

DNS Security Facilitation Initiative Technical Study Group (DSFI-TSG)

Merike Käo (DSFI TSG Lead / Coordinator)



14 October 2021

Agenda

- ⦿ **Introducing the DSFI-TSG**
- ⦿ **Attack Vectors in the DNS Ecosystem**
- ⦿ **Mitigations**
- ⦿ **Recommendations**
- ⦿ **Questions**

Introducing the DSFI-TSG

DSFI - TSG



In line with the FY21-FY25 Strategic Plan, ICANN org committed to work with the community to strengthen collaboration and communication on security and stability issues through a technical study group (TSG). In May 2020, the ICANN CEO established the Domain Name System Security Facilitation Initiative – Technical Study Group to:



Provide technical expertise and guidance on the technical work ICANN can initiate to investigate possible DNS security facilitation functions.



Provide recommendations on ways to:

- Establish and promote best practices
- Facilitate communication between ecosystem participants
- Implement processes to help stakeholders handle threats



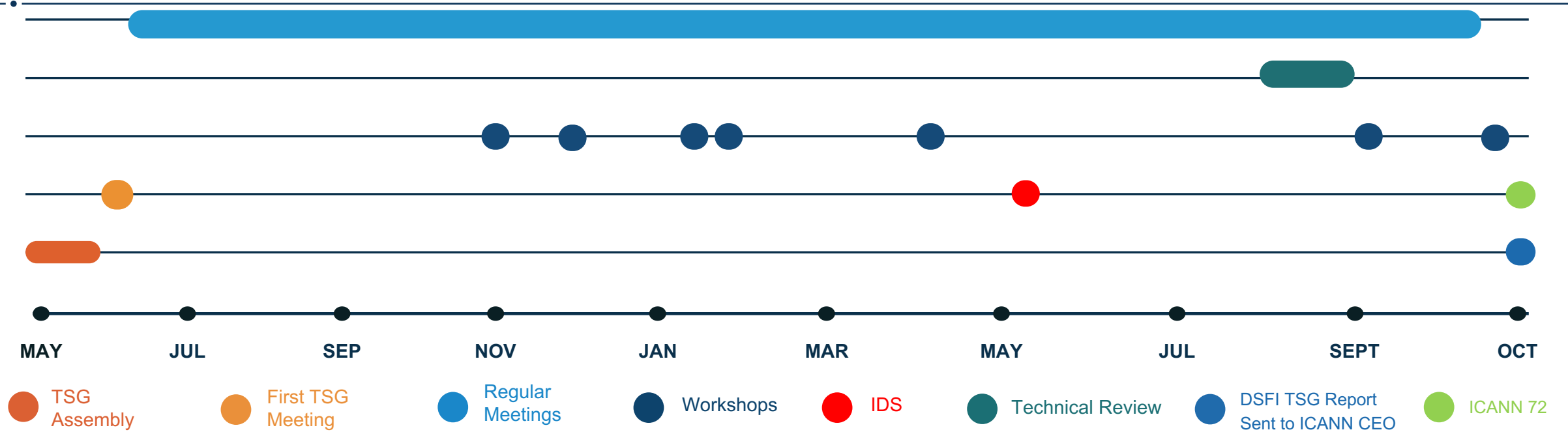
The recommendations will involve discussion and consultation with relevant stakeholders to address the important questions:

- What can and should ICANN be doing to improve DNS security profile?
- What should ICANN NOT be doing?



- ⦿ Alarming attacks on the Domain Name System:
 - The [Sea Turtle hijacking](#)
 - [DNSpionage](#)
 - DNS Changer
- ⦿ Attacks rarely impact only one actor in the Internet ecosystem; we need to come together and respond.
- ⦿ The solutions that would best improve the security and stability of the DNS ecosystem are not yet clear.
- ⦿ A new level of collaboration and understanding is required.

Timeline



- Enumerate root causes and Vectors of Attack Matrix
- Vector Priority List
- Key Questions
- Mitigations and Recommendations
- Draft Document
- Technical Review
- Final Technical Report

2020

- **Project Start 4/2**
- **First TSG Meeting: 6/16**
- **Defined Scope and Key Questions**

2021

- **TSG review recommendations template and first recommendations: 5/4**
- **Final updates to recommendations as per direction of TSG: 7/14 - 7/16**
- **Draft and review CEO Report (w/recommendations): 7/19 - 7/27**
- **DSFI Technical Consultation: 8/2 - 8/27**
- **Final revisions and updates: 9/29 - 10/8**
- **DSFI TSG to transmit Technical Report to ICANN CEO: 10/11**
- **Present Final Document at ICANN72**

TECHNICAL STUDY GROUP

Merike Käo – DSFI-TSG Lead/Coordinator

Chief Information Security Officer (CISO) of Uniphore
Security and Stability Advisory Committee (SSAC) Liaison
to the ICANN Board of Directors

Tim April

Principal Architect, Akamai Technologies

Gavin Brown

Head of Registry Services and Chief Innovation Officer,
CentralNic

John Crain

Chief Security, Stability and Resilience Officer, ICANN Org

Rod Ramussen

Chair of ICANN SSAC, and retired Security Executive

Marc Rogers

Vice President of Cybersecurity, Okta

Katrina Sasaki

Chief Executive, NIC.LV (Latvia) and Council member of the
country code Names Supporting Organization (ccNSO)

