SAC097
SSAC Advisory Regarding the Centralized Zone Data Service (CZDS) and Registry Operator Monthly Activity Reports

An Advisory from the ICANN Security and Stability Advisory Committee (SSAC)
12 June 2017

Preface

This is an advisory to the ICANN Board from the ICANN Security and Stability Advisory Committee (SSAC) on the Centralized Zone Data Service (CZDS) and Registry Operator Monthly Activity Reports.

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), administrative 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.

Table of Contents

1 Introduction

Top level domain (TLD) zone files are vital resources for performing Domain Name System (DNS) research, security research, and anti-abuse operations. The stated goals of the Centralized Zone Data Service (CZDS) program were standardization and easy, reliable operations for participants who have a requirement to access these zone files. The CZDS has often succeeded in these goals. However, after three years of operation, community members have documented problems where the CZDS does not deliver on these objectives. Policy and process difficulties prevent subscribers from gaining and then maintaining reliable access to zone files. These problems affect the ability of subscribers to perform research and security functions that benefit the public interest. Furthermore, certain registry metrics related to zone files and WHOIS queries are being reported in an inconsistent fashion. This advisory details these problems and recommends improvements.

2 Background

Since 1999,[1] immediately after ICANN's founding in 1998, ICANN has required generic TLD (gTLD) registry operators to provide free daily copies of their zone files to interested parties. The DNS is public infrastructure, ICANN accredits gTLD registry operators, and zone files are essential for a variety of legitimate purposes that are in the public interest. Providing free gTLD zone file access is therefore in keeping with ICANN's mission.[2]

This access has historically been provided via zone file access agreements between the registry operators and their zone file subscribers. These agreements were executed individually, and then the gTLD operators provided the subscribers with credentials to download the zone files, usually via File Transfer Protocol (FTP).[3] Until 2013 the number of gTLDs was small, and so the signup and access process did not have to scale. For any gTLD delegated into the root zone prior to 2013, the zone file access agreement (including approved uses) is found in Appendix 3 of the Registry Agreement. For any gTLD delegated in or after 2013, the access requirements are found in Specification 4, Section 2 of the new gTLD Registry Agreement.[4]

The uses of TLD zone files include DNS research, security research, and anti-abuse operations. A TLD's zone file provides the only comprehensive list of domains that may resolve, and provides an incomplete but useful list of what domains exist in a TLD

[1] See https://archive.icann.org/en/nsi/nsi-registry-agreement-04nov99.htm paragraph 19.

[2] See https://www.icann.org/resources/pages/governance/bylaws-en/#article1

[3] For a typical example, see: https://www.verisign.com/en_US/channel-resources/domain-registry-products/zone-file/index.xhtml

[4] See https://www.icann.org/resources/pages/zfa-2013-06-28-en

registry.[5,6] The regular examination of zone files is an important way to understand what domains have been added and removed from the zone, and also leads to a better understanding of the DNS infrastructure being used to serve domains. This information is fundamental to DNS research, and is invaluable for identifying domains involved in malicious behavior.[7] For example, the examination of zone files allows researchers to understand what domains in one or more TLDs are delegated to particular name servers and are resolving to particular Internet Protocol (IP) addresses, providing a map of sorts of the DNS and allowing researchers to see associations and usage patterns. Researchers and operational security professionals regularly correlate and enrich zone file data with related data such as domain registration records. See Appendix B for illustrative examples. Entities also use zone files to find domain names that infringe upon intellectual property rights. As ICANN says on the CZDS help page, "… zone file access provides anticrime organizations, businesses, law enforcement and researchers with a means to download the entire zone file 'in bulk'. These organizations apply the bulk zone data in many ways, and among the most important of these applications are efforts to combat phishing, spam, brand and trademark infringement, and other malicious uses of domains."[8] If TLD zone files are not made available, it negatively impacts the research, security systems and activities that rely on the data.

