SAC125

SSAC Report on Registrar Nameserver Management

A Report from the ICANN Security and Stability Advisory Committee (SSAC)
09 May 2024

Preface

This is a report to the ICANN Board, the ICANN organization staff, the ICANN community, and, more broadly, the Internet community from the ICANN Security and Stability Advisory Committee (SSAC) about mitigating a domain resolution hijacking risk that results from creating unsafe sacrificial nameservers.

The SSAC focuses on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., pertaining to the correct and reliable operation of the root zone publication system), technical administration matters (e.g., pertaining to address allocation and Internet number assignment), and registration matters (e.g., pertaining to registry and registrar services). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no authority to regulate, enforce, or adjudicate. Those functions belong to other parties, and the advice offered here should be evaluated on its merits. SSAC members participate as individuals, not as representatives of their employers or other organizations. SSAC consensus on a document occurs when the listed authors agree on the content and recommendations with no final objections from the remainder of the SSAC, with the exception of any withdrawals included at the end of the document.

Table of Contents

List of Figures

List of Tables

Executive Summary

During domain registration, a minimum of two nameservers are typically required, and this remains a requirement for any future updates to the domain. Often, domains are delegated to nameservers that are subordinate to some other domains, creating inter-domain dependencies. This network of dependencies creates a scenario where the functionality of a domain depends on the operational status of another domain. This setup lacks contractual or procedural safeguards against disruption or misuse, especially when the nameserver parent domain expires.

Most registries forbid deleting an expired domain if other domains depend on it for name resolution. These constraints aim to prevent disruptions in DNS resolution for the dependent domains. However, this also means that the expired domain remains in a liminal state, neither fully operational nor completely removed. When registrars cannot delete expired domains with dependents, they are forced to bear the burden of sponsoring the domain without remuneration from the registrant. A peer-reviewed study, "Risky BIZness: Risks derived from Registrar Name Management," observed that some registrars have found and utilized a loophole to these constraints by renaming the host objects that are subordinate to the expiring domain.[1] Once renamed, the host objects are what Akiwate et al.—and subsequently the SSAC—refers to as *sacrificial nameservers*.

This report focuses on a specific type of sacrificial nameserver where the parent domains of the renamed host objects are considered to be *unsafe* because they are registrable. Registrable parent domains of sacrificial nameservers introduce a new attack surface for domain resolution hijacking, as malicious actors can exploit unsafe sacrificial nameservers to gain unauthorized control over the dependent domains, leading to manipulation or disruption. Unlike traditional domain hijacking techniques that exploit compromised account credentials or manipulate the resolution protocol, this report focuses on this unforeseen risk arising from a longstanding practice employed by some registrars.

As of September 2020, the practice of creating unsafe sacrificial nameservers had inadvertently exposed over 500,000 domains within generic top-level domains (gTLDs) to resolution hijacking risk.This resulted in the resolution of over 163,000 domains falling under unauthorized control.[2] This analysis leveraged zone files from the Centralized Zone Data Service (CZDS), which does not include zone files for country code top-level domains (ccTLDs). Consequently, the extent of this practice and its potential consequences within ccTLDs remain unknown.

[1] See Akiwate, Gautam, Stefan Savage, Geoffrey M. Voelker, and K C Claffy. "Risky BIZness: Risks Derived from Registrar Name Management." In Proceedings of the 21st ACM Internet Measurement Conference, 673–86. Virtual Event: ACM, 2021. https://doi.org/10.1145/3487552.3487816.

[2] Akiwate et al., "Risky BIZness: Risks Derived from Registrar Name Management."

Previous SSAC advisories identified and discussed security risks related to dependencies on expired domains, but the onus of mitigating risks often fell on registrants. However, this approach may be unrealistic for the vast majority of registrants who lack the resources or expertise for continuous domain management. Additionally, these advisories did not explore the potential for registrar-initiated domain renaming to create a new attack surface.

In this report, the SSAC explores potential solutions to remediate exposed domains and prevent the creation of new unsafe sacrificial nameservers. The SSAC examines each proposed solution for its feasibility, effectiveness, and potential to reduce the attack surface without introducing undue complexity or new vulnerabilities into the DNS ecosystem.

Remediating exposed domains involves registrants, registrars, and registries. However, each remediation option faces unique challenges, such as awareness, technical capability, logistical and liability concerns. The complexity of coordinating efforts among these entities poses a significant barrier to effective remediation.

The SSAC examines two primary categories of solutions to prevent the risk of domain resolution hijacking. The first category would grant registrars more flexibility to delete host objects of expired domains. Deleting the host objects would eliminate the need for sacrificial nameservers altogether. This approach improves security significantly by averting the hijacking risk associated with unsafe sacrificial nameservers. The second category includes several standardized renaming methods for sacrificial nameservers so their parent domains are not registrable. This category acknowledges the constraints registrars face and focuses on minimizing risks. While an improvement, these methods still carry inherent complexities and residual risks. None of the options in either category fully address the underlying vulnerability of relying on domains that can expire.

Recognizing the need for balance between operational efficiency, security, and the minimization of unintended consequences, the SSAC recommends a multifaceted approach involving industry engagement and the development of new DNS management practices that prioritize security and stability without compromising the functionality and accessibility of the DNS.

Recommendation 1: The SSAC recommends that the registry and registrar communities collaborate to develop and implement a comprehensive code of conduct to mitigate the risks associated with registrable sacrificial nameservers.

Recommendation 2: SSAC recommends that ICANN org design, develop, and regularly publish aggregated statistics specifically focused on the prevalence of unsafe sacrificial nameservers and the effectiveness of different mitigation measures.

Recommendation 3: SSAC recommends ICANN org directly engage with registries and registrars to assist in mitigation and prevention efforts based on the insights gleaned as a result of implementing Recommendation 2.

1 Introduction

This report explores potential strategies for mitigating and preventing a long-standing domain name system (DNS) resolution hijacking risk, motivated by a peer-reviewed study, "Risky BIZness: Risks Derived from Registrar Name Management" by Akiwate et al.[3,4] Unlike traditional domain hijacking techniques that exploit compromised account credentials or manipulate the resolution protocol, this report focuses on an unforeseen risk arising from a longstanding practice employed by some registrars.

This risk stems from an inherent aspect of the DNS: the dependency of one domain's name resolution (Domain A) on another domain (Domain B), which may be owned and managed by different entities. This setup lacks contractual or procedural safeguards against disruption or misuse, especially when Domain B expires and can no longer provide name resolution to Domain A. Expired domains with dependents cannot be deleted due to a combination of Extensible Provisioning Protocol (EPP) constraints and registry policies. When registrars cannot delete expired domains with dependents, they are forced to bear the burden of sponsoring the domain without remuneration from the registrant.[5] A common workaround among registrars for managing expired domains has been to rename unwanted nameserver host objects to unregistered domains in a separate top-level domain (TLD). There is evidence that these registrar practices have unintentionally exposed over 500,000 domains within generic Top-Level Domains (gTLDs) to resolution hijacking risk, affecting names in most popular gTLDs, as well as gTLDs with tight registration control. More concerning, multiple actors have actively exploited these practices, assuming control over 163,000 domains within gTLDs without having any formal or operational responsibility for those names.[6] This analysis leveraged zone files from the Centralized Zone Data Service (CZDS), which does not include zone files for country code top-level domains (ccTLDs). Consequently, the extent of this practice and its potential consequences within ccTLDs remain unknown.

In this report, the SSAC examines risks that emerge from the expiration of domains that provide name resolution for other domains. The SSAC also evaluates options for remediating and preventing this domain resolution hijacking risk. This report describes and analyzes the benefits, burdens, and residual risks of possible alternatives for primary stakeholders.

This document has three objectives:

1. Define and describe the problem's origin, including a catalog of previous SSAC reports spanning two decades that warned about the risks of domains expiring with

[3] See Akiwate, Gautam, Stefan Savage, Geoffrey M. Voelker, and K C Claffy. "Risky BIZness: Risks Derived from Registrar Name Management." In *Proceedings of the 21st ACM Internet Measurement Conference*, 673–86. Virtual Event: ACM, 2021. https://doi.org/10.1145/3487552.3487816.

[4] Note that the primary author, Gautam Akiwate, is an SSAC member and a listed contributor to this report.

[5] Move sponsoring footnote up to here

[6] Akiwate et al., "Risky BIZness: Risks Derived from Registrar Name Management."

dependencies. None of these advisories identified or discussed the risks of registrars themselves renaming domains to create a new domain resolution hijack attack surface. The report also describes how the renaming practices of registrars affect domains across registry boundaries creating risks that are more challenging to remediate.

2. Draw on the peer-reviewed security study by Akiwate et al. to analyze remediation options of this domain resolution hijacking risk, focusing on the benefits, burdens, and residual risks of possible solutions.
3. Explore potential alternatives for operational changes that would avoid creating new instances of this domain resolution hijacking risk.

1.1 Intended Audience and Use

The target audience for this work party is the registrar and registry community, the ICANN organization, and those interested in improving Internet infrastructure security. The principal objective of this work is to motivate the multistakeholder community to focus on this vulnerability and replace current practices that exacerbate the vulnerability with less risky practices. Although the prevailing philosophy has been that registrants are solely responsible for monitoring their domains, this expectation is beyond the capability of the vast majority of registrants. In fact, parties who have taken on responsibility for managing domain names can mitigate this long-standing vulnerability by adopting safer operational practices. Although a perfect and complete solution to the problem is unlikely, a set of stakeholders motivated to reduce the attack surface can create a path forward for doing so.

1.2 Definitions

The terminology used in this document is consistent with the terminology in RFC 8499: DNS Terminology. Each definition, whether directly from RFC 8499 or supplementary, is accompanied by citations to relevant RFCs to provide further context.

Domain name: In DNS protocol terminology, a domain name is "an ordered list of one or more labels" [RFC 8499]. Domain names are presented as these labels separated by the period or "dot" character. E.g., "www.example.com". For this report, we generally refer to domain names as something that registrants can register or something an end-user might enter when using the Internet.

Nameserver: A server that receives DNS queries and returns DNS responses. In simple terms, there are two types of nameservers: recursive and authoritative. A recursive nameserver – sometimes known as a recursive resolver – receives queries from end users and determines which authoritative servers to ask for a particular query. Recursive nameservers also usually keep a cache of previous responses to reduce latency. This document primarily focuses on authoritative nameservers. Unless stated otherwise, *nameserver* refers to an authoritative nameserver. Note that nameservers have names and IP addresses. For example, `ns.icann.org` is the name of an authoritative nameserver that serves the `icann.org` domain. `ns.icann.org` has an IPv4 address (199.4.138.53) and an IPv6 address (2001:500:89::53).

Zone: The complete set of information for a particular "pruned" subtree of the domain space [RFC 3375]. Zones are structured hierarchically.

Top-level domain (TLD): A top-level domain which consists of a single label. IANA maintains a list of TLDs: https://data.iana.org/TLD/tlds-alpha-by-domain.txt

Resolution: Resolution is the process of following delegation paths from a starting point (the root zone) down to a particular domain name. Resolution generally involves querying (or using cached data from) numerous nameservers involved along the path of delegations from the root to the domain name.

Registrant: An entity that registers domain names in a registry through the services provided by a registrar. Registrants include individuals, organizations, and corporations. [RFC 3375]

Registrar: An entity that provides front-end domain name registration services to registrants, providing a public interface to registry services. [RFC 3375]

Registry: An entity that provides back-end domain name registration services to registrars, managing a central repository of information associated with domain name delegations. A registry is typically responsible for the publication and distribution of zone files used by the Domain Name System. [RFC 3375]

Delegation: In the DNS hierarchy, delegations are the connections between zones. A parent zone contains a delegation to a child zone in the form of nameserver (NS) records. We say the parent zone delegates the child zone to the nameservers specified in the NS records. For example, these records published in the ORG zone specify a delegation to nameservers authoritative for the ICANN.ORG zone:

```
icann.org.          IN   NS   c.icann-servers.net.
icann.org.          IN   NS   b.icann-servers.net.
icann.org.          IN   NS   ns.icann.org.
icann.org.          IN   NS   a.icann-servers.net.
```

Glue Record: Recursive resolvers sometimes need to look up a nameserver's IP address before they can query it. A problem arises when a domain's nameserver is in that same zone or a child of that zone. We call that an "in-domain nameserver." To break this cyclic dependency, the DNS uses a concept called **glue**. A zone must include glue records (an A or AAAA resource record) for any NS records whose names are under that zone. For example, the .COM zone must include glue records for any nameservers in the .COM zone, or child zones of .COM.

Orphan glue records: A glue record becomes an "orphan" when the delegation point NS record referencing it is removed from a zone file without also removing the corresponding glue record.

