SAC 056

SSAC Advisory on Impacts of Content Blocking via the Domain Name System

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

09 October 2012

Preface

This is an Advisory of the Security and Stability Advisory Committee (SSAC). The SSAC advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., matters pertaining to the correct and reliable operation of the root name system), administrative matters (e.g., matters pertaining to address allocation and Internet number assignment), and registration matters (e.g., matters pertaining to registry and registrar services). The 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 official authority to regulate, enforce or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

The contributors to this Advisory, reference to the committee members' biographies and statements of interest, and committee members' objections to the findings or recommendations in this Advisory, are at end of this Advisory.

Table of Contents

1. Executive Summary

The use of Domain Name System (DNS) blocking to limit access to resources on the Internet has become a topic of interest in numerous Internet governance venues. Several governments around the world, whether by law, treaty, court order, law enforcement action, or other actions or agreements, have either implemented DNS blocking or are actively considering doing so. However, due to the Internet's architecture, blocking by domain name can be easily bypassed by end users and is thus likely to be largely ineffective in the long term and fraught with unanticipated consequences in the near term. In addition, DNS blocking can present conflicts with the adoption of DNS Security Extensions (DNSSEC) and could promote balkanization of the Internet into a country-by-country view of the Internet's name space.

This document is limited to an exploration of technical impacts related to DNS blocking including:

- Domain blocking via:
  - A registry or registrar;
  - An authoritative server;
  - In a recursive resolver via redirection, non-existent domain name, a query refused response code, other response codes, or a query non-response.
- DNS blocking in recursive resolvers and conflicts with DNSSEC;
- Conditioning end users toward more end-to-end encryption;
- Over-blocking;
- Typographical errors;
- Routing DNS traffic away from a nation that imposes blocking;
- Impacts of users switching resolvers; and
- Breaking Content Distribution Network (CDN) localization if users switch resolvers.

While there are also non-technical issues such as limitations on freedom of expression, these issues will not be addressed in this document. The Internet community, governments, and others should ensure that they understand and carefully consider all of the issues related to DNS blocking, both technical and non-technical.

2. Introduction

This document builds upon "SAC050: DNS Blocking: Benefits Versus Harms – An Advisory from the Security and Stability Advisory Committee," which may be of interest to readers of this document.[1]

In 2011 and 2012 several governments proposed or established formal guidelines, laws, court orders, or law enforcement actions related to DNS blocking, DNS filtering, and/or domain name seizure.[2] In some cases the objective of these activities was to develop new legislation aimed at controlling Internet usage, while in other cases courts or law enforcement agencies have relied on DNS blocking or domain name seizures as a mechanism to block access to certain Internet sites or addresses.[3,4,5,6]

This document examines the technical impacts of various types of DNS blocking that have been implemented or proposed. The aim of this paper is to inform the Internet community, policymakers, government officials, and others of the high-level technical implications of using the DNS blocking to control access to Internet resources.[7]

3. DNS Blocking: Benefits Versus Harms

The major conclusions of SAC050 are:

> "Domain name or Internet Protocol (IP)-address based filtering (or preventing access to for example web content that infects computers with viruses or are deemed an inappropriate use of employer resources) may be viewed by some organizations as a

---

[1] See "SAC050: DNS Blocking: Benefits Versus Harms – An Advisory from the Security and Stability Advisory Committee on Blocking of Top Level Domains at the Domain Name System," Internet Corporation for Assigned Names and Numbers (ICANN), Security and Stability Advisory Committee, 14 June 2011, http://www.icann.org/en/groups/ssac/documents/sac-050-en.pdf.

[2] See H.R. 3261 (Stop Online Piracy Act), United States House of Representatives, 112th Congress, version dated December 16, 2011 and Estonian law regarding blocking of illegal gambling sites, https://www.riigiteataja.ee/akt/125042012010.

[3] See OpenNet Initiative, http://opennet.net/youtube-censored-a-recent-history.