Zone file subscriptions also provide important transparency. Zone files contain vital operational information including name server records that may be used by domain names in other TLDs, TTL (time-to-live) values, and DNS Security Extensions (DNSSEC) records. Subscribers can examine zone files for failures by registries to conform with relevant Requests for Comments (RFCs) and contractual requirements, such as those related to "controlled interruption" and the use of DNS wildcarding.[9,10]

ICANN's New gTLD program posed a challenge: how to manage zone file access subscriptions for more than 1,000 new gTLDs? The Zone File Access (ZFA) Advisory Group[11] was formed to examine the problem and provide community input during the

[5] Note that gTLD registries contain domain names that are registered but do not resolve. These include domains without name server records, and domains on ServerHold or ClientHold statuses. All domains in Redemption Grace Period (RGP) fall into the latter category; See https://www.icann.org/resources/pages/errp-2013-02-28-en

[6] gTLD registries generally do not provide complete lists of all of their domain registrations to third parties. Instead, zone files are used to fill that need. The only other way to obtain a list of domains in a TLD is to try to reconstruct a zone through passive DNS data. However, a passive DNS system relies on the traffic passing through its network of sensors, and will therefore always provide less accurate and incomplete data than a gTLD zone file for the types of information being discussed here.

[7] https://www.icann.org/resources/pages/zfa-2010-02-22-en

[8] See *CZDS Help*, https://czds.icann.org/en/help

[9] See *Oh, those wild and crazy new TLDs*, https://jl.ly/ICANN/newtldcrud.html and SAC041: "Recommendation to Prohibit Use of Redirection and Synthesized Responses by New TLDs" at https://www.icann.org/en/system/files/files/sac-041-en.pdf

[10] See the New gTLD Base Registry Agreement: Specification 6 paragraphs 1.1 and 2.1, at https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm

[11] See https://www.icann.org/resources/pages/zfa-2010-02-22-en

formulation of the new gTLD Applicant Guidebook.[12] From this effort, ICANN decided to create the CZDS. The CZDS was ICANN's solution "for scaling zone data provision as hundreds of new TLDs are added to the Internet."[13] All new gTLD registries were contractually required to participate in the CZDS program. For registries, "CZDS simplifies the process of entering into zone data contracts. Rather than creating and executing a contract for every request, registries can simply approve or deny requests with one click. Registries can save additional time by appointing ICANN to handle zone data file transfer (AXFR), formatting, and distribution to approved end-users instead of using internal resources."[14] For subscribers, the CZDS provides a central place to request zone files, to execute one standard access agreement, and to download the files themselves.

A beta version of CZDS was introduced in 2013, and the system went into production in 2014. A few of the legacy TLDs launched before 2014 have been made available via CZDS, while the rest of the legacy gTLD zone files remain available through their existing registry-specific processes.

This advisory was informed by several SSAC members who are users of the CZDS system. Other CZDS users were also surveyed, especially those within the operational security community.

3 Contractual and Administrative Issues

3.1 Subscribers Lose Access to Zone Files Regularly

Historically, once a subscriber received access to a zone file, that access was usually continuous and predictable—the access was not disabled unless there was some sort of problem (e.g., a violation of acceptable use, compromised passwords, etc.). However, under the CZDS, many subscribers' access is interrupted on a regular basis. This problem appears to be the result of an unfortunate implementation choice, and the situation can be improved with an alternate implementation.

Prior to 2013, gTLD access agreements stated: "This Agreement is effective for a period of three (3) months from the date of execution by [registry operator] (the "Initial Term"). Upon conclusion of the Initial Term, this Agreement will *automatically renew* [emphasis added] for successive three-month renewal terms (each a "Renewal Term") until terminated by either party".[15] Because of the automatic renewal, access to the zone file

[12] See the ZFA Advisory Group, https://www.icann.org/resources/pages/zfa-2010-02-22-en . This group noted that access to zone data is an effective and necessary tool for combating Domain Name System (DNS) abuse. Such was also noted in the New gTLD Applicant Guidebook.

[13] See CZDS, https://www.icann.org/resources/pages/czds-2014-03-03-en

[14] *ibid.*

[15] See for example https://www.icann.org/resources/unthemed-pages/appendix-03-2006-03-01-en and https://www.icann.org/resources/unthemed-pages/appendix-03-64-2006-12-08-en

was uninterrupted as long as either party did not explicitly terminate the agreement. The default was for continuing access without undue overhead for either party.

However, the new gTLD Base Registry Agreement is phrased differently. The new agreement states: "Term of Use. Registry Operator, through CZDA Provider, will provide each user with access to the zone file for a period of not less than three (3) months. Registry Operator will allow users to renew their Grant of Access."[16] So under the CZDS language, auto-renewal of access is apparently allowed, but is no longer a requirement.

