Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG DNS Abuse Prevention, Remediation, and Mitigation Practices for Registrars and Registries

January 2024

The reference URL for this document:
http://www.m3aawg.org/DNSAbusePreventionRegReg2024

Preface

This document is intended to provide concrete best practices for preventing or mitigating malicious or compromised domains at the registry or registrar level. Other DNS security-oriented publications have focused on defining DNS abuse and how to report it to the appropriate entities. ICANN has included typical and best practices for registrars in presentations,[1] but has not formalized these recommendations. A fundamental gap within the DNS community exists for how registries and registrars can best operationally effectuate anti-abuse mechanisms specific to malicious or compromised domains. M³AAWG hopes this document will help inform relevant DNS stakeholders and promote a safer and more secure DNS ecosystem.

[1] L. Kapin, G. Mounier and G. Andrews, "Current Concerns and Issues Regarding DNS Abuse (PSWG)," 15 10 2019. https://meetings.icann.org/sites/default/files/dns_abuse_webinar_slide_deck.pdf

Table of Contents

Preface 1
Introduction 3
- Intended Use and Audience 3
- Definitions 3
- Guardrails for Registries and Registrars 4

DNS Abuse Security Threat Types 4
- Malware 4
- Botnets 5
- Phishing 5
- Pharming 5
- Spam 5
- Other Security Threats 5

Anti-Abuse Techniques for Registrars and Registries 6
- Prevention 6
- Mitigation and Remediation 16
- Other Considerations 20
- Sinkholing 20
- Contractual Obligations and Law Enforcement Requests 21
- Evidentiary Evaluation of RBLs, Abuse Reports, and Trusted Notifiers 21
- Contractual Tools to Reduce Residual Risk and Harm 22
- Final Disposition 23

Conclusion 24

Introduction

The purpose of this document is to collect and curate existing industry good practices that focus on preventing, mitigating, and remediating DNS abuse. Per the definition in ICANN contracts, DNS abuse is generally constrained to four types:

- Malware distribution
- Botnet command and control
- Phishing
- Pharming

Note that these contractual-based definitions may change in the future, and this document should apply to those and other abuses not formally covered by ICANN contracts that contracted parties deal with on their own recognizance. Spam, when used as a delivery mechanism for another type of abuse, is also included. This document presents relevant techniques for each type of DNS abuse within an operational context for registrars and registries. Since registries and registrars have a limited set of tools and actions they can take against DNS abuse, it is imperative that those controls be properly utilized to achieve maximum efficacy. This document is intended to convey how to best apply those tools and actions as well as other relevant industry security standards.

Intended Use and Audience

This report is intended for audiences across registries, registrars, cybersecurity industries, law enforcement, and the broader internet community. This report provides a suite of security practices to help form a defense-in-depth approach to addressing DNS abuse in a sustainable, replicable, and industry-wide manner. It does not concern itself with ICANN contracts or potential modifications.

This document is not intended to provide legal advice or to restrict court orders. Nor is the information stated herein intended to provide legal advice as to any matter and cannot substitute for advice and counsel from a properly qualified and licensed attorney. Within the context of addressing DNS abuse threats, registries and registrars must comply with the requirements of their contracts with ICANN.

This document is not focused on DNS abuse detection or evidentiary collection and evaluation. Those topics are well documented in ICANN's SAC115 report,[2] in "Internet & Jurisdiction – Domains & Jurisdiction Program,"[3] and in some of FIRST's publications.[4]

Definitions

The following techniques fall into two broad types depending on whether their primary effect occurs before or after the abuse has occurred. In some cases, such as account monitoring, this may be an artificial distinction, as a technique may have effects across multiple parts of the abuse timeline. In these cases, the techniques have been listed in the first step in which they are effective.

> **Prevention** techniques focus on miscreant actions before abuse. These include methods to prevent miscreants from creating accounts, registering domains, hijacking domains, and

[2] ICANN Security and Stability Advisory Committee (SSAC), "SAC 115: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS," 19 03 2021. https://www.icann.org/en/system/files/files/sac-115-en.pdf

[3] Internet & Jurisdiction Policy Network, "Domains & Jurisdiction Program: Operational Approaches Norms, Criteria, Mechanisms," 04 2019. https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf

[4] Forum of Incident Response and Security Teams (FIRST), DNS Abuse Techniques Matrix. https://www.first.org/global/sigs/dns/DNS-Abuse-Techniques-Matrix_v1.1.pdf

misusing domains. Even when they are not 100% effective, preventative techniques help discourage miscreants by driving up costs.

Mitigation techniques focus on decreasing the impact of abuse. These include methods to decrease the severity of the harms and minimize the damage associated with the abuse.

Remediation techniques focus on actions taken to restore, reverse or stop the impact of abuse. These include methods to eradicate or correct actions taken by miscreants that are associated with the abuse.

Guardrails for Registries and Registrars

Responses to DNS abuse must be proportional to the harm caused by the abuse. Registrars and registries have limited options to react to DNS abuse. Modifications to the DNS have global impact and may have unanticipated effects on innocent and reputable third parties, such as dependent domains, hosting services, and other service providers (e.g., URL shorteners). Clear evidentiary standards and escalation policies should be established before registries or registrars act. ICANN's "The value of assessing collateral damage before requesting a domain seizure"[5] advises consideration of the effects on innocent third parties before taking action.

It is critical to understand the nature and context of the threat before acting. A domain's registrant may not be able to immediately and readily remove malicious web content associated with a domain. In these circumstances, acting against a domain risks disproportionate harm to a potentially innocent registrant and collateral damage to other users without significantly disrupting the abusive activity. Understanding the nature of the threat and potential collateral damage will enable the registry or registrar to tailor its actions to maximize the effectiveness of their actions while minimizing negative ramifications.

DNS Abuse Security Threat Types

The following malicious activity types are enumerated for gTLD operators in Specification 11 (3)(b) of ICANN's model contract for registries.[6] They consist of malware, botnets, phishing, pharming, and other types of security threats. Understanding the purpose and enabling infrastructure of a security threat will help identify the appropriate and proportional actions that can be taken by a registry or registrar to counter that threat. General descriptions[7] of the abuses are listed below with relevant resources for additional information.

Malware

Malware is software that acts against user intent by deliberately damaging systems, disrupting access, stealing information, or otherwise creating harm. Examples include ransomware, spyware, and viruses. Malware may be delivered to a system via means such as email attachments, website downloads (with or without user knowledge), or unauthorized access. Malware is best prevented by regular patching, system configuration, and security strategies such as zero trust, least privilege, and defense in depth.

---

[5] D. Piscatello, "The value of assessing collateral damage before requesting a domain seizure." https://www.icann.org/en/system/files/files/seizure-collateral-assess-24jan13-en.pdf

[6] Internet Corporation for Assigned Names and Numbers (ICANN), Advisory, New gTLD Registry Agreement Specification 11 (3)(b), 08 07 2017. https://www.icann.org/resources/pages/advisory-registry-agreement-spec-11-3b-2017-06-08-en

[7] Internet & Jurisdiction Policy Network, Domains & Jurisdiction "Program, Operational Approaches: Norms, Criteria, Mechanisms." 04 2019. https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf

Botnets

Botnets consist of compromised hosts ("bots") running malware that can conduct various distributed tasks such as distributed denial of service, sending spam email, fast fluxing hosting, and cryptomining. Instructions are given to the bots through command-and-control servers. Botnet software may contain static lists of command-and-control IP addresses or rendezvous domain names from which to download instructions. They may also make use of a domain generation algorithm to dynamically create lists of potential command-and-control domains to ensure the botmaster can regain control of his botnet if their primary C&C host is suspended or rendered unreachable. As a form of malware, botnet client software is prevented by measures similar to those mentioned for malware. Access to botnet C&C servers is best prevented by intrusion detection systems and network access controls.

