DNS Security Facilitation Initiative Technical Study Group - Final Report

Executive Summary

The practices around securing the Domain Name System (DNS) are as varied as the entities supporting it. Attacks against the DNS, or those who use the DNS, significantly impact the trust and stability of the Internet. ICANN org is in a position to help improve the security of the DNS directly, through funded research and education, and indirectly through partnerships, community collaboration, and contractual controls. The DNS Security Facilitation Initiative Technical Study Group (DSFI-TSG) offers 12 recommended actions ICANN org can take to facilitate and promote better security practices throughout the DNS:

- Recommendation O1: Develop a Tabletop Exercise Program
- Recommendation R1: Continue Existing Work on DNS Abuse
- Recommendation R2: Investigate DNS Security Enhancements
- Recommendation R3: Investigate Appropriate Best Practice for Authentication
- Recommendation C1: Empower Contracted Parties
- Recommendation F1: Bug Bounty Program Feasibility Funding
- 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

While all recommendations are considered important and immediately relevant, the DSFI-TSG agreed that if a priority were to be assigned, two recommendations would be the highest priorities to consider: Recommendation R3: Investigate Appropriate Best Practice for Authentication and Recommendation E5: Incident Response.

This document is not exhaustive; the DSFI-TSG focused on the areas they believe are of maximum immediate value for the ICANN CEO to address and make the best use of ICANN's current resources.

This document represents the rough consensus of the DSFI-TSG members and does not reflect the views of any individual member, their employees, or other affiliated organizations.

Introduction

ICANN CEO, Göran Marby, commissioned the DSFI-TSG to investigate potential mechanisms to strengthen collaboration and communication on the security and stability issues that impact the DNS, and to offer recommendations for how ICANN org may best serve to improve the security, stability, and resiliency of the global DNS.

ICANN org is just one partner in the DNS; input from a variety of stakeholders will be necessary to create a more secure DNS. The DSFI-TSG brought together experts in DNS standards and operations, including those who have experience handling cybercrime, security incidents, registry/registrar operations, and critical infrastructure operations.

This report offers a review of the common vectors of attack on or involving the DNS. By examining the common patterns for attacks, the DSFI-TSG was able to work through some of the reasons why those attack vectors are successful, and consider possible mitigations for each (detailed in Appendix 4. Mitigations for Various Attack Vectors). With an understanding of the attack vectors firmly in mind, the DSFI-TSG considered how ICANN might positively influence the mitigation of those vectors, resulting in the recommendations that wrap up the main body of the report.

The DSFI-TSG offers 12 recommendations for consideration, primarily in the areas of education and awareness, and suggests areas of research where best practice guidance is lacking. The DSFI-TSG determined that research, education, and awareness offer more opportunities for ICANN org to have a strong and positive impact on the global DNS. In particular, Recommendation R3: Investigate Appropriate Best Practice for Authentication, and Recommendation E5: Incident Response, are considered particularly important for ICANN org to address. Each recommendation provides measurable and actionable activities; evaluation of the implementation is out of scope for this DSFI-TSG but may inform the charter for a future technical study group.

Process

The DSFI-TSG focused on real and known threats to the DNS by examining several incidents that reflected multiple attack vectors; many of these incidents are documented in the footnotes for each attack vector. The group then discussed existing mitigations that could have prevented or lessened the severity of those incidents. From that point, the DSFI-TSG considered where ICANN org could best serve the global DNS by encouraging the adoption

of those mitigations more broadly or facilitating discussion within the community to develop new mitigations where options are lacking. The emphasis was on efforts that did not otherwise already exist within ICANN org. In some cases, the attacks and their mitigations were based solely on the knowledge and experience of the DSFI-TSG members; some incidents were not made public and could only be discussed generally due to formal or informal agreements.

As per the DSFI-TSG's charter, the group worked under the following considerations:[1]

- Theoretical attacks are unlikely to result in concrete recommendations. However, any recommendations that the DSFI-TSG makes must take into account the evolving landscape and must be able to adjust over time.
- The recommendations will be based on the mechanics of broad security issues.
- Any recommendations made to ICANN org will attempt to avoid conflicting with ICANN org bylaws.
- Although the DSFI-TSG's recommendations are to the ICANN CEO, they may require effort from a broader set of stakeholders.
- Recommendations will span multiple areas and may include, but are not limited to best practice, information sharing, and incident response considerations.
- This group will not make policy, however it may recommend that policy changes be considered.
- There are other dependencies to the DNS (e.g., routing) that may impact the recommendations and may be taken into consideration.
- This group will not focus on the content of the attacks, and instead will focus on the mechanism by which the attack is carried out.

Background

As noted by Göran Marby, "Attacks on the Domain Name System (DNS) rarely impact only one actor on the Internet. With significant recent attacks, such as the Sea Turtle hijacking and the DNSpionage, we see an urgent need to come together and respond. The solution, or solutions, that would best improve the security and stability of the DNS ecosystem (the complex technical and contractual relationships that exist between registrars, registries,

[1] DNS Security Facilitation Initiative Technical Study Group (DSFI-TSG), Project Charter and Scope, 1 September 2020, https://community.icann.org/display/DSFI/Project+Charter+and+Scope.

registrants, and policy authorities) are not yet clear. However, it is clear that a new level of collaboration and understanding is required."[2]

ICANN org is in a unique position to offer resources to help improve the security of the DNS. A variety of activities, some of which are already promoted or supported by ICANN org and others, are underway, including the Internet Society's Mutually Agreed Norms for Routing Security (MANRS),[3] Knowledge-sharing and Instantiating Norms for DNS and Naming Security (KINDNS),[4] and a variety of training courses focused on security.[5] The DSFI-TSG took those activities into account while considering what recommendations to offer for further improvements around the security of the DNS.

Attack Vectors in the DNS Ecosystem - Key Findings

The DSFI-TSG identified seven categories of attack vectors. These attack vectors are described in more detail below and may unavoidably overlap in attacks and resulting recommendations.

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

Within each category, the DSFI-TSG focused on specific areas and associated incidents. By analyzing real-world incidents and attack scenarios, the group focused on immediate and practical information to inform its recommendations to the ICANN CEO.

---

[2] Marby, Göran, "Introducing the DNS Security Facilitation Initiative Technical Study Group," ICANN blogs, 6 May 2020, https://www.icann.org/news/blog/introducing-the-dns-security-facilitation-initiative-technical-study-group.

[3] Internet Society, "Mutually Agreed Norms for Routing Security," MANRS, https://www.manrs.org/.

[4] "Knowledge-sharing and Instantiating Norms for DNS and Naming Security (KINDNS)," ICANN Community wiki, https://community.icann.org/display/KINDNS.

[5] "Technical Engagement Training Course Catalogue," ICANN website, https://www.icann.org/resources/pages/tech-engagement-training-course-catalogue-2021-04-22-en.

For each attack vector, the DSFI-TSG 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 technical requirements needed to address the gaps?
    - What operational best practices need to be developed, modified, promoted, or implemented to address the gaps?
    - What are hindrances to deployments of best practices and other technical measures?
- What are the risks associated with these gaps that may not be well understood?
    - What are the risk considerations?
    - Where are there gaps in knowledge of the threat models to the DNS ecosystem?
    - What externalities do people need to be aware of?
- Does the DNS have unique characteristics that attract security problems, which other Internet services don't have?
    - What can we learn from other protocols or industries that face similar issues (e.g., critical infrastructure industries)?
    - How can we improve on any existing practices?

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 their systems, ICANN org support systems, and data escrow services, while registrars see logins from registrants and resellers.[6] Attacks on and through the credential systems result in issues such as the modification of registration data, leading to domain hijacking, traffic interception, social engineering attacks, and more.

Examples of this kind of compromise include:

- "Onamae.com" May 2020 - leading to the hijacking of crypto domain Coincheck[7]
- "Webnic.cc" February 2015 - leading to the hijacking of Lenovo.com[8]

---

[6] ICANN Security and Stability Advisory Committee, "SAC074 - SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle" 3 November 2015, https://www.icann.org/en/system/files/files/sac-074-en.pdf.

[7] Baker, Paddy, "Coincheck Customers Fall Victim to Data Breach After Domain Account Error," Coindesk, 3 June 2020, https://www.coindesk.com/crypto-exchange-coincheck-victim-domain-data-breach.

[8] Krebs, Brian, "Webnic Registrar Blamed for Hijack of Lenovo, Google Domains," Krebs on Security, 26 February 2015, https://krebsonsecurity.com/2015/02/webnic-registrar-blamed-for-hijack-of-lenovo-google-domains/.

- "Moniker.com" October 2014 - leading to mass customer domain hijacking[9]
- "MelbourneIT" August 2013 - leading to the hijacking of the NYTimes, Twitter, and HuffPost[10]
- DNSpionage[11]
- "EA/Origin subdomain hijack" June 2019 - demonstrating a real-world subdomain hijack method[12]

This section considers the impact of credential compromises for registrants, registries, registrars, and resellers, as well as specific mitigations for those types of attacks.

Registrant Credential Compromise

Registrants are individuals or entities who register domain names.[13] Upon registration of a domain name, a registrant enters into a contract with a registrar or registry (some registries, for example some ccTLDs, do not use registrars).[14] The contract describes the terms and conditions under which the registrar agrees to register and maintain the requested name.[15]

In most cases, registrants must procure their domain names. This occurs via a registrar (either a registry that acts as registrar, an ICANN-accredited in the case of gTLDs, or a registrar directly accredited by the registry in the case of ccTLDs) or a reseller of a registrar (collectively referred to as a "retailer").[16]

---

[9] Zoch, Jamie, "Massive Moniker.com Breach, Valuable Domains Stolen," dotWeekly, 7 October 2014, http://dotweekly.com/massive-moniker-com-breach-valuable-domains-stolen/.

[10] Reuters staff, "Melbourne IT says reseller credentials used in hacking of NYT, other media," Reuters, 27 August 2013, https://www.reuters.com/article/media-hacking-melbourne/melbourne-it-says-reseller-credentials-used-in-hacking-of-nyt-other-media-idUSL2N0GT01K20130828.

[11] Krebs, Brian, "A Deep Dive on the Recent Widespread DNS Hijacking Attacks," Krebs on Security, 18 February 2019, https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/.

[12] Salter, Jim, "Security firms demonstrate subdomain hijack exploit vs. EA/Origin," Ars Technica, 26 June 2019, https://arstechnica.com/information-technology/2019/06/security-firms-demonstrate-subdomain-hijack-exploit-vs-eaorigin/.

[13] Vertically integrated new gTLDs and some legacy gTLDs (e.g., .GOV) operate their own registrar as well. With some large gTLDs (e.g., COM & NET), the terms of service are solely between the registrant and the registrar OR reseller; the only leverage the registrar has is the RRA with the registry as there is no contractual relationship between the registry and registrant.

[14] Many registries (mostly ccTLDs) offer direct registrations. In such cases registries act as registrars.

[15] ICANN, "ICANN Acronyms and Terms: Registrant," https://www.icann.org/en/icann-acronyms-and-terms/registrant-en.

[16] Note that this does not apply to .mil and .gov registrations.