[4] See http://arstechnica.com/tech-policy/2011/01/amidst-chaos-and-riots-egypt-turns-off-the-internet/.

[5] See http://www.dhs.gov/ynews/releases/pr_1297804574965.shtm.

[6] See http://www.telegraph.co.uk/technology/internet/9084540/Serious-Organised-Crime-Agency-closes-down-rnbxclusive.com-filesharing-website.html.

[7] For a description of the DNS see http://queue.acm.org/detail.cfm?id=1242499

> natural extension of historical polices that block people within those organizations from incurring telephone toll charges.
> …
> Regardless of the mechanism used, organizations that implement blocking should apply these principles:
>
> 1. The organization imposes a policy on a network and its users over which it exercises administrative control (i.e., it is the administrator of a policy domain).
> 2. The organization determines that the policy is beneficial to its interests and the interests of its users.
> 3. The organization implements the policy using a technique that is least disruptive to its network operations and users, unless regulations specify certain techniques.
> 4. The organization makes a concerted effort to do no harm to networks or users outside its policy domain as a consequence of implementing the policy.
>
> When these principles are not applied, blocking using the DNS can cause collateral damage or unintended consequences with limited or no remedies available to affected parties."

To expand on the conclusions of SAC050, both due consideration and overall Internet stability require that any DNS blocking policy or action be fully disclosed to affected parties including end users, service providers, and application designers. DNS blocking in the absence of such disclosure will lead to unnecessary troubleshooting activities as well as adaptive and perhaps even unintended bypass activities by network operators and end users. Such disclosures should include motivations, intended effects, and expected side effects. Absent such transparency, DNS blocking can be misdiagnosed as an outage or as a malicious attack and may result in responses from end users, network administrators, service providers, etc. that attempt to mitigate the damage.

This potential for misdiagnosis and the inevitable search for workarounds can result in collateral damage or unintended consequences. Independent public review was also called for in the Office of the United Nations High Commissioner for Human Rights Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression which states:

> "31. […] Thirdly, even where justification is provided, blocking measures constitute an unnecessary or disproportionate means to achieve the purported aim, as they are often not sufficiently targeted and render a wide range of content inaccessible beyond that which has been deemed illegal. Lastly, content is frequently blocked without the intervention of or possibility for review by a

judicial or independent body."[8]

An exploration of the types and impacts of DNS blocking is the subject of the remainder of this document.

4. Blocking Content in the Context of the Internet's Architecture

One of the fundamental tenets of the Internet architecture is its 'end-to-end' abstraction, which minimizes the need for intelligence in the core (middle) of the network but embraces intelligence at the edge (on individual hosts). This architecture has enabled a tremendous range and depth of innovation by, for example, allowing a developer at one edge of the network to deploy a new application on a host and an end user at the other edge to install a corresponding client enabling new forms of communication, without requiring any special permission or controls within any other part of the network.

Content blocking via the Domain Name System has been implemented sometimes in the Internet "core" and sometimes at the Internet "edge." Connections between an access provider and its traffic sources and traffic sinks are called "edge." Connections inside or between operators are called "core." Examples of edge-based blocking would include black lists in web browsers and filtering IP traffic at one end of a connection. If edge-style blocking were applied in the network core, affected end users could bypass the blockage by changing DNS providers or by using VPNs, proxies, or plugins. Edge-style DNS blocking will only be effective where policy-based filtering is present in all possible paths between affected end users and any networks with which they might exchange packets. Examples of such topologies include national and enterprise firewalls.