Phishing

Phishing attempts to steal users' personal information, including login credentials, through fraudulent communications (e.g., emails and SMS) that often use deceptive domain names leading to lookalike websites resembling legitimate websites. Phishing is best prevented through the use of reputation blocklists, user education, and domain monitoring. Its effects can be mitigated with multifactor authentication and secure networking principles and policies (such as zero trust).[8]

Pharming

Pharming, like phishing, attempts to steal users' personal information, including login credentials. However, where phishing relies on non-technical means of deception, such as deceptive emails, pharming involves the modification of DNS entries, typically via hijacking or poisoning.[2] Pharming is best prevented by correct configurations and maintenance of DNS zones (e.g., avoiding lame delegation) and through the use of DNSSEC.

Spam

Unsolicited bulk messages are included in DNS abuse when used as a delivery mechanism for another type of abuse. From a DNS perspective, spam is best prevented by filtering with RPZ-based DNS firewalls or DNS-based blocklists, utilizing email authentication technologies that restrict senders (SPF), authenticate email content (DKIM), and provide policy and capture reports of abuse (DMARC). All of these email preventative measures are particularly important for domains that are not intended to be used for email.[9]

Other Security Threats

Other DNS-oriented security threats include DNS rebinding, stub resolver hijacking, DNS tunneling, and more. The practices in this document would indirectly create barriers to these threats by making domain registration by malicious actors more difficult and providing guidelines for disabling those domains based on policy decisions. FIRST's DNS Abuse SIG has published advice for incident responders on what kinds of organizations might be productively contacted at different incident response phases for different DNS abuse techniques.[4]

---

[8] Office of Management and Budget, Executive Office of the President, Memorandum for the Heads of Executive Departments and Agencies, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," 26 01 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[9] Anti-Phishing Working Group (APWG) Internet Policy Committee, "Anti-Phishing Best Practices Recommendations for Registrars," 10 2008. https://docs.apwg.org/reports/APWG_RegistrarBestPractices.pdf

Anti-Abuse Techniques for Registrars and Registries

Effective prevention, remediation, and mitigation strategies are needed to formulate a defense-in-depth approach to addressing DNS Abuse threats. Fighting DNS Abuse presents unique challenges for any organizations working to keep the Internet safe and secure. To limit the possibility of abuse, registry and registrar operators should use a variety of techniques pre- and post-abuse events.

There are several ways DNS abuse may arise. First, at an account level, miscreants may create registry or registrar accounts for the purpose of abuse or may compromise otherwise legitimate registry or registrar accounts. Compromise may occur by stealing credentials or social engineering of a registrar or registry customer service. Second, at a domain level, miscreants may create domains for the purposes of abuse, using accounts that they control. Miscreants may also "hijack" a legitimate domain, obtaining control over its configuration (or some part of it) through account compromise or through domain misconfiguration (e.g., lame delegation). Hijacking a domain allows the miscreant to redirect or control requests for the domain or its resources. Third, miscreants may compromise third-party services, such as web, mail, or DNS hosts.

Understanding whether abuse is caused by compromised accounts or hijacked domains helps to clarify the limits of a registry or registrar's remediation and mitigation capabilities and the importance of protecting the interests of legitimate registrants.

Prevention

Prevention techniques focus on prohibiting, deterring, and minimizing miscreant actions before abuse takes place. These include methods to prevent miscreants from:

- Creating fraudulent accounts
- Compromising existing accounts
- Registering domains
- Hijacking domains, and
- Misusing domains for abusive purposes

Prevention and early intervention strategies can significantly reduce the impact of DNS abuse. Below is a set of best practices that focus on frequently exploited or abused processes within the lifecycle of a domain name and the registry-registrar ecosystem.

Fraudulent Account Creation

Ensuring accurate registration data is critical to helping combat DNS abuse. Miscreants are unlikely to provide accurate registration details at account creation. Validating registration details makes spurious account creation more difficult, creating a barrier to abuse. In "SAC058: Report on Domain Name Registration Data Validation,"[10] ICANN SSAC identifies four types of validation for elements of the registration data: name, postal address, email address, and telephone numbers.

[10] ICANN Security and Stability Advisory Committee (SSAC), "SAC 058 SSAC Report on Domain Name Registration Data Validation," 27 03 2013. https://www.icann.org/en/system/files/files/sac-058-en.pdf

1. **Syntactic validation** refers to the assessment of data with the intent to ensure that they satisfy specified syntactic constraints, conform to specified data standards, and are transformed and formatted properly for their intended use.
2. **Operational validation** refers to the assessment of data for their intended use in their routine functions.
3. **Identity validation** refers to the assessment that the data correspond to the real-world identity of the entity.

The SSAC report finds that certain verification measures can be automated, some with only a small amount of investment, and that doing so improves the quality of registration data.

In addition, registration data is typically the only source for contact information available to DNS abuse reporters or to legal or law-enforcement personnel. Valid registration data is also important for informing legitimate registrants of the compromise of their accounts, domains, or services. The APWG's "Anti-Phishing Best Practices Recommendations for Registrars"[11] lists data that registrars should collect at registration for law enforcement notification.

NIST's SP 800-63A "Enrollment and Identity Proofing"[12] and 800-63B "Authentication and Lifecycle Management"[13] documents recommend particular types of account management and authentication processes. Accounts should be validated, e.g., requiring clicking on a confirmation email. Account creation should be examined for suspicious activity such as use of third-party or anonymizing VPNs, mismatched IP geolocation, use of free email accounts, or multiple account creation from an IP over a short duration.

With regards to registrar accounts, ICANN follows an established registrar accreditation process.[14] That accreditation process requires multiple steps such as reviewing financial considerations and governing policies, signing various agreements, and more. Official ICANN Registrar accreditation requires entering into the Registrar Accreditation Agreement with ICANN and paying the full accreditation fee for the first year of accreditation.

Upon receiving ICANN accreditation, registrars may become a registrar for top level domains offered by various registrars. Registry operators should clearly document[15] the authentication, authorization, and contractual relationship requirements for registrars. Registry operators should require each registrar to be authenticated before establishing an account. Registrars should recognize that they are similarly responsible for the actions of resellers, and should vet them accordingly. The registry, or a service provider on behalf of the registry, should contact the registrar to request documents as proof of the registrar's business and their authority to represent and act on behalf of the registrar. The registry should require:

---

[11] Anti-Phishing Working Group (APWG) Internet Policy Committee, "Anti-Phishing Best Practices Recommendations for Registrars," 10 2008. https://docs.apwg.org/reports/APWG_RegistrarBestPractices.pdf
[12] National Institute of Standards and Technology (NIST), "NIST Special Publication 800-63A: Digital Identity Guidelines Enrollment and Identity Proofing," 02 03 2020. https://doi.org/10.6028/NIST.SP.800-63a
[13] National Institute of Standards and Technology (NIST), "NIST Special Publication 800-63B: Digital Identity Guidelines Authentication and Lifecycle Management," 02 03 2020. https://doi.org/10.6028/NIST.SP.800-63b
[14] Internet Corporation for Assigned Names and Numbers (ICANN), "How to Become a Registrar." https://www.icann.org/resources/pages/accreditation-2012-02-25-en
[15] Verisign, "Become A Domain Name Registrar." https://www.verisign.com/en_US/channel-resources/become-a-registrar/verisign-domain-registrar/index.xhtml

1. Registrars to enter into a Registry-Registrar Agreement with the registry operator for each TLD
2. Copies of corporate formation documents to verify the legal entity with which the registry is entering into a contract, in which the corporate name used on all forms must match the legal name used for ICANN accreditation
3. Completion and return of the FCPA[16] form to certify that the registrar will comply with the applicable laws and requirements under the Foreign Corrupt Practices Act

Additional technical requirements may be required by the registry to ensure the registrar can demonstrate full and correct operation of client systems within the Operational Test and Evaluation (OT&E) environment before connecting to the Shared Registration System (SRS). Additional security requirements may be placed on SSL/TLS certificates used by the registrar to communicate with the SRS system.