Most retailers provide web-based account management tools to allow their customers to register, renew, and modify their domain names, along with value-added products and services associated with those domain names (such as web and email hosting, TLS certificates, and so on).

Registrants must authenticate with the retailer before accessing their web-based domain configuration page, using a username/email address and password in the majority of cases.

Should the registrant's credentials be compromised, an attacker would be able to impersonate the registrant and can then modify domain registration data to:

- Transfer the domain out of the registrant's control.
- Modify the domain's DNS servers to allow intercepting of traffic or redirecting to a criminal destination.
- Modify the domain's Authoritative DNS Servers allowing attackers to monitor, alter or deny queries and possibly redirect end users to malicious endpoints or services.
- Modify DNSSEC related data by removing the DS records, thus removing the protections provided by DNSSEC.
- Modifying authoritative records of the domain name, i.e., domain registration records or service records in case of Managed DNS.
- Delete or de-register the domain.

If the registrant also buys DNS, web, or email hosting from the retailer, the attacker will also have the ability to directly access and modify DNS information (e.g., to create secondary or managed DNS subdomains) and website content, read emails, procure TLS certificates (to facilitate further malicious activity), etc.

Like all end users, registrants are vulnerable to credential compromise through various vectors, including:

- Credential stuffing[17] and password spraying[18] attacks
- Phishing (including SMS and voice phishing)

[17] Wikipedia contributors, "Credential stuffing," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Credential_stuffing&oldid=1034364071.

[18] P, Andy, "Spray you, spray me: defending against password spraying attacks," blog, National Cyber Security Centre, 15 May 2018, https://www.ncsc.gov.uk/blog-post/spray-you-spray-me-defending-against-password-spraying-attacks.

- Social engineering
- Compromise of email accounts (which allow attackers to perform password resets)
- Password compromise through malware, spyware, and machine-in-the-middle attacks
- Poor password management (such as the reuse of passwords, guessable passwords, short passwords, etc.)
- Insider credential theft and abuse

Registry, Registrar, and Reseller Credential Compromise

Registry operators are in charge of Top-Level Domains (TLDs) and the affiliated zones. As such, they represent an attractive target for malicious actors. Registries are also subject to all of the forms of credential compromise that can affect any other business, with the nuance that their place in the DNS ecosystem may make the results of such compromises far-reaching.

A credential compromise within a registry's systems has the potential to affect all the registrars, resellers, and registrants below them in the DNS hierarchy.

Registries typically operate a broad spectrum of network services, each of which may have its own unique attack surface, credentials, risks, and mitigation strategies. These are not limited to services that are unique to registry services; the standard apparatus of any online business, such as mail, DNS, and web services is also at risk. Other systems may be dedicated to the registry business, such as the databases used to create TLD zone files. A successful attack on any one service may create a point of leverage or an opportunity for an attacker to "pivot" within a network, if adequate security controls are not in place.

Either due to common practice or requirements in the DNS industry, registries use registrars to sell names to registrants. Through this system, the registry may not have a direct relationship with the registrant of a particular domain. Instead, it will rely on the registrar to perform any authentication of requested changes.

The registry will, however, use various credentials with the registrar for querying, purchasing, updating, or deleting domain names or other information stored in the registry on behalf of registrants.

For each registry operator that a registrar is contracted with, a collection of credentials is used to authenticate the registrar to the registry. These are required to query or make changes to its registry database. These credentials may take multiple forms, including but not limited to: Extensible Provisioning Protocol (EPP) username(s) and password(s), certificate pairs, API keys, registry system portal passwords, or any number of multi-factor authentication methods (passphrase, pre-shared one-time use tokens, TOTP secrets, HOTP secrets, hardware verification devices, etc.). Compromising one or more of these credentials can result in partial or total loss of control of the registrar or reseller for any registry objects they control.

Abuse of Credentials to Initiate Transactions at the Registry

If an attacker is able to circumvent one or more controls through compromise (e.g., theft, brute force, or failure) of existing staff, system, or operations credentials, they gain access to potentially critical registry operations. The credentials in question either provide enough access for the attacker to impersonate legitimate operations staff and perform registrar transactions or to pivot and gain access to additional systems or credentials where they can perform registrar transactions.

Access Control and Authorization Issues

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.

While related to credentials, access control weaknesses introduce vulnerabilities related to permissions and what an individual is allowed to do in a system. Properly managing accounts and their permissions, including creating and removing accounts as circumstances change, is an ongoing challenge for most organizations.

Compromises related to this type of vulnerability are rarely made public. One example, however, of this type of compromise is the Spammy Bear event.[19]

Unauthorized Subdomain Takeover

Subdomain takeover is the act of a non-authorized user gaining access to publish content under a DNS label that they have not been authorized to control. For example, if the DNS record for *.example.com is mapped to a content delivery network (CDN) or service provider, and only foo.example.com and bar.example.com are configured on that platform by the legitimate owner, any scenarios where another user configures baz.example.com without the authorization of the owner is problematic. This type of registration can lead to any number of attacks on the credibility of the actual owner. It may even allow an attacker to use some appearance of an affiliation to the other sites to decrease the level of suspicion for the registered name.

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 common network management tactic, such as with captive portals that restrict access from an internal network to the public Internet. Other cases can result in redirection to malicious targets, which, for example, could support the distribution of malware or be used to harvest end-user data.

Impersonation of Recursive Resolvers

A recursive resolver is an intermediary between Internet users and authoritative DNS servers. Recursive resolvers process DNS queries from end-user devices, querying authoritative servers at the root, top-level and lower levels, while also storing responses in cache in order to respond more quickly to future queries.[20] Impersonating a resolver (by intercepting traffic to it at the network layer) is a distinct threat from changing the user's configuration (a client-side compromise).

---

[19] Krebs, Brian, "Tag Archives: Spammy Bear," blog posts, Krebs on Security, https://krebsonsecurity.com/tag/spammy-bear/.

[20] Lee, Donald, "Recursive DNS: What It Is And Why You Should Care," Neustar blog, 18 July 2016, https://www.home.neustar/blog/recursive-dns-what-it-is-and-why-you-should-care.

DNS hijacking, also known as DNS redirection, is a type of attack in which DNS queries are incorrectly resolved in order to redirect users to malicious sites or otherwise inspect or modify queries or responses.[21] To perform the attack, perpetrators may install malware on the user's computer or take over on path networking equipment, like routers or switches, to redirect the user to malicious sites via false DNS information. When a small office or home office (SOHO) router is compromised, the DNS settings for the recursive resolver are changed so that requests are sent to a "rogue" DNS server controlled by the attackers. This rogue DNS server impersonates the Authoritative Server of the domain being hijacked and behaves as a regular recursive for other domains.

Examples of these types of attacks include the DNSChanger and GhostDNS botnet attacks.[22]
Note that captive portals, known to have incomplete firewall rule sets, often employ authoritative nameserver impersonation as a technique to direct unauthenticated users to an authentication page prior to granting access to the network or public Internet.[23]

Impersonation of Authoritative Server (and associated infrastructure)

Impersonation of a nameserver can be described as when a party other than the legitimate server operator is able to receive (and potentially respond to) DNS queries destined for an authoritative nameserver. By performing such impersonation, the impersonating party is able to observe DNS query messages and return incorrect response data, either all or some of the time. Attackers may use geolocation to hide their activities so that only certain geographic areas see altered data. The impersonator may return correct responses (e.g., by proxying, forwarding, or relaying queries to and responses from the real server) that can make the activity particularly difficult to detect. Impersonation of an authoritative server can lead to lingering impacts if a recursive cache is populated with incorrect results.

---

[21] "Domain name server (DNS) Hijacking," Imperva Learning Center, https://www.imperva.com/learn/application-security/dns-hijacking-redirection/.

[22] Gallagher, Sean, "How the most massive botnet scam ever made millions for Estonian hackers," ArsTechnica, 10 November 2011, https://arstechnica.com/tech-policy/2011/11/how-the-most-massive-botnet-scam-ever-made-millions-for-estonian-hackers/ and Byers, Nick, and Josh Hopkins, "GhostDNSbusters: Illuminating GhostDNS Infrastructure," Dragon News Blog, September 8, 2020, https://team-cymru.com/blog/2020/09/08/illunimating-ghostdns-infrastructure-part-1/.

[23] "Captive Portal Workaround," Keuper ICT, 7 January 2020, https://keuperict.nl/posts/security/2020/01/07/work-around-captive-portal/.

Impersonation of Infrastructure Using Look-alike Domains (Facsimile Domains)

This class of attack vectors relies on abusing similarities in domain names to mislead an unaware user into interacting with a bogus website or other resources. There are several ways to take advantage of domain similarity.[24]

1) Domain suffix appending: For example, `www.icann.org.example.com` instead of `www.icann.org`. Note that this is subtly different from domain search suffix appending by some stub resolvers. Although one might think it is obvious that the longer name is bogus, with HTML, it is possible to easily hide the longer links (e.g., the link underlying the following: `www.icann.org <www.icann.org.example.com>`). This obfuscation is possible in other protocols as well. A user might not notice the longer, bogus name unless they manually inspect the link prior to clicking. Certain mobile user interface constraints may make link inspection difficult.

2) Typos, aka typosquatting: Subtle misspellings of domain name labels may be hard to spot—for example, `faceboook.com` instead of `facebook.com`, `googIe.com`, or `goggle.com` instead of `google.com`. Typosquatting became a topic of discussion in the early-2000s with the advent of sites directing unsuspecting visitors to faux search pages that generated ad revenues. Typosquatting is still a common attack vector for phishing and is often used in combination with internationalized domain names (IDN).[25]

3) Internationalized domain name homographs: For example, applé.com instead of apple.com. Due to the large number of language-specific scripts and alphabets that can be represented with Unicode, there are many ways to combine them into similar-looking domain names. Although the different "é" in the example above is relatively easy to spot, there are many characters that appear identical (depending on the choice of font) but have different underlying encoding.[26]

---

[24] For more information, see section "12.5. Visually Similar Characters" of Saint-Andre, P. and M. Blanchet, "PRECIS Framework: Preparation, Enforcement, and Comparison of Internationalized Strings in Application Protocols", RFC 8264, DOI 10.17487/RFC8264, October 2017, <https://www.rfc-editor.org/info/rfc8264>.

[25] Wikipedia contributors, "Lamparello v. Falwell," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Lamparello_v._Falwell&oldid=991268275.

[26] Nadler, Asaf, "Watch Your Step: The Prevalence of IDN Homograph Attacks," Akamai Security Intelligence & Threat Research, 27 May 2020, https://blogs.akamai.com/sitr/2020/05/watch-your-step-the-prevalence-of-idn-homograph-attacks.html.

4) Bitsquatting: Similar to typosquatting, bitsquatting refers to the registration of domain names that are one bit different from existing domains. This is an opportunistic attack that seeks to catch system-level data errors. When such a bit difference occurs, the user requesting the domain may be directed to a website registered under a domain name similar to a legitimate domain, except with one bit flipped in their respective binary representations.[27]

Domain name impersonation is often used in conjunction with phishing attacks.[28] If the intended victim is fooled by similar domain names, they may be convinced to enter sensitive information, such as usernames, passwords, account numbers, etc., into websites controlled by the attacker.

