, Inc.

Digital Ocean is an IAAS advertising itself as cheap cloud computing for developers

It advertises 10 ASNs

What Do Others Report About the Neighborhood?

Dashboard | Whois-RWS | IP to ASN Mapping - Tea | Dave

https://dashboard.se...

SECLYTICS

HOME | STATS | API DOCS | BLOG | MY ACCOUNT

Lookup IPs, CIDRs, Hashes, Hosts, ASNs or Organization Name

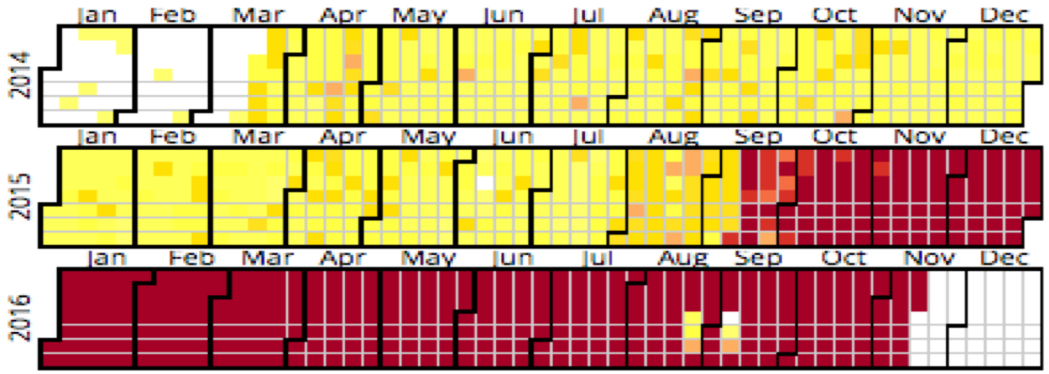
14061

ASN - 14061

Export as JSON via API

ASN	14061 DIGITALOCEAN-ASN - Digital Ocean, Inc.
Country	United States
Registry	ARIN
Reported by	1d4us_ssh abuse_ransomware abuse_ssl abuse_ssl_ipbl alienvault_rep apwg apwg_fb badips bambenek_osint bf_blocker blocklist blocklist_ua botnet_tracker botscout

Days Reported

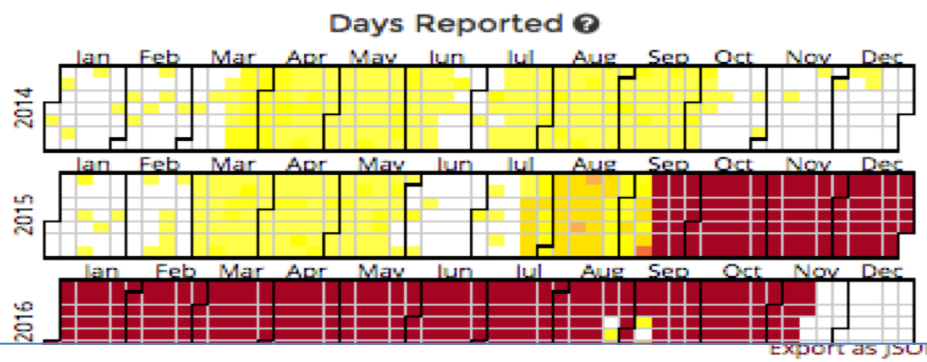


ASN 14061 has substantial reports of abuse of all kinds from numerous reporters

All The Hosting Provider's Neighborhoods Have Poor Reputations

ASN 200130
DIGITALOCEAN-ASN-1
Country
Registry RIPE

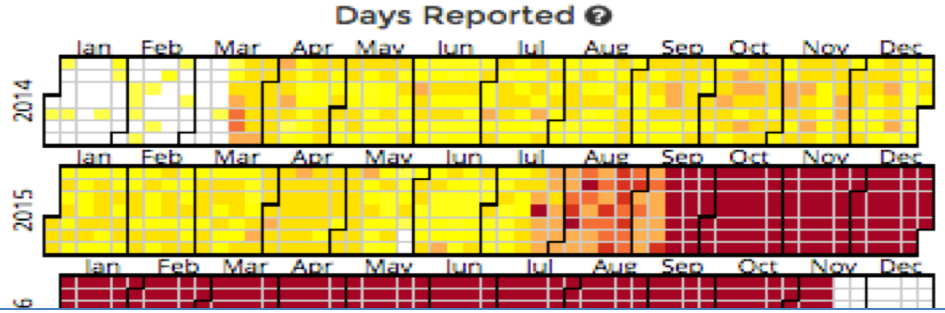
Reported by
abuse_ransomware
abuse_ssl
abuse_ssl_ipbl
alienvault_rep
apwg
apwg_fb
arbor_attacks
badips



Export as JSON via API

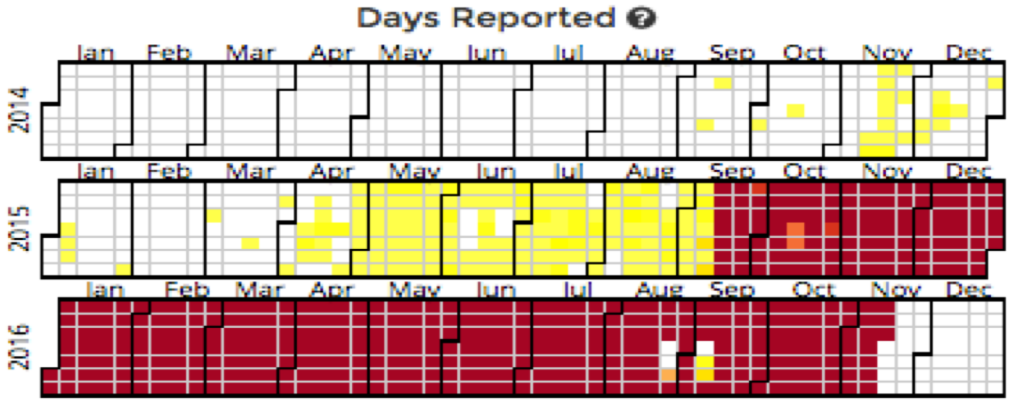
ASN 62567
DIGITALOCEAN-ASN-NY2 - Digital Ocean, Inc.
Country United States
Registry ARIN

Reported by
1d4us_ssh
abuse_ransomware
abuse_ssl
abuse_ssl_ipbl
alienvault_rep
apwg



ASN 202018
DIGITALOCEAN-ASN-3
Country Netherlands
Registry RIPE

Reported by
abuse_ransomware
abuse_ssl
abuse_ssl_ipbl
alienvault_rep
apwg
apwg_fb
badips
bambenek_osint
bf_blocker
blocklist



All 10 Digital Ocean ASNs have similar levels of abuse reports

Reputation may also be an indicator of the degree of cooperation you'll encounter from an operator

Who?, What?, When?, Where?, How?

- Who is the target of your action?
  - Registrant
  - Hosting operator (Web, Mail, DNS…)
  - Network (ISP)
  - Registrar (or reseller),
  - Registry Operator
- What is the goal of the action?
- When will you act? In synchrony with others?
- Where in the world are the people, content, networks, or systems that you're targeting?
  - Many investigations involve parties or criminal assets in several jurisdictions
- How will you take action?
  - Court order, acceptable use, compliance violation

What do you want the DNS to do?

- How should DNS respond to queries for seized domains?
  - Is name resolution service (DNS) to be suspended,
    - i.e., *the DNS should not resolve the name to an address*
  - Is redirection to a text of notice page required?
  - Is redirection(sinkholing) of Internet hosting from the criminal's IP address to one you oversee required?

- Who will operate DNS for seized domains?
  - Is the party that provides name resolution service (DNS) to be changed?

What should WHOIS display?

- Is the domain name to be transferred to a different sponsoring registrar?
- Are you transferring the registration? To whom? Have you investigated fee waivers?
- What name server is hosting name resolution?
- What status should the registry set for the domain?
  - E.g., prevent transfer, update, or delete?

Minimizing collateral harm

Examples of questions to ask before you file:

- Will your action disrupt
  - Name service for other (reputable) domains?
  - Hosting services for parties other than those named in your order?
- What services other than web are affected by your action on the domain name?
- What do you expect as the “long term disposition” of the domain name?
- Could your actions interfere with other active investigations, monitoring, surveillance… ?

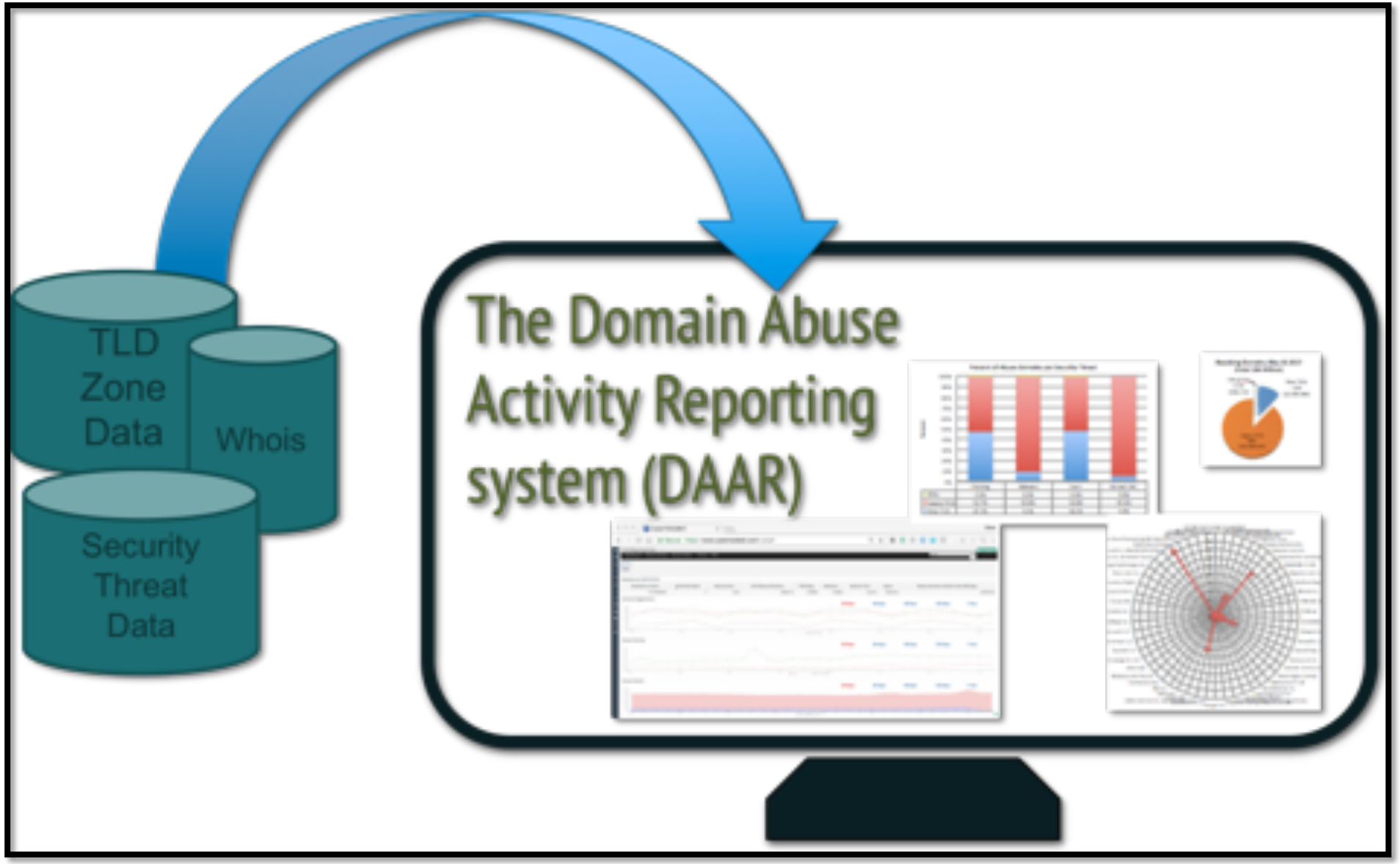
Steps to investigate domains

1. Collect evidence of abuse
2. Determine hosting provider or registrar
   A. Is there a reseller of that registrar involved?
3. Contact hosting provider or registrar abuse desk
   A. Provide evidence of abuse
   B. Point out registration or content problems
   C. Ask if a TOS, ICANN, ccTLD registry domain suspension policy applies
4. No success? Contact registry
   A. Same supporting info as registrar
5. Escalate
   A. Sharing/intel networks
   B. National CERT or local LE
   C. Whois Data Problem Reporting System/RDS Reporting
   D. ICANN Compliance

If you are looking at a suspicious domain, someone else is, too.