As a side effect of this architecture, efforts to block traffic, whether by domain name (such as example.com) or by IP address (such as 192.0.2.117), at any point in a network other than at the edge *can be circumvented*, for example by the use of a virtual private network (VPN).[9] VPNs and similar methods are readily available and easy to adopt by even relatively unsophisticated users. Even in cases where complete administrative and operational control over Internet access networks is possible (such as within an Internet Service Provider (ISP) or at some Internet exchange points[10]), end users have still been able to access prohibited

[8] Frank La Rue, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," A.HRC.17.27., http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

[9] See http://www.prlog.org/11725655-how-to-bypass-blocked-sites-with-vpn-account.html or http://vpn-account.com/bypassblockedsites.html.

[10] See http://en.wikipedia.org/wiki/Internet_exchange_point.

content.[11]

The common characteristic of these more successful types of filtering is that the end user and her network operator agree explicitly or implicitly to what is filtered and how the blocking of content is done. In this case, the end user sees DNS blocking as a valuable service.

5. Types of DNS Blocking Observed or Proposed

Various methods of blocking DNS have been proposed or implemented in recent years. Some methods pose greater technical concerns than others. A non-exhaustive list follows:

1. **Domain Seizure via a Registry or Registrar**: This method removes DNS data from its source via a DNS registry or registrar acting as the registry's agent. A registry is the entity responsible for creating the authoritative database of DNS data including the domains to be blocked. An example of this method would be a government serving a domain name "take-down" order to a registrar or registry who is lawfully subject to such an order. A registry or registrar's response to such a take-down demand depends on the specifics of the order. Options include removing a domain name from the zone (known as a "domain hold" when the registration data for that domain is maintained) thereby preventing end users from resolving a domain name associated with a specific site, or mapping the domain name to a different nameserver that will then redirect users to a web page displaying additional information such as law enforcement notices of the take-down. In the "domain hold" situation, once the domain's DNS record's "Time To Live" (TTL) settings expire, usually over the course of a few hours or days, the domain becomes unresolvable globally. This means that when a user types in that domain name, a "domain does not exist" response will be returned. If the correct domain names are seized, there are no direct negative technical implications unique to the "domain hold" method. Indirect negative technical implications can include failures in distant services if other domains depend for name service or e-mail service or web service on the domain subject to such a "hold". In either the "domain hold" or name server change method, the registrar or registry must also update or remove any DNSSEC data for the targeted domain. Failure to do so would cause DNSSEC-compliant applications to detect invalid data in responses to DNS queries that would prevent any communication at all, even to explain to users why the domain was no longer available.
2. **Domain Blocking in an Authoritative Server**: This type of blocking, implemented by the operator of the authoritative name servers of the affected domain name, bypasses the registry and possibly also the

[11] See http://www.foreignpolicy.com/articles/2011/01/26/can_governments_really_block_twitter.

registrar, and targets directly the mechanism by which the domain name is made available on the Internet. Once a registrant has obtained and correctly configured a domain name, the registry generates the DNS data and publishes that data to a set of "authoritative servers." In many cases the registrar operates these authoritative servers, but this is not a requirement, nor is it a requirement that all of a domain's authoritative servers be operated by the same entity. Regardless of who operates the authoritative servers, the servers are a publishing mechanism and are therefore a point at which DNS blocking can be implemented. An example of this form of blocking would be a government serving a domain name take-down order to an operator of a DNS server that is authoritative for the targeted domain name. That operator would then remove or modify their copy of the authoritative DNS records for that domain name. Assuming the take down order was sent to and implemented by all operators of authoritative servers for the domain, the domain would become immediately unreliable on a global basis and eventually unresolvable after the TTL of the domain's DNS records expires. In addition to different entities implementing the blocking, this method differs from registry/registar-based blocking in that it can create difficulties if DNSSEC is in use since the authority server operator may not be able to preserve the registry's DNSSEC signatures when altering registry domain content.