Extensible Provisioning Protocol (EPP): The Extensible Provisioning Protocol is "an application-layer client-server protocol for the provisioning and management of objects stored in a shared central repository" [RFC 5730]. EPP is the protocol that registrars and registries use to interact with each other using domain name mappings [RFC 5731] and host mappings [RFC 5732].

EPP Objects: A DNS EPP object repository contains two kinds of objects relevant to this report: **domain objects** and **host objects.** There are other object types, primarily contact objects, but they are not relevant to this topic.

Domain objects: EPP objects that represent the information about registered domain names.

Host objects: EPP objects that hold information about nameservers, including their host name.

EPP Repository: The set of TLD registries operated by a single registry operator. The boundary of an EPP repository is not necessarily restricted to a single TLD registry boundary, i.e., an EPP repository may have the data for more than one TLD present, which is common for Registry Service Providers hosting more than one TLD.

Sacrificial nameserver: The name of an EPP host object [RFC 5732] that has been renamed in order to make it no longer subordinate to an expired parent domain. This renaming serves as a strategic measure to navigate around the constraints imposed by EPP and registry policies that prevent the deletion of a domain with subordinate host objects referenced by other domains. A sacrificial nameserver can be classified as **unsafe** when its parent domain is available for registration or as **safe** when its parent domain is not available for registration.

Domain resolution hijacking risk: a specific consequence of unsafe sacrificial nameservers, where the unclaimed or neglected resources are actively exploited by malicious entities to take over the resolution function for a domain.

2 Problem Statement: Creating Unsafe Sacrificial Nameservers

This section explores how challenges in managing expired domains have led to the long-standing domain resolution hijacking risk that motivated this report. Three factors contribute to this risk:

1. the requirement from RFC 1034 to specify at least two nameservers for a domain when registering it and throughout its lifespan;
2. procedures and policies implemented to prevent the creation of orphan glue records; and
3. the operational and economic incentives for registrars navigating these constraints.

This section highlights how the intersection of technical requirements, policy implications, and registrar strategies shapes the landscape of domain name management, focusing on the security risks posed by the current handling of expired domains.

When registrants register a new domain name, they commonly specify the domain's nameservers. Most registrars and registries require two nameservers at the time of registration. This requirement stems from a statement in RFC 1034, "by administrative fiat, we require every zone to be available on at least two servers, and many zones have more redundancy than that."[7] This requirement also applies to future updates to the domain. A registrant or registrar is generally not permitted to make a change that would leave a domain with only one nameserver.

When a domain name registration expires, the domain cannot be deleted if other domains depend on it. More precisely, a combination of Extensible Provisioning Protocol (EPP) constraints and registry policies prevents the simple deletion of a domain with subordinate host objects referenced by other domains (See Figure 1).

Deleting domains with subordinate host objects also raises concerns about *orphan glue*. As the name implies, an orphan glue record lacks a parent (see Section 3.5). If the parent domain is removed from the DNS, but the subordinate (child) host (glue) record remains in the registry, it could become orphan glue. The desire by some registries to minimize or eliminate orphan glue may be the reason for policies that prevent the simple deletion of expired domains that other domains depend on.

When registrars cannot delete expired domains with dependents, they are forced to bear the burden of sponsoring[8] the domain without remuneration from the registrant. To avoid this

[7] See RFC 1034, Domain Names - Concepts and Facilities; Section 4, Name Servers; https://datatracker.ietf.org/doc/html/rfc1034.

[8] From RFC 5720, Extensible Provisioning Protocol (EPP), “A protocol client that is authorized to manage an existing object is described as a "sponsoring" client throughout this document,” https://datatracker.ietf.org/doc/html/rfc5730

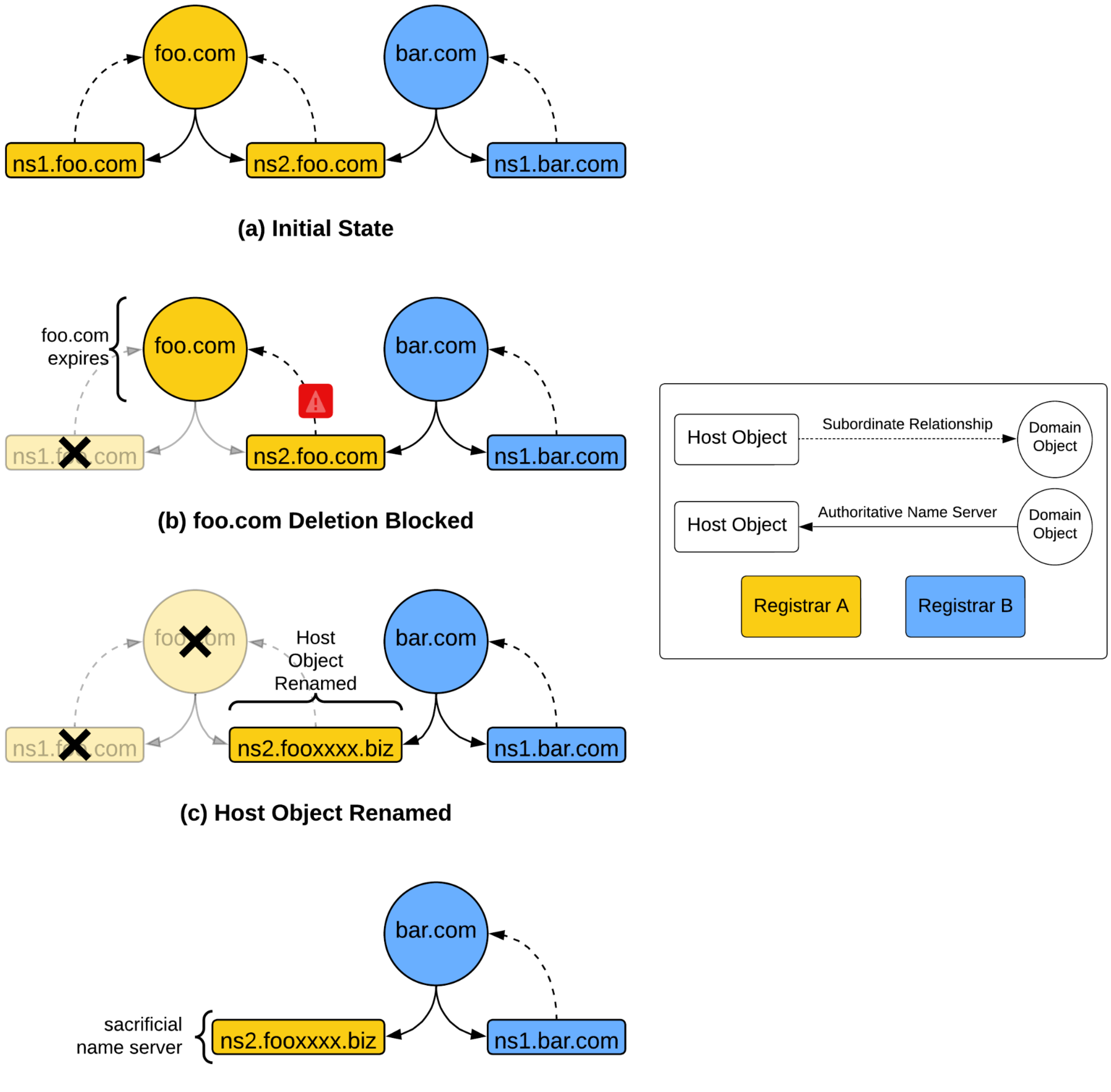
burden, some registrars have found and utilized what appears to be a loophole in these constraints by using the EPP <update> command to rename the host objects that are subordinate to the expiring domain. This renaming is a critical step - it breaks the existing dependencies of the other domains on the expiring domain. From the registrar's point of view, the least burdensome approach is to rename the host object to a host name in a non-existent domain in a separate TLD managed in a separate EPP repository. Once renamed, the host objects are referred to as *sacrificial nameservers*.[9] By doing this, registrars can remove the expired domains from the registry, avoiding the burden of sponsoring them. The renamed host objects—now bearing no relation to the expired domains—continue to exist independently.

While this approach provides a workaround for the burden registrars face, these sacrificial nameservers can create new vulnerabilities and complexities within the DNS. Akiwate et al. observed a specific practice of creating sacrificial nameservers with registrable domain names in a different TLD managed in a separate EPP repository.

Figure 1 shows an example scenario of creating unsafe sacrificial nameservers:

- There are two domains—`foo.com` and `bar.com`—each with two nameservers.
- Registrar A maintains `foo.com`, which depends on `ns1.foo.com` and `ns2.foo.com`, both subordinate to `foo.com`.
- Registrar B maintains `bar.com`, which depends on
  - `ns2.foo.com`—subordinate to `foo.com`
  - and `ns1.bar.com`—subordinate to `bar.com`.
- When `foo.com` expires, the relationship between `bar.com` and `ns2.foo.com` blocks Registrar A from deleting `foo.com`.
- Registrar A renames the host object to `ns2.fooxxxx.biz` to avoid the burden of sponsoring `foo.com` for `bar.com` name resolution.
- By doing so, Registrar A can now delete `foo.com`.
- Because `fooxxxx.biz` is available for registration, `ns2.fooxxxx.biz` is an unsafe sacrificial nameserver.

[9] Note that the term sacrificial nameserver, at its point of creation, does not necessarily refer to an actual nameserver – it could be merely referring to a resource record.



(a) Initial State

(b) foo.com Deletion Blocked

(c) Host Object Renamed

(d) Final State

Figure 1: Renaming a host object to an unsafe sacrificial nameserver to bypass domain deletion constraints (Figure 1 of Akiwate et al.)[10]

Looking at actual zone data on 30 June 2019, the domain `whitecounty.net.` had this NS record in the registry:[11]

```
whitecounty.net.    IN   NS   ns2.internetemc.com.
```

[10] Image courtesy of Akiwate et al., from"Risky BIZness: Risks Derived from Registrar Name Management"

[11] See "whitecounty.Net - DZDB." https://dzdb.caida.org/domains/whitecounty.net

On 1 July 2019, the registrar sponsoring this domain renamed the nameserver host object such that the registration had this NS record:

```
whitecounty.net.    IN   NS   ns2.internetemc1aj2tkdy.biz.
```

This report focuses on this specific type of sacrificial nameserver where the parent domains of the renamed host objects are considered to be *unsafe* because they are registrable. This scenario is an example of a dangling NS record, which inherently poses a risk of a domain resolution hijack.[12,13] Malicious actors could register the sacrificial nameserver's parent domain and hijack name resolution for all domains that previously depended on the expired domain—either partially or entirely—depending on how many NS domains are taken over by the attacker. Bryant documented a large-scale version of this problem in which stale NS records at the .IO registry provided a mechanism to hijack all .IO domains.[14]

2.1 Additional risks related to DNSSEC

An attacker controlling one nameserver can use DNSSEC to take over the victim domain completely if the victim domain does not use DNSSEC. Suppose the registry operator or registrar processes child-side CDS/CDNSKEY records for automated DS maintenance but neglects to check them for consistency across the domain's nameservers.[15] In that case, the domain will eventually end up with DS records derived from the attacker's CDS/CDNSKEY records. This scenario requires some statistical luck, as the parent zone's CDS/CDNSKEY query, or sometimes queries, need to hit the attacker's nameserver. After a successful query, validating resolvers will no longer accept responses from the remaining legitimate nameservers. Subsequently, if the parent supports CSYNC, the attacker may use it to update the delegation's NS records, replacing the remaining legitimate nameservers entirely with ones under the attacker's control.[16]

[12] See Liu, Daiping, et al. "All Your DNS Records Point to Us: Understanding the Security Threats of Dangling DNS Records." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Association for Computing Machinery, 2016, pp. 1414–25, https://doi.org/10.1145/2976749.2978387.