Domain Abuse Activity Reporting System (DAAR)

DAAR Data Sources



The Domain Abuse Activity Reporting System

What is it?

- A system for reporting on domain name registration and abuse data across TLD registries and registrars

How does DAAR differ from other reporting systems?

- Studies all gTLD registries and registrars for which we can collect zone and registration data
- Employs a large set of reputation feeds (e.g., blocklists)
- Accommodates historical studies
- Studies multiple threats: phishing, botnet, malware, spam
- Takes a scientific approach: transparent, reproducible

https://www.icann.org/octo-ssr/daar

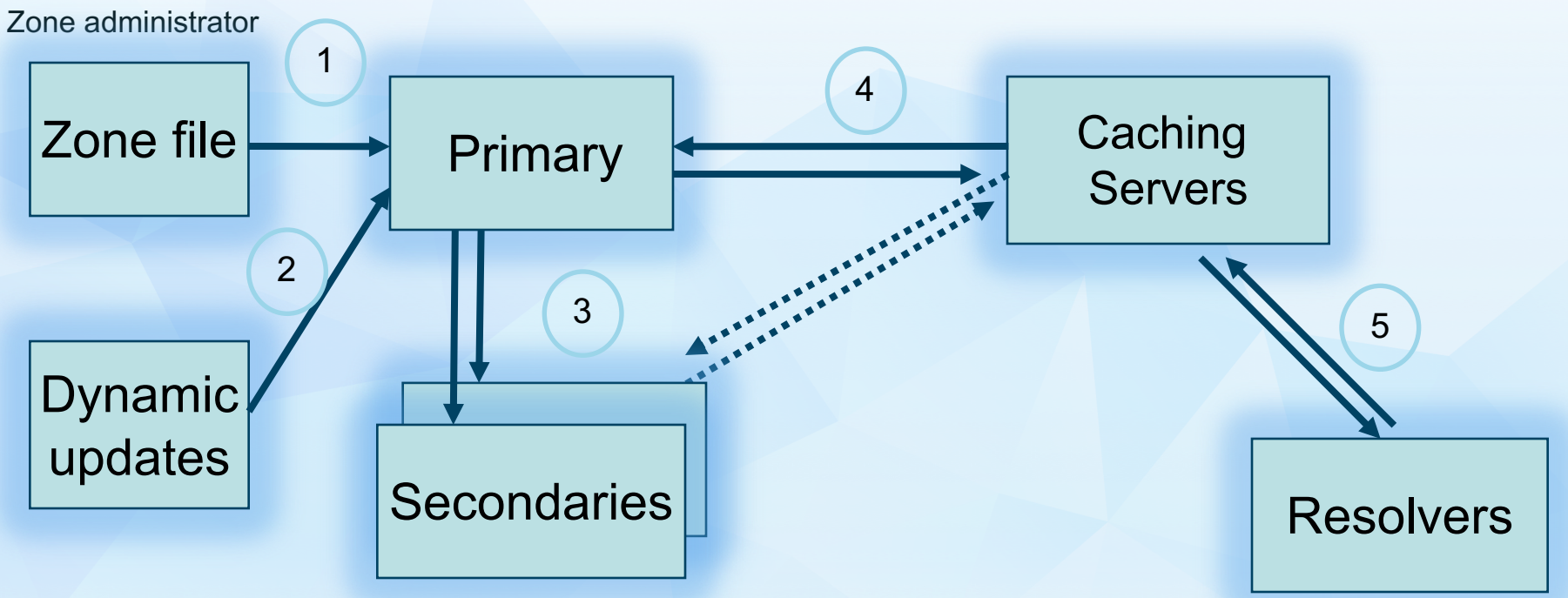
Project Goals

- **DAAR data can be used to**
  - **Report on threat activity at TLD or registrar level**
  - **Study histories of security threats or domain registration activity**
  - **Help operators understand or consider how to manage their reputations, their anti-abuse programs, or terms of service**
  - **Study malicious registration behaviors**
  - **Assist operational security communities**

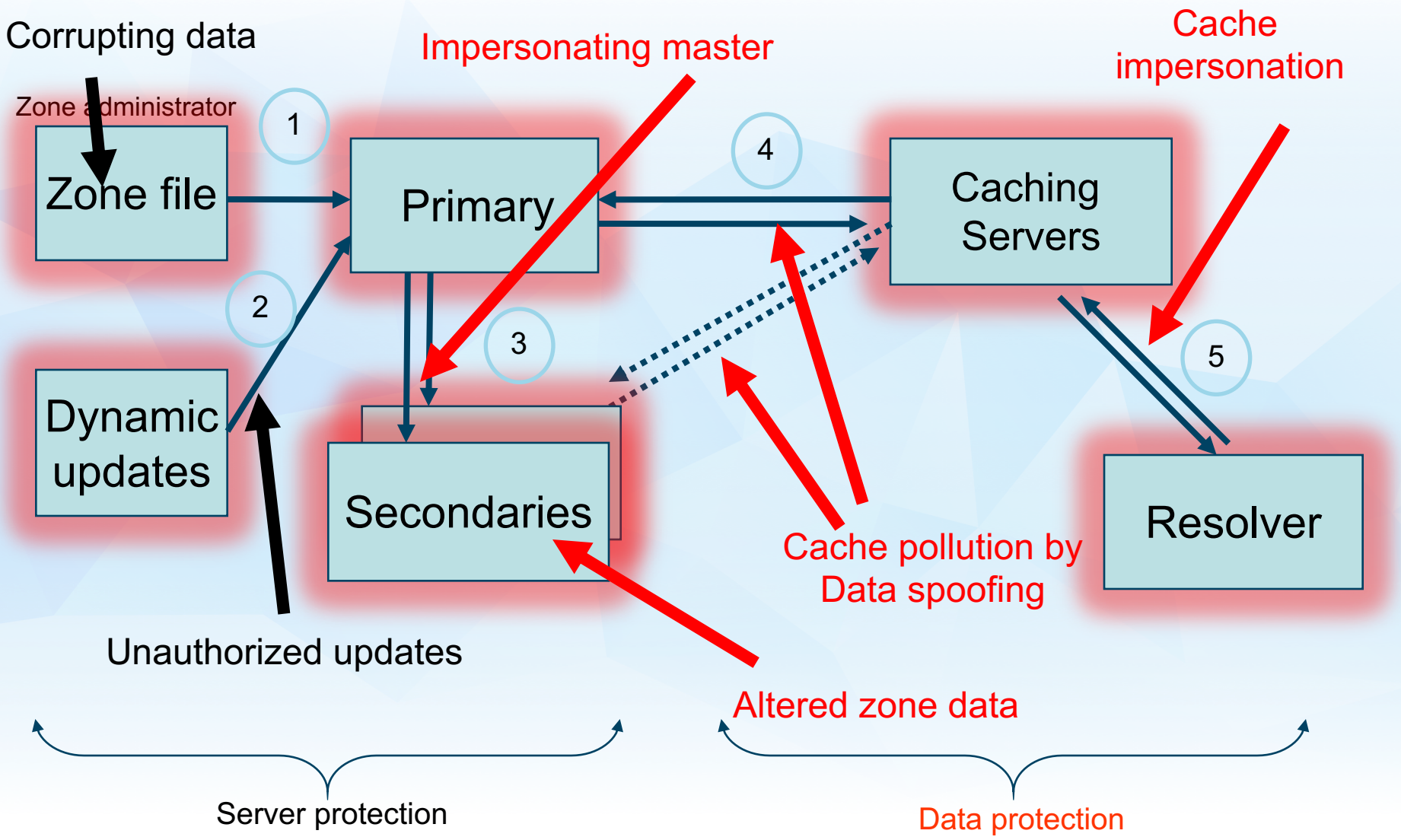
The purpose of DAAR is to provide data to support community, academic, or sponsored research and analysis for informed policy consideration