3. **Domain Blocking in a Recursive Resolver**: Recursive resolvers are a common place to implement DNS blocking with a number of tools (both commercial and open source) that allow resolver operators to easily implement blocking.[12] However, due to the DNS architecture, blocking in a recursive resolver is among the most easily bypassed. Recursive resolvers, typically operated by the end user's ISP, fetch DNS data from authoritative servers on request from end users. When an end user wishes to connect to a web site or other service, the recursive resolver serving that end user translates the domain name of that site or service into IP addresses. DNS blocking via recursive resolvers aims to filter, edit, or block this translation and can be done in a number of ways:

    a. **Via Redirection**: In this form of recursive resolver blocking the response from the authoritative server is modified to substitute values specified by the DNS blocking policy. For example, instead of returning the IP address of the offending web server, the recursive resolver returns an IP address of a remediation server that

[12] See http://blog.operationreality.org/2011/10/05/belgian-isps-to-block-pirate-bay-domain-names/ and http://news.cnet.com/8301-13578_3-57472718-38/pirate-bay-blocks-did-little-to-curb-file-sharing/.

displays a message indicating the site is being blocked.[13]

This form of blocking requires the remediation server to support any protocols or services supported by the original target servers for which displaying a redirection banner is technically possible. That is, if the target of the blocking is using the File Transfer Protocol (FTP) to provide content, the server to which the user is redirected must also use FTP in order to display the banner.[14] Due to the way some protocols work, this type of redirection may not be feasible in all cases.[15] However for common protocols such as Hypertext Transfer Protocol (HTTP, the core protocol for the World Wide Web), this kind of redirection is achievable.

b. **Via a Non-Existent Domain Name (NXDOMAIN) Response Code**: As with redirection, this form of blocking modifies the response from the authoritative server; however instead of returning the IP address of another server, the response is modified to indicate the requested domain does not exist.

c. **Via a Query Refused Response Code**: The DNS protocol has a response code, REFUSED, which is intended to signify that a domain is not resolvable for administrative reasons. DNS blocking can be implemented by changing the response from an authoritative server to a REFUSED response for blocked domains.

   One perfectly valid and reasonable interpretation of the DNS protocol specification is that REFUSED response codes indicate the name server should not be queried at all, which may result in the operating system removing that recursive resolver from its list of name servers. This is because the REFUSED response is interpreted as an access control problem for the client and for all domain names requested by that client, rather than as a refusal to answer for some specific domain name. With a sufficient number of end user queries, this type of blocking could result in all of the name servers used by the end user being removed, rendering the end user's computer being unable (or unwilling) to query any name. Thus, resolvers returning REFUSED for a domain being blocked are likely to result in unacceptable collateral damage.

---

[13] See http://www.sigcomm.org/sites/default/files/ccr/papers/2012/July/2317307-2317311.pdf.

[14] See "File Transfer Protocol" at http://en.wikipedia.org/wiki/File_Transfer_Protocol.

[15] See "Redirection in the COM and NET Domains (9 July 2004)", ICANN Security and Stability Advisory Committee at http://www.icann.org/en/groups/ssac/report-redirection-com-net-09jul04-en.pdf.

d. **Via Other Response Codes:** There are additional response codes specified in the DNS protocol that can be used to signal that a domain is not resolvable, usually indicating some sort of error has occurred. These response codes include "server failure" (SERVFAIL), "not implemented" (NOTIMPL), and "format error" (FORMERR).

   As with REFUSED, blocking via these response codes may result in the operating system declaring the recursive resolver as non-functional and removing it from the list of recursive name servers the operating system queries. For this reason, none of these alternative responses are suitable for DNS blocking.

e. **Via Query Non-Response**: Finally, the recursive resolver could be configured to ignore queries for a requested domain. This may result in applications attempting to connect to the blocked site to reattempt the resolution through multiple query iterations.

   As with REFUSED and other error response codes, the operating system may remove the recursive resolver from its list of name servers it queries for any name (not just the blocked name). However, unlike blocking via the response codes described above, blocking by not returning a response results in a significantly worse end user experience since the application must wait for all of the lookups to time out. This may encourage users to change to alternate recursive resolvers, potentially using servers not covered by the takedown order or desired blocking policy.