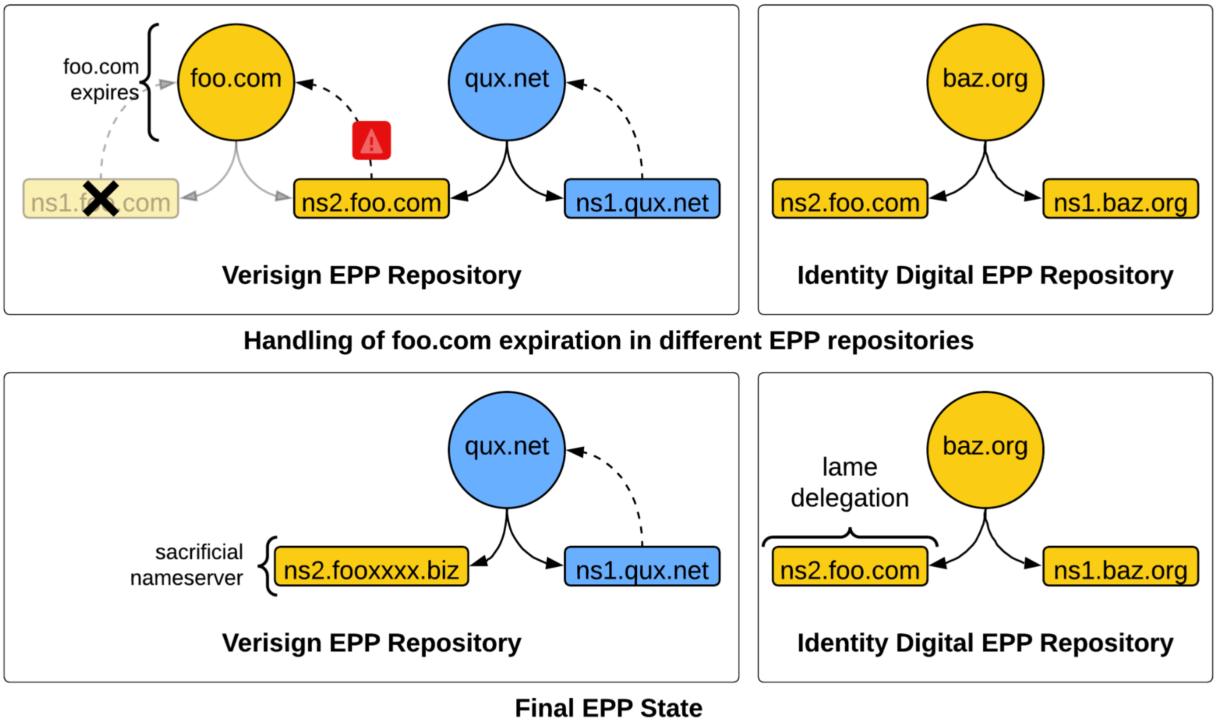
[13] The terms *dangling record* and *dangling delegation* are deliberately avoided in this report due to their ambiguity and the breadth of interpretation they can elicit. Instead, this report focuses on a specific risk associated with unsafe sacrificial nameservers and the potential for domain resolution hijacking.

[14] See Bryant, Matthew. "The .Io Error – Taking Control of All .Io Domains With a Targeted Registration." The Hacker Blog, 10 July 2017, https://thehackerblog.com/the-io-error-taking-control-of-all-io-domains-with-a-targeted-registration/.

[15] At the time of publication, the IETF is considering an addendum to the CDS/CDNSKEY specification that would mandate such consistency checks. See draft-ietf-dnsop-cds-consistency-04, "Consistency for CDS/CDNSKEY and CSYNC is Mandatory." Internet Draft (work in progress). Internet Engineering Task Force, 2 October 2023. https://datatracker.ietf.org/doc/draft-ietf-dnsop-cds-consistency/

[16] See RFC 7477: Child-to-Parent Synchronization in DNS, https://datatracker.ietf.org/doc/rfc7477/

2.2 Intra Registry vs Inter Registry Scoping



Handling of foo.com expiration in different EPP repositories

Final EPP State

Figure 2: Handling domain expiration in different EPP repositories (Figure 2 of Akiwate et al.)[17]

A sacrificial nameserver renaming operation covers the EPP repository—the collective set of TLD registries operated by a single registry operator—not individual TLDs. In Figure 2, Verisign also operates .net in a shared EPP repository with .com, so a renaming will also update the domain `qux.net` (that pointed to `ns2.foo.com`) to use the new sacrificial nameserver `ns2.fooxxx.biz`. In the top left, Verisign would not allow the expiration of foo.com because other domains in the same EPP repository depend on it. Other EPP repositories (the right-hand graphs) are unaffected by this renaming – but the domain `baz.org` still suffers from a vulnerability after the expiration of foo.com. Indeed, since `baz.org` still relies on an expired domain, anyone could subsequently register that expired domain (`foo.com`) and then participate in the resolution of names in the `baz.org` zone.

Thus, even though both domains were originally delegated to the same nameserver—`ns2.foo.com`—the final delegation after the expiration of `foo.com` depends on which registry holds the domain. This scoping property implies that even restricted TLDs (e.g., .gov) can be vulnerable to this renaming even though they do not use registrars.

[17] Image courtesy of Akiwate et al., from"Risky BIZness: Risks Derived from Registrar Name Management"

The asymmetry between the intra-registry and inter-registry scenarios is also important when considering the solution space, as there is currently no mechanism, policy, or standard to support inter-registry notification of nameserver changes. Section 5.2 analyzes a potential option to prevent the creation of new sacrificial nameservers by providing a notification method that would enable consumers or other relying parties to receive notifications upon changes to the database that impact their domains.

2.3 Scale of the Issue

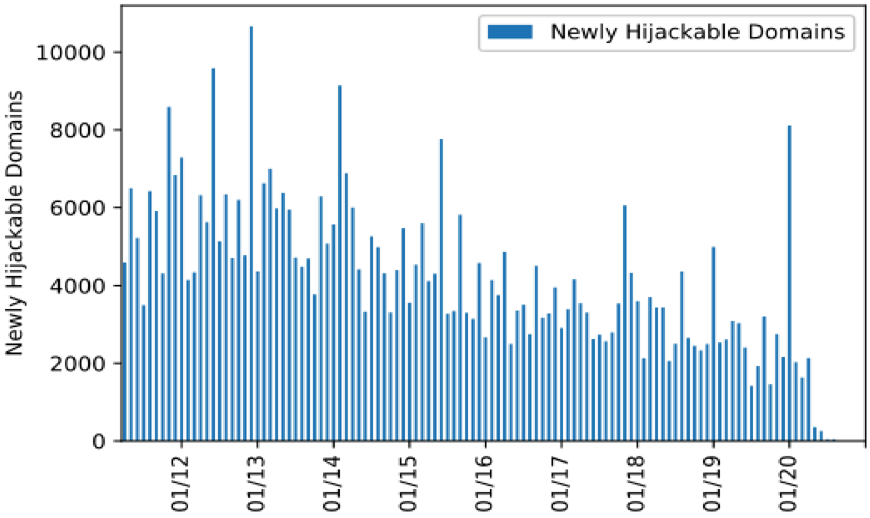
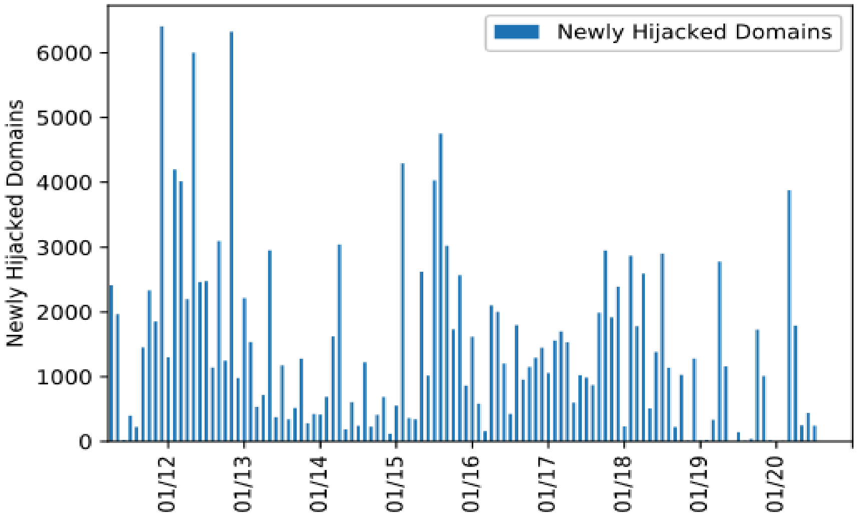


Figure 3: Domains vulnerable to resolution hijack newly identified each month, April 2011 to September 2020 (Figure 3 of Akiwate et al.)[18]



[18] Image courtesy of Akiwate et al., from "Risky BIZness: Risks Derived from Registrar Name Management"

Figure 4: Domains experiencing new resolution hijack incidents, April 2011 to September 2020 (Figure 4 of Akiwate et al.)[19]

Between 2011 and 2020, nearly half a million domains were affected due to sacrificial nameservers.[20] Of these domains, nearly a third were resolution-hijacked.

These registrar renaming practices have been used for many years, at least going back to April 2011.[21] The establishment of the Centralized Zone Data Service (CZDS) platform provided easier access for researchers to acquire the data needed to investigate this phenomenon over the last decade. Figure 3 shows that the number of domains under gTLDs that the authors inferred became vulnerable to resolution hijack in the given month for nine years due to sacrificial nameservers. While the authors inferred a downward trend over the years, thousands of domains were newly placed at risk of resolution hijack each month. Figure 4 shows the number of domains under gTLDs newly hijacked each month. Unfortunately, unlike the clear downward trend in newly hijackable domains, the trend in newly hijacked domains is bursty. It is clear that resolution hijacking has been a long-standing risk. As such, finding a solution to prevent the creation of new sacrificial nameservers is important to protect domain integrity and enhance overall Internet security.

3 Previous advice on the risks of DNS resolution hijacks due to expired domains

The SSAC reviewed previous SSAC reports related to the risks of DNS resolution hijacks and summarized each in this report. While the collection of these reports provides a thorough understanding of how expired domains could be compromised, they have not specifically addressed the risk where registrars inadvertently create new vectors for domain resolution hijack attacks by renaming domains.

July 2005
SAC007: Domain Name Hijacking: Incidents, Threats, Risks and Remediation
SAC007 emphasizes the importance of robust security measures and accurate registration information to prevent unauthorized control of domains.

July 2006
SAC011: Problems caused by the non-renewal of a domain name associated with a DNS Name Server

[19] Image courtesy of Akiwate et al., from "Risky BIZness: Risks Derived from Registrar Name Management"
[20] Akiwate et al., "Risky BIZness: Risks Derived from Registrar Name Management"
[21] Akiwate et al., "Risky BIZness: Risks Derived from Registrar Name Management"

SAC011 highlights the importance of registrants keeping their information accurate and registries/registrars collaborating on awareness efforts. However, the SSAC no longer finds it realistic to recommend that registrants are the best possible actors to identify and remediate certain vulnerabilities. Registries and registrars should be assuming meaningful roles in creating a collaborative, robust solution for registrants.

August 2009
SAC040: Measures to Protect Domain Registration Services Against Exploitation or Misuse
SAC040 emphasizes the importance of registrars having strong security practices to protect against domain registration modifications. It recommends measures like independent security audits and a trusted security mark program.

November 2010
SAC044: A Registrant's Guide to Protecting Domain Name Registration Accounts
SAC044 emphasizes selecting registrars with strong security practices and offers a security checklist. However, it also acknowledges the limitations of expecting all registrants to have the technical expertise for effective monitoring.

May 2011
SAC048: SSAC Comment on Orphan Glue Records in the Draft Applicant Guidebook
SAC048 recommends careful management and evidence-based removal of orphan glue records to avoid disrupting legitimate uses.

November 2015
SAC074: SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle
SAC074 emphasizes the importance of ongoing security measures throughout the lifecycle of credentials to improve overall domain name system security. It highlights the importance of transparency and shared learning within the domain name industry.

Initially, the onus was placed on registrants to monitor their domain's dependencies, yet this approach has not proved practical. The progression of the reports reflects a growing understanding of the vulnerabilities that can disrupt the stability and security of the DNS. Collectively, they point toward a shift in the focus of responsibility from registrants to a broader engagement involving registrars and registries, suggesting a collaborative approach to managing the risks associated with domain expiration and the potential for malicious domain resolution hijacking. This evolution in perspective is pivotal to addressing the risks posed by creating unsafe sacrificial nameservers.

3.1 SAC007: Domain Name Hijacking: Incidents, Threats, Risks and Remediation

In July 2005, the SSAC issued SAC007: Domain Name Hijacking: Incidents, Threats, Risks and Remediation.[22] SAC007 provides a detailed overview of domain hijacking—the wrongful taking of control of a domain name from the rightful name holder. SAC007 examines domain hijacking incidents, analyzes their impacts, and proposes potential security enhancements. Domain hijacking can significantly affect a registrant by stripping them of their online identity and can lead to extortion. It disrupts business operations through denial of email services, unauthorized information disclosure, and damage to reputation through website defacement. Moreover, the harm often extends beyond the primary victim, with customers, business partners, and unrelated parties experiencing collateral damage.

SAC007 identifies the main causes of hijacking incidents as flaws in registration processes, non-compliance with transfer policies, and poor domain name administration by registrars, resellers, and registrants. To mitigate these risks, it suggests measures for all parties involved. Registrants are advised to keep their registration information secure and up-to-date, use Registrar-Lock, and monitor their domain name status. Registrars and registries are encouraged to ensure the unique application of EPP authInfo codes and improve the accuracy of registrant records. Additionally, the SSAC recommends developing best practices for domain name protection, including public awareness campaigns and establishing emergency contacts and procedures for urgent domain restoration.