Securing the DNS Infrastructure

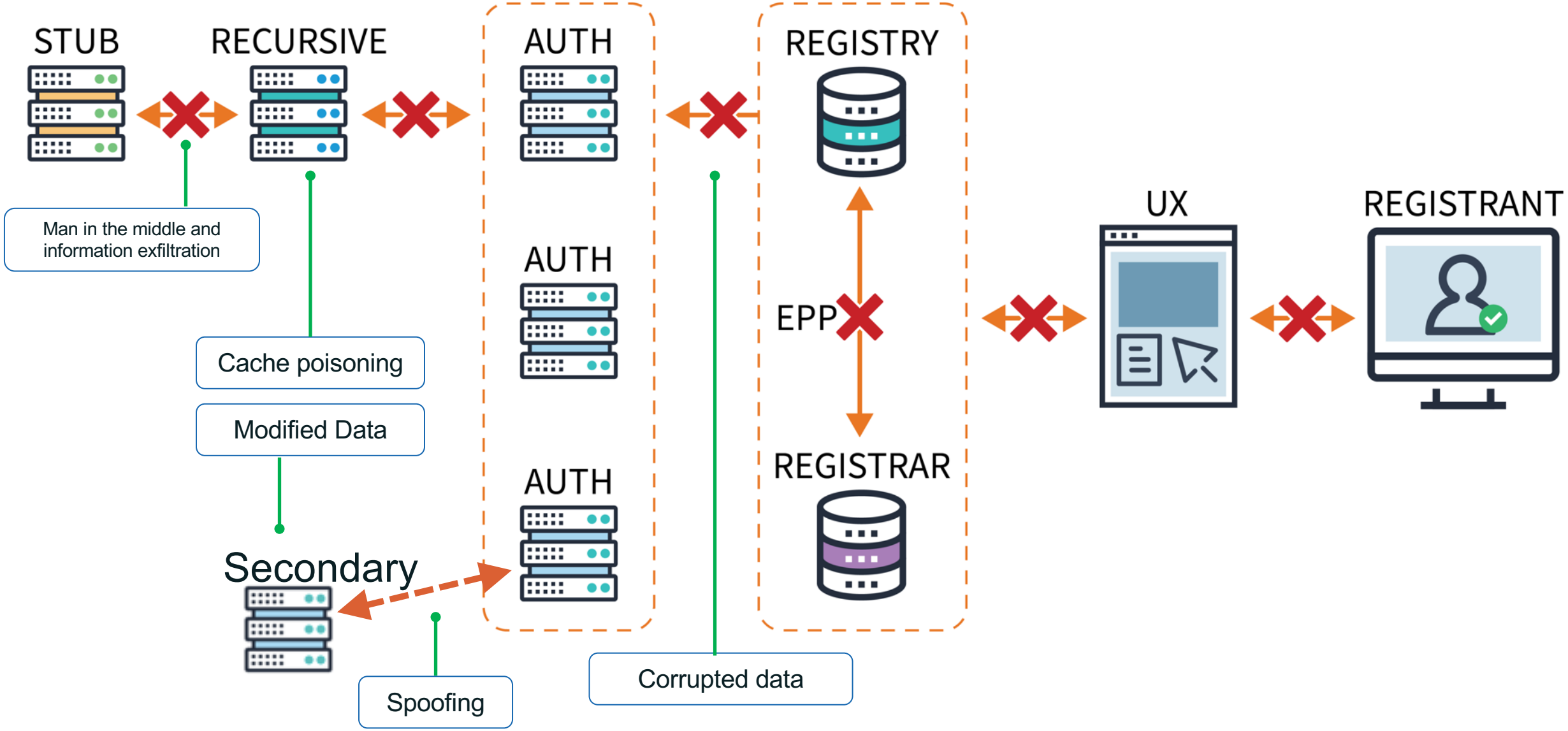
DNS: Data Flow



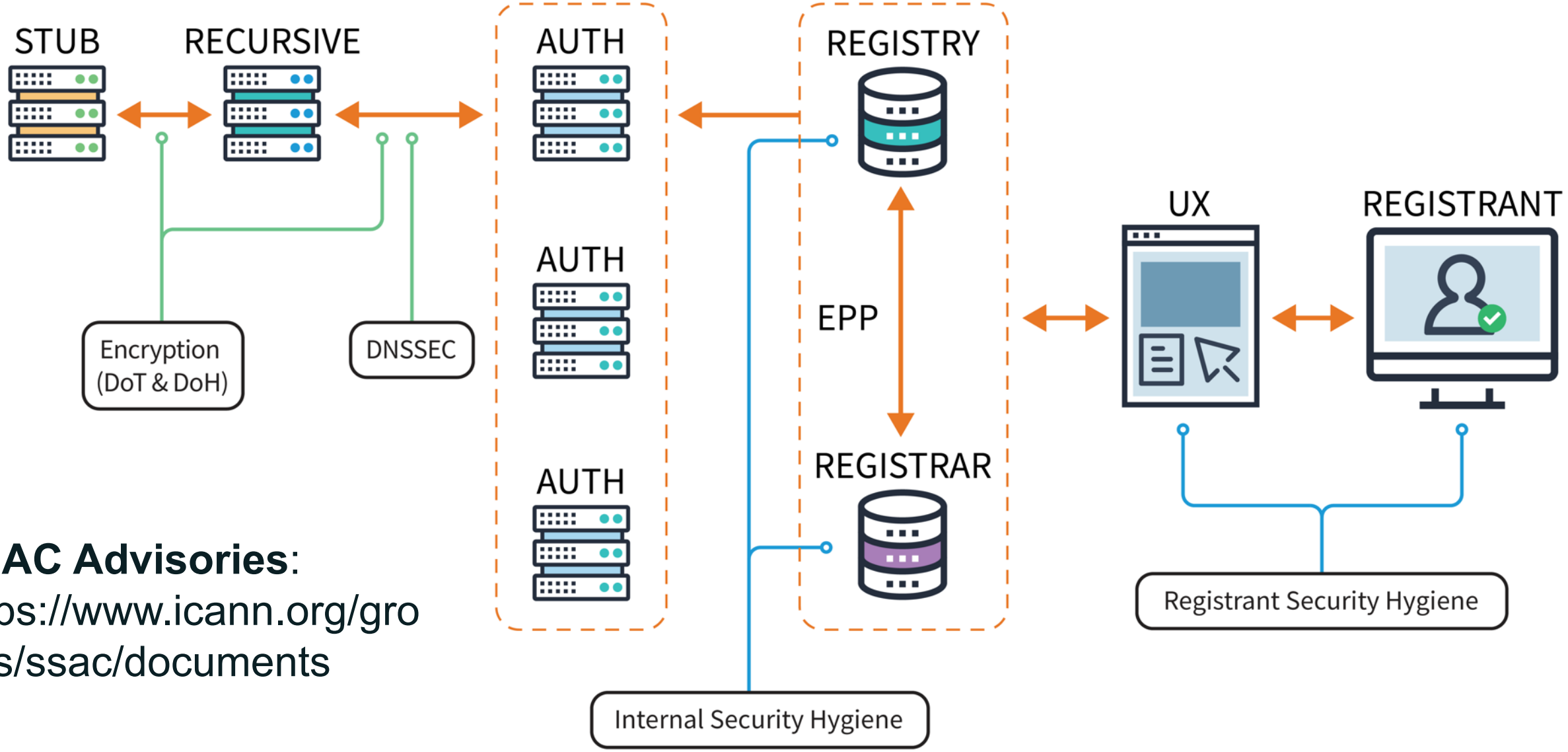
DNS Vulnerabilities



Some of the Potential Target Points of the DNS



A More Secure DNS Ecosystem



SSAC Advisories:
https://www.icann.org/groups/ssac/documents

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

DNSSEC

One of the most important recommendations is to implement DNSSEC: “Domain Name System Security Extensions”

- DNSSEC introduces PKI cryptography that provides assurances to users that DNS data they are seeing is valid and true
- To implement DNSSEC
  - **SIGN** all DNS data you own
  - **VALIDATE** all DNS data passing through your DNS resolvers

Zone Integrity

It is important to periodically **audit** the authoritative DNS data you are publishing

- Compare your source database vs. the actual zone file being published -- is the zone file compromised?
- Review and validate entries in any available log files of changes made

Authorization

- Conduct a thorough review of who has administrator access (”root”) to both DNS and network infrastructure elements
- Audit the controls over granting root access to all systems that contribute to building your authoritative zone files
- Periodically review log files for unauthorized access to systems

Authentication

- Practice good hygiene on password management:
  - Enforce sufficient password complexity, especially length of password
  - Ensure that passwords are not shared with other users
  - Ensure that passwords are never stored or transmitted in clear text
  - Enforce regular and periodic password changes
  - Enforce a password lockout policy
  - Implement multi-factor authentication to all systems (especially for administrator access)

Patching

- The most obvious software exploits are those that have already been fixed!
- Ensure all system security patches have been reviewed and have been applied

E-mail Security

- E-mail is still a significant and vulnerable system that bad actors use to infiltrate networks
- Ensure your email domain has a DMARC policy with SPF and/or DKIM and that you enforce such policies provided by other domains on your email system
  - **SPF** (Sender Policy Framework): validating that the originating mail server IP address matches the MX record defined by the mail server's domain records
  - **DKIM** (Domain Keys Identified Mail): Reputation based e-mail system
  - **DMARC** (Domain-based Message Authentication Reporting and Conformance): mechanism to validate that legitimate e-mail conforms with local SPF and DKIM policies, and that illegitimate e-mail purporting to come from domains you control is blocked.

Securing your Organization's Domain Registrations

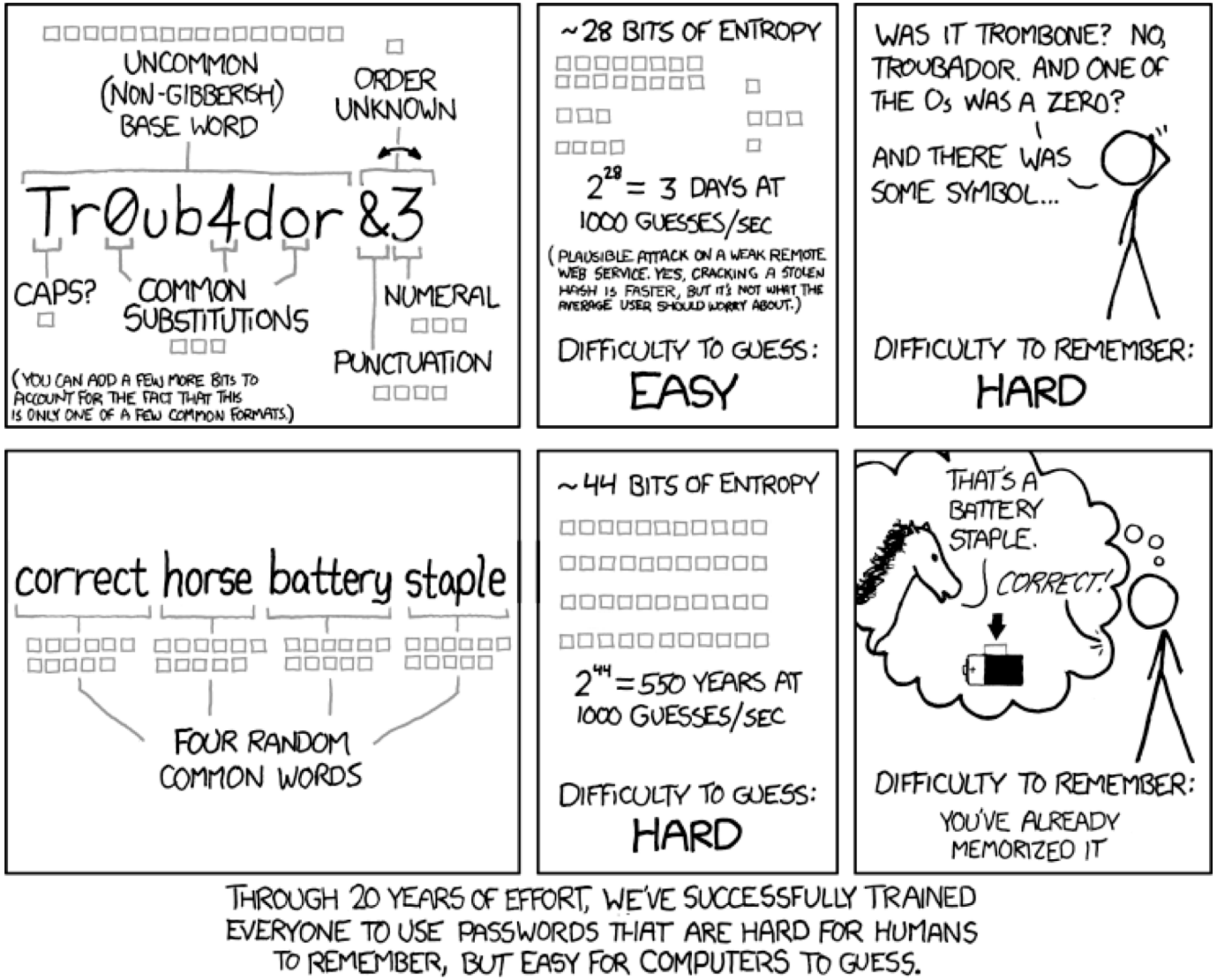
Credential Management

- Registrant credentials are critical for protecting zones
- Strong passwords are **very** important
- Multi-factor Authentication adds an additional layer(s) of protection, specifically helps against some MITM attacks etc
- The email address used for registrar communications should also have strong credentials as this path is used to reset registrar passwords and are targeted frequently
- Don’t forget credentials for email...

Credential Management: MFA

- Multi Factor Authentication(MFA) or 2-Factor Authentication(2FA)
- Use when offered, ask for it when it’s not
- Provides an additional layer of security over just using passwords

Credential Management: Passwords



Source: https://xkcd.com/936/

Credential Management: Passwords

- Microsoft Security baseline for Windows 10 (23 May 2019)
- Dropping password expiration policies
  - “periodic password expiration is an ancient and obsolete mitigation of very low value”
  - Strongly recommends adoption of measures such as banned-password lists, MFA, detection of anomalous login attempts, detection of password-guessing attacks

(https://blogs.technet.microsoft.com/secguide/2019/05/23/security-baseline-final-for-windows-10-v1903-and-windows-server-v1903/)

Credential Management: Review

- Do:
  - Use strong unique passwords
  - Use a password manager
  - Use MFA
- Don’t:
  - Share passwords
  - Re-use passwords across multiple accounts

Registry Locks

- Enable registry locks when available
- Registry locks must be disabled to make changes to records
- Not all registries or registrars support registry locks
  - Often comes at an extra charge
- Area for future work: registry lock process standardization

(see panel from May 2019 Registration Operations Workshop)

DNSSEC

- Sign your DNS zones
- Require users and services to use validating resolvers
- Will not protect from all types of attacks, but provides enhanced integrity protection
- DNSSEC Signed zones were less impacted than others in recent attacks
- DNSSEC Signed zones were like canaries in recent attacks

Be Careful What Nameservers You Use

- The security practices of your nameserver domain name and operators are just as important to the security of your own domain name

Monitoring

- Monitor your DNS infrastructure
- Monitor your DNS zones
- Monitor parent/registry for changes
- Monitor TLS certificate transparency logs
- Monitor for DNSSEC validation failures
- Monitor your nameserver records

Credits:

- ICANN SSAC – presentation from ICANN 64
- ICANN Office of the CTO

Relevant SSAC Publications

Relevant SSAC Publications

- SAC040: Measures to Protect Domain Registration Services Against Exploitation or Misuse
- SAC044: A Registrant's Guide to Protecting Domain Name Registration Accounts
- SAC049: SSAC Report on DNS Zone Risk Assessment and Management
- SAC074: SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle

DNSSEC

DNSSEC Overview

How much trust do we put in the Internet?

- Billions of mobile phones
- Internet of Things to Internet of Everything
- Depending on estimates 30+ billion by 2020

Identifier Operations: What is DNSSEC?