It is unknown why the language changed from the old convention to the new. The change was not recommended by the ZFA Advisory Group and the access period was not discussed in its report. The revised language first appeared in the first draft of the new gTLD Registry Agreement[17].

The new language opened the door to an implementation that regularly interrupts subscribers' access. CZDS requires registry operators to set an expiration date (at least three months in length) for each subscriber, at which time zone file access expires and is *automatically terminated,* and the subscriber must apply for access anew. The current implementation of CZDS does not give registry operators an auto renewal option.

The result is that subscribers regularly lose access to some zone files, as frequently as every three months; they must reapply each time, and wait for the registry operator to approve access. The ensuing gaps in coverage can vary in length from one day to more than a month, according to the experiences of those surveyed. This situation makes zone file access unreliable and subject to unnecessary interruptions. The missing data introduces "blind spots" in security coverage and research projects, and the reliability of software - such as security and analytics applications - that relies upon zone files is reduced. Lastly, the introduced inefficiency creates additional work for both registry operators and subscribers.

Automatic termination and forced re-application, and a lack of auto-renewal, appears to be an implementation choice made when the CZDS was built. The SSAC suggests a different implementation choice: the CZDS can have automatic renewal as the default. This can provide convenience for both registry operators and subscribers, and more reliability for subscribers. CZDS could also allow registry operators to opt out of the default on a per-subscriber basis, forcing an explicit re-application at the end of the subscriber's term. In any case, it is important for registry operators to have the means to immediately terminate problematic subscribers who do not honor the terms of the zone file access agreement. This immediate termination functionality currently exists in CZDS and should be retained.

[16] See Specification 4, 2.1.6 at https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm
[17] See http://archive.icann.org/en/topics/new-gtlds/data-pub-24oct08-en.pdf

3.2 Compliance Complaints and Denials of Legitimate Subscription Requests

Some registry operators have denied subscription requests from parties with legitimate use cases, and have taken long periods of time to renew subscriptions. Complaints about zone file access have become the largest category of complaints about registries made to ICANN. Below we provide background in the hope that ICANN organization staff can find ways to ameliorate the situation.

There is a presumption that zone file access will be granted to those who execute the legal agreement. The new gTLD Base Registry Agreement states that "Registry Operator *will enter* into an agreement with any Internet user, which will allow such user to access an Internet host server or servers designated by Registry Operator and download zone file data", and that "Registry Operator *will permit* user to use the zone file for lawful purposes".[18] [Emphasis added.]

A registry operator may reject a request for access under certain conditions, namely that the user "does not provide correct or legitimate credentials," or where the registry operator reasonably believes the user will or has already violated these terms:

> "2.1.5 Use of Data by User. Registry Operator will permit user to use the zone file for lawful purposes; provided that (a) user takes all reasonable steps to protect against unauthorized access to and use and disclosure of the data and (b) under no circumstances will Registry Operator be required or permitted to allow user to use the data to, (i) allow, enable, or otherwise support the transmission by email, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations to entities other than user's own existing customers, or (ii) enable high volume, automated, electronic processes that send queries or data to the systems of Registry Operator or any ICANN-accredited registrar."[19]

While many registry operators are prompt and helpful, subscribers have encountered a variety of situations in which registry operators have denied access. This has occurred even when applicants identified themselves as legitimate security researchers. ICANN's Contractual Compliance Monthly Reports[20] provide a statistical view of the problem. These reports compile statistics about contractual compliance matters and not technical issues. The first available report is for July 2014 and the latest available report at the time of this writing was for March 2017. The reports reveal that *zone file access has been the largest category of complaints about registries*—33% of all total complaints over the covered period. The problem has been consistent—zone file access was the biggest

[18] See Specification 4, paragraphs 2.1.1 and 2.1.5 at https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm

[19] Specification 4 paragraph 2.1.5 of the new gTLD Base Registry Agreement.

[20] See the reports at https://features.icann.org/compliance/dashboard/report-list and the ICANN Contractual Compliance Monthly Dashboard Explanation, https://features.icann.org/compliance/dashboard/archives

registry complaint category in 25 of the 34 months for which reports are available, and in several months zone file access complaints constituted the majority of registry-related complaints. In total, zone file access complaints generated 2,082 compliance tickets in the period. The extracted statistics are presented in this paper's Appendix A.