Robert Schischka

Chief Executive Officer, NIC.AT (Austria) and Director of
the Computer Emergency Response Team (CERT.at)

Duane Wessels

Distinguished Engineer, Verisign

DSFI TSG Technical Consultation Reviewers

- ⦿ Christopher Baker
- ⦿ Carel Bitter
- ⦿ Kimberly Claffy (kc claffy)
- ⦿ Leslie Daigle
- ⦿ Anne-Marie Eklund-Löwinder
- ⦿ Cristine Hoepers
- ⦿ Hiro Hotta
- ⦿ Warren Kumari
- ⦿ Erwin Lansing
- ⦿ Jacques Latour
- ⦿ Dave Lawrence
- ⦿ Kurtis Lindqvist
- ⦿ Danny McPherson
- ⦿ Damian Menscher
- ⦿ George Michaleson
- ⦿ Eric Osterweil
- ⦿ Phil Regnauld
- ⦿ Kristof Tuyteleers
- ⦿ Ulrich Wisser

DSFI ICANN SUPPORT

ICANN BOARD

- Harald Alvestrand
- Göran Marby
- Danko Jevtovic
- Merike Kää

ICANN Org

- David Conrad
- Ashwin Rangan

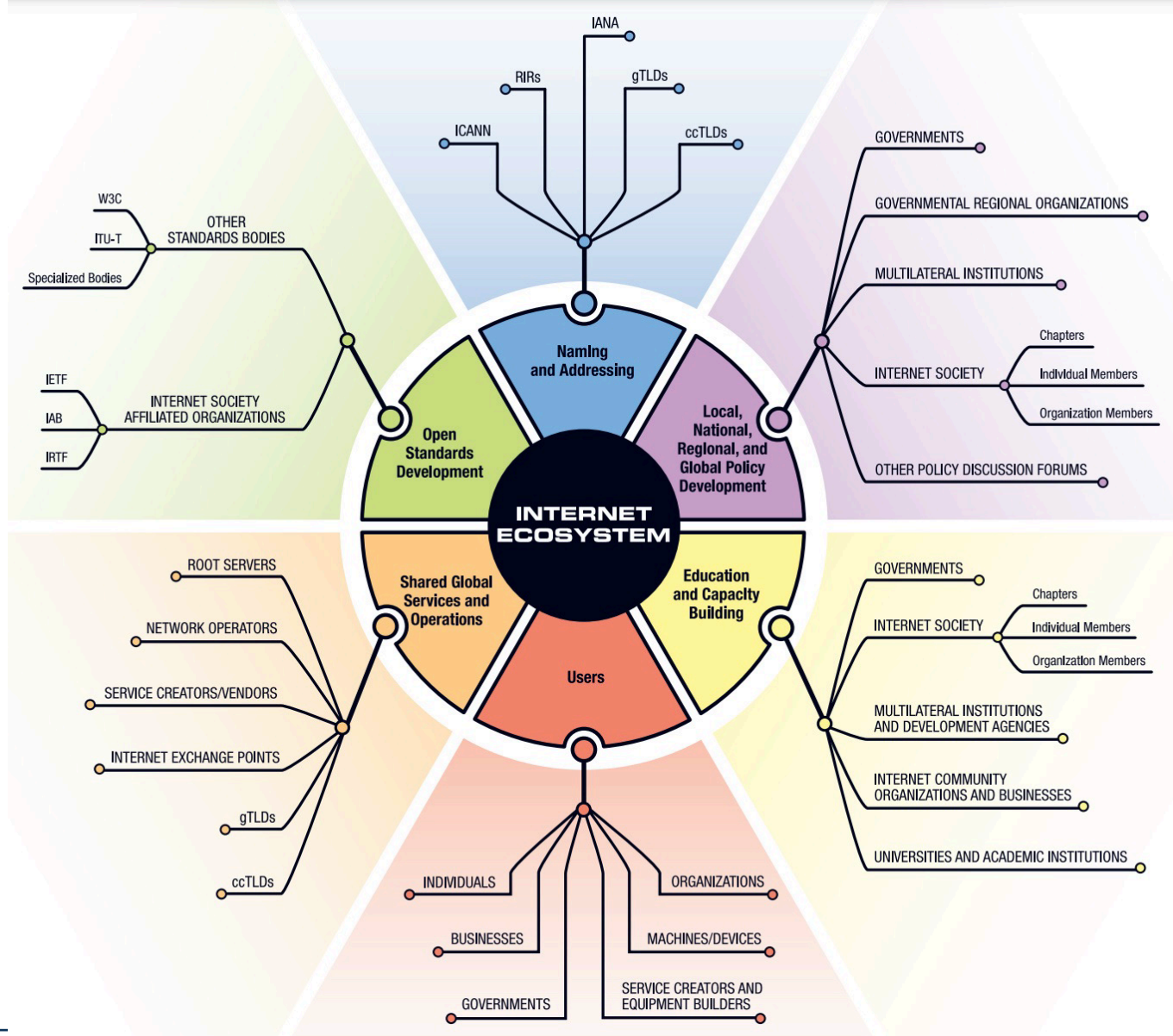
ICANN Staff Support

- Steven Kim
- Sally Newell Cohen
- Wendy Profit
- Samaneh Tajalizadehkhoob

Technical Writer (Consultant)