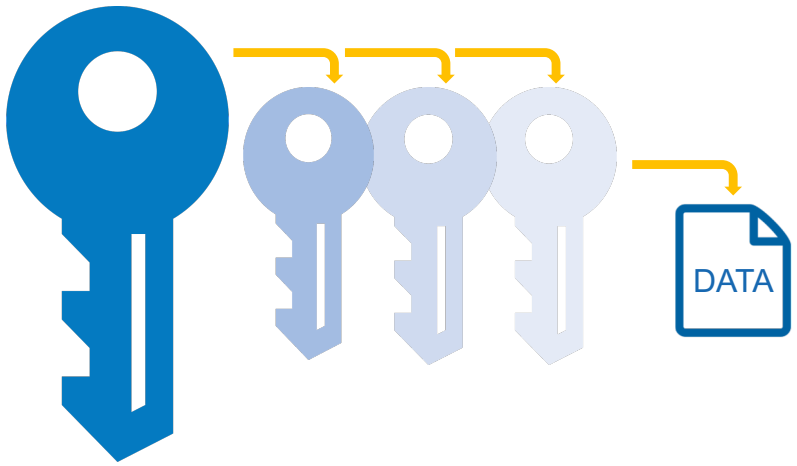
Domain Name System Security Extensions (DNSSEC)

- 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

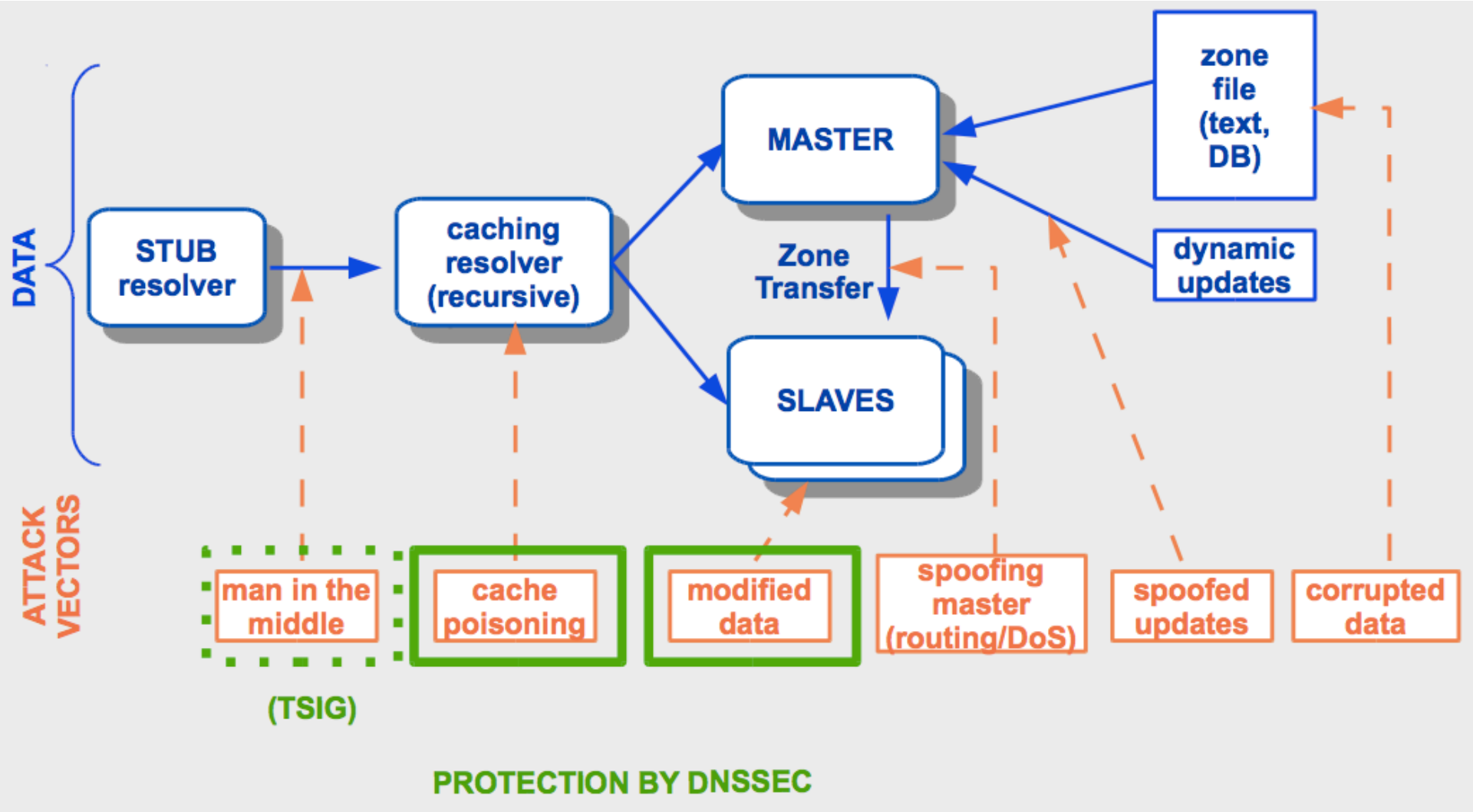
Identifier Operations: DNSSEC Keys

DNSSEC uses Public Key Infrastructure (PKI) technology:

- The “key signing key” (KSK) is the top-most cryptographic key in the DNSSEC hierarchy.
- The KSK is a cryptographic public-private key pair:
  - Public part is the trusted starting point for DNSSEC validation
  - Private part signs the “zone signing key” (ZSK)
- The KSK builds a “chain of trust” of successive keys and signatures to validate the authenticity of any DNSSEC-signed data.



What does DNSSEC protect?



DNS Security Extensions

- Provides origin authentication
- Integrity assurance services for DNS data
- Authenticated denial of existence of DNS data

Benefits

- End User – gain confidence of reaching intended website
- Registrant – fraud mitigation & greater brand protection
- Registrar – Comply with industry standards & meet registrant demands for increased security
- Registry – Meet industry best practices & registrar demands for increased domain security

Benefits

- Protects the directory lookup
- Complements other technologies (https)
- Provides platform for other security improvements

Benefits

- Attract and retain security & reputation-focused registrants
- Create new service offerings
- Adding to trust overall

DNSSEC: So what's the problem?

- Not enough IT departments know about it or are too busy putting out other security fires?
- When they do consider it, they hear old stories of FUD and lack of turnkey solutions?
- Registrars*/DNS providers see no demand leading to "chicken-and-egg" problems.

*but required by ICANN Registrar Agreement

The Business Case for DNSSEC

- Cybersecurity is a significant concern to enterprises, government, and end users. DNSSEC is a key tool and differentiator.
- DNSSEC is the biggest security upgrade to Internet infrastructure in over 20 years. It is a platform for new security applications (for those that see the opportunity).
- DNSSEC infrastructure deployment has been brisk but requires expertise. Getting ahead of the curve is a competitive advantage.

Physical Security

- Environmental
- Tiers
- Access Control
- Intrusion Detection
- Disaster Recovery

- ICANN uses two key facilities, currently in Virginia & California

Physical Security

- Decisions are based on your risk profile
- Suitable power, air; protection from disaster
- Tiers
- Tamper evident packaging

Inside a key management facility

Key Ceremonies

State of DNSSEC Deployment (16 Feb 2020)

Over 90% of TLDs are signed

- 1516 TLDs in root
- 1389 are signed, 1376 have trust anchors published
- About 50% ccTLDs are signed
- Recent adoption in Lao IDN, Greek EU, Kuwait, Slovakia, Venezuela

State of DNSSEC Deployment

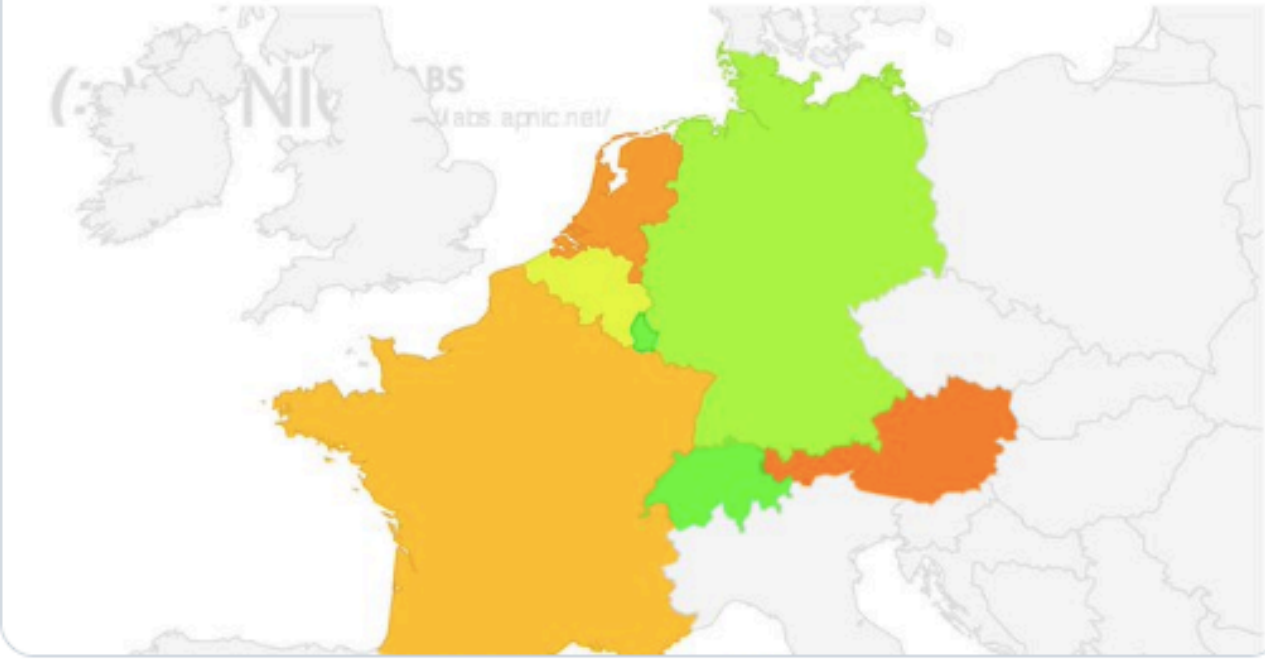
Michael Hausding @mhausding · Jan 6

100'000 .ch domain names are secured with DNSSEC!

the number of **#DNSSEC** signed .ch domain names grows 54% within a year. DNSSEC validation in Switzerland is up to 65%.

securityblog.switch.ch/2020/01/06/100...

Region Map for Western Europe (155)



(Source: Twitter 6 Jan 2020)

State of DNSSEC Deployment

dubai.	YES	YES	NO
duck.	YES	YES	NO
dunlop.	YES	YES	NO
dupont.	YES	YES	NO
durban.	YES	YES	NO
dvag.	YES	YES	NO
dvr.	YES	YES	NO
dz.	YES	YES	NO
earth.	YES	YES	NO
eat.	YES	YES	NO
ec.	NO	NO	NO
eco.	YES	YES	NO
edeka.	YES	YES	NO
edu.	YES	YES	NO
education.	YES	YES	NO
ee.	YES	YES	NO
eg.	NO	NO	NO
email.	YES	YES	NO
emerck.	YES	YES	NO
energy.	YES	YES	NO
engineer.	YES	YES	NO
engineering.	YES	YES	NO
enterprises.	YES	YES	NO
epson.	YES	YES	NO
equipment.	YES	YES	NO
er.	NO	NO	NO
ericsson.	YES	YES	NO

(Source http://stats.research.icann.org/dns/tld_report/)

State of DNSSEC Deployment

Adoption rate higher in new top-level domains

- .bank & .insurance
- .ovh (French ISP)
- .frl (Friesland), .amsterdam, .paris
- .taxi

DNSSEC Adoption

- Now need ISPs & application providers to implement
- At regional level, looking to banks, infrastructure providers and government agencies to adopt
- Adds level of trust for government domains, banks, ISPs

Source Material

- Champika Wijayatunga, Matt Larson, John Crain, ICANN
- ICANN DNSSEC deployment statistics
- NSRC DNSSEC training material
- Olaf Kolkman, Internet Society
- ICANN slides on root key rollover
- Internet Society Deploy360 programme
- IIS (.se)
- Nic.cr & SIDN.nl
- NTLDstats
- ICANN IDN programme statistics
- BCP 219 (Jan 2019)

DNS Privacy

June 2013

This article is more than **6 years old**

NSA collecting phone records of millions of Verizon customers daily

Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama

- Read the Verizon court order in full here
- Obama administration justifies surveillance

Snowden

The Snowden Legacy, part one: What's changed, really?

In our two-part series, Ars looks at what Snowden's disclosures have wrought politically and institutionally.

SEAN GALLAGHER - 11/21/2018, 8:00 AM

Enlarge / Remember this guy?

(ARS Technica, Nov 2018, https://arstechnica.com/tech-policy/2018/11/the-snowden-legacy-part-one-whats-changed-really/)

RFC 7258/BCP 188 – Pervasive Monitoring is an Attack

- IETF community's technical assessment is that PM is an attack on the privacy of Internet users and organizations
  - Discussed at IETF Technical Plenary in 2013
  - Published as BCP in May 2014
  - Led to DPRIVE Working Group; development of DoT, DoH

Use of Public DNS

(https://www.mic.com/articles/85987/turkish-protesters-are-spray-painting-8-8-8-8-and-8-8-4-4-on-walls-here-s-what-it-means)

Use of Public DNS

APNIC

Get IP Manage IP Training Events Research Commu

One in four Google Public DNS requests are being intercepted in China: report

By Baojun Liu on 17 Jul 2019

Category: Tech matters

Tags: DNS, Guest Post, Security, measurement

Like 2 Share

Pocket

Blog home

The Domain Name System (DNS), which resolves domain names into IP addresses for browsers and other applications, serves as one of the most fundamental Internet components.

Unfortunately, almost all DNS packets are sent unencrypted at present. This design makes DNS traffic vulnerable to snooping and manipulation, which is widely considered as one of the Internet's biggest bugs. For example, in the real word, some unscrupulous Internet Service Providers (ISPs) are exploiting this for error traffic monetization, redirecting customers whose DNS lookups fail to advertisement-oriented web servers.