The Contractual Compliance Monthly Reports note that the average complaint ticket, across all complaint categories, goes from opening to closure in 9 to 18 business days. As zone file subscribers rarely file a complaint immediately, it may take significantly longer. SSAC members have experienced cases that have taken as long as 38 business days from initial complaint to resolution.

Examples of problems that SSAC members and other legitimate researchers have encountered include:

- Some registry operators deny requests without giving a reason.
- A gTLD operator denied a request because the operator said he did not personally know the subscriber.
- A brand gTLD operator denied a request because it required users to sign a separate contractual agreement containing terms above and beyond the CZDS zone file access agreement. This extra contract required that the subscriber provide a list of all individuals at the subscriber who would have "access",[21] that the subscriber was to comply with additional security protocols, and more. A complaint to the ICANN Contractual Compliance Department was resolved satisfactorily and the applicant received access.
- A gTLD operator took advantage of the requirement for "correct or legitimate credentials" and required an applicant to provide official government documents showing the subscriber's address. After a complaint, the ICANN Contractual Compliance Department allowed the registry operator to define what the registry operator considered "correct or legitimate credentials".

Ultimately it falls to the ICANN Contractual Compliance Department to pursue legitimate complaints and bring non-compliant registry operators into compliance. SSAC encourages the ICANN Contractual Compliance Department and the ICANN Complaints Officer to reduce the number of zone file access complaints, and the amount of time required to resolve them.

[21] It was unclear to the subscriber what "access" meant in this context.

4 Monthly Registry Operator Reports

The ICANN community depends on accurate and standardized reporting as an input into policy development,[22] and such reporting is one way that ICANN delivers transparent and responsible DNS management.[23] For example, discussion of the requirements for the next round of gTLDs are underway,[24] and WHOIS query numbers are an input into policy discussions about registration data that are currently underway in the Generic Names Supporting Organization (GNSO).[25] The reporting of contractually mandated metrics about zone file access appears to be unstandardized and therefore inaccurate.

As part of its commitments, ICANN has always contractually required every registry operator to file monthly Activity Reports with ICANN.[26] The Activity Reports are collected and posted monthly on the ICANN Web site.[27] In the reports, registry operators are required to state how many active zone file access passwords they have granted.[28] Historically, registry operators had to grant an access password to every zone file subscriber, and the function of this statistic was to reveal how many zone file subscribers each gTLD had.

The CZDS tells each registry operator how many subscribers it has, and who the subscribers are. Some operators report the number of zone file subscribers they have granted in CZDS, and this is what we would expect to see reported. However, many operators are reporting that they have issued zero zone file access passwords, when in fact they have many zone file subscribers who are actively receiving zone files. Some registry operators have evidently decided to report "0" because subscribers access the CZDS and do not directly receive passwords from the registry operators, or are not accessing the registry's systems.[29] SSAC suggests that this distinction defeats the purpose of the contractual reporting requirement.

Whatever the genesis of the problem is, the result is inconsistent reporting among registry operators. The ICANN Contractual Compliance Department should provide clarity to gTLD registry operators about what they should report. SSAC suggests that registry operators should accurately report the number of zone file subscribers.

[22] For example see: https://gnso.icann.org/en/issues/dmpm-final-09oct15-en.pdf and https://www.icann.org/resources/pages/metrics-gdd-2015-01-30-en

[23] See paragraphs 3.1 and 3.2 of the ICANN Bylaws, https://www.icann.org/resources/pages/governance/bylaws-en/#article3

[24] See https://newgtlds.icann.org/en/reviews

[25] See https://gnso.icann.org/en/group-activities/active/rds

[26] In gTLDs launched prior to 2013 these provisions appear in varying places in the contracts. In the new gTLD Base Registry Agreement the monthly registry reports are detailed in Specification 3. See https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm

[27] See https://www.icann.org/resources/pages/registry-reports

[28] In the new gTLD Base Registry Agreement, see Specification 3, paragraph 2, at https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm

[29] See thread at: http://mm.icann.org/pipermail/gtld-tech/2014-March/thread.html#256

In a similar vein, SSAC observes that some new gTLD operators are under-reporting the number of web-based WHOIS queries they serve each month. The reason for this is unclear; it was not an issue with TLDs launched before 2014, and some new gTLD operators appear to be tracking and reporting this metric without issue.