- Heather Flanagan

Breadth and Depth of Comprehensive DNS Ecosystem

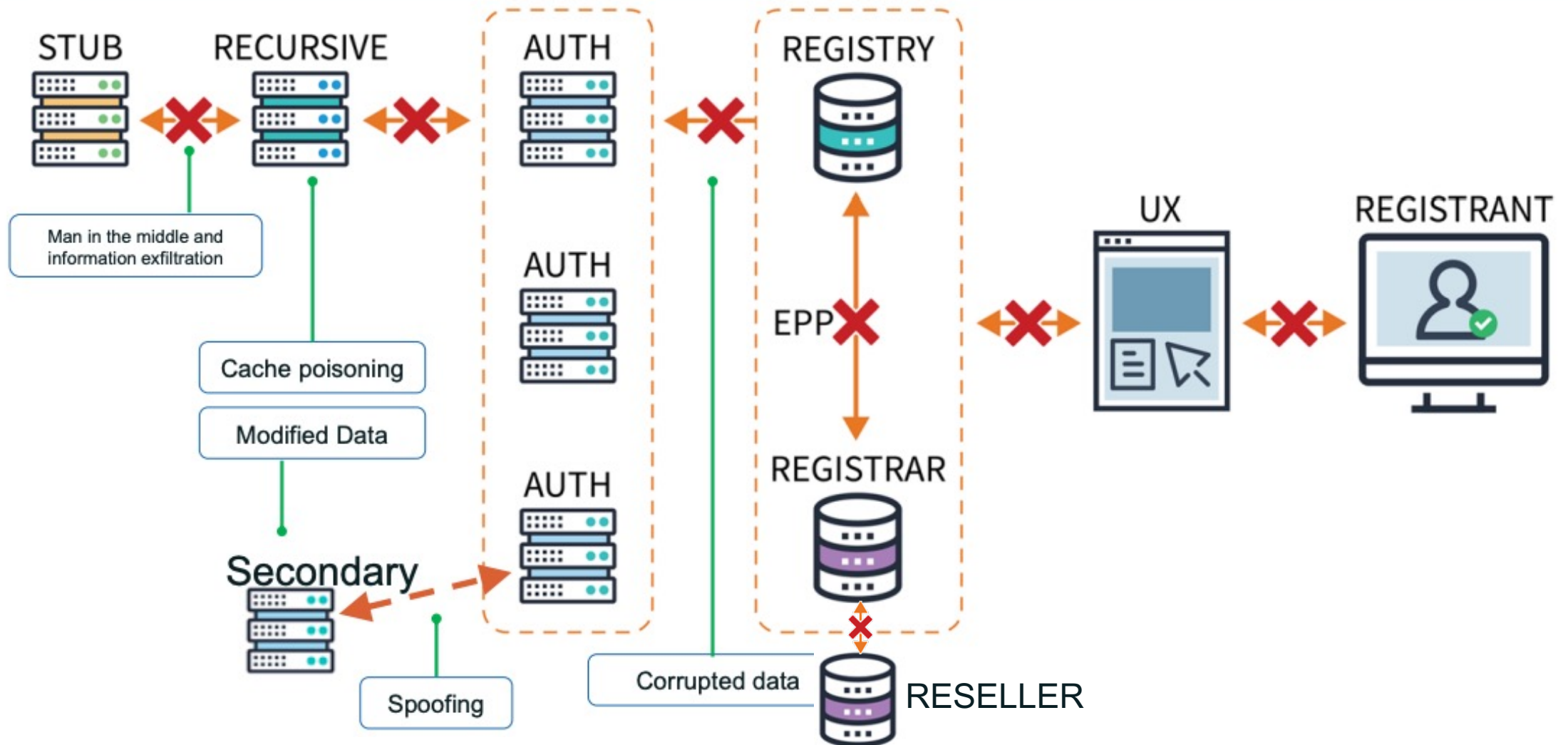


- ⊙ Unique Identifiers: Naming and Addressing
- ⊙ Technical Standards
- ⊙ Operational Services (ISPs, CDNs, Hosting Providers, etc)
- ⊙ Users Deploying and Utilizing DNS Services
- ⊙ Security Services and Incident Response

Attack Vectors in the DNS Ecosystem

Attack Vector Targets

Some of the Potential Target Points of the DNS Ecosystem



Attack Vector Identification

- ⦿ How they were chosen:
 - Within each category, the study group focused on specific areas and associated incidents.
 - By analyzing real-world incidents and attack scenarios, the study group focused on immediate and practical information to inform its recommendations to the ICANN CEO

- ⦿ For each attack vector, the study group considered these questions:
 - What are the mechanisms or functions currently available that address DNS security?
 - Can we identify the most critical gaps in the current DNS security landscape?
 - What are the risks associated with these gaps that may not be well understood?
 - Does the DNS have unique characteristics that attract security problems, which other Internet services don't have?