(Source: APNIC Blog, 17 July 2019)

Use of Public DNS

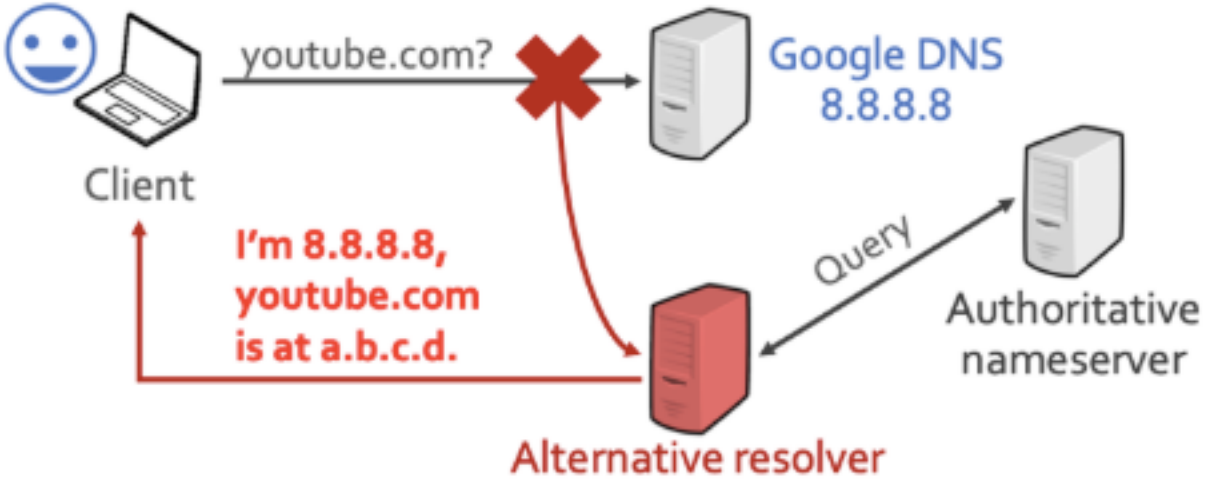


Figure 1 — Google DNS traffic can be intercepted via middleboxes.

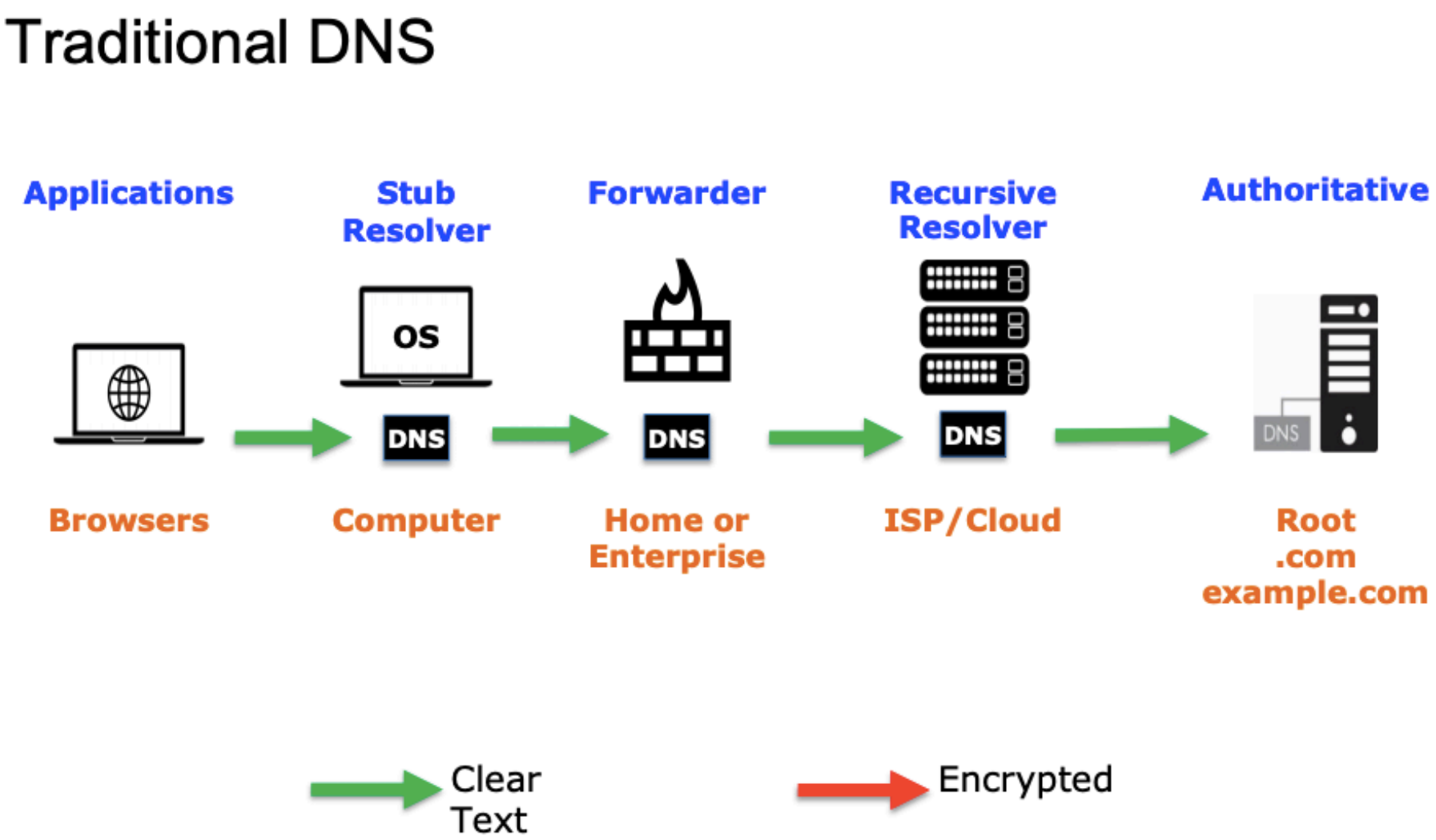
(Source: APNIC Blog, 17 July 2019)

Applications doing DNS

Applications doing DNS

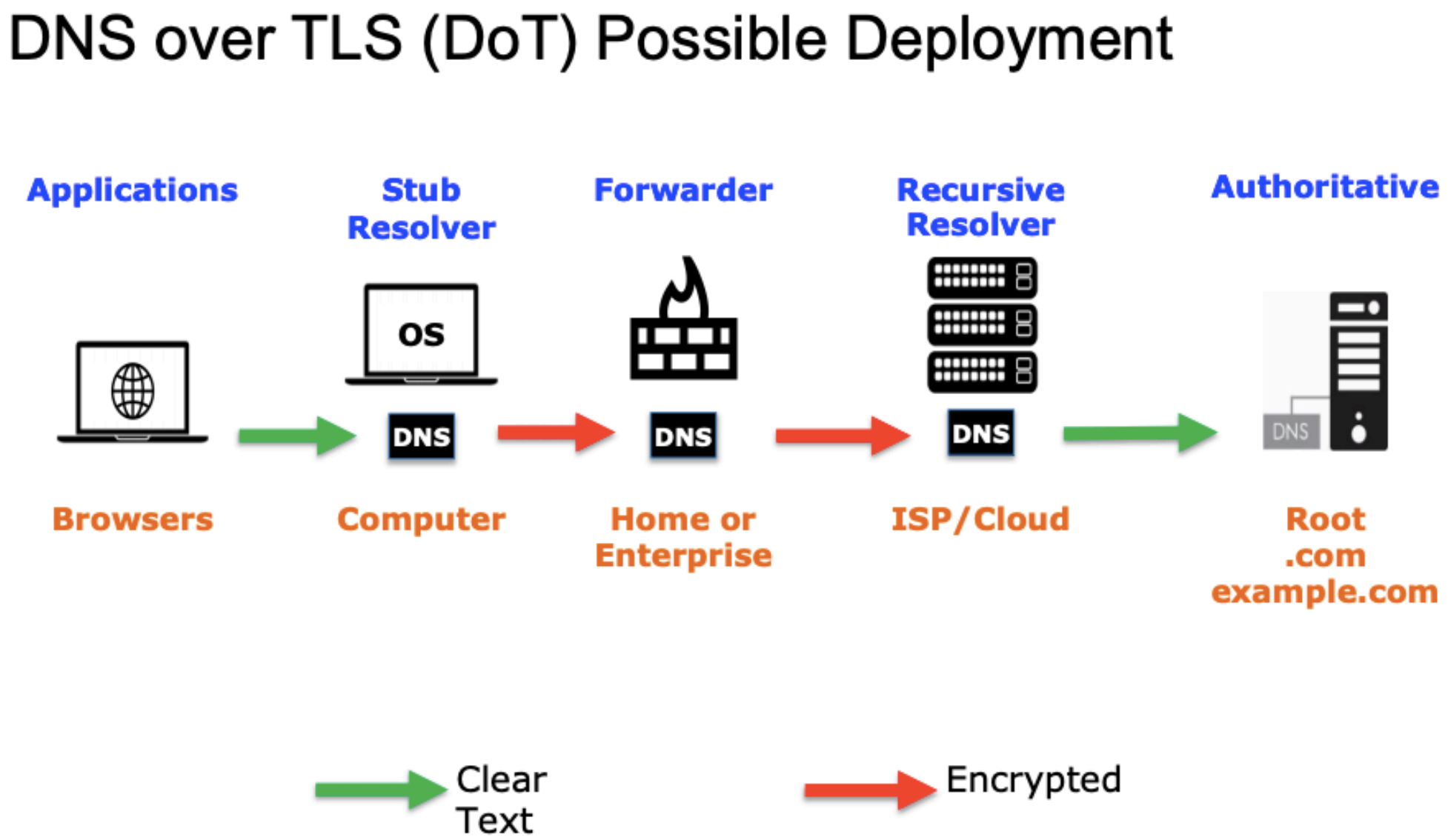
- DNS over TLS, introduced in 2016
- DNS over HTTPS, introduced in 2018
- Both aim to improve privacy for Internet users & security for DNS by adding encryption to DNS requests

Explaining DoH/DoT (from ICANN 65)



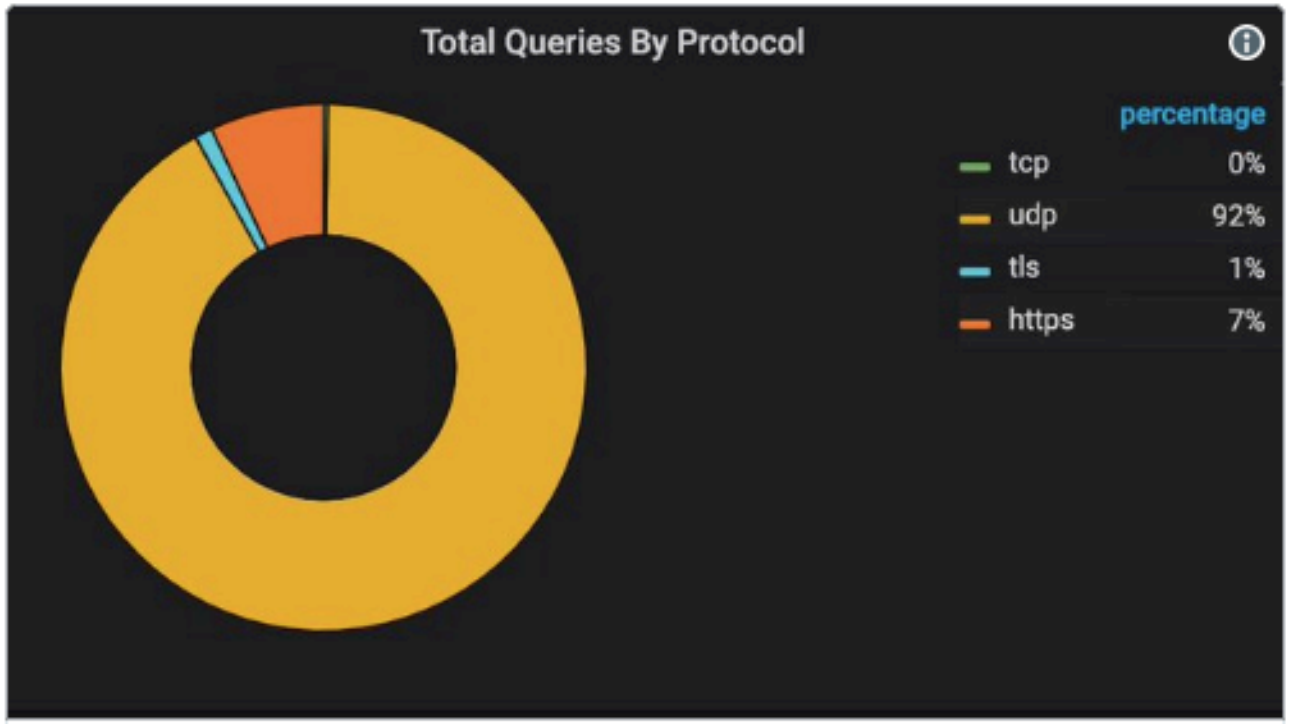
(https://static.ptbl.co/static/attachments/214639/1561448975.pdf?1561448975)