Reconfiguring recursive resolvers is operating system dependent but typically requires a small number of clicks in the "System Preferences" graphical user interface, and many available 'apps' operating systems in general operating systems and smart devices alike make this a one-click process as well. In almost all cases, this reconfiguration is within the capabilities of all but the most non-technical users.

As mentioned earlier, blocking via recursive resolvers is a common form of DNS blocking in use today; however end users can bypass this form of blocking by using a recursive resolver that does not implement the blocking, e.g., an "open" resolver that accepts queries from any source IP address[16] or by running their own recursive resolvers.

In addition, since recursive resolver-based DNS blocking re-writes or modifies the DNS responses received from the authoritative servers, the

[16] Popular open resolvers include OpenDNS (http://www.opendns.com/) and Google Public DNS (https://developers.google.com/speed/public-dns/).

chain of trust model used by DNSSEC will be broken and DNSSEC-related errors will be generated. These errors may lead an end user to conclude that the DNS recursive resolver has a problem or is under attack. This conclusion would be credible because with DNSSEC, DNS responses rewritten under government mandate are technically indistinguishable from what may be observed during malicious cache poisoning.

6. Contrasting Authoritative or Registry-Based DNS Blocking with Recursive Resolver Blocking

Some countries, such as the United Kingdom taking action against names in the .uk TLD[17] or the United States taking action against names in the .com Top Level Domain (TLD)[18] have seized domain names that are maintained by a registry that operates within their borders. In some cases, the domain name was placed on registry hold; in other cases, DNS records were modified to direct traffic to a government-controlled web site.

Assuming that the blocked domain names are few in number and that it is not trivial or cost-free to create new domain names serving the same audience and the same purpose, domain name seizure can be effective in blocking Internet content. Since actions in a TLD are taken at the publication point all DNS recursive resolvers globally will usually have the blocked names removed within a relatively short timeframe, specifically within the TTL of the DNS records being blocked.

When domains are seized at the registry level, DNSSEC[19] continues to operate as intended since this action is a modification to DNS content at its source and thus, assuming the DNSSEC signatures are regenerated appropriately, the DNSSEC chain of trust is unbroken.

However, if the registry providing the names to be blocked is located in a different legal venue, cooperation of law enforcement or government officials in different jurisdictions may be required. This can be problematic in the cases where the other country's laws are incompatible, or the law enforcement organizations do not have explicit mutual legal assistance treaties, teaming agreements, cooperation or coordination agreements via for example Interpol. As such, registry level domain take-down is most practical within a single legal jurisdiction although improvements in the coordination and cooperation among law enforcement agencies have recently been visible. For example, cooperation may be achieved via law enforcement participation in the multi-stakeholder

[17] See http://news.techworld.com/personal-tech/3319654/police-take-down-2000-couk-domains-selling-counterfeit-goods/.

[18] See http://en.wikipedia.org/wiki/Operation_In_Our_Sites_v._2.0.

[19] See http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions.

ICANN process, and by creation of special task forces within organizations like the creation of European Cybercrime Center (E3C) within Europol.[20]

DNS blocking at the authority server requires that each authoritative server operator makes changes to the zone it receives from the registry, without authorization by that registry. In the case where the authoritative servers are operated by more than one organization, this may be challenging. Should one or more authoritative server operators fail to reflect the same change within the same version of the zone, incoherent results could be returned for the same query depending on which resolvers were queried, which authoritative servers were queried by the resolvers, when the queries occurred, etc. Further, unless the authoritative server operator also happens to be the holder of the zone signing key (ZSK), the modifications to the zone made by the authoritative server operator would not be signed, thereby causing the DNSSEC chain of trust checks to fail for resolvers that do validation. As a result, this form of blocking tends to be impractical.