Attack Vectors

- Insecure 3rd Party Networks (not under direct control of target)
- Effect of Fate-Sharing
- Inadequate Access control
- Registrant Credential Compromise
- Registrar/Reseller Credential Compromise
- Registry Credential Compromise
- Impersonate Authoritative Server (and associated infrastructure)
- Impersonate Recursive Resolver
- Impersonation of Infrastructure using look alike domains (Facsimile Domains)
- Vulnerability Exploitation
- Use DNS as Covert Channel
- Use DNS as Data Exfiltration
- Abuse of credentials to initiate transactions at the registry
- DNS Cache Poisoning
- Denial of Service
- Fraudulent Certificates
- Long TTLs
- Short TTLs
- Poor Implementation Choices
- Protocol Weaknesses
- Subdomain Takeover
- Route Hijack

Categorizing the Attack Vectors

The DSFI-TSG identified seven categories of attack vectors:

- ⦿ Identity and Access Management
- ⦿ Inadequate Access Control and Authorization Issues
- ⦿ Resource Impersonation
- ⦿ Code and Protocol Vulnerabilities
- ⦿ Infrastructure Choices
- ⦿ DNS as the Attack Vector
- ⦿ Denial of Service

Attack Vectors in Detail (1)

Identity and Access Management

Credentials are used at nearly every point in the DNS ecosystem. For example, staff at registries and registrars log in to DNS provider systems, ICANN org support systems, and data escrow services, while registrars see logins from registrants and resellers.

Attacks on and through the credential systems result in issues such as the modification of registration data to allow for domain hijacking and/or traffic interception, support for social engineering attacks, and more.

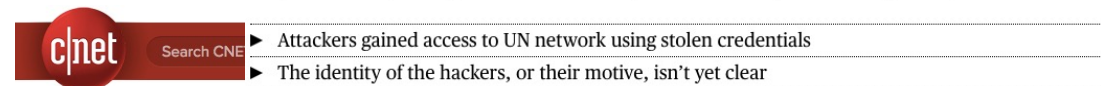
- Registrant Credential Compromise
- Registry, Registrar, and Reseller Credential Compromise
- Abuse of Credentials to Initiate Transactions at the Registry

Cybersecurity

UN Computer Networks Breached by Hackers Earlier This Year

By [William Turton](#) and [Kartikay Mehrotra](#)

September 9, 2021, 4:00 AM PDT Updated on September 9, 2021, 11:52 AM PDT



The image shows a snippet from a CNET article. On the left is the CNET logo. To its right is a search bar with the text "Search CNET". Below the search bar are two bullet points: "Attackers gained access to UN network using stolen credentials" and "The identity of the hackers, or their motive, isn't yet clear".

CNET > Security > Black market lights up with 360M stolen credentials -- report

Black market lights up with 360M stolen credentials -- report

Some 360 million account credentials are newly available for sale on the black market, according to one security firm, and may be from several yet-to-be-reported security breaches.

photographer: i nomas

Inadequate Access Control and Authorization Issues

Inadequate access control refers to situations where an entity that is authenticated to access a specific service or data may also inadvertently gain access to unauthorized services and/or data.

It also refers to situations where validation to execute on some actions is lacking, such as allowing anyone to add a domain to their account without validating that the person requesting the change actually owned the domain.

◎ Subdomain Takeover

sub.test.org 60 IN CNAME knot.hacker.com

- User visits sub.test.org website.
- The CNAME points to another domain (knot.hacker.com)

Resource Impersonation

There are various ways to redirect DNS queries to a third party. This redirection has several potential implications, depending on which type of system is being impersonated or imitated.

While there are cases where this is done as a legitimate business tactic, such as with captive portals that restrict access from an internal network to the public Internet, there are also cases where this results in redirection to malicious targets, potentially for the distribution of malware or used to harvest end user data, for example.

- ⦿ Impersonate Recursive Resolver
- ⦿ Impersonate Authoritative Server (and associated infrastructure)
- ⦿ Impersonation of Infrastructure using look-alike domains (Facsimile Domains)
- ⦿ Fraudulent Certificates
- ⦿ Route Manipulation

Resource Impersonation

Impersonation of Infrastructure using look-alike domains (Facsimile Domains)

Homographic Attacks

Take the non-internationalized name of a well-known website and register a homograph:

Facebook.com
Facebook.com
Făcebook.com
Fačebook.com
Facěbook.com
Faceḃook.com
Faceböök.com
Faceboòk.com
Faceboòk.com

Code and Protocol Vulnerabilities

Another attack vector involves vulnerabilities in the software used to run a DNS service or the protocol that defines the DNS.