Account and Service Protection

DNS abuse may occur due to registrant or registrar account compromises which allow miscreants to modify domains without the actual account-holder's consent. Registries and registrars should implement account protections, including strong password policies, multi-factor authentication, and other account protections (e.g., notifying previous contacts on attempts to change contact details, notifying registrants on logins from new devices or IP addresses). SAC074 offers best practices throughout the credential lifecycle.[17]

Multifactor authentication (MFA) is a technology that requires multiple methods of authentication from independent categories of credentials. Use of MFA technology can dramatically reduce the risk of successful account-oriented attacks. M^{3}AAWG's "Multifactor Authentication Recommendations"[18] provides a set of recommendations and considerations to optimally deploy and use MFA. M^{3}AAWG also provides a set of password recommendations for account providers as well as a few password practices to avoid.[19] Another M^{3}AAWG paper provides password manager recommendations.[20]

Additional registry-registrar protections could include stringent network access controls, such as providing a limited number of IP addresses through which the registrar can access the registry's system, and additional stringent security measures, such as client certificates, hardware tokens (e.g., FIDO), and so on.

In general, service providers such as registries and registrars must maintain constant vigilance to make sure their systems are not compromised or abused. M^{3}AAWG's

---

[16] Text of the U.S. Foreign Corrupt Practices Act available at https://www.justice.gov/criminal/criminal-fraud/foreign-corrupt-practices-act

[17] ICANN Security and Stability Advisory Committee (SSAC), "SAC 074: SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle," 03 11 2015. https://www.icann.org/en/system/files/files/sac-074-en.pdf

[18] Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG), "M^{3}AAWG Multifactor Authentication Recommendations," 02 2017. https://www.m3aawg.org/multifactor-authentication-bp

[19] Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG), "M^{3}AAWG Password Recommendations for Account Providers," 02 2017. https://www.m3aawg.org/password-recommendations-providers

[20] Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG), "M^{3}AAWG Password Managers Usage Recommendations," 03 2017. https://www.m3aawg.org/sites/default/files/m3aawg-password-managers-bps-2017-03.pdf

"Anti-Abuse Common Practices for Hosting and Cloud Service Providers"[21] presents a set of recommendations focused on preventing abuse. These include:

- Vetting customers before they cause problems
- Requiring customers to keep software updated
- Preventing abusers from becoming customers
- Training customer-facing staff in security awareness

Beyond these account protection mechanisms, the M[3]AAWG document details a set of technical best practices to help prevent abuse at the network edge. Some of these technical security mechanisms include deploying:

- Hardware-based intrusion detection systems and firewalls
- Software-based security scans
- Web application firewalls
- Tiered-rights allocation for valued customers

Communication

Registrars should communicate (or offer to communicate) with registrants about various account and domain events. These may include

- Account creation
- Changes to account credentials
- Changes to account details
- Domain registration
- Domain status changes
- Domain configuration or details changes (e.g., authoritative nameservers, authoritative nameserver glue records)
- Domain transfers

When possible, communication should take place across multiple channels, e.g., email and SMS messaging. Communications should provide clear instructions for what to do if the change was not initiated by the registrant. Registrars should follow the guidelines of SAC028,[22] including limiting customer information in the communication, avoiding hyperlinks, providing warnings about phishing, and using anti-spoofing measures (including Sender Policy Framework (SPF),[23], DomainKeys (DKIM),[24] and Domain-based Message Authentication, Reporting, and Conformance (DMARC).[25] These security and authentication

[21] Messaging, Malware and Mobile Anti-Abuse Working Group (M[3]AAWG) and the Internet Infrastructure Coalition, "M[3]AAWG Anti-Abuse Best Common Practices for Hosting and Cloud Service Providers," 03 2015. https://www.m3aawg.org/sites/default/files/document/M3AAWG_Hosting_Abuse_BCPs-2015-03.pdf

[22] ICANN Security and Stability Advisory Committee (SSAC), "SSAC Advisory on Registrar Impersonation Phishing Attacks," 05 2008. https://icann.org/committees/security/sac028.pdf

[23] S. Kitterman, "RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1," 04 2014. https://www.rfc-editor.org/rfc/rfc7208

[24] D. Crocker, T. Hansen and M. Kucherawy, "RFC 6376: DomainKeys Identified Mail (DKIM) Signatures," 09 2011. https://www.rfc-editor.org/rfc/rfc6376

[25] M. Kucherawy and E. Zwicky, "RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC)," 03 2015. https://datatracker.ietf.org/doc/html/rfc7489

mechanisms are also described in M[3]AAWG's "Email Authentication Recommended Best Practices."[26]

Registrars may also require additional confirmation before making some changes (or delaying implementing changes to allow registrants time to intervene). The registrant may be able to specify which changes require additional confirmation, or the registrar may require them based on specific aspects of the change (such as its severity) or suspicious circumstances (e.g., request from an IP geolocated outside the registrant's known country). SAC044 offers best monitoring practices for registrants.[27] Registrars should emphasize to registrants the need to exercise due care concerning the domains they register.

Registrants may request to update an email address. This change should require that they reauthenticate. An email should be sent to the new email address to confirm its functionality and allow its owner to verify consent to receive emails. Registrars should also attempt to send email to the previous email address concerning the change and to send messages via other available channels (e.g., text, app alerts). However, this may cause problems when the email address no longer is active or available, when the registrant no longer has access to the email, or when the registrant does not control the email address (possibly due to a malicious takeover). Emails should not contain personally identifiable information (e.g., new email address, exact geolocation, IP address) but may contain anonymized information (e.g., "a request was made to update the account email to a***b@c***d.com from a Macbook with an IP address in Wisconsin, US"). Emails should also provide a mechanism for appeal (e.g., "if you did not make this request, click here or call this number"). Confirmation may also be requested from the previous email address. However, because the registrant may not be able to confirm, a secondary method of confirmation (e.g., calling support, confirmation within a mobile app) should be requested.

Registry operators should provide a clear and direct mechanism for registrars to handle any type of communication request for technical troubleshooting, product/service inquiries, billing updates, and security concerns or incidents. Registry support should include a 24/7 service center, online support tools such as a product portal, and "push" delivery of alerts and notifications about product updates, new releases, and maintenance windows. One issue that can sometimes arise is the support for languages other than English (or whatever the registry's default language may be). We encourage registries to post when staff with non-default language skills may be available (e.g., "During 8AM-5PM Eastern time, we also have Spanish-speaking help desk staff available.").

Domain Registration and Payment Processing

There are numerous security strategies to help prevent ecommerce fraud. Common types of domain registration fraud include card testing fraud, generic online payment fraud, and account takeover fraud.[28]

---

[26] Messaging, Malware and Mobile Anti-Abuse Working Group (M[3]AAWG), "M[3]AAWG Email Authentication Recommended Best Practices," 09 2020. https://www.m3aawg.org/sites/default/files/m3aawg-email-authentication-recommended-best-practices-09-2020.pdf

[27] ICANN Security and Stability Advisory Committee (SSAC), "SAC 044: A Registrant's Guide to Protecting Domain Name Registration Accounts," 05 11 2010. https://www.icann.org/en/system/files/files/sac-044-en.pdf

[28] E. Dopson, "Ecommerce Fraud Prevention: Strategies to Protect Your Business Against Fraud," 27 05 2022. https://www.shopify.com/enterprise/ecommerce-fraud-prevention

Card testing fraud is a tactic scammers use to determine whether a stolen credit card works. Scammers often make a small, low-value purchase so the fraudulent transaction goes under the radar of the card holder. Once the card is verified, they go on to make more expensive purchases using the stolen card.

Online payment fraud happens when scammers steal another person's payment details and use them to make purchases.

Account takeover fraud happens when scammers break into a customer's online account and use stored payment cards to make fraudulent purchases.