Below are numbers from the December 2016 Activity Reports for the eight largest new gTLDs, and then several smaller, randomly selected TLDs. These tables illustrate the uneven manner in which new gTLD registry operators are reporting these statistics. It appears that different operators (and/or their back-end providers) may be interpreting the ZFA contractual requirement differently, or perhaps may not be logging or reporting the required metrics accurately. It seems unlikely that large gTLDs are receiving only one or two queries per month on their web-based WHOIS pages, especially while smaller TLDs report many more.

	zfa-passwords	**web-whois-queries**
.xyz	0	1
.top	0	97
.loan	0	2
.win	0	41
.wang	0	44
.club	0	10,728
.vip	773	125
.online	0	184

	zfa-passwords	**web-whois-queries**
.black	1,549	170
.lol	0	436,577,936
.blog	373	1,438
.technology	0	1,620
.realtor	303	291

5 Recommendations

Recommendation 1: The SSAC recommends that the ICANN Board suggest to ICANN Staff to consider revising the CZDS system to address the problem of subscriptions terminating automatically by default, for example by allowing subscriptions to automatically renew by default. This could include an option allowing a registry operator to depart from the default on a per-subscriber basis, thereby forcing the chosen subscriber to reapply at the end of the current term. The CZDS should continue to provide registry operators the ability to explicitly terminate a problematic subscriber's access at any time.

Recommendation 2: The SSAC recommends that the ICANN Board suggest to ICANN Staff to ensure that in subsequent rounds of new gTLDs, the CZDS subscription agreement conform to the changes executed as a result of implementing Recommendation 1.

Recommendation 3: The SSAC recommends that the ICANN Board suggest to ICANN Staff to seek ways to reduce the number of zone file access complaints, and seek ways to resolve complaints in a timely fashion.

Recommendation 4: The SSAC recommends that the ICANN Board suggest to ICANN Staff to ensure that zone file access and Web-based WHOIS query statistics are accurately and publicly reported, according to well-defined standards that can be uniformly complied with by all gTLD registry operators. The Zone File Access (ZFA) metric should be clarified as soon as practicable.

6 Acknowledgments, Disclosures of Interest, Dissents, and Withdrawals

In the interest of transparency, these sections provide the reader with information about four aspects of the SSAC process. The Acknowledgments section lists the SSAC members, outside experts, and ICANN staff who contributed directly to this particular document. 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 Dissents section provides a place for individual members to describe any disagreement that they may have with the content of this document or the process for preparing it. The Withdrawals section identifies individual members who have recused themselves from discussion of the topic with which this Report is concerned. Except for members listed in the Dissents and Withdrawals sections, this document has the consensus approval of all of the members of SSAC.

6.1 Acknowledgments

The committee wishes to thank the following SSAC members and external experts for their time, contributions, and review in producing this Advisory.

SSAC members

Greg Aaron
Benedict Addis
Jaap Akkerhuis
Jeff Bedser
Don Blumenthal
Ben Butler
KC Claffy
Jay Daley
James Galvin
Robert Guerra
Geoff Huston
Merike Kaeo
Mark Kosters
John Levine
Carlos Martinez
Danny McPherson
Rod Rasmussen

ICANN staff
David Conrad
Julie Hedlund
Andrew McConachie (editor)
Dave Piscitello
Kathy Schnitt
Steve Sheng

6.2 Disclosures of Interest

SSAC member biographical information and Disclosures of Interest are available at: https://www.icann.org/resources/pages/ssac-biographies-2017-06-14-en

6.3 Dissents

There were no dissents.

6.4 Withdrawals

There were no withdrawals.