SAC007 highlights the critical importance of robust security measures and accurate, up-to-date registration information to prevent unauthorized domain control and ensure the stability of the DNS. SAC007's findings and recommendations are still relevant in understanding the vulnerabilities and risks associated with creating sacrificial nameservers. SAC007's emphasis on the need for unique EPP authInfo codes, Registrar-Lock, and rigorous verification and authorization processes for domain transfers and changes mirror the concerns observed in Section 2 regarding the potential for domain resolution hijacking through the exploitation of unsafe sacrificial nameservers. Implementing SAC007's recommended security measures could mitigate some of the risks associated with these practices by enhancing the overall security posture of domain registrations and transfers.

[22] See SAC007: Domain Name Hijacking: Incidents, Threats, Risks and Remediation, https://archive.icann.org/en/announcements/hijacking-report-12jul05.pdf

3.2 SAC011: Problems caused by the non-renewal of a domain name associated with a DNS nameserver

In July 2006, the SSAC issued SAC011: Problems caused by the non-renewal of a domain name associated with a DNS nameserver.[23] SAC011 directly addresses the complications that emerge when a domain's nameserver depends on another domain that expires. As described in SAC011 and Section 2, this scenario can disrupt or destabilize the name resolution for the original domain, potentially leading to unpredictable name resolution or malicious redirection, such as phishing or email interception, by a new owner of the expired domain.

SAC011 highlights the dependency between domain name service operations and domain registrations, particularly when DNS records are hosted on systems under different domain names, sometimes called out-of-bailiwick services. In SAC011, the SSAC emphasizes the onus on the registrants to maintain accurate and current contact and DNS nameserver information to avoid service interruption and vulnerability to attacks. The SSAC also recommends that registries and registrars collaborate on raising awareness about the importance of accurate nameserver information. The SSAC then examines methods for monitoring name service and intervening when discrepancies are detected. Protective actions include establishing clear lines of responsibility within organizations for DNS matters, ensuring accurate contact information is on file, and actively monitoring DNS service for accuracy.

This report is a direct descendant of SAC011, as both reports focus on the vulnerabilities for dependent domains introduced by expiring domain registrations. SAC011 also underscores the necessity of active monitoring of nameservers as well as robust management practices to prevent the unintended consequences of expired domain registrations. The problems identified in SAC011, such as service interruption and susceptibility to malicious redirection, are the same observed almost twenty years later about unsafe sacrificial nameservers. When SAC011 was published, it is likely that the operational practice of registrars creating the vulnerability of unsafe sacrificial nameservers had not yet begun.

However, SAC011 emphasizes registrant action and remediation by maintaining accurate registration and contact information. As the DNS ecosystem has significantly evolved since SAC011 was originally published, the SSAC no longer finds it realistic to recommend that registrants are the best possible actors to identify and remediate this vulnerability. The skill required to do so is beyond the capability of the vast majority of registrants. Instead, the SSAC proposes that proactive measures and heightened awareness around domain registration and DNS management can mitigate the risks associated with expired domains and dependent

[23] See SAC011: Problems caused by the non-renewal of a domain name associated with a DNS nameserver, https://www.icann.org/en/system/files/files/renewal-nameserver-07jul06-en.pdf

services. However, the SSAC now finds that registries and registrars should assume meaningful roles in creating a collaborative, robust solution to be effective.

3.3 SAC040: Measures to Protect Domain Registration Services Against Exploitation or Misuse

Then, in August 2009, the SSAC issued SAC040: Measures to Protect Domain Registration Services Against Exploitation or Misuse.[24] In SAC040, the SSAC highlights how unauthorized modifications to domain registration information and DNS configurations can lead to severe disruptions, financial losses, and damage to reputation. SAC040 calls attention to notable incidents of security breaches, highlighting the attractiveness of DNS and domain registration accounts to attackers, and analyzes the methods attackers used to gain control and the ensuing consequences. SSAC040 also identifies best practices and protective measures that registrars can adopt to shield against such threats.

A notable aspect of SAC040 is its reflection on the insights and recommendations of SAC007, particularly regarding the protection against domain hijacking. The security vulnerabilities highlighted in SAC040 and the detailed analysis of past incidents provide a comprehensive understanding of the potential risks and the necessity for enhanced protective measures. By drawing on SAC007's insights, SAC040 reaffirms the critical nature of security in domain registration and DNS management and extends the scope of responsibility to registrars, emphasizing their role in safeguarding the domain registration ecosystem. SAC040 recommends that registrars offer additional security services as optional enhancements and engage in educational initiatives to heighten registrants' understanding of the security risks and protective measures available.

SAC040 expands on SAC007 by proposing that registrars undergo voluntary independent security audits to assess their adherence to best security practices. This recommendation highlights the importance of external validation in ensuring that registrars maintain high-security standards. Furthermore, SAC040 introduces the concept of a trusted security mark program coordinated by ICANN to recognize registrars that meet established security benchmarks. The recommendation aimed to facilitate registrants' ability to make informed decisions based on the security postures of their registrars, indirectly bolstering the security of the DNS and domain registration ecosystem at large.

SAC040 and this report both highlight the integral role of proactive security measures and informed decision-making by registrars in maintaining the stability and security of DNS infrastructure. SAC040's focus on protecting domain registration services against misuse or

[24] See SAC040: Measures to Protect Domain Registration Services Against Exploitation or Misuse, https://www.icann.org/en/groups/ssac/documents/sac-040-en.pdf

exploitation is directly relevant to the current discussion on the complexities surrounding expired domain registrations and the creation of unsafe sacrificial nameservers. The vulnerabilities highlighted in SAC040 resonate with the risks identified in Section 2, especially concerning unauthorized modifications of DNS configurations that could arise from operational practices surrounding expired domain names. The recommendations in SAC040, which build upon and expand on those in SAC007, suggest a comprehensive approach to enhancing security in domain registration services. Such a strategy is directly relevant to addressing the vulnerabilities identified in Section 2 of this report, highlighting the importance of registrar accountability, registrant awareness, and robust security measures to maintain the integrity and stability of the DNS and domain registration processes.

SSAC040's emphasis on independent security audits and the suggestion for a trusted security mark program further underscore the importance of transparency and trust in the domain registration ecosystem. The recommendations from SAC040 for registrars to offer stronger protection measures and enhance security awareness among registrants align with the need for more robust security protocols in managing domain registrations and DNS configurations, as discussed in Sections 4 and 5. Implementing these recommendations could help mitigate the risks associated with creating unsafe sacrificial nameservers and prevent the potential for domain resolution hijacking.

3.4 SAC044: A Registrant's Guide to Protecting Domain Name Registration Accounts

In November 2010, the SSAC issued SAC044: A Registrant's Guide to Protecting Domain Name Registration Accounts.[25] SAC044 is a comprehensive guide for registrants to safeguard their domain name registration accounts against potential threats. It uses an analogy between virtual assets in the domain space and tangible assets in the physical world. The SSAC outlines a broad spectrum of protective measures that individuals and organizations can adopt to shield their domain names from unauthorized access, hijacking, and misuse. SAC044 also reviews the threat landscape, examines risks associated with domain registration accounts, and suggests a risk management approach for organizations to effectively assess and mitigate these risks.

SAC044 encourages organizations to implement protective measures either in-house, through contracted third parties, or directly via registrars or registries, weighing the pros and cons of outsourcing versus internal management. It also stresses the importance of redundancy in protective measures and provides a comprehensive security checklist for organizations to use when selecting registrar services.

[25] See SAC044: A Registrant's Guide to Protecting Domain Name Registration Accounts, https://www.icann.org/en/groups/ssac/documents/sac-040-en.pdf

SAC044 significantly expands on the foundational security practices outlined in previous SSAC reports by detailing specific measures that registrants can adopt (e.g., multi-factor authentication for account access, routine monitoring of WHOIS and DNS data for unauthorized changes) and recommending that registrants select registrars based on their security practices. This approach to domain name security, emphasizing both registrar and registrant responsibilities, addresses the multifaceted threats faced in the digital landscape, ensuring that domain names remain secure and resilient against attacks.

SAC044 complements SAC040, but SAC044 shifts the focus toward registrants by focusing on actions that registrants themselves can take to secure their domain name registration accounts from exploitation or misuse. Like SAC040, SAC044 also echoes the sentiments of SAC007 regarding the importance of domain name security, expanding on the concept by providing registrants with a toolkit of measures to safeguard their virtual assets. This registrant-centric approach is intended to empower individuals and organizations with the knowledge to assess their risk exposure and select appropriate protective measures, whether implemented directly or through enhanced services offered by registrars.

While SAC044 provides registrants with knowledge and strategies to protect their domain names, it implicitly acknowledges the limitations faced by individual registrants, especially those without the technical expertise or resources to monitor and secure their domain names effectively. The legacy of SAC044 highlights a critical finding: the prevailing expectation that registrants should monitor their domains is, in reality, beyond the capabilities of the vast majority. This acknowledgment shifts the discourse surrounding domain name security, suggesting that the burden of security should not rest solely on registrants but should be a shared responsibility with registrars and registries.

3.5 SAC048: SSAC Comment on Orphan Glue Records in the Draft Applicant Guidebook

In May 2011, the SSAC issued SAC048: SSAC Comment on Orphan Glue Records in the Draft Applicant Guidebook.[26] In SAC048, the SSAC defines orphan glue records as address records that become "orphans" when their corresponding delegation point nameserver record is deleted without removing the glue record itself, leading to potential administrative and security issues. SAC048 proposed including a specific definition in the Applicant Guidebook for clarity. SAC048 also recommended that the management of orphan glue records should not be categorized under "abuse prevention and mitigation" since they mostly support the normal operation of the DNS. SSAC's conclusion in 2011 was that while orphan glue could be used maliciously, it also identified legitimate uses and advised that any removal should be

[26] See SAC048: SSAC Comment on the Orphan Glue Records in the Draft Applicant Guidebook, https://www.icann.org/en/groups/ssac/documents/sac-048-en.pdf

approached with evidence of malicious intent. While the comments made in 2011 may have been aligned with the best practices and understanding of DNS management at that time, it is important to acknowledge that these guidelines may not represent the current landscape of orphan glue records in light of how the DNS ecosystem has evolved in the last thirteen years. The SSAC also observed in 2011 that existing policies on glue records varied, with some registries allowing direct registration of glue records and others allowing orphan records to exist until all associations are removed or not permitting them. This variability could affect the reachability of domains depending on their DNS service architecture.

Understanding how to manage orphan glue records helps explain why registrars sometimes rename host objects. However, this practice can unintentionally introduce invalid or outdated NS records, which could be vulnerable to exploitation by malicious actors. SAC048 acknowledged the potential for abuse with orphan glue records, paralleling the SSAC's concern in the current report with the vulnerabilities introduced by unsafe sacrificial nameservers. While SAC048 does not specifically address sacrificial nameservers, its recommendations for evidence-based removal of orphan glue and refined management are examples of security-conscious approaches to dealing with expired domains.

3.6 SAC074: SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle

In November 2015, the SSAC issued SAC074: SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle.[27] SAC074 delves into the significant risk of attacks compromising domain registrant data and DNS settings, impacting registrars, registries, registrants, and end users. SAC074 notes that breaches affecting registrant information or DNS configurations of domain names remain a major issue not only for registrars and registries but also for registrants and Internet users.

SAC074 explains the credential management lifecycle and presents guidelines and best practices for enhancing domain names' security and supporting systems. SAC074 emphasizes the importance of robust security measures, including promoting multi-factor authentication and developing global training programs. These initiatives should aim to educate registrars and registries on securing credentials throughout their lifecycle, from creation and distribution to renewal and destruction. By addressing these areas, the SSAC provides a comprehensive strategy for mitigating unauthorized access and manipulation of domain names to improve the overall security and stability of the domain name system.

[27] See SAC074: SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle, https://www.icann.org/en/system/files/files/sac-074-en.pdf

SAC074 highlights the importance of transparency and shared learning within the domain name industry, helping registrars and registries better understand the threat landscape and adapt their security measures accordingly. The recommendation in SAC074 for ICANN to facilitate global hands-on training programs highlights an important facilitation role that ICANN is uniquely positioned to fill in tackling security problems through education and capacity building.

4 Options to Remediate Exposed Domains

In the context of this report, we consider an exposed domain to be one whose nameservers have been renamed to registrable sacrificial nameservers as described in Section 2, and when the changed sacrificial nameserver domain is either available for registration or has already been registered (presumably by a malicious actor). It may be possible to remediate the resolution hijacking risk for exposed domains, subject to some constraints and willingness of various parties involved.