Explaining DoH/DoT (from ICANN 65)



(https://static.ptbl.co/static/attachments/214639/1561448975.pdf?1561448975)

Use of DNS over TLS



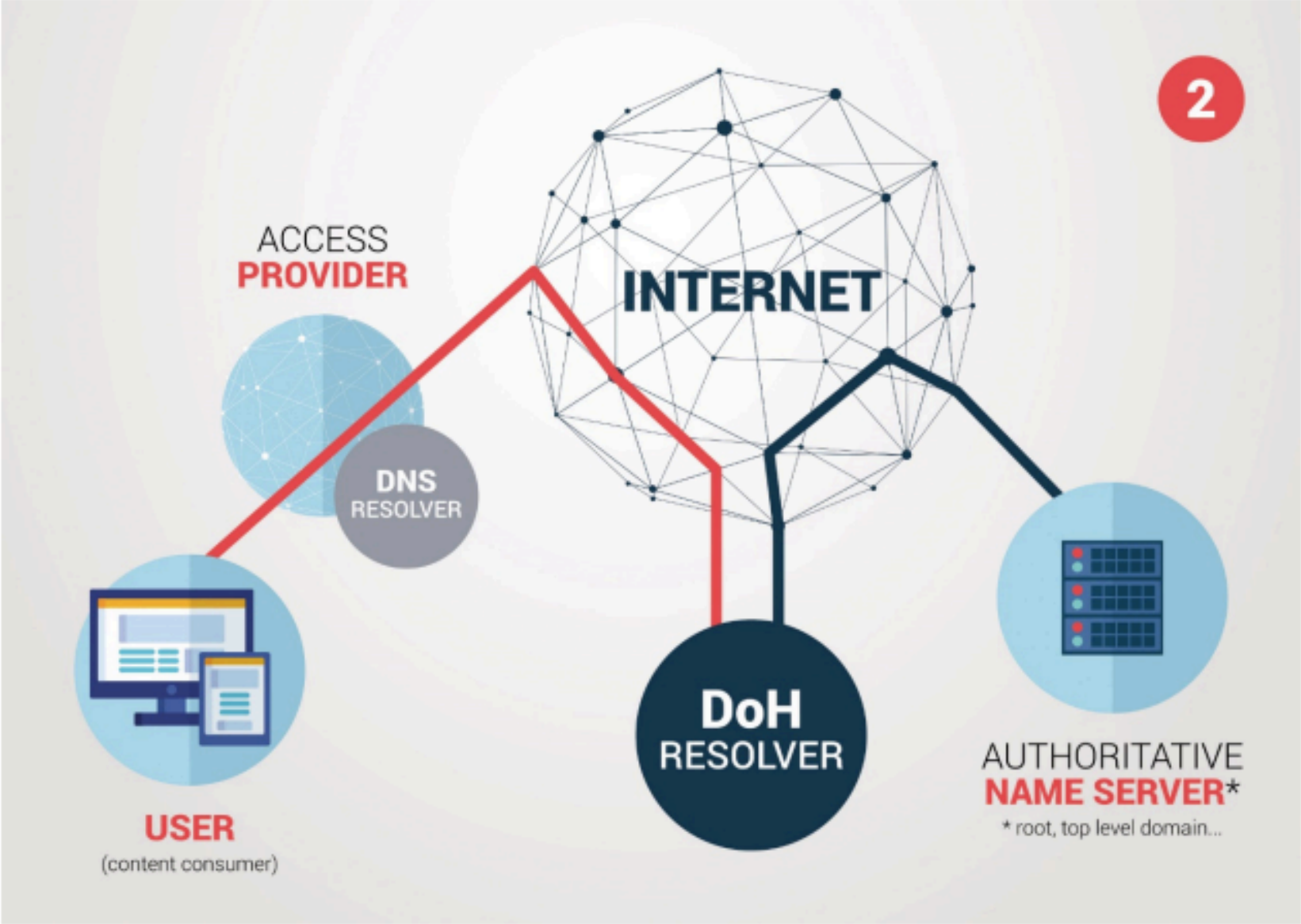
Matthew Prince
@eastdakota

8% of queries to @Cloudflare's 1.1.1.1 (one.one.one.one) are now encrypted via DNS over TLS or DNS over HTTPS. #betterinternet

128 12:57 PM - May 24, 2019

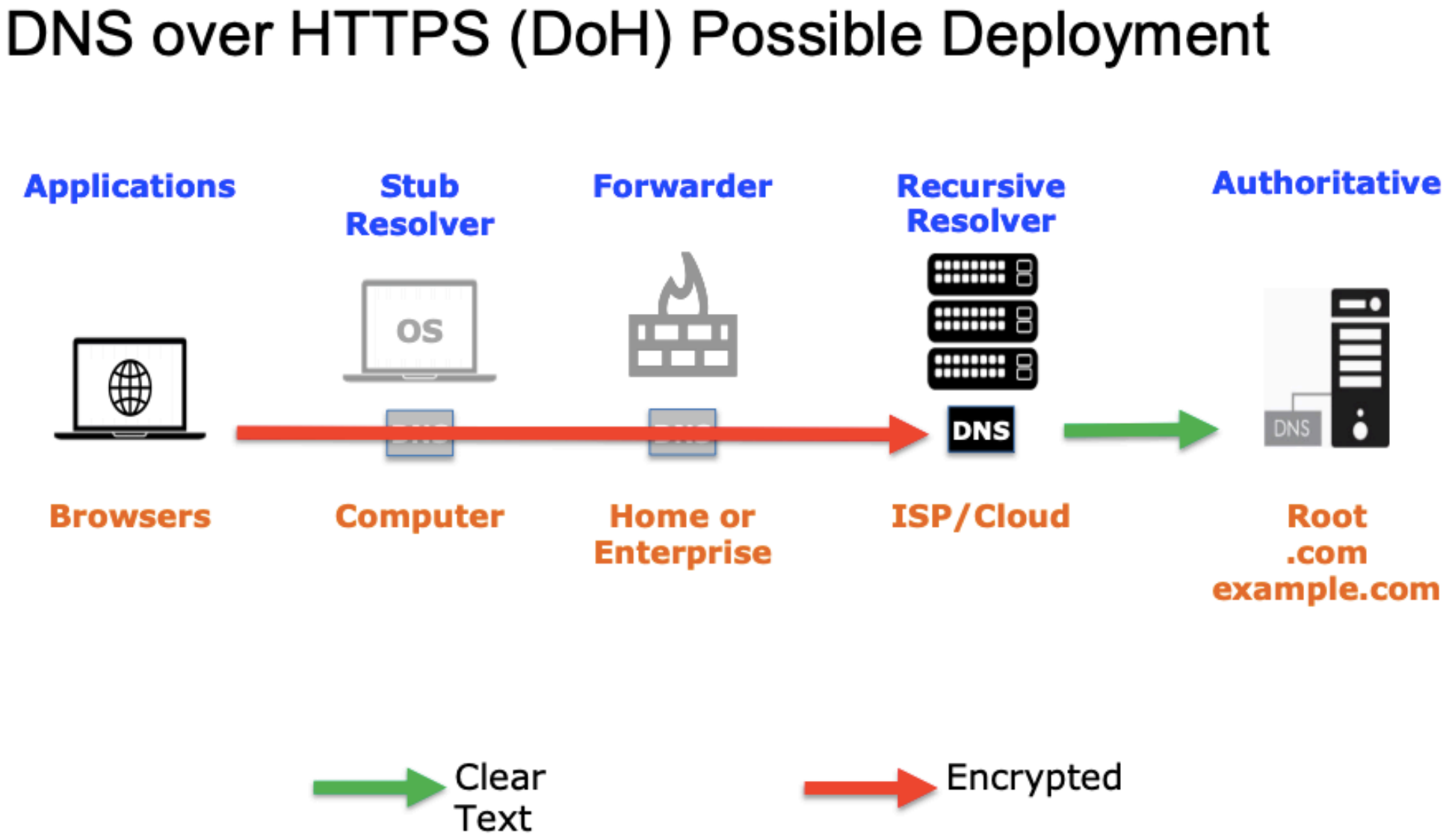
(Source: Matthew Prince, 24 May 2019)

DNS over HTTPS



(Source: CENTR DoH Paper, 12 June 2019)

Explaining DoH/DoT (from ICANN 65)



(https://static.ptbl.co/static/attachments/214639/1561448975.pdf?1561448975)

New challenges

ZDNet

VIDEOS 5G WINDOWS 10 CLOUD AI INNOVATION SECURITY MORE NEWSLETTERS ALL

MUST READ: Windows 10: Has Microsoft cleaned up its update mess? (Spoiler: no)

First-ever malware strain spotted abusing new DoH (DNS over HTTPS) protocol

Godlua, a Linux DDoS bot, is the first-ever malware strain seen using DoH to hide its DNS traffic.

By Catalin Cimpanu for Zero Day | July 3, 2019 -- 13:17 GMT (06:17 PDT) | Topic: Security

(Source: ZDNet, 3 July 2019)

Guidance from Dutch National Cyber Security Centre

(Source: NCSC.nl, 2 Oct 2019)

SSAC on DNS & IoT

SAC105: The DNS and the Internet of Things

- SAC105: The DNS and the Internet of Things: Opportunities, Risks, and Challenges, published June 3rd, 2019
- A different kind of SSAC report:
  - **No recommendations** to the ICANN Board
  - A tutorial-style discussion intended to trigger and **facilitate dialogue** in the broader ICANN community
  - More **forward looking** than operational in nature
  - Partly within SSAC and ICANN's remit, but also goes beyond it
- Many aspects of our discussion are not new, except as they consider new challenges from IoT

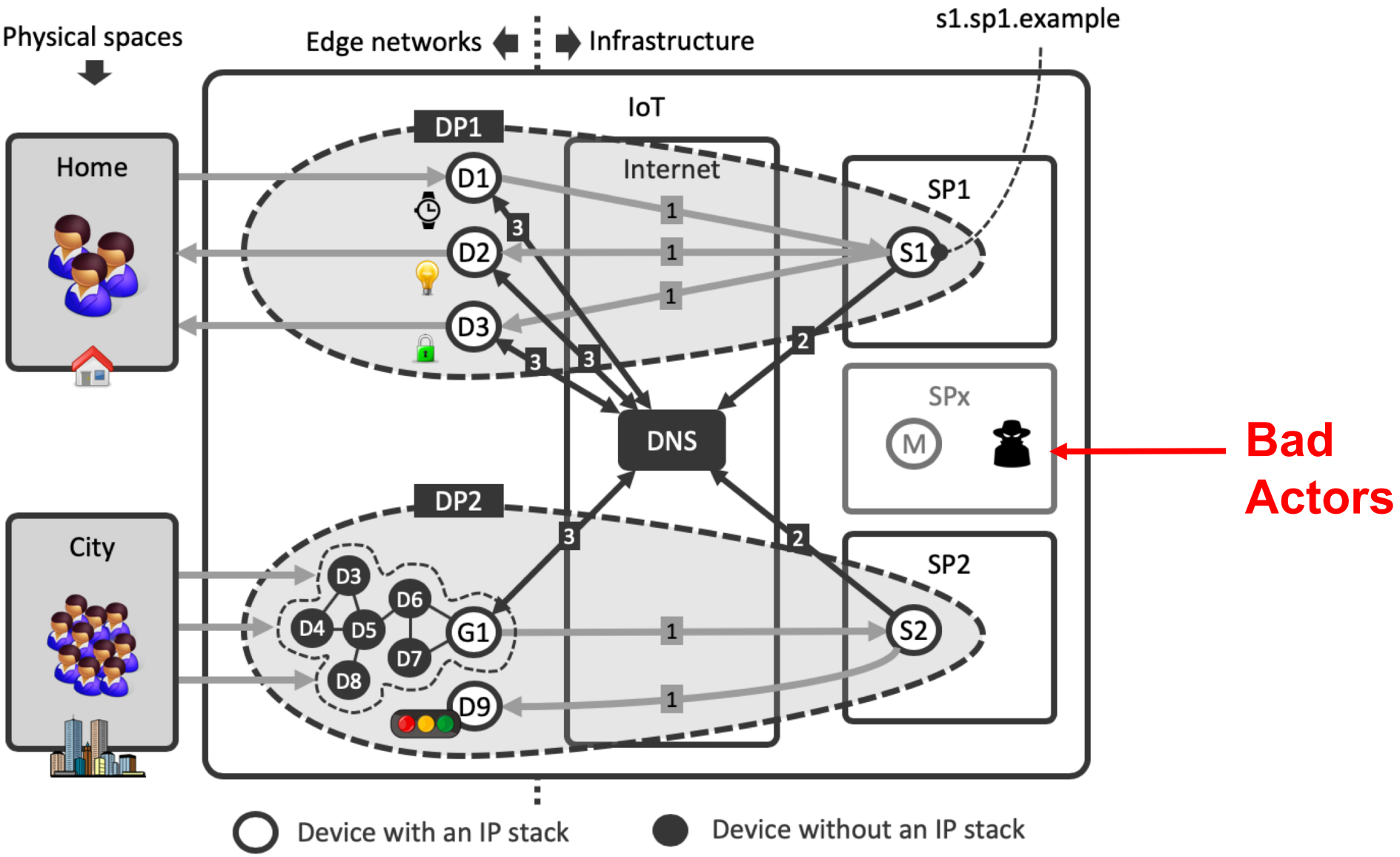
The Internet of Things (IoT)