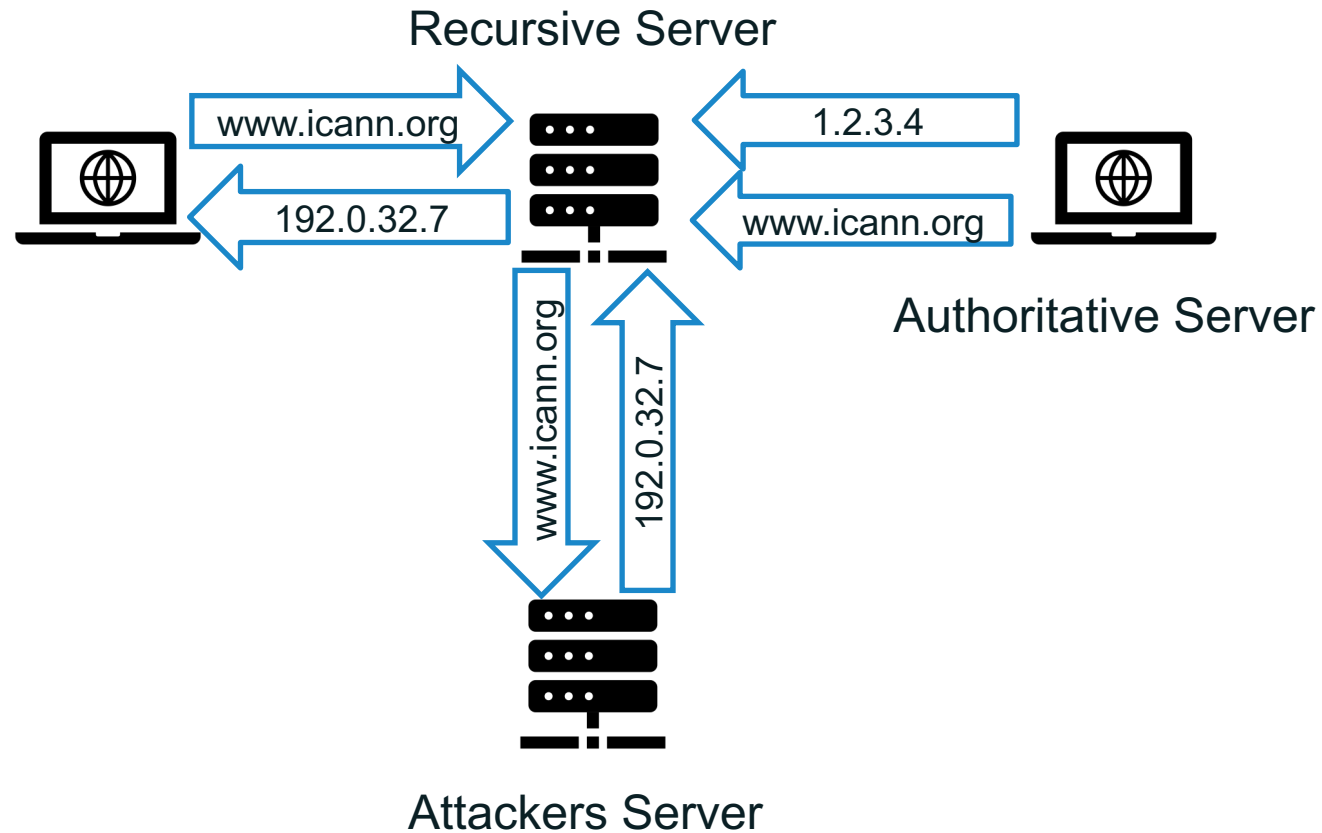
These vulnerabilities may allow an attacker to access information or systems they should not have access to, to overwrite information in a cache or file system, or otherwise negatively impact the systems running the vulnerable services.

- Protocol Weaknesses
- Vulnerability Exploitation
- DNS Cache Poisoning

Attack Vectors in Detail (6)

Code and Protocol Vulnerabilities

DNS Cache Poisoning



Infrastructure Choices

In certain situations, an attack vector is opened because of the choices an administrator has made regarding the configuration of DNS services such as the Time-To-Live (TTL) values or the choice of software used such as older, unpatched versions of name server software.

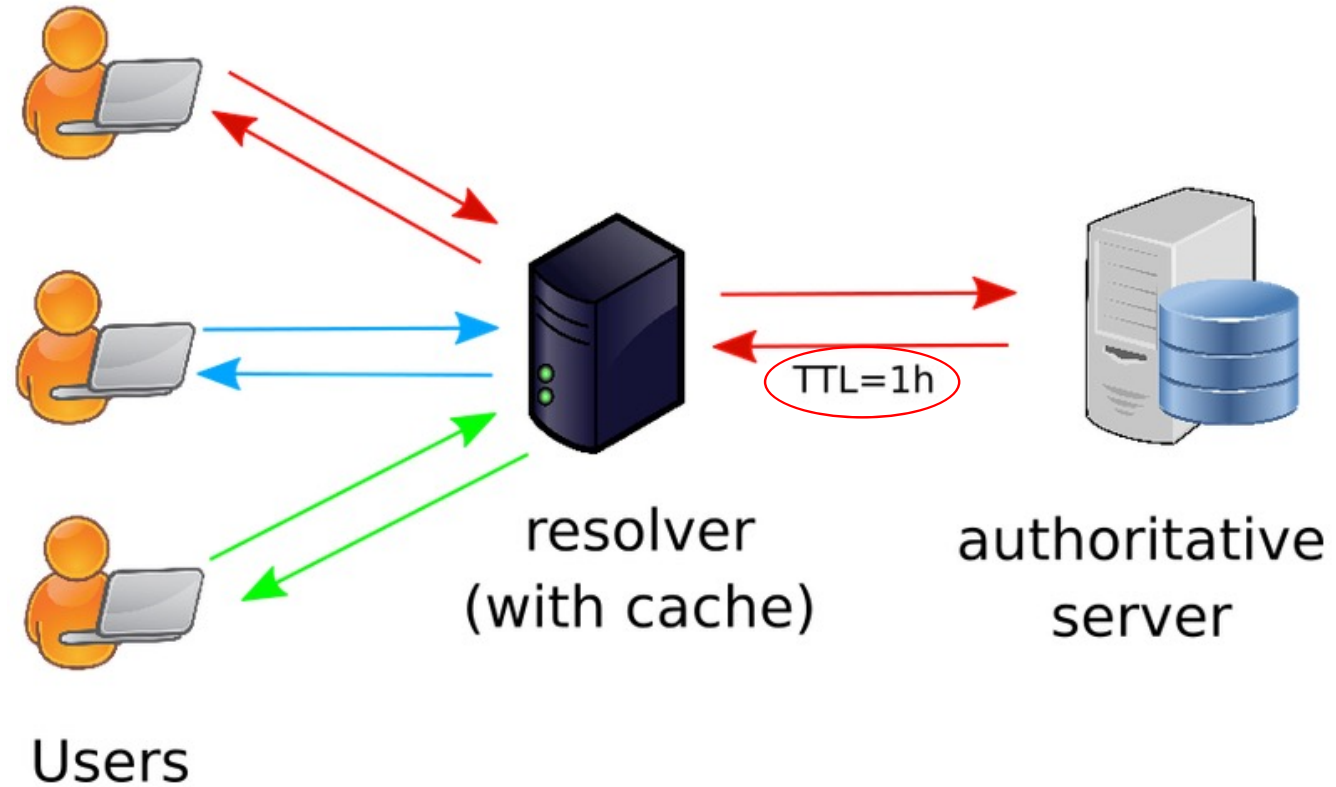
Those choices may be valid for one set of use cases but introduce the vulnerability in a slightly different scenario. Infrastructure choices require a thoughtful risk assessment as part of the decision-making process on what is appropriate for a given service.