Appendix A: Zone File Access Complaints

Source: ICANN Contractual Compliance Monthly Reports[30]

	Zone File Access (ZFA) Complaints	Registry Complaints, Total (all categories)	ZFA as % of total registry complaints	ZFA was largest category of registry complaints in the month
Mar-17	11	168	6.5%	
Feb-17	27	138	19.6%	
Jan-17	46	177	26.0%	X
Dec-16	36	119	30.3%	X
Nov-16	63	138	45.7%	X
Oct-16	56	124	45.2%	X
Sep-16	92	141	65.2%	X
Aug-16	141	196	71.9%	X
Jul-16	107	208	51.4%	X
Jun-16	65	105	61.9%	X
May-16	64	135	47.4%	X
Apr-16	39	100	39.0%	X
Mar-16	55	154	35.7%	X
Feb-16	171	541	31.6%	
Jan-16	180	270	66.7%	X
Dec-15	73	146	50.0%	X
Nov-15	22	241	9.1%	
Oct-15	37	166	22.3%	
Sep-15	67	220	30.5%	X
Aug-15	70	108	64.8%	X

[30] See https://features.icann.org/compliance/dashboard/archives

Jul-15	93	234	39.7%	X
Jun-15	26	141	18.4%	X
May-15	51	108	47.2%	X
Apr-15	48	153	31.4%	X
Mar-15	68	210	32.4%	X
Feb-15	76	199	38.2%	X
Jan-15	82	258	31.8%	X
Dec-14	43	164	26.2%	X
Nov-14	32	108	29.6%	X
Oct-14	40	420	9.5%	X
Sep-14	74	418	17.7%	
Aug-14	12	211	5.7%	
Jul-14	15	93	16.1%	
TOTAL	2,082	6,312	33.0%	

In the monthly Compliance dashboard statistics, there is a "Zone File Access" category. Sometimes, although rarely, a "Bulk ZFA" category will also appear containing an additional handful of complaints. We have totaled these two categories. The distinction between "Zone File Access" and "Bulk ZFA" may be immaterial, and the "Bulk ZFA" category contains far too few entries to account for complaints about zones available via CZDS.

Appendix B: Zone Files and Security

Security researchers use TLD zone data while investigating malicious activities and use of the DNS. The below list contains illustrative examples of security and DNS research that relied upon zone files, but is not meant to be exhaustive.

Center for Applied Internet Data Analysis, "Metadata Management Software Tools to Support Cybersecurity Research and Development of Sustainable Cyberinfrastructure (DatCat)." Accessed May 19, 2017, http://www.caida.org/funding/sdci-datcat/sdci-datcat_proposal.xml

Halvorson, Tristan, Matthew F. Der, Ian Foster, Stefan Savage, Lawrence K. Saul, and Geoffrey M. Voelker. "From. academy to. zone: An analysis of the new TLD land rush." In Proceedings of the 2015 ACM Conference on Internet Measurement Conference, pp. 381-394. ACM, 2015.

Hao, Shuang, Nick Feamster, and Ramakant Pandrangi. "Monitoring the initial DNS behavior of malicious domains." In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference, pp. 269-278. ACM, 2011.

Hao, Shuang, Matthew Thomas, Vern Paxson, Nick Feamster, Christian Kreibich, Chris Grier, and Scott Hollenbeck. "Understanding the domain registration behavior of spammers." In Proceedings of the 2013 conference on Internet measurement conference, pp. 63-76. ACM, 2013.

Liu, He, Kirill Levchenko, Márk Félegyházi, Christian Kreibich, Gregor Maier, Geoffrey M. Voelker, and Stefan Savage. "On the Effects of Registrar-level Intervention." In LEET. 2011.

McGrath, Kevin D., and Minaxi Gupta. 2007. "Behind Phishing: An Examination of Phisher Modi Operandi." LEET 8 (2008): 4.

M3AAWG (Message, Mobile and Malware Anti-Abuse Working Group). "Comments on the Expert Working Group Initial Report."
https://www.m3aawg.org/sites/default/files/document/m3aawg_icann_ewg_initial_report-2013-08_0.pdf

NORC at the University of Chicago. 2014. "WHOIS Accuracy Reporting System Pilot Report." Accessed May 19, 2017, http://whois.icann.org/sites/default/files/files/ars-pilot-23dec14-en.pdf

Pitsillidis, Andreas, Chris Kanich, Geoffrey M. Voelker, Kirill Levchenko, and Stefan Savage. "Taster's choice: a comparative analysis of spam feeds." In Proceedings of the 2012 ACM conference on Internet measurement conference, pp. 427-440. ACM, 2012.