To identify and detect fraudulent payments, registrars and registries should monitor for some common payment warning signals:

- High or aberrant volume orders
- Low value or small monetary charges
- Multiple different cards used for purchases
- Repeated declined transactions
- Unusual IP address locations
- Unexpected or anomalous billing address usage

Beyond the tactical operational strategies provided above, a more sustainable and repeatable ecommerce fraud prevention strategy and best practice should include:

- Manually reviewing risky orders
- Limiting order quantities
- Showing clear policies to the user
- Being vigilant around peak shopping seasons and any promotional periods
- Use verification software as well as IP fraud scoring tools
- Build and maintain block lists and ensure they are current and still relevant
- Being Payment Card Industry (PCI) compliant

Domains registered for abusive purposes are often paid for with stolen credit cards or via some other form of payment fraud. To minimize payment fraud, registrars should, when able, implement the best security practices as defined in the PCI Data Security Standard.[29] PCI Data Security Standard (DSS) compliance is important to organizations that accept payment cards or transmit, process, or store payment card data. The controls described in the PCI DSS reduce the risk of credit and debit card data loss. Becoming PCI compliant helps protect the organization should a data breach occur and cardholder data become exposed. Furthermore, failure to comply with PCI DSS may result in fines as well as terminating a business' ability to conduct e-commerce, accept payment cards, or accept online payments in the future.

[29] PCI Security Standards Council: Best Practices for Securing E-commerce Special Interest Group, "Best Practices for Securing E-commerce," 04 2017. https://listings.pcisecuritystandards.org/pdfs/best_practices_securing_ecommerce.pdf

Bulk Domain Registration

Accounts engaging in bulk domain registration should face greater scrutiny, as bulk registrations have been connected to malicious campaigns.[30] Spamhaus has noted that "Cybercriminals rely upon domain names that can be rapidly acquired, used in an attack, and abandoned before they can be traced."[31] Interisle observes that "Cheap domain names, accessible in bulk, contribute to a criminal marketplace in which small investments can yield extraordinary returns."[32] Interisle recommends:

- Requiring registrants to apply for bulk registration services
- Requiring that non-natural persons be disallowed from using redacted WHOIS/RDAP
- Publishing a list of validated bulk registrants
- Disallowing bulk registration of apparently algorithmically-generated names
- Disallowing the re-registration of any bulk-registered domain used in abuse

Discount Pricing and Promotions

Bad actors will naturally utilize service providers that offer free or heavily discounted services and products that facilitate their malicious infrastructure. This has been clearly documented in the Anti-Phishing Working Group's quarterly reports, in which free TLS certificate service providers enable a significant amount of phishing DNS threats.[33] Naturally, the attractive marketing concept of free or heavily discounted domain prices is also susceptible to abuse. M^{3}AAWG itself commented on this in "M^{3}AAWG Recommendations for Preserving Investments in New Generic Top-Level Domains (gTLDS)."[34]

Several researchers have argued that miscreants take advantage of low or promotional pricing among registrars.[35,36,37] Miscreants may also choose to use TLDs that offer lower pricing.[30] Registries and registrars alike should consider the ramifications of offering special pricing promotions and discounts. For example, besides attracting budget-conscious "bottom feeders," competing on price also limits revenue that may be needed to pay for anti-abuse services.

---

[30] A. Affinito, R. Sommese, G. Akiwate, S. Savage, K. Claffy, G. M. Voelker, A. Botta and M. Jonker, Domain Name Lifetimes: Baseline and Threats, *Proceedings of Network Traffic Measurement and Analysis Conference (TMA)*, 2022.

[31] D. Piscitello, "Weaponizing Domain Names: how bulk registration aids global spam campaigns," 31 03 2020. https://www.spamhaus.org/news/article/795/weaponizing-domain-names-how-bulk-registration-aids-global-spam-campaigns

[32] D. Piscitello and C. Strutt, "Criminal Abuse of Domain Names Bulk Registration and Contact Information Access," 17 10 2019. https://interisle.net/sub/CriminalDomainAbuse.pdf

[33] Anti-Phishing Working Group (APWG), "Phishing Activity Trends Report: 1st Quarter 2021," 08 06 2021. https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf

[34] Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG), "M^{3}AAWG Recommendations for Preserving Investments in New Generic Top-Level Domains (gTLDS)," 02 2018. https://www.m3aawg.org/sites/default/files/m3aawg-gtld-investments-2018-01.pdf

[35] European Commission, Directorate-General for Communications Networks, Content and Technology; Paulovics, Ivett; Duda, Andrzej; Korczynski, Maciej, "Study on Domain Name System (DNS) abuse," 2022. https://data.europa.eu/doi/10.2759/616244

[36] Y. Cheng, Y. Liu, L. Wang, Z. Zhang, T. Chai and Y. Du, "Evaluating the Effectiveness of Handling Abusive Domain Names by Internet Entities," *Electronics*, vol. 11, no. 8, p. 1172, 2022.

[37] G. Aaron, L. Chapin, D. Piscatello and C. Strutt, "Phishing Landscape 2020: A Study of the Scope and Distribution of Phishing," 13 10 2020. https://www.interisle.net/PhishingLandscape2020.pdf

Domain Security Mechanisms

Registrars should provide a lock service to registrants that requires an additional, preferably manual check before modifying the domain's configuration or transferring the domain.[38] Registrars should inform the registrant when the lock is removed along with instructions in case the change was accidental or malicious.

By default, the DNS does not provide adequate integrity checks. This makes various attacks on DNS queries and responses possible, such as modification of responses (man-in-the-middle) or cache poisoning. These attacks are used in pharming abuse. DNSSEC[39] provides cryptographic signatures for DNS data. Registrars and registries should use DNSSEC on their own service-related domains when possible and enable DNSSEC security mechanisms on the domains they sponsor. Registries should sign zones (TLDs) for which they provide authoritative service and allow registrars to configure DNSSEC-related records for sponsored domains when possible. Registrars should provide simple interfaces for registrants to enable DNSSEC on their registered domains when possible.

One source of domain hijacking is misconfiguration of DNS zone files, such as lame delegation of subdomains. Lame delegation[40,41] occurs when a DNS record in a domain's zone refers to a resource that should not be expected to provide a service for the domain, e.g., when a NS record refers to a nameserver that should not answer for the domain (often for a subdomain), potentially allowing a miscreant to configure the nameserver to return a response unintended by the domain's registrant. Similar scenarios occur for other types of records, e.g., A, AAAA, MX. Lame delegations are also the result of stale configurations (particularly out-of-domain dependencies on third-party domains that are allowed to lapse or cease operation).

Registrars seeking to delete domains should not rename dependent nameserver records to presumed non-existent, out-of-bailiwick domains. Registrars should either rename the nameserver to a non-resolvable domain, e.g., an as112.arpa subdomain, or maintain a sacrificial nameserver for this purpose.[42]

Registrars often act as authoritative DNS providers, bundling name server service with registrations. They should act to prevent or detect these misconfigurations where possible. When transferring a domain from another registrar, transferring DNS service from another provider, or transferring a domain among DNS provider service tiers, they should not blindly copy the zone contents but instead minimize the chances of creating lame delegation and other problems, e.g., by defaulting to a clean zone template, or by explaining to registrants that subdomains or IP addresses are hosted outside the provider's space. In addition, zones should be scanned for inconsistencies and repairs suggested. Web user

---

[38] S. Hollenbeck and M. Srivastava, NSI Registry Registrar Protocol (RRP) Version 1.1.0 § 6.1 Domain Status Code Description, 05 2000. https://www.rfc-editor.org/rfc/rfc2832.html#section-6.1

[39] S. Weiler and D. Blacka, "RFC 6840: Clarifications and Implementation Notes for DNS Security (DNSSEC)," 02 2013. https://www.rfc-editor.org/rfc/rfc6840

[40] D. Barr, "RFC 1912: Common DNS Operational and Configuration Errors," 02 1996. https://www.rfc-editor.org/rfc/rfc1912.html#section-2.8

[41] A. Romao, "RFC 1713: Tools for DNS debugging," 11 1994. https://datatracker.ietf.org/doc/html/rfc1713#section-2.3

[42] G. Akiwate, S. Savage, G. M. Voelker and K. Claffy, "Risky BIZness: Risks Derived from Registrar Name Management," *ACM Internet Measurement Conference (IMC '21)*, Virtual Event, 2021. https://cs.stanford.edu/~gakiwate/papers/risky_bizness_imc21.pdf

interfaces to configure domain DNS records should not allow inconsistent or incorrect records by default, though working in 'expert mode' with normal protection disabled may still make this possible.