Fraudulent Certificates

Online transactions rely heavily on the authentication of the communication endpoints and/or users. Using Transport Layer Security (TLS) certificates is the de-facto standard to provide encryption and authentication, and protect against men-in-the-middle attacks and credential theft.

Fraudulent Certificates are TLS certificates issued to a requester who is not the legitimate operator of the service secured by this certificate.[29] Manipulation as a result of, for example, inadequate access controls of DNS entries (e.g., A records, MX records, NS records) and/or BGP route manipulation play prominent roles in intervening with the certificate issuing process. This gained even more momentum with the growing success of free or low-cost certificate providers like the Let's Encrypt initiative and the slow adoption of DNS-based Authentication of Named Entities (DANE).[30] It is also worth mentioning that technologies that are meant to ensure more trust in certificates are not always utilized and therefore create a lack of checks in validating certificates. Examples of such technologies include the Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP),

---

[27] Macarie, M. "DNS Bitsquatting in the Wild." University of Twente, 2020. http://essay.utwente.nl/82361/.

[28] Aaron, Greg, Lyman Chapin, David Piscitello, Dr. Colin Strutt, "Phishing Landscape 2020: A Study of the Scope and Distribution of Phishing," Interisle Consulting Group, LLC, 13 October 2020, p 5, http://interisle.net/PhishingLandscape2020.pdf.

[29] Wikipedia contributors, "DNS Certification Authority Authorization," *Wikipedia, The Free Encyclopedia*, https://en.wikipedia.org/w/index.php?title=DNS_Certification_Authority_Authorization&oldid=1021637900.

[30] Barnes, R., "Use Cases and Requirements for DNS-Based Authentication of Named Entities (DANE)", RFC 6394, DOI 10.17487/RFC6394, October 2011, <https://www.rfc-editor.org/info/rfc6394>.

which are often not employed by user agents due to bandwidth or latency concerns with user interaction.[31] Google's Safebrowsing is an attempt to augment these shortcomings, but is only widely deployed for web browsers. Proof-of-possession of a certificate, however, is an issue that goes beyond the DNS and into more general concerns regarding certificate management processes.

Route Manipulation

Route Manipulation (sometimes referred to as prefix hijacking, route hijacking, IP hijacking, or path injection) is the "illegitimate takeover of groups of IP addresses by manipulating Internet routing tables maintained using the Border Gateway Protocol (BGP)."[32]

BGP, the core protocol to exchange routing information between Autonomous Systems, was not designed with security in mind (this is also true for many other protocols in the network stack used today). A high level of implicit trust between peers leads to a design that makes it easy to inject false routing announcements, either by accident or on purpose. In the case of "private peering," only the hijacker and the targeted party can see this happening, which makes Internet-wide detection much more difficult. By manipulating routing information, a number of different attacks can be launched (e.g., machine-in-the-middle, credential harvesting, server impersonation, etc.), particularly if there is a lack of appropriate authentication by applications relying on correct routing.

Examples of this type of attack vector include, but are not limited to:

- YouTube Hijacking: A RIPE NCC RIS case study[33]
- Bitcanal attacks[34]

---

[31] See Cobb, M., "Certificate Revocation Lists," TechTarget, May 2016, https://searchsecurity.techtarget.com/definition/Certificate-Revocation-List, and Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 6960, DOI 10.17487/RFC6960, June 2013, <https://www.rfc-editor.org/info/rfc6960>.

[32] Wikipedia contributors, "BGP hijacking," *Wikipedia, The Free Encyclopedia*, https://en.wikipedia.org/w/index.php?title=BGP_hijacking&oldid=1027353815 (accessed July 19, 2021).

[33] "YouTube Hijacking: A RIPE NCC RIS case study," RIPE Network Coordination Centre, 17 March 2008, https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study.

[34] Krebs, Brian, "Notorious 'Hijack Factory' Shunned from Web," blog posts, Krebs on Security, 11 July 2018, https://krebsonsecurity.com/2018/07/notorious-hijack-factory-shunned-from-web/.

- US Payment Processing services attacks[35]
- Akamai, Amazon, and Alibaba BGP hijack[36]

Code and Protocol Vulnerabilities

Another attack vector involves vulnerabilities in the software used to run a DNS service or in the protocol that defines the DNS. It is not always clear-cut whether the mitigation lies squarely in the code or in the protocol. Some vulnerabilities arise from the developer having a slightly different or incomplete understanding of a part of the protocol specification, ambiguous specifications, and writing code according to their best guess. Sometimes that code offers improvements and mitigations to potential vulnerabilities. Other times it may open up a vulnerability the protocol was designed to prevent. It is an open question whether the protocol itself needs to be clarified or modified or the developers' understanding improved. 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.

Examples of attacks on the DNS via code or protocol vulnerabilities include, but are not limited to:

- Dan Kaminsky's cache poisoning attack[37]
- Sad DNS[38]
- NXNS[39]
- DNSpooq[40]

---

[35] Abrams, Lawrence, "U.S. Payment Processing Services Targeted by BGP Hijacking Attacks," Bleeping Computer, 6 August 2018, https://www.bleepingcomputer.com/news/security/us-payment-processing-services-targeted-by-bgp-hijacking-attacks/.

[36] Radar, "This is how you deal with route leaks," blog, Qrator Labs, 2 April 2020, https://blog.qrator.net/en/how-you-deal-route-leaks_69/.

[37] "Multiple DNS implementations vulnerable to cache poisoning: Vulnerability Note VU#800113," Carnegie Mellon Institute, Software Engineering Institute, CERT Coordination Center, last revised 14 April 2014, https://www.kb.cert.org/vuls/id/800113.

[38] Man, Keyu, Zhiyun Qian, Zhongjie Wang, Xiaofeng Zheng, Youjun Huang, Haixin Duan, "DNS Cache Poisoning Attack Reloaded: Revolutions with Side Channels,"conference proceedings, *ACM Conference on Computer and Communications Security* (CCS`20), 9-13 November 2020, https://doi.org/10.1145/3372297.3417280.

[39] Yehuda, Afek, Anat Bremler-Barr, Lior Shafir, "NXNS Attack: Recursive DNS Inefficiencies and Vulnerabilities," August 2020, https://cyber-security-group.cs.tau.ac.il/.

[40] Kovacs, Eduard, "DNSpooq Flaws Expose Millions of Devices to DNS Cache Poisoning, Other Attacks," SecurityWeek, Wired Business Media, 20 January 2021, https://www.securityweek.com/dnspooq-flaws-expose-millions-devices-dns-cache-poisoning-other-attacks.

Protocol Weaknesses

Protocol vulnerabilities are often more significant than vulnerabilities in implementations. While individual implementations can usually be fixed relatively quickly once discovered (although deployment can often take much longer), protocol weaknesses are often much more difficult to mitigate. Any modification to the protocol may cause interoperability issues and requires coordination among a large number of implementers and operators. That coordination, however, may not be seen as a priority by all of those required to remedy the issue.

Vulnerability Exploitation

An attacker is able to gain access to critical or trusted components within the DNS infrastructure chain through an exploitable software flaw. The flaw must be sufficient to allow control of, or denial of service to, infrastructure directly involved in the delivery and management of DNS, or be in a component with a direct link through trust or lateral movement that allows this level of access.

DNS Cache Poisoning

DNS Cache Poisoning is the act of inserting incorrect data into a recursive nameserver cache, with the intention that end-users of that server receive and utilize the incorrect data.[41] Poisoning can occur either when a malicious server includes bad data in a response, when an on-path attacker intercepts a query and generates its own response, or when an off-path attacker is able to successfully spoof a response that appears to come from a legitimate responder. The incorrect data may remain in the cache for an amount of time determined by the Time-To-Live (TTL) values in the poisoning response (TTL impacts are discussed later in this paper).

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 TTL values, the choice of software used (such as older, unpatched versions of nameserver software), or the decision

[41] "What is DNS cache poisoning? | DNS spoofing," Cloudflare Learning Center, https://www.cloudflare.com/learning/dns/dns-cache-poisoning/.

to build in less redundancy with an eye toward keeping costs down.[42] 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.[43]

Examples of this type of attack vector include, but are not limited to:

- The New York Times domain hijacking attack[44]
- The Craigslist.com domain hijacking attack[45]
- The Dyn Distributed Denial of Service (DDoS) attack[46]
- Various attacks associated with weak cryptography[47]

There are contextual differences in every environment, which makes offering specific recommendations to fix every situation impossible. Administrators must be thoughtful about the context their environment operates in, including the trust relationships and configurations. Reviewing this context must be repeated on a regular basis, as while the infrastructure itself may not change, the usage and the environment around it may. Any changes in context will have a significant impact on the infrastructure's usefulness and security.

Long TTLs

Data published in the DNS is given a Time to Live (TTL) value, which was designed to enable caching in a way that puts the data publisher in control. Zone owners expect that data is cached and reused for an amount of time not to exceed its TTL. Choice of TTL values

---

[42] Wikipedia contributors, "Comparison of DNS server software," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Comparison_of_DNS_server_software&oldid=1033478299 (accessed July 30, 2021).

[43] Vlajic, N., M. Andrade, U.T. Nguyen, "The Role of DNS TTL Values in Potential DDoS Attacks: What Do the Major Banks Know About It?," Procedia Computer Science, Volume 10, 2012, Pages 466-473, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2012.06.060.

[44] Lee, Tim B., "The New York Times Web site was taken down by DNS Hijacking. Here's what that means," *Washington Post*, 27 August 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/08/27/the-new-york-times-web-site-was-taken-down-by-dns-hijacking-heres-what-that-means.

[45] Support Mozilla outage report, http://blog.craigslist.org/2014/11/24/craigslist-dns-outage/, 24 November 2014, https://support.mozilla.org/bm/questions/1032801.

[46] Sullivan, Andrew, "Dyn, DDoS, and DNS," presentation at ICANN 58 Tech Day, 13 March 2017, https://ccnso.icann.org/sites/default/files/file/field-file-attach/2017-04/presentation-oracle-dyn-ddos-dns-13mar17-en.pdf.

[47] Beagle Security, "Importance of TLS 1.3: SSL and TLS Vulnerabilities," Beagle Security blog, 6 July 2020, https://beaglesecurity.com/blog/article/importance-of-tls-1-3-ssl-and-tls-vulnerabilities.html.

represents tradeoffs between resilience, agility, performance, and in some cases, server load. Longer TTLs favor resilience and performance, while shorter TTLs favor agility. Short TTLs are generally on the order of minutes or seconds, while long TTLs are on the order of hours or even days.

For most organizations, there are only two times when TTLs really matter: when updating records or when faced with an attack on authoritative nameservers.[48] Here, we focus only on the attack scenario. A service that finds itself under attack may want to make a change to help mitigate the attack, for example, adding capacity, changing data centers, or changing providers. When DNS records have long TTLs, changes propagate slowly and the service takes a long time to recover. Interestingly, when a service's DNS provider is under attack (such as a DDoS attack), long TTLs are preferable.[49] It is worth noting that while TTLs can be modified by the domain operator, in many cases, they rely on a parent zone that has fixed TTLs.