- ⦿ Long TTLs
- ⦿ Short TTLs
- ⦿ Poor Implementation Choice
- ⦿ Fate Sharing

Attack Vectors in Detail (8)

Infrastructure Choices

Long/Short TTLs

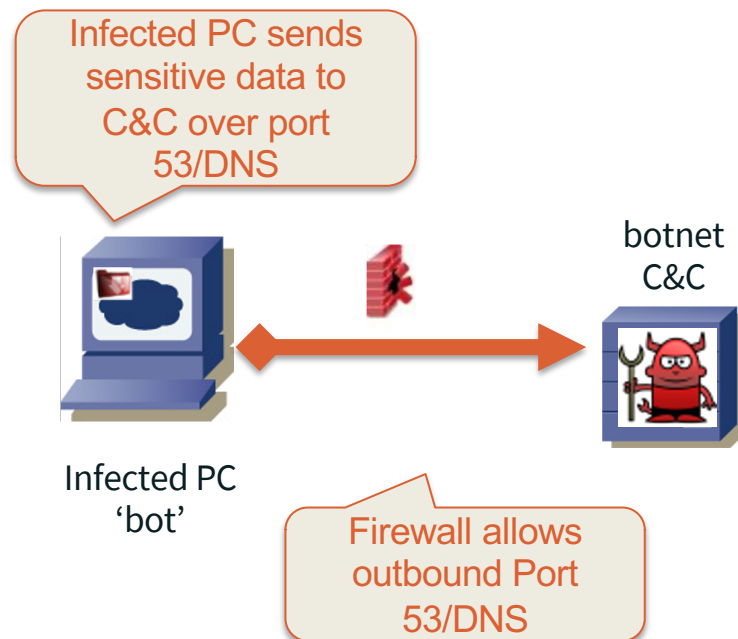


Attack Vectors in Detail (9)

DNS as the Attack Vector

The DNS is not always the direct target of an attack; it may be used instead as a channel to enable other attacks to infiltrate a system or network and extract data from that system or network.

- Covert Channel

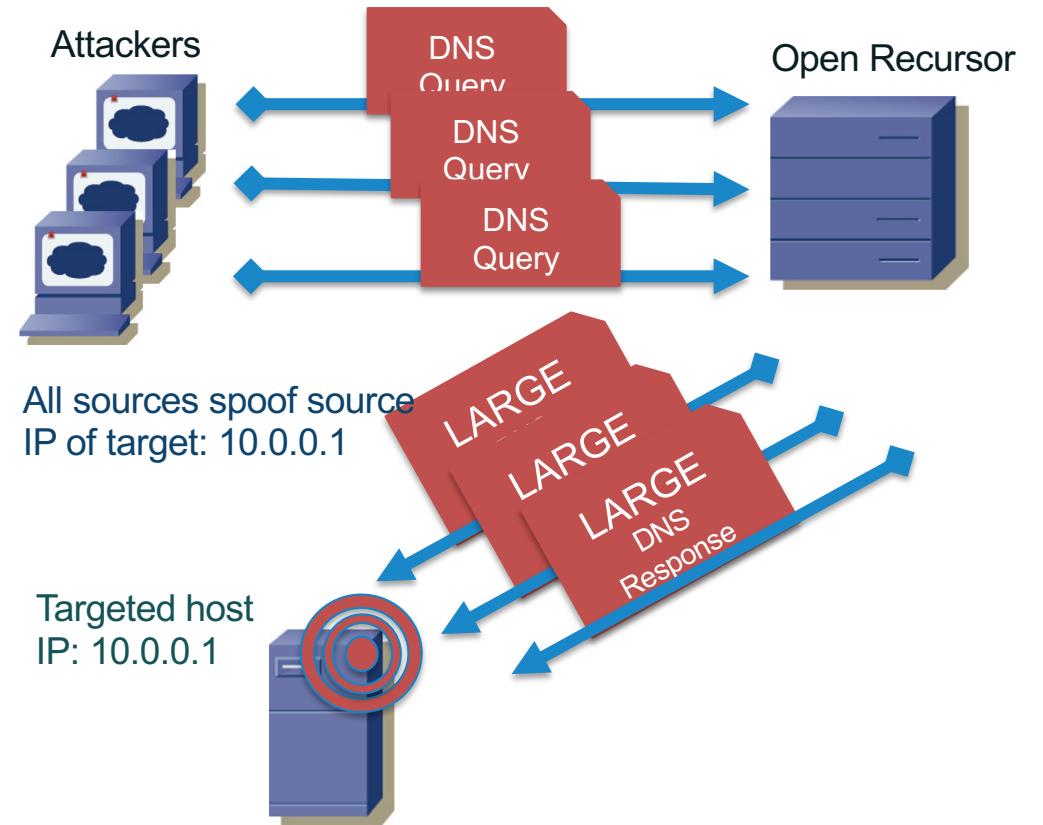


Attack Vectors in Detail (10)