Spam emails are considered DNS abuse when they are used to deliver other types of abuse, e.g., phishing emails and emails containing malware attachments. General spam (unsolicited commercial bulk email) is beyond the scope of this document, which is limited to DNS abuse. In order to mitigate these types of abuse, registrars should encourage the use of various spam prevention and reporting technologies, including Sender Policy Framework (SPF), DomainKeys (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC). This may include providing instructions for configuration and automatic configurations (e.g., "DKIM helper tools") where possible. This is particularly important for domains that are not intended to send email, in which case the registrar as authoritative DNS host should provide simple instructions or automatic wizards to configure relevant records.

Domains are frequently registered without an immediate intent to use them, or to use them only in a limited context.[43] These domains, often referred to as "parked domains," are typically not meant to either send or receive email. As previously mentioned, the suite of email-oriented DNS security mechanisms such as SPF, DKIM, and DMARC should be used to prevent email abuse on those domains. "M^{3}AAWG Protecting Parked Domains Best Common Practices"[44] provides a set of recommendations to deploy those security mechanisms. In addition, parking services should seek to use reputable advertising and hosting services, as parked domains have been associated with malicious behaviors.[45]

Domain Usage Monitoring

Actively and adequately monitoring large sets of domains for abusive behavior is difficult and may be impossible. It represents an undue burden on registries and registrars. Registrants may also perceive monitoring as an abuse of privacy and autonomy, even when the registrant is capable of deploying mechanisms such as Captcha to deter automated monitoring. Moreover, automated abuse detection systems are unreliable and incomplete. However, monitoring for specific misuses for limited sets of domains may be feasible. For example, if a botnet is known to use a particular port, web service endpoint, or DNS subdomain, then a potential command-and-control domain could be scanned for matching services. The APWG recommends that DNS fast fluxing be minimized or prohibited.

One of the most common sources of identifying DNS threats is Reputation Block Lists (RBLs). Registrars and registries should consider ingesting and monitoring these feeds for domains under their management either via bulk download or through some API-based

[43] J. Zirngibl, S. Deusch, P. Sattler, J. Aulbach, G. Carle and M. Jonker, "Domain Parking: Largely Present, Rarely Considered!," in *Proc. of Network Traffic Measurement and Analysis Conference (TMA '22)*, 2022. https://www.net.in.tum.de/fileadmin/bibtex/publications/papers/zirngibl2022prevalenceofparking.pdf

[44] Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG), "M^{3}AAWG Protecting Parked Domains Best Common Practices," 12 2015. https://www.m3aawg.org/sites/default/files/m3aawg_parked_domains_bp-2015-12.pdf

[45] T. Vissers, W. Joosen and N. Nikiforakis, "Parking Sensors: Analyzing and Detecting Parked Domains," *NDSS*, San Diego, 2015.

mechanism. ICANN's Domain Abuse Activity Reporting (DAAR) effort enumerates several RBL feeds[46] used by ICANN to measure DNS abuse rates.

Per ICANN's DAAR page, "The aggregated statistics and anonymized data collected by the DAAR system can serve as a platform for studying, reporting daily or historically the registration data, or the abuse activity by each registry. This aggregated data is currently pushed to the registries using ICANN's Service Level Agreement Monitoring (SLAM) system." ICANN's Monitoring API (MoSAPI)[47] allows registry operators to retrieve information collected by the SLAM system. This data may be useful for registry operators to better monitor and understand DNS abuse threats and rates. While this data is not yet available for registrars, they may wish to directly engage with the RBL providers to better monitor their domains under management.

Botnet Domain Registration or Resolution

Botnets and other malware require command-and-control servers to provide instructions for the bots. Bots request instructions from either a static list of domains or IPs, or a dynamic list of domains created by a domain generation algorithm (DGA), typically based on time intervals and possibly public sources of information. Security researchers study malware (e.g., by decompiling or otherwise reverse-engineering it) to discover the static lists or the DGA used by the malware. When domains are discovered, registrars and registries may block their registration or allow restricted registration, e.g., blocking resolution or increasing monitoring. Domains generated by time-based DGAs must be restricted during the interval in which the botnet would use them but may be released before and after the interval. However, depending on the implementation of the DGA, blocking or proactively registering those domains may not scale as the algorithm may generate tens or hundreds of thousands of DGA domains.

ICANN's Public Safety Working Group and the gTLD Registries Stakeholder Group's "Framework on Domain Generating Algorithms (DGAs) Associated with Malware and Botnets"[48] addresses the role of both registries and law enforcement in handling malware and botnet infrastructure using the DNS specifically because of illegitimately used DGAs. These actions broadly include reserving a domain name, creating a domain name, filing the appropriate Security Request Waiver (SRW) with ICANN, and general cooperation with law enforcement and appropriate parties. While these actions may be more specific to botnets, malware and DGA-oriented DNS threats, registry operators should always consider the broader "Framework for Registry Operators to Respond to Security Threats"[49] for additional preventative measures.

---

[46] Internet Corporation for Assigned Names and Numbers (ICANN), "Frequently Asked Questions: ICANN's Domain Abuse Activity Reporting (DAAR) Project," https://www.icann.org/octo-ssr/daar-faqs

[47] Internet Corporation for Assigned Names and Numbers (ICANN), "Monitoring System API Specification." https://www.icann.org/mosapi

[48] Governmental Advisory Committee Public Safety Working Group (PSWG); the Registries Stakeholder Group (RySG), "Framework on Domain Generating Algorithms (DGAs) Associated with Malware and Botnets," https://www.rysg.info/wp-content/uploads/assets/Framework-on-Domain-Generating-Algorithms-DGAs-Associated-with-Malware-and-Botnets.pdf

[49] Internet Corporation for Assigned Names and Numbers (ICANN), "Framework for Registry Operator to Respond to Security Threats," https://www.icann.org/resources/pages/framework-registry-operator-respond-security-threats-2017-10-20-en

Other Preventative Actions

The preventative measures and actions previously described are mainly focused on registries and registrars. However, it is important that registrants also be informed and well-educated on best practices to prevent abuse of their domain registrations. ICANN has curated a set of best practices for Securely Managing Domain Names[50] that registries and registrars should promote to registrants. The document sets out best security practices around passwords, contact information, phishing awareness, DNSSEC, and much more.

Registrars and registries should also monitor their own critical domains for signs of hijacking by checking for changes in their public DNS records and certificate transparency logs, and for signs of phishing by using DNS Twist[51] or brand monitoring services.[52]

Mitigation and Remediation

Mitigation techniques focus on decreasing the effectiveness or impact of DNS abuse. These include methods to decrease the severity of the harms and minimize the damage associated with the abuse. Remediation techniques focus on actions taken to restore, reverse, or stop the impact of abuse. These include methods to eradicate or correct actions taken by miscreants associated with the abuse.

On the modern internet, many intermediaries are present between users and malicious content. Users connect to the internet through internet service providers (ISPs). Content is hosted, potentially on a content platform, and possibly delivered by a content delivery network (CDN). The DNS and domain infrastructure, meanwhile, provide a user-friendly addressing namespace. The participants in this space include recursive DNS resolvers, authoritative DNS resolvers, domain registrants, registrars, resellers, registries, and regulators.[53]

[50] Internet Corporation for Assigned Names and Numbers (ICANN), "Securely Managing Your Domain Name." https://www.icann.org/resources/pages/securely-managing-domain-name-2020-08-26-en

[51] Dnstwist: Domain Name permutation engine for detecting homograph phishing attacks, typo squatting, and brand impersonation. https://github.com/elceef/dnstwist

[52] G. Akiwate, S. Raffaele, J. Mattijs, Z. Durumeric, K. Claffy, G. M. Voelker and S. Stefan, "Retroactive Identification of Targeted DNS Infrastructure Hijacking," *ACM Internet Measurement Conference (IMC '22)*, Nice, France, 2022.