This section explores potential remediation actions for exposed domains. Remediation actions would need to be initiated by one of the following stakeholders:

- Registrants
- Registrars
- Registries
- Third Parties, e.g., entities operating sacrificial namespaces

Table 1 compares the benefits, burdens, and residual risks of various entities taking remedial action. Understanding each approach's benefits, burdens, and residual risks is a beneficial context for determining the most efficient and responsible course of action in mitigating the risks associated with exposed domains.

Table 1: Comparison of Benefits, Burdens, and Residual Risks of Entity Taking Remedial Action

Entity taking Remedial Action	Benefits	Burdens	Residual Risks
Registrants	Maximum incentive alignment	Registrants generally are not DNS experts and may lack technical understanding to see the need for remediation	Low adoption rate
Registrars	Empowered to take action on behalf of	Misplaced incentive	Possible reliance on external parties to

	registrant customers		identify exposed domains. Liability if mistakes occur.
Registries	Could have the biggest remediation impact	Misplaced incentive; don't normally initiate changes	Possible reliance on external parties to identify exposed domains; undesirable precedent
Third-Party Defensive Registrations	Minimal policy impact	Misplaced incentive, i.e., unclear who would maintain Uncertain up-front and ongoing burdens	No exit strategy

4.1 Registrants

In most cases, registrants should be able to easily remediate their exposed domains by interacting with their registrar and updating the domain's nameserver records appropriately. The primary challenge here, however, is that most registrants are likely unaware of the exposed nature of their domains. Due to the robustness of the DNS protocol and recommendations to have multiple nameservers—even across TLDs—to improve resilience, the exposure may go unnoticed as long as the domain has at least one properly operating nameserver.[28] It may be possible to notify registrants regarding domain exposure. However, this would require close cooperation with registrars and would probably have a low response rate.

4.2 Registrars

Since the concerns addressed in this document originated with practices implemented by registrars, we consider their role in remediation. Presumably, registrars are in a good position to know which domains are exposed and to make remediation changes in bulk. However, due to the operation of the EPP host object update (see Figure 1), registrar A can cause domains sponsored by registrar B to become exposed. In these cases, it is impossible to rename the host a second time since RFC 5732 forbids updating the name of an external host when it is linked to domains sponsored by other registrars.[29] Since it is impossible to roll back the action taken by Registrar A, the only remedy is for Registrar B (and other affected registrars) to update the delegations for the affected domains individually. However, there is no existing mechanism for

[28] Sommese, Raffaele, Mattijs Jonker, Jeroen van der Ham, and Giovane C. M. Moura. "Assessing E-Government DNS Resilience." In 2022 18th International Conference on Network and Service Management (CNSM), 118–26, 2022. https://doi.org/10.23919/CNSM55787.2022.9965155.

[29] RFC 5732, Section 3.2.5, EPP <update> Command, "changing an external host object that has associations with objects that are sponsored by a different client…MUST fail with EPP error code 2305."

Registrar B to know that their domains have been affected, except for continuous monitoring of all domains in its portfolio.

More generally, registrars could periodically reconcile nameserver host objects used for their registered domains to determine if the nameserver's domain exists at the referenced TLD registry. If the domain does not exist, the registrar could remove the nameserver from the affected domains. This process would involve querying the TLD registry using EPP, not just conducting a DNS lookup. The registry holds definitive information on domain registration regardless of whether the domain resolves to nameservers. This reconciliation process would be a massive undertaking for registrars, with the potential for serious liability if mistakes were made, so it is unlikely to get voluntary traction. Updating registrants' nameservers without registrants' knowledge is a delicate situation, and this approach would need to be tested thoroughly by registrars undertaking it. Additionally, the domains would remain exposed from the time of deletion until the reconciliation occurs.

4.3 Registries

While registries may be well-suited to make impactful bulk changes, it is generally expected that registries only make changes requested by the sponsoring registrars.

4.4 Third Party Defensive Registrations

Another option for domains that are exposed but not yet hijacked is for someone (e.g., a quarantine registrar) to defensively register the associated sacrificial nameserver domains to prevent them from falling into the hands of malicious actors. ICANN org could help facilitate this type of defensive registration.

Third-party defensive registrations would seem to represent a misalignment of incentives: expecting someone to solve problems created by others. At the scale described in section 2.3 such registrations would lead to significant long-term costs for the third-party registrant, especially without any sort of plan to remediate the problems at the sources.

4.5 Additional Feasibility Challenges

Remediation efforts for exposed domains whose associated sacrificial nameserver domain has already been legitimately registered face additional feasibility challenges in addition to the challenges noted for each party. The fallibility of heuristics used to identify sacrificial domains raises concerns about the appropriateness of remediating all algorithmically flagged instances. This complexity underscores the need to accurately identify exposed domains, which may require ICANN org or a third party to produce and validate lists of exposed domains. However, it is important to recognize that registrars and registries might hesitate to engage in remediation efforts without a clear and strong policy direction, as they would take on any liability resulting from a mistaken remediation.

5 Alternative Options When a Domain with Dependents Expires

This section provides a brief overview of several proposed operational practices that could prevent future exposure. It then dives into a detailed examination of each practice (Sections 5.1-5.6), discussing its benefits, any burdens it may impose on various stakeholders, and the residual risks associated with its adoption. Following the individual analyses, Section 5.7 will pivot to an comparison of all options through a series of tables:

- Table 2: Registry-Specific Comparison of Alternative Options when a Domain with Dependents Expires
- Table 3: Registrar-Specific Comparison of Alternative Options when a Domain with Dependents Expires
- Table 4: Registrant-Specific Comparison of Alternative Options when a Domain with Dependents Expires
- Table 5: Comparison of Alternative Options when a Domain with Dependents Expires for Additional Parties (beyond registries, registrars, and registrants) with Potential Benefits, Burdens, or Residual Risks

The presence of an operational practice in this report should *not* be understood to be an endorsement of the practice. Instead, we endeavored to include and evaluate all possible practices that may be adopted. Note that the scope for these solutions is the EPP repository of the expired domain (see Figure 2). As such, most of these options only solve the problem for domains managed by the same registry operator within the same EPP repository and would not address unsafe sacrificial nameservers introduced by expiring domains in other EPP repositories.[30]

Figure 5 below shows a flowchart that depicts the alternative approaches examined in this section for handling the expiration of `foo.com`, as described in Figure 1. It is noteworthy that with or without sacrificial nameservers, a domain's availability degrades when it depends on another domain that expires. However, some alternatives do not render `bar.com` vulnerable to domain resolution hijacking, which improves the overall security for the registrant of `bar.com`.

[30] See Section 5.2 for an ambitious option that addresses dependencies across EPP repositories.

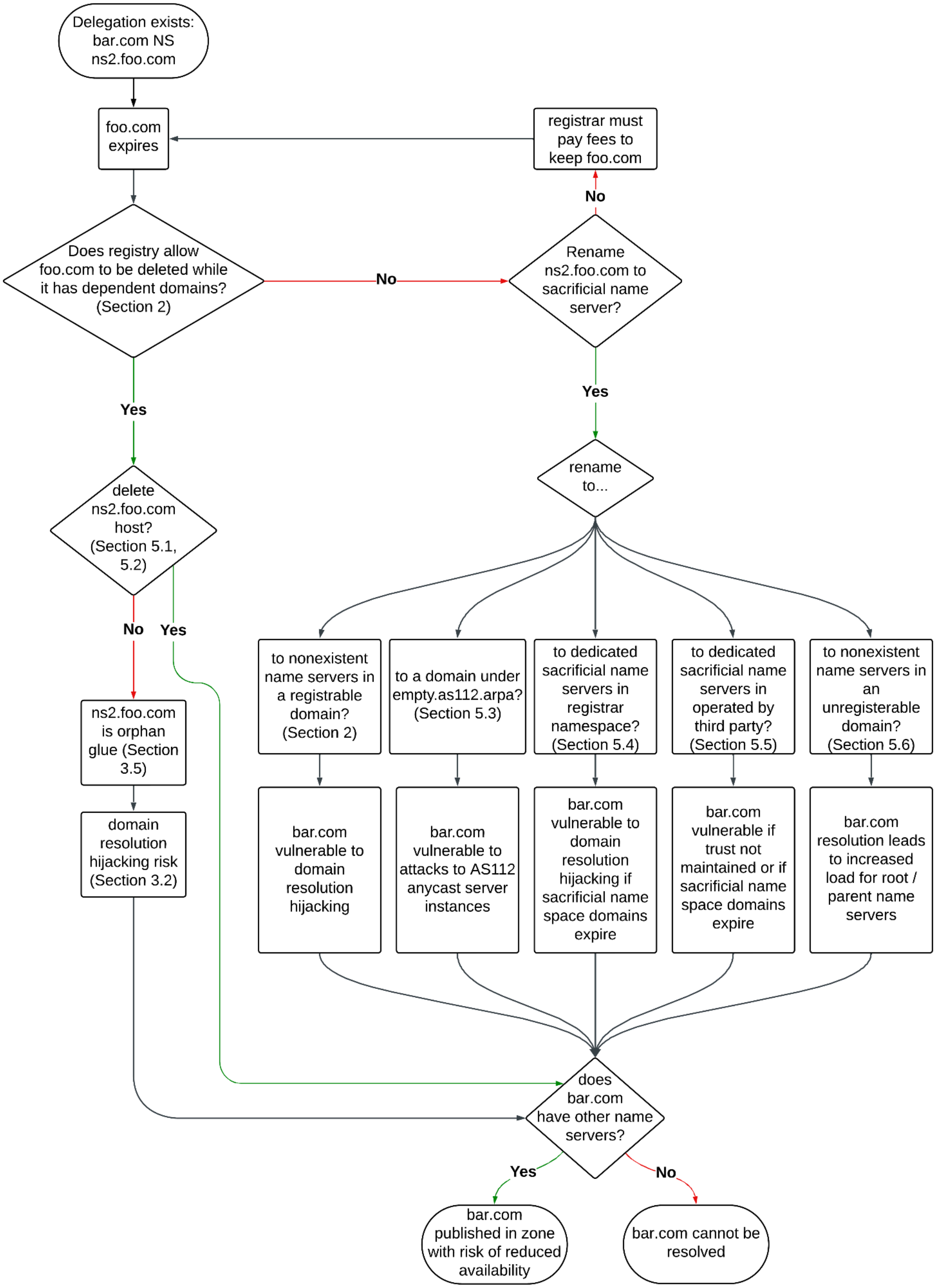

Delegation exists: bar.com NS ns2.foo.com
foo.com expires
registrar must pay fees to keep foo.com
No
Does registry allow foo.com to be deleted while it has dependent domains? (Section 2)
No
Rename ns2.foo.com to sacrificial name server?
Yes
Yes
delete ns2.foo.com host? (Section 5.1, 5.2)
rename to...
No
Yes
ns2.foo.com is orphan glue (Section 3.5)
domain resolution hijacking risk (Section 3.2)
to nonexistent name servers in a registrable domain? (Section 2)
to a domain under empty.as112.arpa? (Section 5.3)
to dedicated sacrificial name servers in registrar namespace? (Section 5.4)
to dedicated sacrificial name servers in operated by third party? (Section 5.5)
to nonexistent name servers in an unregisterable domain? (Section 5.6)
bar.com vulnerable to domain resolution hijacking
bar.com vulnerable to attacks to AS112 anycast server instances
bar.com vulnerable to domain resolution hijacking if sacrificial name space domains expire
bar.com vulnerable if trust not maintained or if sacrificial name space domains expire
bar.com resolution leads to increased load for root / parent name servers
does bar.com have other name servers?
Yes
No
bar.com published in zone with risk of reduced availability
bar.com cannot be resolved

Figure 5: Flowchart of different approaches if foo.com expires and their effects on bar.com.

5.1 Delete Host Object

In this option, the registry would relax their requirements that forbid deletion of the host object. The registrar would issue an EPP request for the registry to delete the host object, and the registry would execute such a request. Such a deletion can be combined with the <restore> operation in RFC 3915 to prevent malicious or accidental deletions of host objects. Note that this approach does not remediate the resolution hijacking risk created by sacrificial nameservers that cross EPP repository boundaries (e.g., a nameserver domain in .com used by domains in .org). Note that deleting host objects that are nameservers may leave a domain without any nameservers at all. However, this deletion might trigger removal of the domain from its parent zone while the domain remains registered in the EPP database. We do not consider this an additional risk beyond the current mode of renaming a host object, which leaves the domain open to resolution hijack.

5.1.1 Benefit

Registry: Does not create orphan glue.

As a secondary benefit, due to the fact that some recursive name servers aggressively retry resolution failures,[31] deleting host objects and their corresponding nameservers should lead to a reduction in DNS query traffic compared to the practice of creating sacrificial nameservers. This is especially true for the registry of the sacrificial name servers, and less relevant for the registry of the dependent domain. Although additional DNS queries do not directly lead to security risks, the DNS contains a significant volume of extraneous and purposeless query traffic and any efforts to reduce that should be welcomed.