Denial of Service

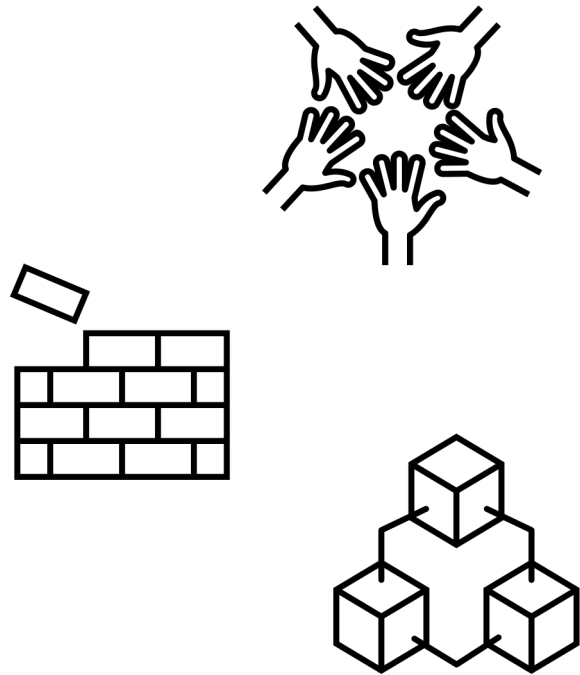
A Denial of Service (DoS) attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of a host connected to the Internet.

DoS attacks on DNS service providers (root servers, registries, registrars) have the potential of disrupting the work of significantly more organizations than it would be possible by launching direct attacks on those organizations.



Mitigations

MITIGATIONS - SCOPE



- ◉ The TSG has considered many mitigations which could be used to counter the attacks described.
- ◉ Not all mitigations will make it into the final report.

MITIGATIONS - Authentication

- ⦿ Complex Passwords
- ⦿ One-time Use Credentials
- ⦿ MFA
- ⦿ Password Manager
- ⦿ Risk Awareness (Credential)
- ⦿ Use of Services that Prevent Weak Passwords
- ⦿ Existence of Remedial Solutions in Case of Attack
- ⦿ Domain & Registrant Verification & Validation

MITIGATIONS – Availability, Integrity, Privacy

- ⦿ Availability
 - Avoid DNS Service Behind a Single Point of Failure
 - Secondary DNS Services with Different Platforms
- ⦿ Integrity
 - DNSSEC
 - Registry Lock to prevent domain hijacking
 - Use of CDS/CDNSKEY/CSYNC
- ⦿ Privacy
 - Use of Encrypted DNS Transport

MITIGATIONS – Monitoring and System Safety

- ⦿ Monitoring & Trust
 - Subscribing to Brand Protection Services
 - Monitor Certificate Transparency (CT)
 - Wider use of Certification Authority Authorization (CAA)
 - ROA Publication and Validation (RPKI)
 - Routers optimized for Packet Inspection, Frame Inspection

- ⦿ Software and System Safety
 - Security Development Lifecycle (SDLC)
 - Patch Software Regularly

MITIGATIONS – Access Control

- Access Control
 - Behavior based access architectures (e.g., Zero-Trust)
 - Partition Critical Online Services (service segregation, e.g. email, website)
 - Consider alternate or more restrictive access controls for Sensitive Info/Accounts
 - Restrict access to DNS services to only DNS ports
 - Limit Resolver Use by 3rd Parties

MITIGATIONS – End Point & Network Controls

- ⦿ End Point and Network Controls
 - Antivirus for End Users
 - Strict Control over DNS Resolver Selection
 - DNS Blocking/Redirecting via DNS Resolvers (DNS Firewall)
 - DNS Blocking/Redirecting via Perimeter Firewalls

MITIGATIONS - Categorizations

- ⦿ Credential Challenges
- ⦿ Inadequate Access Control and Authorization Issues
- ⦿ Resource Impersonation
- ⦿ Code and Protocol Vulnerabilities
- ⦿ Infrastructure Choices
- ⦿ DNS as the Attack Vector
- ⦿ Denial of Service
- ⦿ Incident Response Mechanisms

Recommendations

Recommendations

Operational Improvements

- ⊙ Recommendation O1: Develop a Tabletop Exercise Program

Research

- ⊙ Recommendation R1: DNS Abuse
- ⊙ Recommendation R2: Investigate DNS Security Enhancements
- ⊙ Recommendation R3: Investigate Appropriate Best Practice for Authentication