Attackers who are able to cause changes in DNS delegations or zone data can use long TTLs to their advantage. The effects of a hijack remain in DNS caches until the TTL expires, which could be many days after the hijack has been detected and corrected. Additionally, long TTLs on poisoned records have the potential to impact many more DNS requests. The distributed nature of caches could also make detecting poisoned caches incredibly difficult, depending on how the bad data was delivered. DNS caches are so widely distributed, which makes it nearly impossible to purge all of them of bad data.

Short TTLs

Short TTLs are most often associated with services that require flexibility and high availability. These services may also desire the ability to move DNS traffic quickly to another system or provider. For example, short TTLs are often used by content delivery networks to provide agility, adaptability, and traffic engineering.

Short TTLs may be a risk factor in certain types of attacks. For example, an attack on a DNS provider may be felt more widely and more suddenly if the provider's customers utilize short TTLs. Short TTLs can be effective in covering an attacker's tracks due to the

[48] See Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>, and Pappas, Vasileios & Massey, Dan & Zhang, Lixia. (2007). Enhancing DNS Resilience against Denial of Service Attacks. 450 - 459. 10.1109/DSN.2007.42.

[49] Lawrence, D., Kumari, W., and P. Sood, "Serving Stale Data to Improve DNS Resiliency", RFC 8767, DOI 10.17487/RFC8767, March 2020, <https://www.rfc-editor.org/info/rfc8767>.

ephemeral nature of caches and the general lack of logging, which complicates forensics. For example, a spear-phishing campaign launched at the company comptroller with a TTL that is just long enough to cover the bogus address leading to the attacker's site would be extremely difficult to uncover after the damage is done.

Poor Operational Choices

Administrators may make implementation choices for the DNS environment that could result in a weaker defensive posture when faced with an attack than provided by other implementations. This can happen for a variety of reasons ranging from ease of implementation, financial considerations, or a desire for risk mitigation. An administrator may choose to use out-of-the-box DNS software packaged with their operating system of choice without checking that software for patches. They may decide to place or use all authoritative domain servers on the same IPv4 sub-network or physical network, leaving them open to outages from the loss of network connectivity, DDoS attack, or unexpected BGP routing behavior. They may choose to depend on the obscurity of their system to protect it from attacks. These choices are just examples of the many choices administrators make in their environment that have an impact on their security posture.

Fate Sharing

Fate sharing refers to an engineering design philosophy where related parts of a system are interconnected so that they fail together.[50] Running an authoritative DNS server and a recursive DNS server on the same physical device or relying on the same DNS software for all authoritative and/or recursive DNS server deployments where a bug can cause a severe issue and significant downtime are examples of fate sharing. Other examples of enabling fate sharing include putting all critical domains on the same infrastructure or having all "DDoS prone services" on the same provided systems.[51]

---

[50] ICANN Security and Stability Advisory Committee, "SAC005: DNS Infrastructure Recommendations," 1 November 2003, https://www.icann.org/en/groups/ssac/dns-recommendation-01nov03-en.pdf.

[51] More information on fate sharing may be found in Clark, David, "The design philosophy of the DARPA internet protocols," *ACM SIGCOMM Computer Communication Review*, Volume 18, Issue 4, August 1988 pp 106–114, https://doi.org/10.1145/52325.52336.

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 and/or connectivity of a target.[52]A variation of a DoS attack is the Distributed Denial of Service (DDoS) attack, which occurs when multiple systems orchestrate a synchronized DoS attack to a target.

DNS-based DDoS attacks have an amplification effect because response messages are almost always larger (and sometimes many times larger) than the corresponding queries. Often referred to as reflective amplification attacks, a reflective DNS amplification attack is a DDoS attack in which attackers use publicly accessible, open recursive resolvers or botnets to flood a target system with DNS response traffic.[53] These sorts of attacks often maximize the amplification factor by choosing queries that result in large responses, such as those with large Resource Record Sets and those with multiple DNSSEC signatures.

DDoS attacks often make use of UDP-based protocols (such as DNS) since it is connectionless and easily spoofed. TCP, on the other hand, is harder to spoof but requires more system resources (on both client and server). A recent trend in the DNS is to shift more traffic to TCP and encrypted transports such as DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT): these transports can also be susceptible to DDoS attacks, such as SYN floods and “slowloris”-style attacks that attempt to tie up as many connections as possible.[54]

DDoS attacks on DNS service providers (root servers, registries, registrars) have the potential to disrupt more organizations than would be possible by launching direct attacks on those organizations due to the multi-tenant nature of their services, as well as collateral damage to non-targeted entities.

In the DNS environment, DoS attacks can target:

---

[52] Cybersecurity & Infrastructure Security Agency, “DDoS Quick Guide,” U.S. Department of Homeland Security, updated 20 October 20201, https://us-cert.cisa.gov/security-publications/DDoS-Quick-Guide.

[53] United States Cybersecurity and Infrastructure Security Agency, National Cyber Awareness System, “Alert (TA13-088A) DNS Amplification Attacks,” Original release date: 29 March 2013, Last revised: 4 June 2019, https://us-cert.cisa.gov/ncas/alerts/TA13-088A.

[54] Wikipedia contributors, "Slowloris (computer security)," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Slowloris_(computer_security)&oldid=1037208734 (accessed October 7, 2021).

- DNS infrastructure (DNS servers)
- Content delivery infrastructure (website, registry system, email services)
- An organization's infrastructure (servers, workstations, organization's network)

The following DNS-related infrastructure may be leveraged in DoS attacks:

- Open recursive DNS servers[55]
- Devices with malware querying open recursive DNS servers (botnets)

An example of a DNS-related DDoS attack is the Dyn DDoS attack, also referenced earlier in Infrastructure Choices. [56]

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.

Examples of attacks using the DNS as the attack vector include, but are not limited to:

- Home Depot credit card exfiltration[57]
- Sally Beauty credit card exfiltration[58]
- Feederbot[59]

Covert Channel

The use of the DNS as a covert channel, also known as "DNS Tunneling", uses the DNS query and response channels to enable surreptitiously communication between devices

[55] An open recursive server is one that processes DNS requests for the Internet at large, rather than just for a very limited subset of networks, and has little to no access control for DNS queries.

[56] Sullivan, Andrew, "Dyn, DDoS, and DNS" https://ccnso.icann.org/sites/default/files/file/field-file-attach/2017-04/presentation-oracle-dyn-ddos-dns-13mar17-en.pdf.

[57] "New FrameworkPOS variant exfiltrates data via DNS requests," G Data blog, 15 October 2014, https://www.gdatasoftware.com/blog/2014/10/23942-new-frameworkpos-variant-exfiltrates-data-via-dns-requests.

[58] Krebs, Brian, "Deconstructing the 2014 Sally Beauty Breach," blog posts, Krebs on Security, 7 May 2015, https://krebsonsecurity.com/2015/05/deconstructing-the-2014-sally-beauty-breach/.

[59] Dietrich, Christian & Rossow, Christian & Freiling, Felix & Bos, Herbert & van Steen, Maarten & Pohlmann, Norbert. (2011). On Botnets that use DNS for Command and Control. 10.1109/EC2ND.2011.16.

while appearing to be benign DNS traffic. Typically, this uses encrypted data disguised as DNS queries and responses rather than DNS' intended use as a resource lookup protocol.[60]

The DNS may be used as a communications channel between firewalled/protected resources and external third parties with malicious intent. DNS is a needed protocol for nearly every device that resides on a network, and access to the global DNS is provided on most computer networks. As a uniquely essential service that also serves as a signaling mechanism in normal two-way traffic exchanges, it provides a rare opportunity for miscreants to establish covert messaging channels between compromised devices on protected and/or segregated networks and external control nodes or data collection points.

Since DNS traffic is often allowed to traverse network boundaries largely unimpeded and unmonitored, it is possible to create a two-way communications stream using seemingly innocent DNS queries and responses to pass messages such as requests for instructions or exfiltration of data. Queries for various address records underneath a domain controlled by an adversary allow data or other communications to be transmitted from a protected network. Responses to queries in the form of addresses or text can provide further instructions or communications back to a compromised device.[61]

While demonstrably an attack vector using the DNS, awareness of covert channel attacks as an issue that organizations must plan for as an active threat is low.

A specific form of using the DNS as a covert channel involves using that covert channel to surreptitiously exfiltrate data from a protected network and/or asset. Many recent attacks have used the DNS for exfiltration and have gained notoriety as a highly effective attack method.[62] In such attacks, an attacker will use DNS requests as the medium to transmit data to an external resource in an encrypted fashion , typically an authoritative nameserver

---

[60] Piscitello, Dave, "What Is a DNS Covert Channel?" ICANN blog, 8 December 2016, https://www.icann.org/news/blog/what-is-a-dns-covert-channel.

[61] By using a unique query during the Solarwinds attack, the attackers could redirect certain sources to separate infrastructure by creating extra A records for those unique queries that would be favored over the wildcard that would catch everything. While this is not really a covert channel by itself, it does use the DNS system to give the attackers extra obscurity. See "DNS Tunneling In The SolarWinds Supply Chain Attack," Malware News, December 2020, https://malware.news/t/dns-tunneling-in-the-solarwinds-supply-chain-attack/45716.

[62] Sharma, Ax, "Researcher hacks over 35 tech firms in novel supply chain attack," Bleeping Computer, 9 February 2021, https://www.bleepingcomputer.com/news/security/researcher-hacks-over-35-tech-firms-in-novel-supply-chain-attack/.

that records the DNS queries it receives and either decodes the data or passes it along to another resource that can. Since DNS traffic is typically allowed to all network endpoints and lightly monitored, this can be a highly effective method for silently transferring data from a victim. Depending on the nature of the covert channel, there may be minor technical differences and traffic patterns between a data exfiltration via DNS attack and a covert channel using the DNS as a two-way communications conduit. In practice, a data exfiltration via DNS attack is largely identical to a covert channel with respect to prevention, detection, and mitigation. Even if egress DNS is blocked at the edge of a corporate network (to avoid contacting unauthorized resolvers), it would still be possible to use DNS as an exfiltration mechanism, or even as an IP-over-DNS covert channel, by relaying queries through a sanctioned internal forwarder.

Existing Efforts and Activities

Developing best practices and tools to improve DNS security is an effort that goes far beyond ICANN org. Below are key efforts that ICANN org should be aware of as the need arises to partner with others for the broadest impact possible.

DNS Operations, Analysis, and Research Center (DNS-OARC)

The DNS Operations, Analysis, and Research Center (DNS-OARC) primarily provides data, services, and tools related to DNS operations and security.[63] It also provides identity and trusted channel mechanisms for interpersonal communications. DNS-OARC's most popular dataset is the Day In The Life of the Internet (DITL) collection, which happens on an annual basis, and for other notable events such as updating the cryptographic keys for the root zone.[64] DNS-OARC currently provides hosting, but not development, for DNSViz.[65]

[63] DNS-OARC - DNS Operations, Analysis, and Research Center, website, https://www.dns-oarc.net/.

[64] DITL Traces and Analysis, DNS-OARC - DNS Operations, Analysis, and Research Center, https://www.dns-oarc.net/oarc/data/ditl.

[65] "DNSViz is a tool for visualizing the status of a DNS zone. It was designed as a resource for understanding and troubleshooting deployment of the DNS Security Extensions (DNSSEC). It provides a visual analysis of the DNSSEC authentication chain for a domain name and its resolution path in the DNS namespace, and it lists configuration errors detected by the tool." From the DNSViz website, https://dnsviz.net/.