- Internet application that extends “network connectivity and computing capability to objects, devices, sensors, and items **not ordinarily considered to be computers**” (ISOC, 2015)
- Examples: smart homes, smart cities, self-organizing dynamic networks of drones and robots
- Differences with “traditional” applications
  - IoT continually senses, interprets, and acts upon physical world
  - Often without user awareness or involvement (passive interaction)
  - Pervasive 20-30 billion devices operating “in the background” of people’s daily lives
  - Widely heterogeneous devices (hardware, operating systems, network connection)
  - Longer lifetimes (perhaps decades) and unattended operation

IoT and the DNS

- Remote services (cloud services) assist devices in performing their task (e.g., combining and analysing data from multiple sensors)
- Measurement studies show that IoT devices use the DNS to locate remote services (e.g., sleep trackers, light switches)
- **Opportunity:** DNS helps fulfilling IoT's more stringent security, stability, and transparency requirements stemming from seamless interaction with physical world
- **Risk:** IoT stresses the DNS, accidentally (e.g., large number of devices coming online simultaneously after a power outage) or on purpose (IoT-powered DDoS attack)
- **Challenge:** DNS and IoT industries can seize opportunities and address risks

Role of the DNS for the IoT



Opportunities: DNS helps protect the Real World

- DoH and DoT (**resolver verification** and transport encryption)
  - Avoid IoT devices being redirected to malicious resolvers
  - Reduce information devices reveal about themselves
  - Protect user privacy for devices with highly specific tasks
- DNSSEC (DNS response verification)
  - Avoid IoT devices being redirected to malicious services
- Multi-Factor Authentication (MFA) to protect against domain registration hijacks
  - May affect large installed base of IoT devices
  - Attackers might invest more because IoT services become high-value targets
- Visualize DNS queries to make IoT more transparent for users
  - Services and resolvers that IoT devices use
  - Enable users to control resolvers that IoT devices use

Risks to the DNS from the IoT

- DNS-unfriendly programming at IoT scale
  - TuneIn app example → random queries filled resolver cache of mobile operator
    - Only around 700 iPhones, took three weeks for the app to get updated
  - Effects depend on factors like device concentrations and TTLs
  - Unsupported devices that operate unattended for decades
- Larger and more complex DDoS attacks by IoT botnets (Mirai, Hajime)
  - IoT botnets currently around **400-600K bots** (Mirai, Hajime), may increase in the future
  - Set of IP addresses may change quickly
  - Higher propagation rates
    - Hajime exploited a vulnerability in 10 days and increased by 50K bots in 24 hours
  - Vulnerabilities more difficult to fix quickly at scale, botnet infections go unnoticed
- DDoS amplification through open resolvers (on IoT devices)
  - 23-25 million open resolvers and amplification factors in the range 29-64

Challenges for DNS and IoT Industries (1 / 2)

- Developing a **DNS security library** for IoT devices
  - Such as DNSSEC validation, DoH/DoT support
  - User control over DNS security settings and insight into services that IoT devices use
  - Work on various IoT operating systems and CPU types
  - Example starting points: DNSSEC Trigger and Danish
- Training IoT and DNS professionals
  - IoT product managers: understand IoT botnets and open resolvers
  - IoT engineers: understand “DNS friendly” programming and security(e.g., DNSSEC)
  - DNS folks: understand IoT changes domain registration model and security
  - Example starting points: RFC4367 and “Hello DNS”

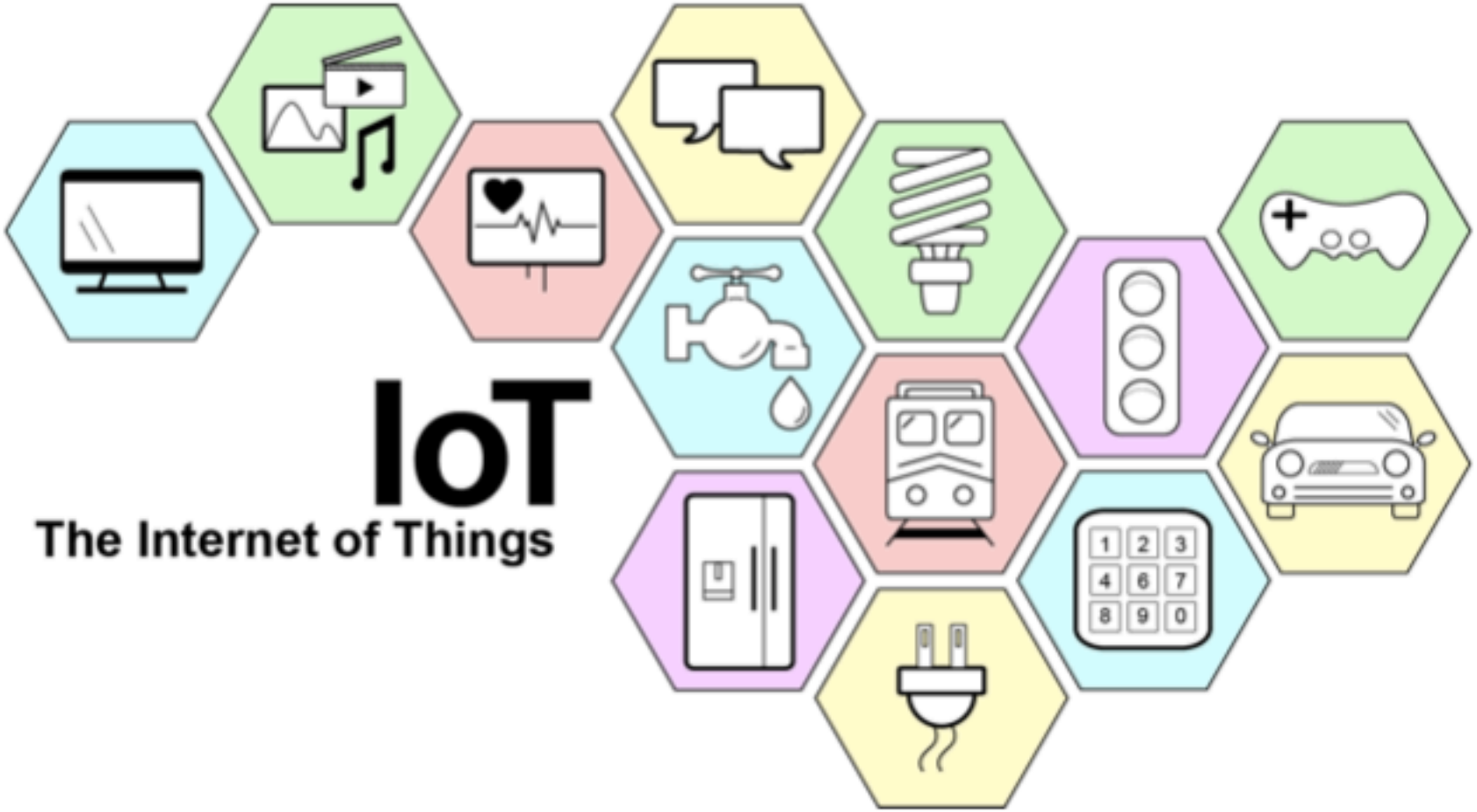
Challenges for DNS and IoT Industries (2 / 2)

- Deploying a cross-DNS operator system to share information on IoT botnets
  - Characteristics of DDoS attacks that DNS operators handle, “fingerprints”
  - Also filtering rules, bot concentrations across AS-es, botnet booters, etc.
  - Example starting points: DDoS-DB, IoT-Pot, Shadowserver’s Open Resolver Scanning Project
- More advanced mitigation of very large IoT-powered DDoS attacks
  - DDOS mitigation broker that enables DNS operators to flexibly share mitigation capacity (e.g., using DOTS signalling)
  - Security systems in edge networks, such as home routers (e.g., using SPIN and SHG)
- Develop a system to measure the evolution of the IoT
  - Device-to-domain name database (e.g., based on publicly available MUD specifications)
  - DNS operators provide coarse grained stats (e.g., counts, origin AS)

Conclusions and Future Work

- The IoT is an emerging distributed Internet application expected to further ease our daily lives and make our society safer and more sustainable
- Might make the role of DNS even more important
  - IoT devices autonomously and seamlessly interact with our physical world through billions of connected sensors and actuators
- SAC105: The DNS and the Internet of Things: Opportunities, Risks, and Challenges
  - Tutorial-style overview of the DNS and the IoT as two co-evolving and interacting ecosystems in terms of opportunities, risks, and challenges
  - https://www.icann.org/en/system/files/files/sac-105-en.pdf
- SSAC wishes to continue discussing our report with the ICANN community
- We welcome your feedback!

Other useful documents on IoT

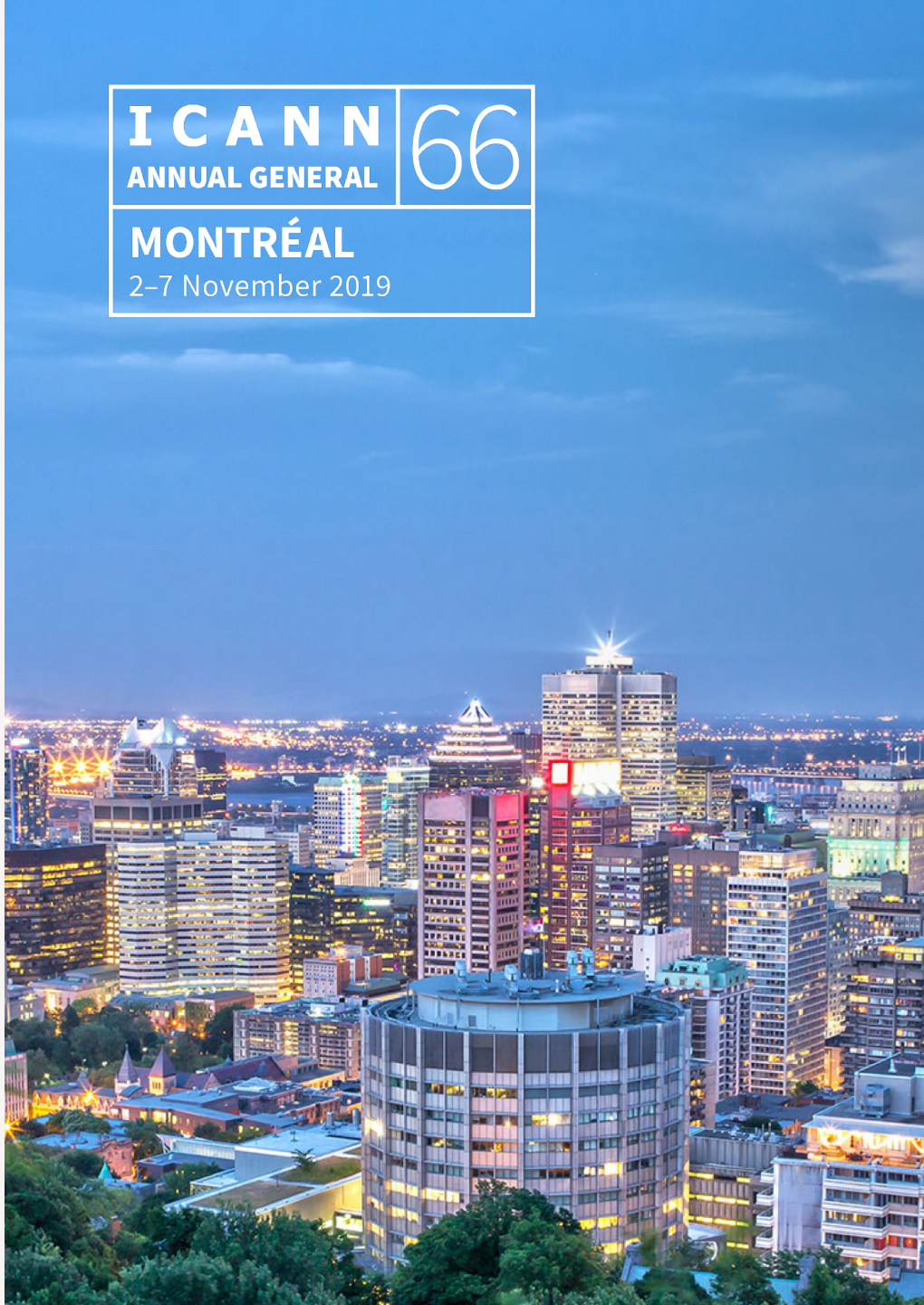


(NIST IR 8228, June 2019)