[53] K. Drazek, "Ongoing Community Work to Mitigate Domain Name System Security Threats," Verisign blog post, 06 12 2021. https://blog.verisign.com/domain-names/ongoing-community-work-to-mitigate-domain-name-system-security-threats/

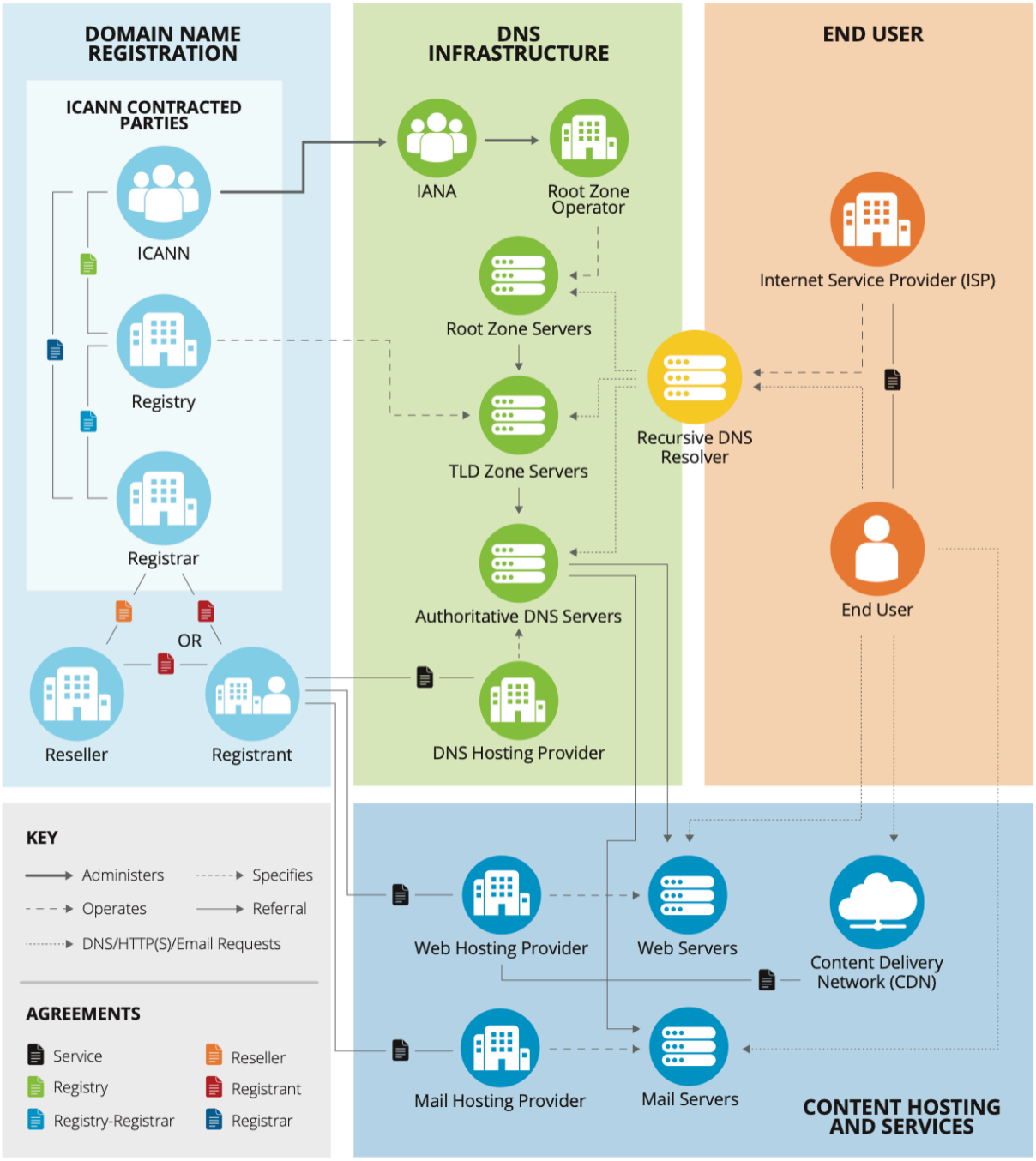

Figure 1: Conceptual Diagram of the DNS Ecosystem Portion Contractually Related to ICANN (image courtesy of Verisign and originally published in SSAC 115)

The appropriate actor to mitigate any particular abuse will vary with the type and severity of the abuse and must be assessed by criteria such as effectiveness, speed, precision, proportionality, and cost.[54]

For compromised accounts, registrars and registries should create policies and procedures concerning evidence to be collected and shared with law enforcement, how and when a domain will be taken down, and how and when it will be restored. The APWG provides a guide for website administrators who discover their sites have been hacked.[55] In the case of accounts and domains that appear to have been registered for malicious purposes, domains should be sinkholed. An educational landing page may be appropriate for phishing.[56]

Account-Based Remediation

Accounts believed to have been created for malicious purposes should be locked. However, there must be an appeals process in place that allows a legitimate registrant to assert that the account or domains were compromised or to provide further explanations. Where possible, account details should be used to prevent future account creation by the same miscreant.

Registrant accounts found to be suspicious or engaging in abuse should be restricted, reviewed, or face additional validations. These restrictions may include blocking activity (e.g., modifications to existing domains, new domain registrations, bulk domain registrations, transferring domains). Domains may face suspension or deletion after multiple or serious abuse incidents. Registrars should create a process that considers the seriousness and immediacy of abuse and consequences to the registrant (e.g., inability to correct a domain takeover) and that offers clear methods for reviewing, providing evidence, and appealing decisions.

Several factors may be considered in determining whether an account was compromised or was created for malicious purposes, including reports by account owners, changed behavior (e.g., logins from new locations, nearly simultaneous logins from different networks or locations).[57]

Third-Party Monitoring

Registrars and registries should monitor third-party feeds and accept reports from third parties. Third parties include reputation block lists (RBLs) operators, CERT organizations, cybersecurity organizations, law enforcement and government agencies, as well as individual customers and members of the public. Third-party feeds and reports have a variety of limitations.

1. Third-party feeds may not be designed for DNS abuse mitigation. For example, RBLs are typically designed as filters for corporate use, which means that false positives (i.e., incorrect reports of abuse) are of less concern than false negatives. However, registrars and registries must protect the interests of registrants, presume innocence, and minimize false positives.

[54] G. Bunton, "DNS Abuse Definition: Attributes of Mitigation," 24 08 2021. https://dnsabuseinstitute.org/dns-abuse-definition-attributes-of-mitigation/

[55] Anti-Phishing Working Group (APWG) Internet Policy Committee, "What to Do if Your Web Site Has Been Hacked by Phishers," 01 2009. https://docs.apwg.org/reports/APWG_WTD_HackedWebsite.pdf

[56] Anti-Phishing Working Group (APWG), "APWG/CMU-CyLab Phishing Education Landing Page Program." http://phish-education.apwg.org/r/about.html

[57] Messaging, Malware and Mobile Anti-Abuse Working Group (M^3AAWG), "M^3AAWG Compromised User ID Best Practices," 03 2018. http://www.m3aawg.org/CompromisedUserID

2. Third-party reports have incomplete coverage. For example, studies have shown that multiple RBLs have little overlap,[58] suggesting that they are incomplete and that RBLs use inconsistent criteria.
3. Third-party reports are delayed, which means they may report a problem after the condition has been mitigated (e.g., after the domain has been put on a hold status or otherwise removed from resolution, after offending content has been removed, or after the domain has expired). RBLs may copy from one another,[59] creating further difficulties in obtaining up-to-date data.
4. Third-party reports may relate to URLs rather than domains, which means a registrant may be unaware of a compromised web server or other resource.