DNS-OARC facilitates regular meetings and workshops where researchers and operators present their work, which often focuses on DNS security topics.

Forum of Incident Response and Security Teams (FIRST)

The Forum of Incident Response and Security Teams (FIRST) is an excellent resource for handling incident response activities.[66] ICANN org already partners with FIRST and should continue that collaboration going forward because FIRST is developing many materials that might inform the recommendations in this document.

DNSTransparency.Org

DNSTransparency.Org is a project that is becoming more active. Originally formed in response to DNSpionage and Sea Turtle, it is in the process of creating a system that "will allow domain owners to protect their domain name resources by making record changes available for the domain owners and other interested parties to verify."[67]

Internet & Jurisdiction Policy Network

ICANN org participates in relevant areas of work within the Internet & Jurisdiction Policy Network, in particular in the Domains & Jurisdiction Program Contact Group.[68] This level of engagement should continue as the Internet & Jurisdiction Policy Network touches on issues in and around the DNS.

IETF DNS-related Activities

ICANN org should continue to support and participate in appropriate IETF activities in support of the DNS. Working groups of particular interest include:

- Adaptive DNS Discovery (add) [69]
- Extensions for Scalable DNS Service Discovery (dnssd)[70]

---

[66] FIRST - Improving Security Together, website, https://www.first.org/.

[67] DNS Transparency website, https://dnstransparency.org.

[68] Internet & Jurisdiction Policy Network, Domains & Jurisdiction Program Contact Group, website, https://www.internetjurisdiction.net/news/domains-jurisdiction-program-contact-group-members.

[69] Adaptive DNS Discovery working group website, IETF, https://datatracker.ietf.org/wg/add/.

[70] Extensions for Scalable DNS Service Discovery working group website, IETF, https://datatracker.ietf.org/wg/dnssd/.

- DNS PRIVate Exchange (dprive)[71]
- Domain Name System Operations (dnsop)[72]
- Registration Protocols Extensions (regext)[73]

Other groups may form over time and as new issues and areas of interest arise.

M^{3}AAWG

ICANN org is a supporting member of the Messaging Malware Mobile Anti-Abuse Working Group (M^{3}AAWG). ICANN org should continue this support as M^{3}AAWG focuses on the mitigations for abuse of the Internet. The Names and Numbers Committee within the M3AAWG may be of particular interest.

APWG

The Anti-Phishing Working Group (APWG) provides a unique perspective into the work to combat phishing, a type of attack that leverages DNS in different ways, including through typosquatting, DNS hijacking, and so on.[74]

TLD-OPS

TLD-OPS is a contacts repository of 400 operational and security contacts from over 200 ccTLDs via a mailing list. This group is administered by the ccNSO secretariat and the TLD-OPS standing committee and develops best practices and conducts workshops at ICANN meetings (for example, on DR/BCP and DDoS mitigation).[75]

Regional Organizations

Regional organizations, including both RIRs and TLD organizations, often include DNS and security subgroups and may be potential partners for cooperation and knowledge exchange. For example:

---

[71] DNS PRIVate Exchange working group website, IETF, https://datatracker.ietf.org/wg/dprive/.

[72] Domain Name System Operations working group website, IETF, https://datatracker.ietf.org/wg/dnsop/.

[73] Registration Protocols Extensions group website. IETF. https://datatracker.ietf.org/wg/regext/.

[74] Anti-Phishing Working Group, website, https://apwg.org/.

[75] Country Code Names Supporting Organisation, "TLD-OPS: ccTLD Security and Stability Together," website, https://ccnso.icann.org/en/resources/tld-ops-secure-communication.htm.

- RIPE's DNS Working Group[76]
- Council of European National Top-Level Domain Registries (CENTR) Security Working Group[77]
- Various Network Operator Groups (NOGs)

Research Venues

There are several research venues in the field of security in general and in DNS security specifically where a significant amount of security research is peer-reviewed, presented, and published. The top venues in this area include:

- USENIX Security Symposium[78]
- ACM Conference on Computer and Communications Security (CCS)[79]
- ACM ASIA Conference on Computer and Communications Security (ASIACCS)[80]
- IEEE Symposium on Security and Privacy[81]
- IEEE European Symposium on Security and Privacy[82]
- Internet Measurement Conference (IMC)[83]
- Internet Research Task Force (IRTF)[84]
- APWG Symposium on Electronic Crime Research[85]

Recommendations

Having set the landscape for where the DNS is either directly at risk or used to attack other systems on the Internet, the DSFI-TSG offers a set of recommendations where ICANN org may be able to improve the security and stability of the DNS. These recommendations are organized according to the type of role and action ICANN org may take, from operational improvements to research, funding, and education and awareness.

---

[76] DNS Working Group, RIPE, https://www.ripe.net/participate/ripe/wg/active-wg/dns.

[77] Security Working Group, CENTR, https://www.centr.org/about/working-groups.html.

[78] Usenix Security Symposium, website, https://www.usenix.org/conference/usenixsecurity21.

[79] ACM Conference on Computer and Communications Security (CCS), website, https://www.sigsac.org/ccs/CCS2021/index.html#about.

[80] ACM ASIA Conference on Computer and Communications Security (ASIACCS), website, https://asiaccs2022.conferenceservice.jp.

[81] IEEE Symposium on Security and Privacy, website, https://www.ieee-security.org/TC/SP2021/cfpapers.html.

[82] IEEE European Symposium on Security and Privacy, website, http://www.ieee-security.org/TC/EuroSP2021/.

[83] Internet Measurement Conference (IMC), website, https://www.sigcomm.org/events/imc-conference.

[84] Internet Research Task Force (IRTF), website, https://irtf.org.

[85] APWG Symposium on Electronic Crime Research, website. https://apwg.org/ecrime2021/.

While all recommendations are considered important and immediately relevant, the DSFI-TSG agreed that if a priority were to be assigned, two recommendations would be the highest priorities to consider: Recommendation R3: Investigate Appropriate Best Practice for Authentication and Recommendation E5: Incident Response.

Operational Improvement

Recommendation O1: Develop a Tabletop Exercise Program

> *ICANN org, together with the SSAC, GNSO, ccNSO, and other entities with relevant expertise as the 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.*

Research

Recommendation R1: Continue Existing Work on DNS Abuse

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

DNS abuse takes many forms. Being able to clearly define what serves as abuse is an important step in determining how to mitigate that abuse.

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 at 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.

The DSFI-TSG recognizes that there are many sources for "best practice" around authentication when it comes to the actors that play a role in the DNS ecosystem, such as registries, registrars, resellers, DNS providers, and registrants.

Contracts

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.

Funding

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 its reports information on the feasibility of

bug bounty programs and what mechanisms are 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.

A bug bounty program may result in DNS protocol or implementation vulnerabilities being discovered and disclosed responsibly. Part of this program may include an interoperability testbed to enable cross-platform verification testing of newly discovered or reported vulnerabilities. In all cases, a bug bounty program would need continual attention and strong cross-functional collaboration.

Education and Awareness

Recommendation E1: Education around Authentication

ICANN org should build 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. ICANN org should also support these programs through communication tactics.

At the time of publication, the DSFI-TSG believes that a training program such as this should include discussion and encouragement of multi-factor authentication and less reliance on solely password-based authentication.

The ICANN community and industry experts could help in drafting such best practices based on their expertise. ICANN org could play a central role in the process of promoting and modeling their use in ICANN infrastructure, policies, and contracts.

The DSFI-TSG recognizes that this recommendation overlaps recommendations offered in SAC074 and offers a strong opportunity for ICANN org to partner with other organizations to extend the education and awareness efforts.[86]

[86] SAC074, https://www.icann.org/en/system/files/files/sac-074-en.pdf.

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.*

ICANN org could do this by working with the technical community and/or by providing funds for research that explores the benefit of such a process as well as facilitating discussions around it. This may build on existing work, such as the Council of European National Top-Level Domain Registries' white paper, "Models of registry lock for top-level domain registries."[87]

Recommendation E3: Awareness of Best Practices for Infrastructure Security

> *ICANN org should continue to participate in initiatives such as MANRS and KINDNS to measure and report on their adoption, and use those reports to create targeted educational material to improve awareness about infrastructure security. ICANN org should take the best practices coming out of those initiatives and ensure 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 understand the risks and benefits of DNS blocking and filtering for security and stability reasons throughout the global DNS infrastructure community.*

---

[87] Council of European National Top-Level Domain Registries, "Models of registry lock for top-level domain registries," 19 August 2020, https://centr.org/library/library/other/models-of-registry-lock-for-top-level-domain-registries.html.

Understandings should include best practices, tooling for understanding DNS interdependencies to avoid large-scale collateral damage, use of the Public Suffix List (PSL)[88], allow lists and similar lists to avoid overblocking, and general hygiene for these types of activities.

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.*

This effort could be based on incident-response best practices from other industries and could be based in part on prior work and recommendations from SSAC's SAC115 and the Security, Stability, and Resiliency Review Team's (SSR2) recommendation 6, "SSR Vulnerability Disclosure and Transparency."[89]

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.*

This may become increasingly important with the wider adoption of DNS encryption protocols and services.

Acknowledgments

This report benefited from the independent review of several technical experts. The DSFI-TSG thanks them for their time and thoughts.

---

[88] Mozilla, "Public Suffix List," website, https://publicsuffix.org/.

[89] ICANN Security and Stability Advisory Committee, "SAC115 - SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS," ICANN SSAC, 19 March 2021, https://www.icann.org/en/system/files/files/sac-115-en.pdf, and "Second Security, Stability, and Resiliency (SSR2) Review Team Final Report," ICANN, p 27, 25 January 2021, https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf.

Conclusion

ICANN org is in the position to support improvements to the DNS at many levels, but it cannot do this alone. ICANN org must always act in a collaborative manner with the other entities in that ecosystem. The DSFI-TSG members look forward to working with ICANN org and the relevant stakeholders to implement these recommendations.