Contracting

- ⊙ Recommendation C1: Empower Contracted Parties

Funding

- ⊙ Recommendation F1: Bug Bounty Program Feasibility Funding

Education and Awareness

- ⊙ Recommendation E1: Education around Authentication
- ⊙ Recommendation E2: Registry Lock
- ⊙ Recommendation E3: Awareness of Best Practices for Infrastructure Security
- ⊙ Recommendation E4: DNS Blocking and Filtering
- ⊙ Recommendation E5: Incident Response
- ⊙ Recommendation E6: Covert Channel Awareness

Recommendation O1: Develop a Tabletop Exercise Program

ICANN org together with the SSAC, GNSO, ccNSO, TLD-OPS, and other entities with relevant expertise as ICANN org is able to identify them, should develop a tabletop exercise program (e.g., a technical study group, a task-specific technical operators' group) to exercise incident-response procedures and identify operational gaps for services provided by registries and registrars. ICANN org should facilitate the closing of operational gaps identified as it is able by working with the relevant parties.

Recommendations - Research

Recommendation R1: DNS Abuse

ICANN org should continue to participate in industry efforts to work on the definitions and actions regarding DNS abuse and support the security and research community in identifying and mitigating DNS abuse via research funding to those identified experts.

Recommendation R2: Investigate DNS Security Enhancements

ICANN org should develop a program to continually investigate the limits, risks, and benefits of various DNS security enhancements such as, but not limited to:

- Scanning of CDS, CDNSKEY, and CSYNC records by registries and registrars as part of education and awareness around the support and administration of DNSSEC.*
- Enhanced visibility into changes in the DNS ecosystem, such as encouraging support for the DNS Transparency Project to notify registrants and impacted users of domain changes.*
- Support for secure authentication technologies such as DANE and alternative transport technologies like DoH, DoT, and DNS-over-QUIC (DoQ) at relevant points (e.g., by authoritative nameservers any level of the DNS hierarchy) in the DNS ecosystem.*

Recommendation R3: Investigate Appropriate Best Practice for Authentication

ICANN org, along with relevant organizations and communities, should conduct a study and offer a report on what should be considered best practice for authentication when considered against the different roles and risks in the DNS.

Recommendations – Contracts and Funding

Recommendation C1: Empower Contracted Parties

ICANN org should work to empower contracted parties to adopt security enhancements to the domain registration systems and authoritative name services as practical.

Recommendation F1: Bug bounty Program Feasibility Funding

ICANN org should lead an effort to work with DNS software, hardware, and service vendors as well as registry and registrar software vendors to investigate the feasibility of funding and/or supporting the creation of DNS-related bug bounty programs. ICANN org should review the findings of that investigation and make recommendations for any further efforts. ICANN org should include in their reports information on the feasibility of bug bounty programs and what mechanisms available for reporting vulnerabilities. As a final step, use the results of these reports to create a central list of all DNS bug bounty programs and reporting mechanisms that will be maintained regularly.

Recommendations – Education and Awareness (1)

Recommendation E1: Education and Awareness

ICANN org should build and communicate educational programs encouraging DNS stakeholders to make available the appropriate standards-based authentication mechanisms for all interactions that should be authenticated, as well as informing those stakeholders of the risks associated with weak authentication schemes.

Recommendation E2: Registry Lock

ICANN org should undertake efforts to improve documentation and understanding of Registry Lock features and to promote their uses, when appropriate, and improve the understanding regarding the differences between Registry and Registrar Lock. Registrants should be able to find clear definitions of what these features provide, what these features do not provide, and the difference between them. ICANN org should consider facilitating the standardization of minimum requirements for Registry and Registrar Lock services.

Recommendations – Education and Awareness (2)

Recommendation E3: Awareness of Best Practices for Infrastructure Security

ICANN org should continue to work with initiatives like MANRS and KINDNS to measure and report on their adoption and use those reports to target educational material that will improve awareness around infrastructure security. ICANN org should take the best practices coming out of those initiatives and make sure that contracted parties and the ICANN community are aware of them. Where current best practices do not exist, ICANN org should work to encourage the development and deployment of said practices and promote the adoption of DNS security-enhancing features throughout the DNS ecosystem (e.g., DMARC, SPF, TLSA, DANE, DNSSEC, etc.).

Recommendation E4: DNS Blocking and Filtering

ICANN org should create informative and educational materials to help the ICANN community, contracted parties, and other interested parties to understand the risks and benefits of DNS blocking and filtering for security and stability reasons throughout the global DNS infrastructure community.

Recommendations – Education and Awareness (3)

Recommendation E5: Incident Response

ICANN org should, together with relevant parties, encourage the development and deployment of a formalized incident-response process across the DNS industry that allows for interaction with others in the ecosystem. Such an effort should include incident-response handling as well as the protected sharing of threat and incident information.

Recommendation E6: Covert Channel Awareness

ICANN org should publish educational material on the use of covert channels as an attack vector, which may be seen as an abuse of the DNS itself and as such, requires handling as with other DNS abuse issues.

Recommendations – Priority Perspective

While all recommendations are considered important and immediately relevant, two in particular are considered particularly important for ICANN to address:

- **Recommendation R3: Investigate Appropriate Best Practice for Authentication**
- **Recommendation E5: Incident Response**

Visit the DNS Security Facilitation Initiative Technical Study Group
Workspace:

- Charter
- Scoping document
- Work plan and timelines
- Meeting agendas and notes
- Resources

<https://community.icann.org/display/DSFI>

Questions