Given these and other limitations (such as lack of technical and forensic expertise and unavailable records), registrars and registries must validate third-party reports to whatever extent is possible and take only actions that can be justified based on that validation. However, not all complaints may be amenable to validation. For example, CSAM may not legally be investigable by non-LEOs. Malware droppers may only offer malware when presented with expected user agents or referrers, or accessed from IP ranges targeted by the malware authors.

Registrars and registries may cooperate with third-party providers in several ways. They may submit reports of abuse, submit additional domains or data, and inform providers of abuse domains that have been successfully mitigated. Providing additional context, e.g., other domains registered by the same account, may enable third parties to scan and respond to abuse more quickly and accurately. That additional context, particularly in an environment where domain WHOIS data may be redacted, is often very important for identifying other related security threats. The APWG offers a list of organization types that may accept reports of abuse incidents.

Botnets and DGAs

Security researchers reverse engineer or decompile botnet malware to discover the malware's mechanisms for obtaining command-and-control domains and IP addresses. These may be static or may use a domain generation algorithm (DGA) based on time or external factors. Registries informed of unregistered DGA domain lists can reserve domains during their active time period, allow registration but block resolution, or create and sinkhole the domains, potentially enabling victim identification. Creating the domains may require additional permissions from regulators, e.g., ICANN.[60]

Registered domains must be treated more carefully, as innocent domains may be included in the static or DGA lists. For example, a malicious botnet creator could include valuable and high-traffic domains in a static list, potentially prompting service disruption by an unwitting registry. Registries should cooperate with registrars to determine the appropriate course of action, which may include additional monitoring, suspension, status locks, redirection to sinkholes, or transfer.

---

[58] M. Kührer, C. Rossow and T. Holz, "Paint it Black: Evaluating the Effectiveness of Malware Blacklists," *International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, 2014. https://christian-rossow.de/publications/blacklists-raid2014.pdf

[59] J. van der Velden, "Blacklist, do you copy? Characterizing information flow in public domain blacklists," *32th Twente Student Conference on IT*, Enschede, the Netherlands, 2020. https://essay.utwente.nl/80567/1/Velden_BA_EEMCS.pdf

[60] gTLD Registries Stakeholder Group (RySG), "Combatting DNS Abuse - Registry Operator Available Actions," 22 03 2021. https://www.rysg.info/wp-content/uploads/archive/DNS-Abuse-RY-Choice-of-Action-22-March-2021.pdf

Registries and registrars must exercise caution in how DGA domain resolution is blocked. Removing the domain from the zone and some error responses has been shown to create high retry rates[61] or other misbehaviors.[62] The best current practice is to return NOERROR or NXDOMAIN responses with TTL of at least one hour. REFUSED or SERVFAIL should not be returned, as these amplify query rates on some implementations.[63] However, as these misbehaviors vary with recursive DNS implementations, these recommendations should be amended so as to minimize load to the DNS infrastructure.

Other Considerations

DNS abuse abatement cannot be done primarily by registries and registrars. Internet intermediaries must work together to solve the problem holistically. DNS hosting providers, recursive DNS providers, content hosting providers, network operators, operating system creators, and more are also all valid points within the ecosystem to address DNS abuse in a more specific or tailored way. Specific actions taken by a subset of stakeholders may only result in temporary or partial prevention, remediation, or mitigation. Addressing the long-term operational concerns and the underlying compromised security vectors needs to be considered to prevent future and repeated DNS abuse incidents.

Sinkholing

Domains used for DNS abuse may be delegated to sinkholes, authoritative nameservers that provide innocuous responses and allow studies of the traffic sources. Sinkholed domains may return various status codes or false responses (e.g., unreachable IP addresses) for requests. The Shadowserver Foundation[64] is a well-known sinkhole provider that collects information about compromised or infected computers and the victims they affect globally. They report on these activities so that the victims can be remediated.

Registries or registrars that operate their own sinkhole nameservers should publicize those services by adding them to sources available to the security community.[65] This enables RBLs to mark sinkholed domains as mitigated. Similarly, registrars often place domains on special nameservers after expiration (e.g., expirenotification.tld or expiredns.tld) and for registrar parked domains unconfigured by the registrant (e.g., domainparkingserver.tld). These special nameservers should be publicized, at least to the security community, and should provide a website that explains their use and abuse contacts. This enables RBLs to remove these domains as active threats. There may be resistance to providing the details of this infrastructure due to the potential for adblocking. Registrars may be reluctant to provide details of this infrastructure due to the potential for these websites to be automatically blocked. Registrars often provide additional information on these pages ("this domain has expired," or "to configure this domain, log in to the admin portal," e.g.) as well as advertisements (including those for internal auctions and registrar services). This may require additional legal usage restrictions before allowing access to such a list.

---

[61] D. Wessels, W. Carroll and M. Thomas, RFC 9520: "Negative Caching of DNS Resolution Failures," IETF Datatracker, 12 22 2023. https://datatracker.ietf.org/doc/rfc9520/

[62] M. Larson and P. Barber, "RFC 4697: Observed DNS Resolution Misbehavior," 10 2006. https://datatracker.ietf.org/doc/html/rfc4697

[63] D. Wessels and M. Thomas, "Botnet Traffic Observed at Various Levels of the DNS Hierarchy," OARC 35 (Online), 07 05 2021. https://indico.dns-oarc.net/event/38/contributions/841/

[64] Shadow Server, "Data Collection," The Shadowserver Foundation. https://www.shadowserver.org/what-we-do/data-collection/

[65] abuse.ch, SinkDB. https://sinkdb.abuse.ch/

Contractual Obligations and Law Enforcement Requests

Within the context of addressing DNS abuse threats, registries and registrars must comply with ICANN's registry and registrar agreements requirements. Likewise, registries and registrars must comply with their local and regional legal and jurisdictional requirements.

Registration and use of domain names in the registry's TLD are subject to all applicable laws and regulations and all Registry Policies and ICANN requirements set out in the Registry Agreement and the Registrar Accreditation Agreement (RAA), including all ICANN Consensus Policies and Temporary Policies.

The RAA places several requirements on registrars with respect to abuse. Registrars are required to "take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse" (§ 3.18.1). "Well-founded" reports of illegal activity must be reviewed within 24 hours (§ 3.18.2). The registrar must publish its procedures for abuse reports (§ 3.18.3). If the registrar is found to have "with actual knowledge (or through gross negligence" permitted Illegal Activity in the registration or use of domain names or in the provision"[66] (§ 5.5.2.1.3), then the registrar agreement may be terminated. Advice for registrar abuse contact information is documented in SSAC038: Registrar Abuse Point of Contact.[67]

Registries and registrars should be prepared to receive legal requests related to DNS Abuse. ICANN has provided law enforcement a best practice on "Guidance for Preparing Domain Name Orders, Seizures & Takedowns"[68] that contain pertinent information that will likely be requested from the registry or registrar or specific actions they must perform. Additional information for investigations can be found in the NIST Guide to Integrating Forensic Techniques into Incident Response[69] as well as the U.S. Department of Justice's Investigations Involving the Internet and Computer Networks.[70]

Evidentiary Evaluation of RBLs, Abuse Reports, and Trusted Notifiers

As DNS abuse has evolved, there have been several efforts to measure[71] DNS abuse to provide accountability to registries and registrars. DNS abuse measurements and incident response are often based on domains listed on RBLs. As mentioned above, RBLs have several limitations due to their purpose as a protective measure rather than as an abuse metric. To use RBLs for abuse metrics, they must be filtered and validated to consider mitigation actions. For example, RBLs should break out domains that have been sinkholed or put into hold status, as these domains have been mitigated by the registry or registrar.