Appendix 1. Acronym List

ACME - Automatic Certificate Management Environment
APWG - Anti-Phishing Working Group
AS - Autonomous System
BEC - Business Email Compromise
BGP - Border Gateway Protocol
ccTLD - Country Code Top-Level Domain
CDNSKEY - Child DNS Key
CDN - Content Delivery Network
CDS - Child Delegation Signer
CRL - Certificate Revocation List
CSYNC - Child-to-Parent Synchronization
DANE - DNS-based Authentication of Named Entities
DoS - Denial of Service
DDoS - Distributed Denial of Service
DITL - Day In The Life of the Internet
DNS - Domain Name System
DNS-OARC - DNS Operations, Analysis, and Research Center
DNSSEC - Domain Name System Security Extensions
DoH - DNS-over-HTTPS
DoQ - DNS-over-QUIC
DoS - Denial of Service
DoT - DNS-over-TLS
DS - Delegation Signer
DSFI-TSG - DNS Security Facilitation Initiative - Technical Study Group
EPP - Extensible Provisioning Protocol
FIRST - Forum of Incident Response and Security Teams
GNSO - Generic Names Supporting Organization
gTLDs - Generic Top-Level Domain
HMAC - Hash-based Message Authentication Code
HOTP - HMAC One-time Password
HTML - Hypertext Markup Language
HTTPS - Hypertext Transfer Protocol Secure
ICANN - Internet Corporation for Assigned Names and Numbers

IDN - Internationalized Domain Name
IoT - Internet of Things
KINDNS - Knowledge-sharing and Instantiating Norms for DNS and Naming Security
M^3AAWG - Messaging Malware Mobile Anti-Abuse Working Group
MANRS - Mutually Agreed Norms for Routing Security
MFA - Multi-factor Authentication
OCSP - Online Certificate Status Protocol
OTP - One-time Password
PDNS - Passive Domain Name System
PSL - Public Suffix List
RIR - Regional Internet Registry
ROA - Route Origin Authorization
RPKI - Resource Public Key Infrastructure
SMS - Short Message Service
SSAC - Security and Stability Advisory Committee
TLDs - Top-Level Domains
TLS - Transport Level Security protocol
TOTP - Time-based One-time Password
TTL - Time-To-Live

Appendix 2. Team Composition

The DNS Facilitation Function Steering Committee is made up of ICANN executives and members of the ICANN Board. The committee will advise on strategic direction, oversee the development of a clear charter, and provide guidance on appropriate protocol and approval to facilitate project progress.

Role	Name
Coordinator / DSFI-TSG Lead	Merike Käo
Steering Committee	Board: Harald Alvestrand Danko Jevtovic Merike Käo ICANN org: Göran Marby, President and CEO David Conrad, SVP & Chief Technology Officer Ashwin Rangan, SVP, Engineering & Chief Information Officer
Team Members	Tim April Gavin Brown John Crain Rod Rasmussen Marc Rogers Katrina Sataki Robert Schischka Duane Wessels
ICANN Org Support Team	Sally Newell Cohen (communications) Steven Kim (project management) Heather Flanagan (technical writer) Wendy Profit (project management support) Samaneh Tajalizadehkhoob (technical support)

Appendix 3. Facsimile Domains

Impersonation of Infrastructure

- Web browsers, mail user agents, and other applications have found it necessary to display more clearly "the domain" in the domain name / hostname part of an identifier. For example, some browsers display the second-level part of a domain name with slightly more emphasis in the URL bar:

- To combat IDN homograph attacks, the application might display the domain name as a so-called ASCII "A-label"[90] [91]:

  Rather than its Unicode "U-label":

- Many popular web browsers include some form of safe browsing or protection from unsafe sites. This heuristic pattern is essentially a crowd-sourced database of possibly unsafe addresses that the browser downloads and/or queries as needed. Users are warned about, or entirely prevented from, visiting addresses determined to be unsafe.
- With respect to typosquatting, domain and trademark holders often have recourse through ICANN's Uniform Domain-Name Dispute-Resolution Policy (UDRP) process, the Anticybersquatting Consumer Protection Act (ACPA) in the U.S., or the World Intellectual Property Organization (WIPO). A successful complaint via one of these contexts should result in the malicious domain becoming transferred to the trademark holder, which can then easily redirect mistyped addresses to the correct site.
- Applications that have auto-completion features can also protect users from these attack vectors. Once the desired address is seen in the auto-complete list, it means the user isn't required to type the remaining characters, which could be mistyped.
- Potential victims might be able to take advantage of brand protection services, but these can be quite expensive.

---

[90] "ICANN61 – Tech Day IDN Abuse," presented by Merike Käo, research by Mike Schiffman and Stephen Watt, 17 October 2017, https://ccnso.icann.org/sites/default/files/field-attached/presentation-tech-day-idn-abuse-12mar18-en.pdf

[91] Documents produced by the Internationalized Domain Name (idn) working group (closed) for the IETF, https://datatracker.ietf.org/wg/idn/documents/.

Appendix 4. Mitigations for Various Attack Vectors

As part of their review of the landscape, the DSFI-TSG discussed existing mitigations that could have prevented or lessened the severity of several incidents that reflected multiple attack vectors. The group identified several commonalities among the different mitigations for the attack vectors; those commonalities, along with considerations of ICANN org's role in the DNS, informed the recommendations of the DSFI-TSG.

Mitigations for Credential Compromise

Known Mitigation Techniques

Managing credentials is an area covered in a wealth of publicly available material.[92] Best practices include (but are not limited to) the use of complex passwords, one-time-use credentials, multi-factor authentication, and the use of password managers. Adopting these best practices is one of the most immediate and impactful ways to address attacks on the credential system. Additional known mitigations include:

- Using services such as 'Have I Been Pwned' to limit the reuse of compromised passwords, which are often used in password spraying or stuffing attacks.[93]
- Ongoing education on risk awareness, common attacks (e.g., phishing), and mitigation techniques for all entities with credentials in the existing systems
- Ensuring segregation of duties and services are deployed as standard practices to ensure that local credentials do not allow access to other critical systems.
- Deploying mechanisms and practices for detection of credential compromises, such as scanning password dumps or monitoring for anomalies in user behavior.
- Proactively monitoring the WHOIS records of your portfolio to detect unauthorized changes quickly.
- Ensuring that procedures for responding to cases of credential compromise are written, reviewed, and tested regularly.

---

[92] For example, ICANN Security and Stability Advisory Committee, "SAC044 - A Registrant's Guide to Protecting Domain Name Registration Accounts" 25 February 2012, https://www.icann.org/resources/pages/sac-044-2012-02-25-en, "Creating and Managing Strong Passwords," Cybersecurity & Infrastructure Security Agency, U.S. government, 27 March 2018, https://us-cert.cisa.gov/ncas/current-activity/2018/03/27/Creating-and-Managing-Strong-Passwords, and the National Institute of Standards and Technology, "Cybersecurity Framework," https://www.nist.gov/cyberframework.

[93] haveibeenpwned.com website, https://haveibeenpwned.com/API/v3#PwnedPasswords.

- Making available (for retailers and registries) or using (for registrants, where available) Registry Lock on high-value domains.[94]
- Supporting out-of-band verification of authentication attempts by requiring another process or a human to confirm the authentication request.
    - Using "risk-based authentication" techniques to identify unusual or suspect account logins.[95]
    - Notifying customers of all attempts to access their account, to reduce the time between compromise and detection.
    - Requiring additional steps for transfer of domains that have a high impact on users and/or infrastructure and monitor unusual ops behavior, enforce existing security protocols.
    - Limiting access to operationally sensitive accounts and require contextual access to resist phishing and other common credential attacks.
- (Registry) Implementing support for CDS/CDNSKEY and CSYNC records in child zones, either by proactively scanning for them or accepting/rejecting EPP <update> commands if the requested change would cause the domain's configuration to be different from the configuration indicated by the CDS/CDNSKEY/CSYNC records published by the DNS operator.
- (Registrar) Implementing support for CDS/CDNSKEY[96] and CSYNC[97] records, either by proactively scanning for them or accepting/rejecting requests to update domains if the requested change would cause the domain's configuration to be different from the configuration indicated by the CDS/CDNSKEY/CSYNC records published by the (third-party) DNS operator.

Operational Gaps in Mitigations

There are many well-documented practices for protecting credentials.[98] However, no network is "100% secure," and no credential is either. Implementation of credential

---

[94] Krebs, Brian, "Does Your Domain Have a Registry Lock?," Krebs on Security, 24 January 2020, https://krebsonsecurity.com/2020/01/does-your-domain-have-a-registry-lock/

[95] "Risk-Based Authentication: What You Need to Consider," Okta, n.d., https://www.okta.com/identity-101/risk-based-authentication/.

[96] Gudmundsson, O. and P. Wouters, "Managing DS Records from the Parent via CDS/CDNSKEY", RFC 8078, DOI 10.17487/RFC8078, March 2017, <https://www.rfc-editor.org/info/rfc8078>.

[97] Hardaker, W., "Child-to-Parent Synchronization in DNS", RFC 7477, DOI 10.17487/RFC7477, March 2015, <https://www.rfc-editor.org/info/rfc7477>.

[98] For example, "Authentication Cheat Sheet," OWASP Cheat Sheet Series, n.d., https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

management best practices, as noted above, is not uniform across the industry; limited budgets and other business drivers cause many organizations to de-prioritize hardening their credential management system in favor of other projects. Some registry operations may be resource-constrained and may not have the resources available to deploy security strategies, such as segregation of duties; it is hard to separate duties in an operation with only a few employees who may be unaware or do not understand the appropriate best practices for their environment.

Registries do not always support strong authentication, and resellers are not subject to any contractual obligations regarding ensuring the security of customer accounts. Two-factor authentication may not be widely supported by many retailers or is hard to find and activate. Validation of passwords against APIs such as pwnedpasswords.com is not widely deployed.

A registrar and registry may have strong security mechanisms, but where a reseller acts as an intermediary between registrant and registrar, they can be the weakest link as they do not have the same obligations or control requirements as ICANN org contracted parties.

Because of the nature of the attacks, compromise events are often kept secret out of fear of potential ramifications, liability issues, or impact to an ongoing investigation. There are also inconsistent legal obligations for reporting breaches that exacerbate this tendency to hide these types of breaches.[99] Without a common understanding of these types of attacks, evaluating the breadth of the problems and pooling resources to collectively resolve them becomes impossible.

When attacks happen or compromises occur, organizations are not typically monitoring for changes. This lack of monitoring is partly a result of the challenge in automating the search for suspicious behavior and taking action; the searches and the appropriate associate actions are subjective and not well defined.

[99] See Simpson, Aaron P., Adam H. Solomon, and Hunton Andrews Kurth, "Complying with Breach Notification Obligations in a Global Setting: A Legal Perspective," Lexology, 19 June 2019, https://www.lexology.com/library/detail.aspx?g=5b89803b-61a6-48c2-8871-b44853ad93df, as compared to Krotoski, Mark L., Lucy Wang, and Jennifer S. Rosen, "The Need to Repair the Complex, Cumbersome, Costly Data Breach Notification Maze," Bloomberg BNA, Privacy and Security Law Report, 2016, https://www.morganlewis.com/~/media/files/publication/outside%20publication/article/bna-need-to-repair-data-breach-notification-maze-08feb16.ashx.

Ultimately, the human factor in security will always be an issue, as the activities of just one individual can have a significant impact on a wide range of systems and services, either through administrative controls or phishing attacks.

Mitigation Limitations

While mitigations exist and are publicly documented, there are limits to what is currently possible for all stakeholders in the DNS ecosystem. Those limits are sometimes a result of limited resources available to the stakeholder or issues with the technologies available. For example, technologies exist to prevent changes to domain registrations (e.g., Registry Lock) or make authentication a much more dynamic and secure action (e.g., multi-factor authentication).

Registry Lock is not widely deployed and is inconsistent across different registries. Most registrars still do not offer the Registry Lock service in a way that is easy for registrants to buy for their domains.

Not all registrars, registries, resellers, or other parties in the DNS landscape have intelligent monitoring architectures such as Zero Trust, which can be used to support contextual access controls to resist phishing and other common credential attacks.[100] Organizations that have strong authentication support for some of their systems should implement this technology for all of their services, both customer-facing and internally. Implementing these technologies requires dedicated resources that may not be available or not prioritized within the existing product roadmap.