Registrar: Registrars simplify their operational practices (e.g., registrars no longer have to find a TLD to create sacrificial nameservers) and do not need to maintain any infrastructure/domains to support sacrificial nameservers (relative to other options).

Registrant: Domains registered in the same EPP repository are not exposed to resolution hijack. A registered domain without any remaining name servers will have its delegation removed from the registry zone, which may more effectively bring the problem to the registrant's attention.

5.1.2 Burden

Registry: Will have to allow and execute EPP requests to delete domain objects including all subordinate host objects. Registries must also remove nameservers from domains using the

[31] See RFC 9520
Negative Caching of DNS Resolution Failures, https://www.rfc-editor.org/rfc/rfc9520.html

deleted host object. This option will require updating policies and software to accommodate new conditions, e.g., a deletion may result in a domain without (two) nameservers.

Registrar: Registrars will also need to update their operational practices to accommodate the deletion of host objects. They may also need to account for staggered uptake of the shared host object deletion at the registries.

Registrant: No additional burden, although host object deletion may violate an implicit principle of least astonishment since such deletions have not been the norm for many years now.

5.1.3 Residual Risk

Registry: None.

Registrar: A non-sponsoring registrar who has domains dependent on the sacrificial nameserver will not be aware of the deletion, thus creating an inconsistency between registry and registrar.

Registrant: None. Note that deleting host objects that are nameservers may leave a domain without any nameserver at all. We do not consider this an additional risk beyond the current mode of renaming a host object, which leaves the domain open to resolution hijack.

5.2 Delete Host Object with Notification

The DNS is a pull-based protocol, which means that aside from the notify option for zone distribution, database consistency across multiple operators is exceedingly difficult and leads to dangerous inconsistencies as the data changes. One strategy for preventing this domain resolution hijacking threat is to operate in a way that is similar to a strongly consistent database, providing a notification method that would enable consumers or other relying parties to receive notifications upon changes to the database that impact their domains.

At a minimum, this sort of system would enable external relying parties to receive timely notifications of changes that may impact their resolution. Potential methods to achieve these notifications could be some push-based notifications when a change occurs[32] to more complex solutions like an acknowledged receipt.[33]

[32] E.g., Pub/Sub, email, webhook.

[33] Strongly consistent databases use protocols like Paxos, https://en.wikipedia.org/wiki/Paxos_(computer_science), or Raft, https://en.wikipedia.org/wiki/Raft_(algorithm).

This approach is tremendously more ambitious than just allowing registrars to delete host objects. It combines protocol and operational changes by asking registries to communicate host object deletions to relying registrars. Akiwate et al. proposed this approach in “Risky BIZNess”:

> *A more ambitious approach would combine protocol and operational changes to remove the underlying "garbage collection" problem for deleted nameserver domains. In particular, by changing the deletion rules in EPP — so that deletion of a domain also removes all references (i.e., nameserver delegations) to any subordinate host objects — would prevent the creation of new dangling delegations inside an EPP repository. However, fully addressing inter-registry links across EPP repositories (e.g., a nameserver domain in .com that is used by domains in .org) would require a new mechanism to report such domain deletions among registries so that they too could automate the removal of links to deleted nameservers.*[34]

The proposed change requires updates for both registries and registrars. Similar to Section 5.1, registries would need to relax their requirements that forbid deletion of the host object. Additionally, registries would be responsible for communicating these deletions to all other registries. These other registries would then notify the registrars of affected domains, allowing them to remove any dependencies associated with those domains. Since no inter-registry notification protocol currently exists, specifying and building one would be necessary.

5.2.1 Benefit

Registry: Does not create orphan glue. Reduced query load as a result of broken delegations being removed.

As a secondary benefit, due to the fact that some recursive name servers aggressively retry resolution failures, deleting host objects and their corresponding nameservers should lead to a reduction in DNS query traffic compared to the practice of creating sacrificial nameservers. This is especially true for the registry of the sacrificial name servers, and less relevant for the registry of the dependent domain. Although additional DNS queries do not directly lead to security risks, the DNS contains a significant volume of extraneous and purposeless query traffic and any efforts to reduce that should be welcomed.

Registrar: Registrars simplify their operational practices, e.g., registrars no longer have to find a TLD in which to create a sacrificial nameserver and do not need to maintain any infrastructure/domains to support sacrificial nameservers.

[34] See Section 7.3 "Robust Long-term Fixes" of Akiwate et al. "Risky BIZNess: Risks Derived from Registrar Name Management", https://cseweb.ucsd.edu/~gakiwate/papers/risky_bizness_imc21.pdf

Registrant: Domains registered in the same EPP repository are not exposed to resolution hijack.

5.2.2 Burden

Registry: This will impose a significant additional burden on registries. In addition to operational changes allowing host objects to be deleted, registries must build mechanisms to notify other registries and act on notifications of deleted host objects from other TLDs to ensure consistent and accurate nameserver mapping and prevent outdated references.

Registrar: Registrars will need to update their operational practices to accommodate requests for deletion of host objects and notification of deletion of host objects in other TLDs. They may also need to account for staggered uptake of the shared host object deletion and notification at the registries.

Registrant: No additional burden, although host object deletion may violate an implicit principle of least astonishment since such deletions have not been the norm for many years now.

5.2.3 Residual Risk

Registry: This approach would require significant protocol and operational changes in addition to building new coordination mechanisms. Those changes will introduce new complexity that produces its own set of risks.

Registrar: A non-sponsoring registrar who has domains dependent on the sacrificial nameserver will not be aware of the deletion, thus creating an inconsistency between registry and registrar.

This approach would require significant protocol and operational changes in addition to building new coordination mechanisms. Those changes will introduce new complexity that produces its own set of risks.

Registrant: This approach would require significant protocol and operational changes in addition to building new coordination mechanisms. Those changes will introduce new complexity that produces its own set of risks.

5.2.4 Fine-grained visibility of changes to zone files.

A potential middle ground for this approach could be to use a publish/subscribe system to enable the relying registries/registrars to monitor changes to relevant zones. The DNS Transparency project—proposed many years ago but not yet deployed—would achieve the required level of transparency, allowing third parties to monitor changes to zones without inducing a vast number of active DNS queries on the Internet.[35,36]

However, this technique may come with additional risks. While the DNS Transparency project aims to provide transparency without overwhelming the internet with queries, such a system would require protections against the risk of misuse by malicious actors. However, it is worth considering the specific threat landscape addressed in this document. We need to weigh the potential for abuse against the benefits of increased transparency in mitigating the risk of unsafe sacrificial nameservers. If the current threat poses a significant risk, a publish/subscribe system with careful security measures might be a viable option, even with some potential for abuse.

Although insufficient, a significant amount of the required information for gTLDs is available through the CZDS. A registrar could download and parse the CZDS zones, looking for nameservers used within their domains that no longer exist. However, relying solely on CZDS zone files presents limitations. These files offer a snapshot of domain name registrations and configurations but do not provide a direct record of changes to host objects over time. Use of these files to infer sacrificial nameservers relies on heuristics to infer the renaming patterns of the registrars, which is inherently limited. Finer-grained data such as that described in the DNS Transparency proposal would allow more direct and precise tracking of the creation and evolution of sacrificial nameservers.

5.3 Rename host object to empty.as112.arpa

One option is to create safe sacrificial nameservers by renaming host objects to empty.as112.arpa—a distributed anycast service that DNS zone administrators established to sink DNS traffic relating to parts of the global namespace under the administrator's control.[37] Doing so would not require coordination among zones and would ensure that another party would never register such nameserver domains. While this is technically an option that would prevent the domain resolution hijacking risk described in Section 2, the empty.as112.zone was intended to be used with DNAME redirection -- to alias a whole zone to emptiness. The use of empty.as112.arpa for sacrificial nameservers was not envisioned by RFC 7535. However, in this report we endeavored to include and evaluate all possible practices that may be adopted.

5.3.1 Benefit

Registry: No change.

[35] Internet Fire Brigade, Implement DNS Transparency v1.0 RFP. https://www.internetfire.org/projects/dns-transparency/rfps

[36] For another example of DNS monitoring services, see DNS Check, Monitor DNS Records, https://www.dnscheck.co/monitor-dns-records

[37] See RFC 7535: AS112 Redirection Using DNAME, https://datatracker.ietf.org/doc/rfc7535/

Registrar: Registrars simplify their operational practices, e.g., registrars no longer have to find a TLD in which to create a sacrificial nameserver and do not need to maintain any infrastructure/domains to support sacrificial nameservers.

Registrant: Domains registered in the same EPP repository are not exposed to this resolution hijack.

5.3.2 Burden

Registry: None.

Registrar: Registrars will need to update their operational practices.

Registrant: No additional burden.

AS 112 operators: Must bear the burden of additional traffic.

5.3.3 Residual Risk

Registry: None.

Registrar: A non-sponsoring registrar who has domains dependent on the sacrificial nameserver will not be aware of the renaming, thus creating an inconsistency between registry and registrar.

Registrant: Creates significant, untrackable new exposure—a malicious AS112 operator could hijack all requests in its vicinity and resolve all such delegations.

Additionally, the AS112 infrastructure relies on volunteers willing to donate resources to operate an AS112 anycast server, and its long-term sustainability is not necessarily guaranteed.

5.4 Per-Registrar Non-Registrable Sacrificial Namespace

Individual registrars maintain their own namespace where sacrificial nameservers can be placed. For example, if a registrar were to register and maintain the domain *foo.biz*, then it could use names such as *sacrificial-0001.foo.biz* for sacrificial nameservers outside of the .BIZ EPP repository. This option achieves the primary goal of making sacrificial nameservers unregistrable by malicious actors. Since sacrificial nameservers cannot be renamed within an EPP repository, a registrar using this approach might need sacrificial namespaces under two or more EPP repositories.

5.4.1 Benefit

Registry: No change.

Registrar: No change

Registrant: Domains registered in the same EPP repository are not exposed to resolution hijack.

5.4.2 Burden

Registry: While this approach does not place any burdens on the deleted-domain registry, it might introduce some burdens for the registry of the sacrificial namespace in the form of unwanted queries.

Registrar: Registrars must revise their operational practices, which could impose a significant burden. This burden includes managing sacrificial namespace domains and potentially operating any supporting infrastructure.

Registrant: None.

5.4.3 Residual Risk

Registry: None.

Registrar: A non-sponsoring registrar who has domains dependent on the sacrificial nameserver will not be aware of the renaming, thus creating an inconsistency between registry and registrar.

Registrant: This solution is inherently fragile because it relies on existing registrars to maintain these sacrificial namespaces in perpetuity (as well as depending on new registrars to adopt similar measures). Registrars have abandoned such domains in the past, leaving registrants exposed.[38]

Furthermore, sacrificial namespaces concentrate delegations, so if the corresponding domain is not renewed, it could allow an attacker to control tens of thousands of domains with a single registration.

[38] See Section 7.2 "Prevent New Exposure" of Akiwate et al. "Risky BIZNess: Risks Derived from Registrar Name Management", https://cseweb.ucsd.edu/~gakiwate/papers/risky_bizness_imc21.pdf

5.5 Global / Community Non-registrable Sacrificial Namespace

Furthermore, ICANN org could consider two versions of a global sacrificial namespace to minimize registrar burden and potentially mitigate residual risks for registrants. One version is to select a third-party service provider to maintain a global, sacrificial namespace. Alternatively, ICANN org could directly assume this responsibility itself. Since sacrificial nameservers cannot be renamed within an EPP repository, it may be necessary to create sacrificial namespaces under two or more EPP repositories.

5.5.1 Benefit

Registry: No change.

Registrar: Registrars simplify their operational practices and do not need to maintain any infrastructure/domains to support the sacrificial namespace.

Registrant: Domains registered in the same EPP repository are not exposed to resolution hijack.

5.5.2 Burden

Registry: The organization (e.g., a registry operator or a third party organization selected by ICANN org) supporting such a sacrificial namespace will need to update its operational practices, which may have a significant burden that includes operating the sacrificial namespace domain and may include operating any supporting infrastructure.

Registrar: Registrars will need to update their operational practices.

Registrant: None.

Third-party service provider: The organization (e.g., a registry operator or a third-party organization selected by ICANN org) supporting such a sacrificial namespace will need to update its operational practices, which may have a significant burden that includes operating the sacrificial namespace domain and may include operating any supporting infrastructure.

5.5.3 Residual Risk

Registry: None.

Registrar: A non-sponsoring registrar who has domains dependent on the sacrificial nameserver will not be aware of the renaming, thus creating an inconsistency between registry and registrar.

Registrant: This solution is inherently fragile because it relies on the chosen entity to maintain these sacrificial namespaces in perpetuity. Sacrificial namespaces concentrate delegations, so if the corresponding domain is not renewed, it could allow an attacker to control tens of thousands of domains with a single registration.