---

[66] Internet Corporation for Assigned Names and Numbers (ICANN), "Registrar Accreditation Agreement," 2013. https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#raa

[67] ICANN Security and Stability Advisory Committee (SSAC), "SAC 038: Registrar Abuse Point of Contact," 25 02 2009. https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-038-en.pdf

[68] Internet Corporation for Assigned Names and Numbers (ICANN), "Guidance for Preparing Domain Name Orders, Seizures & Takedowns." https://www.icann.org/en/system/files/files/guidance-domain-seizures-07mar12-en.pdf

[69] NIST Computer Security Resource Center, "NIST SP 800-86 Guide to Integrating Forensic Techiques into Incident Response," 08 2006. https://csrc.nist.gov/pubs/sp/800/86/final

[70] U.S. Department of Justice, "Investigations Involving the Internet and Computer Networks," 01 2007. https://nij.ojp.gov/library/publications/investigations-involving-internet-and-computer-networks

[71] Internet Corporation for Assigned Names and Numbers (ICANN), "Domain Abuse Activity Reporting." https://www.icann.org/octo-ssr/daar

Similarly, RBLs should be validated to show that domains were registered, in the zone, and not on an expiration nameserver at the time of reporting.

Registrars and registries that receive DNS abuse reports should evaluate the evidence presented to them and solicit the appropriate course of action. There are best practice papers from M[3]AAWG on reporting phishing URLs[72] as well as reporting abusive content.[73] Special prudence and care should be taken by all parties when receiving content such as CSAM, which has also been documented by M[3]AAWG with a set of best practices.[74] More broadly, the SAC115 as well as the Internet and Jurisdiction papers cited earlier[75,76] outline a series of best practices for evaluating DNS abuse evidence and the required evidentiary data needed for registrars and registries to act upon.

In some operational contexts, registrars and registries may wish to engage with a trusted notifier to combat specific types of DNS abuse. A trusted notifier is a designated entity for alerting registries about illegal activity, content, and/or DNS abuse associated with a domain name. Trusted notifiers enter into written agreements with registries or registrars, which outline the roles and responsibilities for handling reports of abuse. Trusted notifiers may see fit

- To include representations and warranties and/or indemnification provisions
- To incentivize expectations of transparency and due diligence
- To ensure that actions taken based on the notice of the trusted notifier – particularly in situations where the notice was to protect commercial interests – were appropriately and properly made.[77]

Trusted notifier arrangements are not one size fits all, and registries and registrars must have latitude to determine on a case-by-case basis which particular trusted notifier model is best.

Contractual Tools to Reduce Residual Risk and Harm

The best practices described in this report are meant to establish a series of defenses to provide a more comprehensive approach to DNS abuse. Unfortunately, DNS abuse may persist despite implementation of these practices, leaving a residual risk for registries and

[72] Messaging, Malware and Mobile Anti-Abuse Working Group (M[3]AAWG), "M[3]AAWG Best Practices for Reporting Phishing URLs," 12 2018. https://www.m3aawg.org/sites/default/files/m3aawg-reporting-phishing-urls-2018-12.pdf
[73] Messaging, Malware and Mobile Anti-Abuse Working Group (M[3]AAWG), "M[3]AAWG Feedback Reporting Recommendation," 02 2014. https://www.m3aawg.org/sites/default/files/document/M3AAWG_Feedback_Reporting_Recommendation_BP-2014-02.pdf
[74] Messaging, Malware and Mobile Anti-Abuse Working Group (M[3]AAWG), "M[3]AAWG Disposition of Child Sexual Abuse Materials Best Common Practices," revised 08 2021. https://www.m3aawg.org/sites/default/files/m3aawg-disposition-cam-2021-08.pdf
[75] ICANN Security and Stability Advisory Committee (SSAC), "SAC 115: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS," 19 03 2021. https://www.icann.org/en/system/files/files/sac-115-en.pdf
[76] Internet & Jurisdiction Policy Network, "Domains & Jurisdiction Program: Operational Approaches Norms, Criteria, Mechanisms," 04 2019. https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf
[77] gTLD Registries Stakeholder Group (RySG), "CPH Trusted Notifier Framework," 06 10 2021. https://www.rysg.info/wp-content/uploads/archive/Final-CPH-Notifier-Framework-6-October-2021.pdf

registrars to address. ICANN has provided both registries[78] and registrars[79] with contractual tools known as Security Risk Waivers (SRW) that can be used to address DNS abuse threats. The SRW service provides a process for ICANN-accredited registrars and for gTLD registries to inform ICANN of a present or imminent security incident and to request a contractual waiver for actions it might take, or has taken, to mitigate or eliminate an incident.

A registry may request this service when one or more of the following incidents occur:

- A malicious activity involving the DNS of such scale and severity that it threatens systematic security, stability, and resiliency of a gTLD or the DNS.
- An occurrence with the potential to cause a temporary or long-term failure of one or more of the critical functions of a gTLD registry as defined in ICANN's Registry Transition Process.
- An unauthorized disclosure, alteration, insertion, or destruction of registry data, or the unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with all applicable standards.
- A court order from a law enforcement agency with jurisdiction over the registry which requires the registry to take action due to a specific security threat.

A registrar may request this service when one or more of the following incidents occur:

- A malicious activity involving the DNS of such scale and severity that it threatens systematic security, stability, and resiliency of a gTLD or the DNS;
- An occurrence with the potential to cause a temporary or long-term threat impacting the registration of domain names at an ICANN-accredited registrar;
- A court order from a law enforcement agency with jurisdiction over the registrar which requires the registrar to take action due to a specific security threat.

Final Disposition

Final disposition techniques focus on actions taken after remediation or mitigation. These include a long-term solution for any actions or desired states of a domain name associated with the abuse. In many cases, especially those involving botnets or DGAs, the final disposition of abused domains remains problematic.

Domains that are used by botnets with static lists of command-and-control domains or other non-time-based DGAs may continue to be unsafe to release for registration or provisioning indefinitely (or pursuant to the longevity of the botnet), which prevents their use by legitimate registrants. Apart from the lost revenue of preventing registration or costs of maintaining registration, the list of prohibited domains may be quite large, imposing additional operating costs. Long-lived botnets such as Conficker[80] and Avalanche[81] illustrate that some domains may remain in a weaponized state for over a decade.

---

[78] Internet Corporation for Assigned Names and Numbers (ICANN), "Security Response Waiver (SRW) Requests for Registry Operators," https://www.icann.org/resources/pages/srw-registries-requests-en

[79] Internet Corporation for Assigned Names and Numbers (ICANN), "Security Response Waiver (SRW) Requests for Registrars," https://www.icann.org/resources/pages/srw-registrars-requests-en

[80] Wikipedia contributors, "Conficker," Wikipedia, The Free Encyclopedia, 28 09 2022. https://en.wikipedia.org/w/index.php?title=Conficker&oldid=1112854659

[81] Europol, 'Avalanche' network dismantled in international cyber operation, European Union Agency for Law Enforcement Cooperation, 01 12 2016. https://www.europol.europa.eu/media-press/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation

Understanding what long-term solutions exist for such scenarios needs to be addressed by ICANN, registries, and registrars. Tools such as ICANN's Security Risk Waivers are likely the best mechanism to address such scenarios. Other solutions may be necessary, such as allowing registration but with additional monitoring, or additional registrar-registrant assurances. The final disposition of abusive domains is likely dependent on the abusive context, the expected length of time the domain remains a threat, and the severity of the threat (e.g., the WannaCry kill switch domain[82]).

Conclusion

Addressing DNS Abuse is a complex global and internet-wide issue to address. While registries and registrars play a crucial role in combating DNS abuse, a more complete and sustainable solution must include all internet intermediaries working together to solve the problem holistically. The best practices described within this document aim to help inform registries and registrars about potential tools, policies, and other security mechanisms that can be used in a defense-in-depth strategy to help combat DNS abuse. While no one solution is a panacea, when these best practices are collectively utilized and deployed at scale across the DNS industry, the attack surface area of the DNS will be dramatically reduced.

As with all documents that we publish, please check the M[3]AAWG website (www.m3aawg.org) for updates.

[82] L. H. Newman, "How an Accidental 'Kill Switch' Slowed Friday's Massive Ransomware Attack," *Wired*, 13 05 2017. https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/