Future Root Zone KSK Rolls

Kim Davies
VP, IANA Services; President, PTI

PTI | An ICANN Affiliate



Problem Statement

- First KSK was created in 2010 (“KSK-2010”)
- Design team was formed to develop a set of recommendations on how to perform a rollover
- Originally scheduled for 2017, the second KSK (“KSK-2017”) ultimately started signing the zone on 11 October 2018
  - One year pause in process to consider impact of anomalous telemetry data
- Rollover successfully occurred with minimal disru
- **What do we want to do now?**

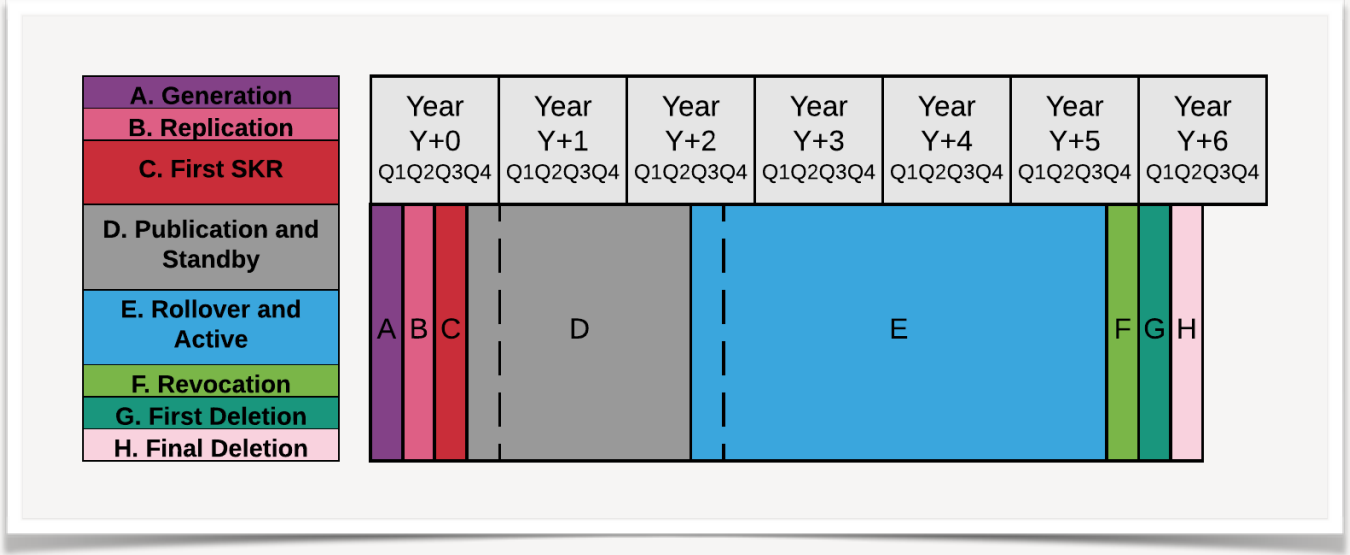
Initial feedback

- Recognizing community interest in the rollover was at its peak during and shortly after the rollover, we solicited comments and directed responses to the ksk-rollover list for capture.
- We undertook to analyze those comments in 2019H2 and produce a recommendation for future rollovers
- Common themes in this early commentary:
  - KSK rollover should be a routine event
  - KSK should be rolled over annually
  - Introduce backup and/or standby keys
  - Perform more monitoring of impacts of larger keysets
  - Consider alternate signing algorithms

Our proposal

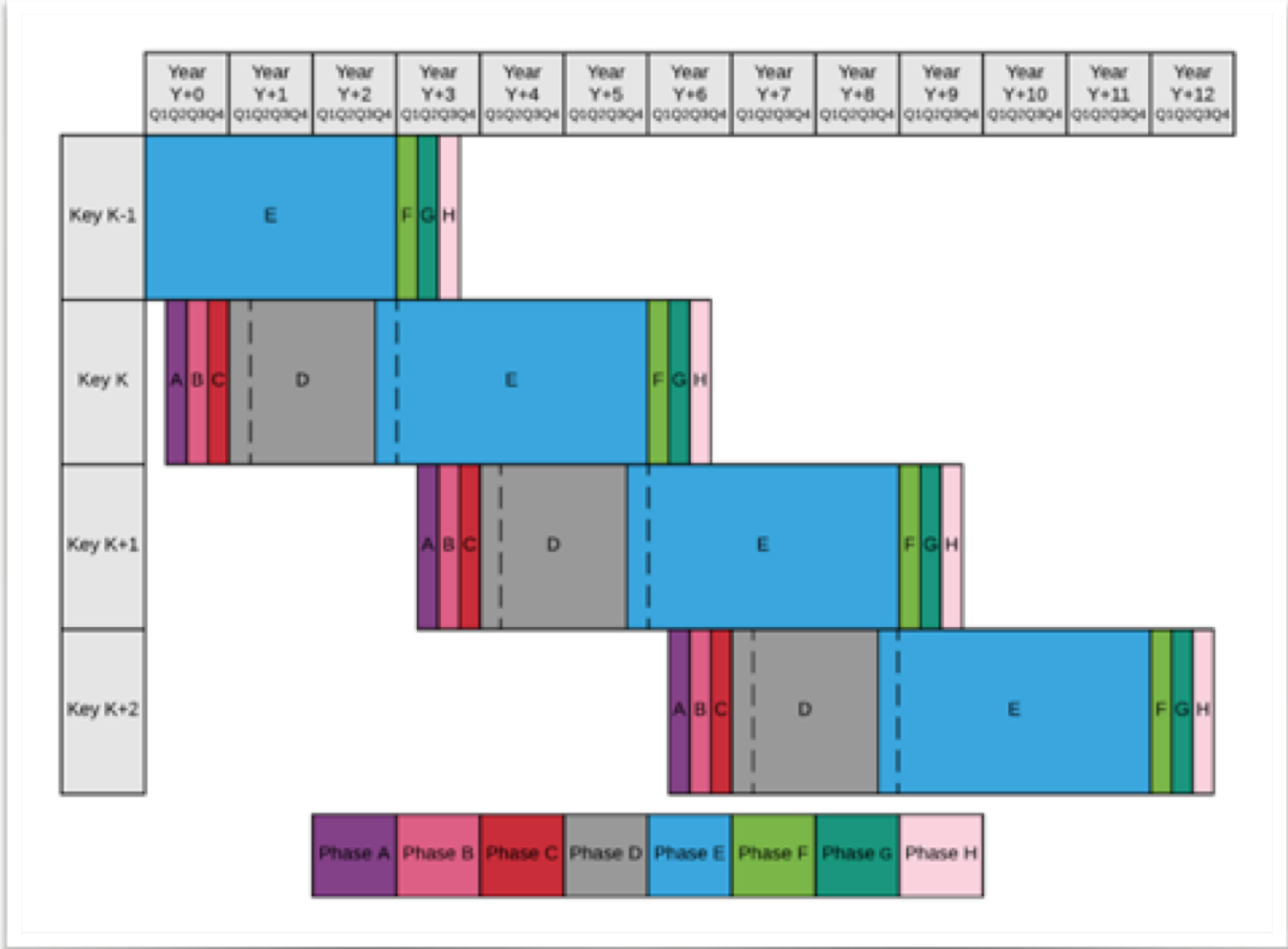
- Create a predictable approach to future rollovers
- Plan for a three-year rollover interval to balance desire for more regular rollovers with the operational complexity involved
- At least two years for the new trust anchor to be published in advance, allowing greater propagation before the rollover
- Use similar phased approach aligned with the quarterly key ceremony schedules

Proposed key lifetime



- It takes 3 quarters to generate and successfully replicate the new KSK
- 7+ quarters in standby state: pre-populated and capable for unscheduled roll
- 12 quarters in active state: signing the zone
- 3 quarters to revoke: revocation period plus destruction in KSKs

Subsequent key lifetimes



Choice of Interval

- A common suggestion from early commenters was to perform an annual rollover.
- Because of the multiple quarters in advance to generate, pre-populate and pre-publish KSKs, plus quarters following for revocation and destruction, and annual cycle (without any delays) would have 4 or more KSKs in play at some times.
- We consider this to result in too much unneeded complexity for KSK operations
  - KSK handling operations in the key ceremony context is time-intensive and each additional act introduces risk of error.
  - KSK ceremonies are already more lengthy due to:
    - Multiple KSRs being signed for multiple phase/fallback scenarios
    - Replacement cycles (HSMs, TCRs, Smart cards, etc.)
  - We want to keep ceremonies to a manageable length to ensure participant focus on the key items

Earlier generation

- The lifecycle results in the earlier generation of the KSK than was used in the KSK-2017 plan
- Provides several benefits:
  - At least two years for software vendors and other distributors of the trust anchor to upgrade their distributions
  - Provides a greater window when, should an emergency unscheduled rollover be performed, have a ready KSK to use that is at least partially shared with operators
- Any negative impacts of sharing the key earlier on security outcomes was considered negligible

No backup or standby key

- We have not proposed a dedicated backup or standby key, other than the pre-published key acting in a standby capacity.
- As we do not have alternate facilities to a suitable specification to store any additional key, the benefit appears to be marginal
  - Storage in the existing 2 KMFs would result in fate-sharing that mitigates the benefits for most scenarios
  - Detailed consideration needed for any kind of storage alternative

Algorithm Change

- We agree this needs to be investigated.
- However, we don’t believe a mature approach is known, and thus it is not an IANA operationalization exercise, but rather first a research exercise.
- We propose activity relating to research into algorithm change be performed as a separate activity, perhaps much like the original rollover explorations.

Public Consultation

- We've published a paper that outlines the approach.
- It is now open for public comment
- https://www.icann.org/public-comments/proposal-future-rz-ksk-rollovers-2019-11-01-en
- Public comment period is posted now, open until end of January
- We will distill the feedback in the new year and turn them into operational practice

In Summary

- The rollover from KSK-2010 to KSK-2017 was widely considered successful
- We seek to replicate this success with a similar methodology
- Our aim is to target a 3-year active period for each KSK
  - Annual rollovers would result in too much overlap between lifecycles, too much operational complexity
  - We create the KSK early to allow greater period of time for pre-population and provides more time for use in an unscheduled/emergency scenario
- Please provide feedback to us, either endorsing the approach and suggesting alternatives
- We will try to finalize the approach in the new year and communicate our operational plan

Bonus Slide: Trusted Community Representatives

- We are almost at the 10 year anniversary for KSK operations
- Trusted Community Representatives are the community volunteers that observe ceremonies, and oversee key shares used to activate the KSK
- Current class of TCRs all originate from the 2010 selection round
- Recognizing some wished to retire and our backup pool of pre-selected TCRs was shrinking, we created an evergreen solicitation for Statements of Interest
  - http://iana.org/tcr
- First selections have been made with the new process
  - Backup pool back to 10 per our target
- Additional selections will be made as backups are promoted to replace active TCRs
- If you are interested, please apply!

Useful reading on the history to date

- Root Zone KSK Rollover Plan (March 2016)
  https://www.iana.org/reports/2016/root-ksk-rollover-design-20160307.pdf
- Review of the 2018 DNSSEC KSK Rollover (March 2019)
  https://www.icann.org/en/system/files/files/review-2018-dnssec-ksk-rollover-04mar19-en.pdf
- ICANN Project page for last rollover
  https://www.icann.org/resources/pages/ksk-rollover

Upcoming Events

Join us next in Paris

(Source: ICANN: http://icann.org/ids)

Engage with ICANN – Thank You and Questions

ICANN

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