Third-party service provider: A global sacrificial namespace could be used for more than the problem described in this document. It could become a general space for broken delegations and unwanted DNS traffic. There is no way to restrict which domains can use the sacrificial namespace for their nameservers.

5.6 Reserved TLDs or Special-Use Domain Names

A special-use domain name, as described in RFC 6761 and SAC113, could be designated for use in naming safe sacrificial nameservers.[39,40] Renaming to a special-use domain eliminates resolution hijacking risks as long as names under the special-use domain are not registrable. Note that the special-use domain designated for this purpose could be a top-level domain, such as .`SACRIFICIAL`, or some other domain within the IANA DNS namespace, such as `sacrificial-nameserver.arpa`. Alternatively, an existing reserved TLD such as .invalid can also be used for such a purpose.

Consider the examples from Figures 1 and 2, where domain `bar.com` has `ns2.foo.com` as a nameserver and domain `foo.com` expires. Instead of renaming `ns2.foo.com` to `ns2.fooxxxx.biz`, registrar A could instead rename it to `ns2.foo.com.sacrificial` or `ns2.foo.com.sacrificial-nameserver.arpa`.

Any special-use domain name designated for this purpose must have the property that names under the special-use domain are not available for registration. This requirement corresponds to Consideration 7 in Section 5 of RFC 6761.

A designated special-use domain name must also have the property that queries at or below the domain are blocked by caching DNS servers and recursive resolvers (consideration #4 in Section 5 of RFC 6761). This requirement eliminates the potentially large amount of undesirable query traffic to the parent zone of the special-use domain and additionally eliminates opportunities for hijacking via response spoofing.

[39] Cheshire, S, and M Krochmal. "RFC 6761: Special-Use Domain Names." Request for Comments. Internet Engineering Task Force, February 2013. https://www.rfc-editor.org/rfc/rfc6761.html.
[40] "SAC113: SSAC Advisory on Private-Use TLDs," https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-113-en.pdf.

5.6.1 Benefit

Registry: None.

Registrar: Registrars simplify their operational practices.

Registrant: Domains registered in the same EPP repository are not exposed to resolution hijack.

5.6.2 Burden

Registry: Would have to update operational practices and software to support special-use TLDs.

Registrar: Registrars must update their operational practices and code to support special-use TLDs.

Registrant: No additional burden.

Root Server Operators: will receive more queries for non-existent names unless resolvers preemptively answer queries under a special-use TLD. However, the response is cacheable, and some resolvers will answer from a local copy of the root zone[41], so the burden may be insignificant (assuming that no more than a few such TLDs are used). Also, QNAME Minimization can mitigate privacy issues.[42,43]

5.6.3 Residual Risk

Registry: None.

Registrar: A non-sponsoring registrar who has domains dependent on the sacrificial nameserver will not be aware of the renaming, thus creating an inconsistency between registry and registrar.

Registrant: None

[41] See RFC 8806: Running a Root Server Local to a Resolver, https://datatracker.ietf.org/doc/html/rfc8806

[42] See RFC 7816: DNS Query Name Minimisation to Improve Privacy, https://datatracker.ietf.org/doc/html/rfc7816

[43] See Report from 2023-10-15 23:18 for 24590 resolver at 12521 probes, Qname Minimization, https://dnsthought.nlnetlabs.nl/#qnamemin

5.7 Comparing Alternative Options by Entity

Please see the tables below for a summary of the benefits, burdens, and residual risks to each stakeholder (registries, registrars, and registrants) for each option.

Table 2: Registry-Specific Comparison of Alternative Options when a Domain with Dependents Expires

Option	Benefit	Burden	Residual Risk
Do nothing/status quo	-	-	-
Delete Host Object	Does not create orphan glue Potential reduction in DNS query traffic	Will have to allow and execute EPP requests to delete domain objects including all subordinate host objects. This will require updating policies and software to accommodate new conditions.	-
Notification + Delete Host Object	Does not create orphan glue Potential reduction in DNS query traffic	Significant additional burden: registries will have to build mechanisms to notify other registries and act on notifications of deleted host objects from other TLDs to ensure consistent and accurate nameserver mapping and prevent outdated references.	Would require significant protocol and operational changes in addition to building new coordination mechanisms. Those changes will introduce new complexity that produces its own set of risks.
Rename host object to empty.as112.arpa	-	-	-
Per-Registrar Non-registrable Sacrificial Namespace	-	Might introduce some burden for the registry of the sacrificial namespace, in the form of unwanted queries.	-
Global / Community Non-registrable Sacrificial Namespace	-	The organization supporting such a sacrificial namespace will need to update its operational practices, which includes operating the sacrificial namespace domain and may include operating any supporting infrastructure.	-

Special Use TLD	-	Would have to update operational practices and software to support special-use TLDs.	-

Table 3: Registrar-Specific Comparison of Alternative Options when a Domain with Dependents Expires

Option	Benefit	Burden	Residual Risk
Do nothing/status quo	-	No additional burden	Registrants continue to suffer resolution hijacking risk
Delete Host Object	Simplifies operational practices. Eliminates infrastructure demand needed to support sacrificial nameservers	Must update operational practices. May also need to account for staggered uptake of the shared host object deletion at the registries.	Non-sponsoring registrar who has domains dependent on the sacrificial nameserver will not be aware of the deletion, thus creating an inconsistency between registry and registrar.
Notification + Delete Host Object	Simplifies operational practices. Eliminates infrastructure demand needed to support sacrificial nameservers	Must update operational practices. May need to account for staggered uptake of the shared host object deletion and notification at the registries.	Non-sponsoring registrar who has domains dependent on the sacrificial nameserver will not be aware of the deletion, thus creating an inconsistency between registry and registrar. This approach would require significant protocol and operational changes, which will introduce new complexity that produces its own set of risks.
Rename host object to empty.as112.arpa	Simplifies operational practices. Eliminates infrastructure demand needed to support sacrificial nameservers	Must update operational practices.	Non-sponsoring registrar who has domains dependent on the sacrificial nameserver will not be aware of the renaming, thus creating an inconsistency between registry and registrar.
Per-Registrar Non-registrable Sacrificial Namespace	-	Must update operational practices, which may be a significant burden. Registrars must maintain sacrificial namespace domains and any supporting infrastructure.	Non-sponsoring registrar who has domains dependent on the sacrificial nameserver will not be aware of the renaming, thus creating an inconsistency between registry and registrar.
Global / Community Non-registrable Sacrificial Namespace	Simplifies operational practices. Eliminates infrastructure demand needed to support sacrificial nameservers	Must update operational practices	Non-sponsoring registrar who has domains dependent on the sacrificial nameserver will not be aware of the renaming, thus creating an inconsistency between registry and registrar.

Option	Benefit	Burden	Residual Risk
Special-Use TLD	Simplifies operational practices.	Must update operational practices and code to support special-use TLDs.	Non-sponsoring registrar who has domains dependent on the sacrificial nameserver will not be aware of the renaming, thus creating an inconsistency between registry and registrar.

Table 4: Registrant-Specific Comparison of Alternative Options when a Domain with Dependents Expires

Option	Benefit	Burden	Residual Risk
Do nothing/status quo	-	Must actively monitor nameservers and safeguard domain from resolution hijacking.	Domains will continue to be exposed to risk of resolution hijacks.
Delete Host Object	Domains registered in the same EPP repository are not exposed to this resolution hijack. A registered domain without any remaining name servers will have its delegation removed from the registry zone, which may more effectively bring the problem to the registrant's attention.	No additional burden, although host object deletion may violate an implicit principle of least astonishment since such deletions have not been the norm for many years now.	-
Notification + Delete Host Object	Domains registered in the same EPP repository are not exposed to this resolution hijack.	No additional burden, although host object deletion may violate an implicit principle of least astonishment since such deletions have not been the norm for many years now.	This approach would require significant protocol and operational changes in addition to building new coordination mechanisms. Those changes will introduce new complexity that produces its own set of risks.
Rename host object to empty.as112.arpa	Domains registered in the same EPP repository are not exposed to this resolution hijack.	-	Creates significant, untrackable new exposure—a malicious AS112 operator could hijack all requests in its vicinity and resolve all such delegations. AS112 infrastructure relies on volunteers, and its long-term sustainability is not necessarily guaranteed.
Per-Registrar Non-registrable Sacrificial Namespace	Domains registered in the same EPP repository are not exposed to this resolution hijack.	-	Solution relies on existing registrars to maintain these sacrificial namespaces in perpetuity. Registrars have abandoned such domains in the past, leaving registrants exposed. Concentrates delegations; if one such domain is not renewed, it could allow an attacker to control tens of thousands of domains with a single registration.

Option	Benefit	Burden	Residual Risk
Global / Community Non-registrable Sacrificial Namespace	Domains registered in the same EPP repository are not exposed to this resolution hijack.	-	Solution relies on the chosen entity to maintain these sacrificial namespaces in perpetuity. Concentrates delegations; if one such domain is not renewed, it could allow an attacker to control tens of thousands of domains with a single registration.
Special-Use TLD	Domains registered in the same EPP repository are not exposed to this resolution hijack.	-	-

Table 5: Comparison of Alternative Options when a Domain with Dependents Expires for additional parties beyond registries, registrars, and registrants that might have notable additional benefits, burdens, or residual risks associated with several options.

Option	Benefit	Burden	Residual Risk
Delete Host Object	No other parties were identified for the analysis of the Delete Host Object option.	-	-
Notification + Delete Host Object	No other parties were identified for the analysis of the Notification + Delete Host Object option.		
Rename host object to empty.as112.arpa		**AS 112 operators:** Must support additional query load.	**AS112 operators:** The AS112 infrastructure relies on volunteers willing to donate resources to operate an AS112 anycast server, and its long-term sustainability is not necessarily guaranteed.
Per-Registrar Non-registrable Sacrificial Namespace	No other parties were identified for the analysis of the per-registrar non-registrable sacrificial namespace option.		
Global / Community Non-registrable Sacrificial Namespace		**Third-party service provider:** the organization will need to update its operational practices, which may be a significant burden that includes operating the sacrificial namespace domain and may include operating any supporting infrastructure.	**Third-party service provider:** a global sacrificial namespace could become a general space for broken delegations and unwanted DNS traffic. There is no way to restrict which domains can use the sacrificial namespace for their nameservers.
Special-Use TLD		**Root Server Operators:** receive more queries for non-existent names.	

6 Monitoring Future Exposure

Since the problem continues, a valuable public service would be to operationalize the monitoring and analysis for domains within gTLDs on an ongoing basis to prevent backsliding.

One limitation of using CZDS zone files in Akiwate's methodology is inferring renaming idioms using heuristics based on the daily changes in zone files. This limitation can be overcome with a richer data set that logs host object changes. ICANN org has expressed interest in using the more granular bulk registration data access (BRDA) data set to understand the current scope of the problem. The SSAC Registrar Nameserver Management work party contacted ICANN org with a request to analyze the current state of this phenomenon, as the Akiwate et al. study is already three years old. Specifically, on 25 July 2023, the work party requested that ICANN's technical staff conduct an analysis that identifies across all gTLDs the numbers of sacrificial nameservers, exposed domains, hijacked nameservers, and hijacked domains. To ensure an accurate and comprehensive analysis, the work party requested aggregation at both the registrar and registry levels, including host objects present in the registry database but absent from DNS zone files.[44] On 6 September 2023, ICANN org responded that they plan to undertake analyses of this issue and share their findings with this work party.[45]

At the time of publication, no organization is responsible or incentivized to perform the monitoring for gTLDs. There is also no other organization with access to the BRDA data that would allow the most accurate exposure analysis.

The research gap identified in gTLD monitoring extends even further to ccTLDs. Unlike ICANN's role with gTLDs, ccTLDs are not subject to the same contractual oversight as gTLDs. The prevalence of unsafe sacrificial nameservers in ccTLDs may remain unknown, but ccTLD operators may still want to participate in monitoring efforts going forward.

7 Integrated Discussion and Findings

This section provides a summary and analysis of the SSAC's examination of a domain resolution hijacking risk caused by the creation of unsafe sacrificial nameservers. Additionally, this section includes the SSAC's Findings.

When registrants register a new domain name, they commonly specify the domain's nameservers. Most registrars and registries require two nameservers at the time of registration,

[44] See claffy, k. "SSAC Registrar NS Management Work Party Questions," 25 July 2023. https://www.icann.org/en/system/files/correspondence/claffy-to-swinehart-25jul23-en.pdf.

[45] See Arias, Francisco. "RE: SSAC Registrar NS Management Work Party Questions," 6 September 2023. https://www.icann.org/en/system/files/correspondence/arias-to-claffy-06sep23-en.pdf.

which persists through future updates. A registrant or registrar is generally not permitted to make a change that would leave a domain with only one nameserver. In many cases, domains can have subordinate host objects that serve as nameservers for other domains. This network of dependencies creates a scenario where the functionality of a domain becomes contingent upon the operational status of another domain acting as its nameserver.