Service operators may not have the recovery practices in place and documented to handle a compromise, or they may have them but do not exercise their remediation techniques.

[100] For more on Zero Trust, see Rose, Scott W. , Oliver Borchert, Stuart Mitchell, Sean Connelly, "Zero Trust Architecture," Special Publication (NIST SP) - 800-207, National Institute of Standards and Technology, 10 August 2020, https://doi.org/10.6028/NIST.SP.800-207.

Mitigations for Access Controls Issues

Known Mitigation Techniques

There are two specific steps that organizations take to mitigate issues around access controls: domain verification and operational validation. To reduce opportunities for abuse, service providers can use domain verification techniques (e.g., secure ID verification) to verify domain/asset ownership/control. This would include having the appropriate processes in place to define who is allowed to take what and under which circumstances and operational validations to periodically ensure that the process is followed as expected.

Operational Gaps in Mitigations

More generally, there are significant challenges in actually implementing proper access control mechanisms. There is no well-defined method to validate the ownership of an asset. There is also no single method to indicate authorization of control from one entity to another or at least none that has been agreed on. And, ultimately, there are no common, simple methods to support testing to ensure that allowed actions are adequately validated.

Mitigation Limitations

In some cases, organizations have chosen not to implement strong access control mechanisms at all, possibly due to the difficulty in educating their customers on how to use the controls and in managing staff to enforce these controls.

Mitigations for Resource Impersonation Attacks

Known Mitigation Techniques

The following techniques are common across many of the resource impersonation types of attacks:

- Use tunneling technologies such as VPNs and to ensure that all of the traffic, including DNS, is transported across the encrypted tunnel. (Note that this does not scale well in large organizations and that the VPN must conduct mutual authentication.)
- Direct authoritative to recursive network interconnection (peering).

- Where allowed, restrict access to DNS ports only to the known resources. (This configuration change will not always be possible in some countries or ISPs).
- Monitor the resolvers and servers used on the network for any unexpected deviation.
- Do not trust the security of the underlying network, as advocated by the MANRS project.[101]

Additionally, these specific mitigation measures may help:

Recursive Resolvers

- End users should install and frequently update endpoint protection software. If necessary, this should be part of an organization's IT management policies.
- Use DHCP since it provides added monitoring capability from logs to see if someone was trying to overwrite a configuration. Generally speaking, use technologies that can help monitor for configuration changes and overwrite fraudulent changes.
- Fundamental good hygiene practices, such as patching are crucial to ensure vulnerabilities get patched before they can be exploited on home routers and the recursive DNS server functionality in these devices. Home routers should have software updates deployed as soon as updates become available.
- Require the use of your own resolvers when they exist.

Authoritative Servers

- DoH can also theoretically avoid resource impersonation of authoritative servers by encrypting the DNS traffic and using HTTPS to encrypt DNS resolution traffic.
- Current standardization efforts (within the IETF) aim to solve the problem of authenticating authoritative servers.
- DNSSEC-signing zones by zone owners and validating DNSSEC signatures at the recursive or stub resolver can enable detection of answers from an incorrect server, but not machine-in-the-middle spying when correct answers are returned. Captive portals in particular often employ authoritative nameserver impersonation as a technique to direct new users to an authentication page prior to granting access to the public Internet.

Impersonation of Infrastructure

[101] MANRS, https://www.manrs.org/.

- Emphasize the domain name of an identifier presented to the user in any application (e.g., web browsers, mail user agents, etc.).
- Display the domain name as a so-called ASCII "A-label" rather than, or in addition to, a Unicode "U-label" as a way to combat IDN homograph attacks.
- Offer safe browsing protection by referencing a database of unsafe addresses and flagging unsafe websites to the end-user.
- Follow through with ICANN's Uniform Domain-Name Dispute-Resolution Policy (UDRP) process, the Anticybersquatting Consumer Protection Act (ACPA) in the U.S., or the World Intellectual Property Organization (WIPO) to mitigate issues of typosquatting.
- Support auto-completion features in applications to help mitigate mistyping and the risk of going to facsimile domains.
- Consider subscribing to brand protection services for high-value brands.

Fraudulent Certs

- Closely monitor Certificate Transparency, preferably in combination with Certificate Authority Authorization (CAA) resource records and DNSSEC, to identify services using fraudulent certificates.[102] Unfortunately, this monitoring discovers issues only "after the fact" and is not a way to actively prevent this exploit.

Route Manipulation

- Using RPKI/ROA records with Regional Internet Registries (RIRs) for origin validation
- DNSSEC to mitigate the implications of successful hijacking
- HTTPS - using HSTS and DANE and educating users.

Operational Gaps in Mitigations

- The largest gap is possibly in the deployment of available tools that could monitor for unexpected IP address changes, such as when the authoritative server changes IP address frequently or without notice. This may be an indicator of both awareness and usability issues.
- Network operators with responsibility for the security of their users (businesses, home networks, constrained networks) do not implement egress filters, monitoring, or otherwise blocking disallowed recursive or authoritative DNS servers which may be contacted by endpoints in their environments. Operators are not always

[102] See CA compromise, Wikipedia contributors, "Certificate authority," *Wikipedia, The Free Encyclopedia*, https://en.wikipedia.org/w/index.php?title=Certificate_authority&oldid=1035134967 (accessed July 30, 2021) and the Certificate Transparency website, https://certificate.transparency.dev/.

transparent about what restrictions, monitoring, or blocking they implement on their networks and how it may impact their users.

- Configuration or redirection of resolvers for mobile and embedded devices is not consistent or exposed clearly to the device users and or operators.
- Many registries do not support the use of CDSKEY/CDNSKEY and CSYNC, reducing the ability to manage DNSSEC keys without having to interact with the registrar, which is a significant challenge to timely operational updates of DNSSEC key material.
- Not all applications display URLs, hostnames, and/or email addresses in a way that makes it clear where the end-user is going, introducing possible impersonation attacks.
- Domain registrants do not have good tools to both identify and take down impersonating sites and/or domains.
- Some of the issues would be mitigated if individuals and organizations upgraded their software in a timely manner; the accepted mitigations may not be deployed in older versions of applications. (Note: timely upgrades are not always possible in situations where certification of platforms is required.)
- DNSSEC deployment is still low, despite potential security benefits.[103]
- Many businesses do not monitor certificate transparency. Especially fraudulent certificates for mail servers might be hard to detect if you are not monitoring them closely.
- RPKI is available and also used by some major ISPs but is far from being universally adopted. There have been continuous improvements on the RPKI issues discussed within the community, and deployment seems to be getting better recently.[104]
- Monitoring and filtering result in enough false-positive or minor errors that any significant issues may be lost in the 'noise.'

[103] Melony, S., "What Are the Benefits of Implementing DNSSEC?," Education News, 20 April 2020, https://www.educationviews.org/what-are-the-benefits-of-implementing-dnssec/.

[104] See "RPKI Deployment Considerations: Problem Analysis and Alternative Solutions," IETF 95 SIDR meeting, 4 April 2016, https://www.ietf.org/proceedings/95/slides/slides-95-sidr-7.pdf, and Liu, Xiaowei, Zhiwei Yan, Guanggang Geng, Xiaodong Lee, Shian-Shyong Tseng, and Ching-Heng Ku. "RPKI Deployment: Risks and Alternative Solutions." In Genetic and Evolutionary Computing, edited by Thi Thi Zin, Jerry Chun-Wei Lin, Jeng-Shyang Pan, Pyke Tin, and Mitsuhiro Yokota, 387:299–310. Cham: Springer International Publishing, 2016. https://doi.org/10.1007/978-3-319-23204-1_30.

Mitigation Limitations

- Offering best practices in this space is becoming more and more difficult as some countries, ISPs, and applications do not allow end-users to configure everything.
- Protocols like DoH and DoT only cover part of the resolution path between the stub and the recursor. The IETF does have ongoing work on implementing encrypted transport for DNS traffic to authoritative nameservers (dprive working group), but it is unclear how this work progresses.
- There is a lack of tools and/or complete documentation to easily deploy, modify/update keys for DNSSEC, as well as tools to help manage if something breaks (e.g., algorithm changes, etc.)
- Tools to monitor a zone's DNSSEC status and provide clear advice to end-users on how to resolve DNSSEC validation issues that are being experienced.[105]
- It is likely that educating end-users about these attacks and risks will be necessary for the foreseeable future because it is unlikely that similar-looking domain names could somehow be broadly forbidden.
- Certificate validity has no link to the domain name owner. If a domain name changes ownership, expires, or is transferred, pre-existing certificates are still trusted after the change takes place. Revocation is a possibility for CAs that support revocation but is not validated in many cases.
- RPKI is still partly not deployed - there is still some hesitation around making routing decisions dependent on certificates.
- RPKI only asserts which origin AS is allowed to advertise which prefixes; there is no deployed system to assert that a route path is valid or correct. RPKI also has no mechanism to ensure that a router is authorized to be a BGP speaker for a given AS.

Mitigations for Code and Protocol Vulnerabilities

Known Mitigation Techniques

Possibly the most powerful method to mitigate code and protocol vulnerabilities is to keep all software patched and up to date.

- Widespread DNSSEC signing and validation of zones is the only way to eliminate cache-poisoning attacks: while other partial mitigations exist, they only increase the effort required to carry out attacks and are ultimately only a temporary fix, since history has shown that new attacks will emerge which bypass them (e.g., SAD DNS).

[105] Tools like https://dnsviz.net/ do exist, but it often takes a technical expert to understand what modifications are needed (and where to make those changes) in order to fix the domain resolution errors.

- Deployment of DNSSEC signing and validation is the best technique for preventing cache poisoning. To be effective, it must be deployed both by zone publishers (signing) and by recursive operators (validation).
- Absent DNSSEC, the next best defense is for recursive resolvers to always match responses correctly to queries and reject out-of-bailiwick data. Matching is made more effective by maximizing the amount of entropy (randomness) present in DNS queries and responses. This additional entropy is generally accomplished by requiring recursive software to use randomized source ports and randomized query IDs. Additional techniques exist, such as DNS Cookies (RFC 7873 and RFC 9018) and mixed-casing of query names (aka DNS 0x20).[106]
- Use of encrypted DNS transport protocols (DoT, DoH, DoQ) between stubs and resolvers mitigates many on-path attacks since query parameters are not visible in the clear.
- Use of encrypted DNS transport protocols (DoT, DoQ) between resolver and authority servers may mitigate many on-path attacks as described above. In addition, DoQ can mitigate reflection and amplification attacks since QUIC is designed to make connection initiation more expensive in terms of bandwidth for the client than for the server.[107]
- Prevent being hampered by code and protocol vulnerabilities through rigorous Security Development Lifecycle (SDL) processes that operate on a secure-by-design principle.
- Build defense-in-depth into infrastructure; consider modern approaches such as Zero Trust.
- Perform detailed monitoring for anomalous activity both on network and host using tools such as IDS, Checksums, and Honeypots.

Operational Gaps in Mitigations

- Adoption of new protocols or new versions of existing protocols is always slow and rarely universal. For example, DNSSEC signing and validation is still not widely deployed after many years.