Complexity arises when a domain registration expires. An expired domain cannot be straightforwardly deleted if other domains depend on it for nameserver functionalities. This policy aims to prevent disruptions in DNS resolution for the dependent domains. However, this also means that the expired domain remains in a liminal state, neither fully operational nor completely removed. This state can extend indefinitely, depending on the dependencies and the actions of registrars and registrants.

> **Finding 1:** Domains can depend on each other in a way that's not guaranteed to be consistent over time. This characteristic of interdependency between domains can lead to several security risks when a domain with dependencies expires.

Since registrars are incentivized to not sponsor lapsed registrations for dependent domain names, they avoid these burdens by using the EPP <update> command to rename a nameserver host object to a non-existent domain in a separate EPP repository. The renamed subordinate host objects are referred to as *sacrificial nameservers*. A recent peer-reviewed study, "Risky BIZness: Risks derived from registrar name management," identified a concerning trend where parent domains of sacrificial nameservers are available for registration, which we call *unsafe* sacrificial nameservers.[46] Registrable parent domains of sacrificial nameservers introduce a new attack surface for domain resolution hijacking, as malicious actors can exploit unsafe sacrificial nameservers to gain unauthorized control over the dependent domains, leading to manipulation or disruption.

> **Finding 2:** A practice of creating unsafe sacrificial nameservers has emerged. Understanding the implications of this evolving practice is crucial for developing effective strategies to detect, mitigate, and prevent domain resolution hijacking risks associated with creating unsafe sacrificial nameservers.

The “Risky BIZness” paper that first documented this phenomenon in 2021 relied on zone files from the Centralized Zone Data Service (CZDS). However, relying solely on CZDS zone files presents limitations. These files offer a snapshot of domain name registrations and configurations but do not provide a direct record of changes to host objects over time. As a result, the researchers had to employ heuristics based on the daily changes observed in these zone files to infer the renaming patterns of the registrars. While applying this method provided

[46] Akiwate et al., "Risky BIZness: Risks Derived from Registrar Name Management."

valuable insights, it is inherently limited in its ability to capture the full scope and nuances of the issue. Had a richer dataset that includes logs of host object changes been available to the researchers, it would have allowed more direct and precise tracking of the creation and evolution of sacrificial nameservers.

ICANN has the capability to access bulk registration data for gTLDs from both registrars and registries. This data goes beyond what is available in CZDS zone files, encompassing detailed logs of domain name registrations, updates, and changes to host objects. By leveraging this data, ICANN could provide a more complete and accurate picture of the prevalence and evolution of sacrificial nameservers across gTLDs.

> **Finding 3:** ICANN is uniquely positioned to track the scope and evolution of this vulnerability for gTLDs using access to the bulk registration data from registrars and registries.

Past SSAC advisories regarding the more general security threat of dependencies on expired domains have had limited impact. However, none of these advisories identified or discussed the risks of registrars themselves renaming domains to create a new domain resolution hijack attack surface.

> **Finding 4:** The prevailing philosophy has been that registrants are solely responsible for monitoring their domains. This expectation is beyond the capability of the vast majority of registrants.

The effective remediation of currently exposed domains requires a multifaceted approach. Registrants, often unaware of their domain's exposure, can directly update their nameserver records, but this relies on their awareness and technical ability. While operationally capable of bulk remediation, registrars face significant logistical and liability challenges, especially when domains are interlinked across different registrars. Registries are generally reluctant to intervene in domain matters not originating from the sponsoring registrar. Third-party interventions, like defensive registrations, present a proactive but complex solution.

The overarching challenge for remediation lies in accurately identifying exposed domains and coordinating remediation efforts among disparate entities. Additionally, registrars and registries might hesitate to engage in remediation efforts without clear policy direction, as they would take on any liability resulting from a mistaken remediation.

> **Finding 5:** The mitigation of the resolution hijacking risk for currently exposed domains may require the involvement of ICANN in creating a structured framework for remediation.

This report examines two primary categories of solutions to prevent the risk of domain resolution hijacking. The first category would require new mechanisms and policy changes within registries to grant registrars more flexibility to delete host objects subordinate to expired domains. This approach aims to reduce the reliance on sacrificial nameservers by enabling a more straightforward deletion process for expired domains, thereby minimizing the risk of hijacking associated with these domains. However, this option only partially resolves the issue, as it still allows for disruptions in DNS resolution for domains that still rely on the host objects of these expired domains.

The second category revolves around creating *safe* sacrificial nameservers using specific renaming strategies. These approaches acknowledge the current practice of using sacrificial nameservers but seek to manage it more effectively by standardizing the renaming action to avert the risks of choosing registrable domain names. However, even with a more controlled renaming process, the use of sacrificial nameservers inherently carries residual risks related to the complexity of each renaming strategy.

> **Finding 6:** The only robust solution to this problem requires new mechanisms and policies to either allow notification of exposed domains or a DNS transparency platform.[47]

While policy development processes (PDP) can lead to significant changes in managing generic top-level domains (gTLDs), their impact is inherently limited to these domains. This limitation poses a significant challenge in addressing the broader issue of domain resolution hijacking, which affects a wide range of TLDs, including country-code top-level domains (ccTLDs). Therefore, a comprehensive solution to this problem requires a solution extending beyond gTLDs and involving the wider DNS community.

A more inclusive and effective approach would be to encourage registrars and registries across all TLDs to voluntarily adopt best practices that prevent resolution hijack exposure. Developing a set of universally accepted norms, similar to the Mutually Agreed Norms for Routing Security (MANRS), could provide a framework for best DNS management and security practices.[48] This would need to be a collaborative effort among registries and registrars to define and adhere to a code of conduct that promotes responsible domain management and enhanced security practices. The SSAC proposes that the key pillars of the code of conduct should include the following measures:

[47] See Section 5.2.4: “Fine-grained visibility of changes to zone files” for more information on DNS transparency platforms. As mentioned, access to such data would require protections against the risk of misuse by malicious actors.

[48] See "About MANRS," https://www.manrs.org/about/.

- **Safe Host Object Management:** Implementing best practices for securely managing domain and host objects. This could include robust access controls, regular security audits, and clear lifecycle management policies to minimize the risk of unauthorized access or manipulation of critical domain data, further reducing the chances of successful resolution hijacking.
- **Enhanced Monitoring Practices:** A commitment to continuously monitor domain dependencies and nameserver configurations. This proactive approach enables the early detection and remediation of vulnerabilities that could be exploited for resolution hijacking attempts.
- **Proactive Notification Systems:** Establishing systems to alert registrants to potential vulnerabilities or suspicious activities related to their domains. This could involve notifications for:
    - Unusual domain configuration changes
    - Detection of suspicious activity on associated nameservers
    - Expired or expiring domains with outstanding dependencies
- **Data-Driven Transparency and Accountability:** Requiring the publication of data enabling independent auditing of compliance with the code of conduct. This fosters transparency and trust within the DNS ecosystem. Data points could include:
    - Number of detected and remediated vulnerabilities
    - Response times to reported incidents
    - Implementation rates with established notification protocols

One ongoing multistakeholder effort working towards a broader solution is an active Internet draft in the Registration Protocols Extensions (REGEXT) Working Group of the Internet Engineering Task Force (IETF).[49] Similar to this report, the Internet draft, titled "Best Practices for Deletion of Domain and Host Objects in the Extensible Provisioning Protocol (EPP)," reviews multiple practices for domain and host object deletion. The draft then proposes two best practices that registries and registrars can adopt to avert the risks associated with domain resolution hijacking:

- **Safe Host Deletion:** This practice allows explicitly deleting domains while retaining the capability to restore associated subordinate host objects, if necessary. Upon deletion, the server keeps the subordinate host objects in a "pendingDelete" state, preventing their use in DNS resolution but allowing them to be retrieved during a redemption period. This approach provides a safety net in case of accidental or malicious deletion actions. This proposal is a more specific version of this report's option to delete host objects (see Sections 5.1 and 5.2 of this report).

[49] See draft-ietf-regext-epp-delete-bcp-00, "Best Practices for Deletion of Domain and Host Objects in the Extensible Provisioning Protocol (EPP)." Internet Draft (work in progress). Internet Engineering Task Force, 20 February 2024. https://datatracker.ietf.org/doc/draft-ietf-regext-epp-delete-bcp/.

- **Renaming to a Special-Use Domain:** This recommendation suggests renaming host objects to a designated "sacrificial" domain or subdomain (see Section 5.6 of this report). IANA would manage this special-use domain, preventing its registration and ensuring it is not used for legitimate purposes. This practice communicates the intent to disable the host object and reduces the risk of its involvement in domain hijacking attempts.

Developing these proposed best practices demonstrates a collaborative approach to addressing issues discussed in this report. While the ongoing work in the IETF represents a valuable starting point for best practices for safe host object management, additional collaboration would still be needed to fully develop the remaining key pillars.

Implementing such a community-driven code of conduct would provide robust protection against domain resolution hijacking and enhance competition in the domain marketplace by empowering registrants to make informed choices about their domain registrations. Registrants could select registrars based on their participation and adherence to these norms, incentivizing registrars to commit to higher security standards.

> **Finding 7:** Achieving robust protection for registrants will require that the broader industry across gTLDs and ccTLDs work to create and adhere to a code of conduct that outlines best practices for preventing domain resolution hijacking

8 Recommendations

Recommendation 1: The SSAC recommends that the ICANN registry and registrar communities collaborate to develop and implement a comprehensive code of conduct to mitigate the risks associated with registrable sacrificial nameservers.

This code of conduct should be detailed, actionable, and encompass the following components:

- **Enhanced Monitoring Practices:** Commit to continuously monitoring domain dependencies and nameserver configurations, enabling the early detection and remediation of vulnerabilities that could lead to hijacking.
- **Safe Host Object Management:** Implement best practices that aim to securely manage domain and host objects, reducing the risk of their malicious compromise.
- **Proactive Notification Systems:** Establish systems for alerting registrants to potential vulnerabilities or suspicious activities, ensuring timely action can be taken to safeguard against hijacking.
- **Data-Driven Transparency and Accountability:** Require the publication of data enabling independent auditing of compliance with these best practices. This step is

crucial for maintaining transparency and ensuring accountability within the DNS ecosystem.

Recommendation 2: SSAC recommends that ICANN org design, develop, and regularly publish aggregated statistics specifically focused on the prevalence of unsafe sacrificial nameservers and the effectiveness of different mitigation measures.

The SSAC suggests the following statistics be included in the published data:

- The number of unsafe sacrificial nameservers identified across TLDs.
- The number of unsafe sacrificial nameservers identified, stratified by mitigation measure implemented.
- Trends in the above over time.

Recommendation 3: SSAC recommends ICANN org directly engage with registries and registrars to assist in mitigation and prevention efforts based on the insights gleaned as a result of implementing Recommendation 2.

ICANN org should work with registries and registrars to develop and implement effective strategies to address the identified issues in this report, such as:

- Educational outreach to registrars on best practices for preventing the use of unsafe sacrificial nameservers.
- Collaboration on technical solutions to identify and remediate unsafe sacrificial nameservers.

ICANN org should maintain regular communication channels with registries and registrars to share insights, gather feedback on mitigation efforts, and assess progress.

9 Acknowledgements, Statements of Interest, and Withdrawals

In the interest of transparency, these sections provide the reader with information about aspects of the SSAC process. The Acknowledgements section lists the SSAC members, outside experts, and ICANN staff who co-authored or contributed directly to this particular documentor who provided reviews. The Disclosures of Interest section points to the biographies of all SSAC members, which disclose any interests that might represent a conflict—real, apparent, or potential—with a member's participation in the preparation of this report. The Withdrawals section identifies individuals who have recused themselves from the discussion of the topic with which this report is concerned. Except for members listed in the Withdrawals section, this document has the consensus approval of all of the members of SSAC.

9.1 Acknowledgements

The committee wishes to thank the following SSAC members and invited guests for their time, contributions, and review in producing this report.

SSAC Members
Maarten Aertsen
Gautam Akiwate
Tim April
Jeffrey Bedser
kc claffy
James Galvin
Matthias Hudobnik
Warren Kumari
Rod Rasmussen
Matt Thomas
Peter Thomassen

Invited Guests
Duane Wessels
Jody Kolker

ICANN Staff
Danielle Rutherford (editor)
Gavin Brown
Kathy Schnitt
Steve Sheng
Moses Baguma

9.2 Disclosures of Interest

SSAC member biographical information and Disclosures of Interest are available at: https://www.icann.org/en/ssac/members

9.3 Withdrawals

There were no withdrawals.