---

[106] Eastlake 3rd, D. and M. Andrews, "Domain Name System (DNS) Cookies", RFC 7873, DOI 10.17487/RFC7873, May 2016, <https://www.rfc-editor.org/info/rfc7873> and Sury, O., Toorop, W., Eastlake 3rd, D., and M. Andrews, "Interoperable Domain Name System (DNS) Server Cookies", RFC 9018, DOI 10.17487/RFC9018, April 2021, <https://www.rfc-editor.org/info/rfc9018>.

[107] Dhillon, Sargun, “On DDoS & QUIC,” blog, 5 February 2015, https://medium.com/@sargun/on-ddos-243983f7fee6 - “the client hello will always be larger than, or equal to the size of the server response... this immediately rules out naive reflection attacks”

- There is no central place where coordination of vulnerability disclosure can happen.
- Vulnerabilities are not always immediately discovered; some vulnerabilities may take years to be found and patched.[108]
- Although DNSSEC has been available for more than a decade, adoption by domain registrants (i.e., second-level domains) remains quite low in many registries.
- DNSSEC validation is moderately deployed, thanks in part to large third-party recursive services (Google, Cloudflare, Quad9). Still, end users are only protected when the domains that they access are signed and the resolvers that they use are validating.

Mitigation Limitations

- DNSSEC signing and validation still are not widely deployed, especially validation on stub resolvers.
- Do{T,Q} between resolver and authority is not yet standardized.
- Post-exploitation detection is crude and evolving. Most advanced techniques, such as Zero Trust, are not deployed.
- Perverse incentives exist to build DNS software in embedded systems cheaply.
- Many users of potentially vulnerable software are "removed" from the software by hardware or software abstraction and are unable to update or even check for vulnerabilities. This is particularly prevalent in the Internet of Things (IoT).
- Popular recursive software products have implemented necessary cache poisoning defenses through years of development work and experience. Occasionally, developers of applications that send and receive DNS queries make the decision to "roll their own" rather than use well-established libraries or services. Such custom implementations are likely to lack all the necessary checks that make them resistant to cache poisoning attacks.
- There still seems to be some lack of awareness of the value of validating DNS queries. Also, there are "costs" involved in deploying DNSSEC (especially signing). The combination of those two can have an adverse impact on any cost-benefit analysis when deciding whether or not to deploy DNSSEC.

[108] SIGRed (see Munos, Jesse, "SIGRed: What Is It, How Serious Is It, and How Should You Respond?" CSO, 3 September 2020, https://www.csoonline.com/article/3574021/sigred-what-is-it-how-serious-is-it-and-how-should-you-respond.html) took 17 years to come to light.

Mitigations for Infrastructure Choices

Known Mitigations

- TTLs should be set based on the type of infrastructure and service being employed. Very short TTLs could result in overloading the authoritative or root servers, whereas very long TTLs increase the chance of cache poisoning types of attacks.
- In the DNS protocol, the TTL is a 32-bit signed integer value expressed in seconds, which in theory means that TTLs could be as long as 68 years. However, popular recursive nameserver implementations place upper limits on TTL values (BIND: 1 week, Unbound: 1 day, Knot Resolver: 6 days). Still, these are quite long time periods when changes are urgently needed. Resolver administrators can set their own caching limits as a matter of local policy while respecting the authoritative DNS servers' policy.
- Recursive nameserver software generally allows an administrator to configure a lower limit on TTL caching. For BIND and Unbound, the default is zero. For Knot Resolver the default is 5 seconds.
- To mitigate against another site's choice of short TTL, services such as the OpenDNS service (now part of Cisco) will cache and utilize DNS data beyond its stated TTL when authoritative servers are unavailable. However, the IETF published RFC 8767, "Serving Stale Data to Improve DNS Resiliency," which includes information regarding why caching DNS data past the record's TTL is a bad idea when using DNSSEC."[109]
- Popular open resolver services (e.g., Google, Cloudflare, and others) provide an interface to flush specific records from their caches.
- Security should be provided by additional layers on top of the original system via techniques such as hard cryptographic keys or soft techniques such as awareness, creating aligned incentives for actors who are in charge of the security and not in the obscurity of the design itself.
- Best practices suggest diversification of DNS operating systems, software, and resources such as IP addresses; in case one goes down, there are more left to operate.[110]

---

[109] Lawrence, D., Kumari, W., and P. Sood, "Serving Stale Data to Improve DNS Resiliency", RFC 8767, DOI 10.17487/RFC8767, March 2020, <https://www.rfc-editor.org/info/rfc8767>.

[110] "Best practices for improving external DNS resiliency," Cira, n.d., https://www.cira.ca/resources/anycast/guide-how/best-practices-improving-external-dns-resiliency.

- DNS servers should not be behind single points of failure (i.e., don't have all servers in one data center or one geographic region and have all servers physically connected to the Internet via different physical and logical paths).
- DNS authoritative servers should be on separate devices from DNS recursive servers.

Mitigation Limitations

- When high-profile hijacks occur, there is often discussion of the need for an industry-standard protocol or mechanism for widespread flushing of resolver caches. To date, such discussions have not been fruitful.
- Lack of knowledge about best practices such as MANRS and KINDNS.
- Lack of resources (technical and/or financial) or incentives to implement best practices.

Mitigations for DNS as the Attack Vector

Known Mitigation Techniques

- DNS Blocking/Redirecting via DNS resolvers: Also known as a DNS firewall, a DNS resolver can be configured to return predetermined responses for known DNS tunneling domains to either provide an NX Domain (does not exist) or false information to the querying device. A DNS firewall must provide entries of known malicious names along with the actions to take (block/redirect), and this can be done via Response Policy Zones or the equivalent technology, using automation with access to appropriate threat intelligence data to keep protection up-to-date.
- DNS Blocking/Redirecting via perimeter firewalls: Perimeter firewalls may be configured to examine DNS traffic traversing network ingress/egress points and triggering rules when potentially malicious hostnames are detected. This detailed examination for malicious hostnames is usually a high-overhead operation when compared to the DNS firewall technique but can catch DNS traffic destined for off-network resolvers, and with deep packet inspection, encrypted or otherwise encapsulated DNS queries.
- Allow-list only DNS resolution: DNS resolvers may be configured to only return responses for an approved list of domain names, hosts, or from trusted authoritative nameservers. A variant of a DNS firewall, this technique is of limited utility for controlled networks that don't require most public Internet information.

- Strict control over DNS resolver selection (e.g., block access to public DNS resolvers): In order to implement any DNS resolution interruption solution, a network operator must ensure that all devices utilize only designated DNS resolvers. This can be accomplished largely through endpoint controls (e.g., desktop configuration management) but may fail in cases where a device has been compromised. Redirection of port 53 traffic to designated resolver or forwarder will mitigate most rogue DNS queries; DoH queries, however, require sophisticated packet analysis and/or HTTPS proxy configurations for edge firewalls to be effective.
- In-line monitoring for unusual DNS query patterns: While threat intelligence data from third parties provide protection against known adversary domains, it is important to monitor for new and/or targeted attacks via analysis of DNS queries at the DNS resolvers in use for a protected network. For example, one can look for unusual patterns like large TXT record exchanges, large numbers of subdomain lookups under the same domain, and unusual DNS record requests/responses. Various statistical and machine-learning techniques can be employed to detect anomalous traffic and flag for investigation and/or remediation.
- Passive DNS (PDNS) monitoring and analysis: PDNS allows for lightweight monitoring of DNS traffic at a resolver, where queries and responses are put into a database without needing to analyze queries or responses on the DNS resolver itself. Alerting and mitigation can be automated in a similar fashion to in-line monitoring with the proper controls configured.

Operational Gaps in Mitigations

- DoH encrypts traffic, typically on a client machine or application, and prevents standard monitoring on-network or via PDNS. This gap can be mitigated by blocking known external DoH recursive DNS services, forcing DoH queries to utilize resolvers controlled by the network operator, or limiting the use of DoH-based applications. Such measures can still be circumvented and may require all HTTPS traffic to be inspected at the perimeter using HTTPS proxy servers and shunting DNS traffic off appropriately.
- Lack of blocking/filtering capability in most DNS recursive infrastructure: Blocking, filtering, and redirecting DNS traffic, while now a capability for most major DNS server distributions, adds overhead, complexity, and potential failure modes to network operations. The technology is in the early stages of adoption.
- Lack of visibility into DNS query/responses in infrastructure: As a “must-have'' foundational network service, DNS has been largely overlooked as an attack vector

for surreptitious communications. Instrumenting recursive servers for such attacks is only recently being undertaken, and PDNS monitoring, while fairly straightforward to implement, provides a large amount of data to inspect. DNS traffic can be configured at the client to travel off-network to an external resolver unless it is redirected using an edge device like a firewall.

- Accurate intelligence on current covert DNS channel domain names: New tools and malware families are being deployed continuously to utilize covert DNS channels. Much like keeping track of new malware families and their attributes, it takes a lot of effort to keep lists of domain names for these channels up-to-date. Typically, the best data sources are either provided via threat-intelligence services or packaged with DNS resolution services and/or hardware.

Mitigation Limitations

- In most environments, particularly in non-corporate environments: Market penetration for DNS firewalls and other DNS monitoring/enforcement solutions has been largely in the corporate and government sectors that employ other traditional perimeter solutions.
- Many open public resolvers have “DNS neutral” policies, which can leave clients susceptible to attacks that make use of the DNS.
- In endpoints: Nearly all DNS resolution is done via a full-fledged resolver and not via the stub resolvers deployed at endpoints. Thus endpoints can be attacked via compromised resolvers or ones that do not provide protection from covert channels. Some endpoint protection software and services exist, often within a particular application, but are not well advanced in capabilities from these attacks.

Mitigations for Denial of Service

Mitigation techniques exist for different aspects of the DNS ecosystem. In the DNS infrastructure, administrators should locate servers in different data centers in different networks and use a distributed anycast network for DNS servers. In a content delivery environment, administrators should partition critical online services (e.g., email, website) to make sure that an attack on one service (e.g., website) does not impact other services.

Known Mitigation Techniques

For organization infrastructure, known mitigations include:

- Firewall optimized for flow inspection, deep inspection
- Router optimized for packet inspection, frame inspection
- DNS Cookies
- Response Rate Limiting

For recursive resolvers, known mitigations expand to include:

- Run a recursive server on a dedicated server.
- Use access control mechanisms to limit the use of the resolver by third parties.
- Configure the recursive server to use DNSSEC validation.
- Monitor the service, examine logs periodically.
- Update software regularly.

Operational Gaps in Mitigations

While various mitigation techniques exist to handle DoS scenarios, there are known gaps in existing techniques:

- Mitigation techniques usually cover actions at the target infrastructure (i.e., they address the result of the attack, not the cause).
- Techniques can be (but are often not) implemented only by the owners of respective infrastructure due to misaligned incentives, different risk policies, etc. (e.g., ISPs that do not implement recommended anti-spoofing measures).
- Organizations must be mindful of the need to keep systems providing DNS services up-to-date. Usually, this means regularly and quickly updating software provided by product vendors. Organizations that are not able to keep systems up-to-date should consider outsourcing DNS services when possible.

Mitigation Limitations

- Unmanaged open resolvers remain an issue.