The use of recursive resolver-based DNS blocking avoids these jurisdictional issues since the take-down orders are addressed to ISPs or other resolver operators within the same legal jurisdiction of the body requesting the take down. The trade-off is that since various network operators all around the world operate recursive resolvers, it is impossible to ensure complete coverage without coordinated and universal data path filtering and payload manipulation. Additionally this would break in the face of end-to-end application-level DNSSEC validation, as discussed in the next section. However, at least one study has shown that because of a phenomenon called "upstream filtering" actions by an ISP in one country to filter or block content, may result in blocked content in another country because of routing arrangements among ISPs.[21] The unintended consequences of this sort of extraterritorial government influence could manifest as increased operating costs and decreased stability for all Internet operators and users.

7. DNS Blocking in Recursive Resolvers Conflicts with DNSSEC

As discussed in previous sections, the implementation of DNSSEC can have significant impact on DNS blocking activities. DNSSEC is a set of enhancements to the DNS protocol designed to address data authenticity issues within the DNS. Although DNSSEC-enabled applications are not yet in widespread use, the need for such applications is a key driver of the development and deployment of DNSSEC. End-to-end deployment of DNSSEC is required to enable support for

[20] See https://www.europol.europa.eu/content/press/european-cybercrime-centre-be-established-europol-1417.

[21] See https://citizenlab.org/2012/07/routing-gone-wild/.

cryptographic authentication in current and future security-sensitive applications, essential to safeguarding the public's trust in the global Internet.

Effective DNS blocking via recursive resolvers conflicts with the purpose and operation of DNSSEC. This is because DNSSEC is designed to detect exactly such changes that blocking intends to introduce, although the term "blocking" implies that the change itself is made in accordance with legislation and/or other rules to which involved parties agreed. The changes that blocking produces are indistinguishable to the changes that DNSSEC makes detectable, such as criminals intentionally injecting false DNS responses so that traffic is redirected to false services. Any modifications made to DNSSEC-signed data look identical to malicious DNS poisoning attempts because there is no feature or signal within DNSSEC to tell a receiver that a given response has been signed by an authority other than the domain holder. This holds true for domain holds where the purpose is to simply black out a web site and also for domain redirections where the purpose is to display a government interception/take-down notice in place of the web site via redirection. In either case an end user's resolver when validating DNSSEC-signed responses will be able to tell that tampering has occurred but will not know the cause of that tampering. The end-user's resolver's actions when it detects this kind of tampering may include the use of workarounds, such as ignoring the local recursive resolver iteratively resolving the entire chain of trust from the root to the authoritative servers itself.

DNS blocking at the recursive resolver level can be a feasible if temporary stopgap. Specifically, if one were to block or filter DNS only when either the domain name holder or the end user did not use DNSSEC then the modified data would still be accepted by end user resolvers and used by applications such as web browsers. However the workaround for a domain holder who does not want their domain name to be blocked would be to sign their DNS data, and the workaround for end users who does not want their content blocked in this way would be to enable DNSSEC in their stub resolvers.[22] Thus the characterization, "temporary stopgap."

While it is often assumed that DNSSEC validation can or should only be done "in the network" this ignores the needs of DNSSEC-aware applications. DNSSEC can be used "in the network" to protect a DNS cache from poisoned data, and in the early years of DNSSEC deployment that is the only use the Internet industry can make of DNSSEC. However, the long-term vision for DNSSEC is to create an entirely new class of DNSSEC-aware end user applications using technologies such as DNS-based Authentication of Named Entities (DANE), an effort underway in the Internet Engineering Task Force (IETF).[23] The DANE working

[22] Stub resolvers are minimal DNS resolvers that use recursive query mode to offload most of the work of DNS resolution to a recursive name server. Almost all Internet devices contain a stub resolver, and almost all access networks provide a recursive name server to their customers. See http://en.wikipedia.org/wiki/Stub_resolver#Stub_resolvers.

[23] See https://datatracker.ietf.org/wg/dane/charter/.

group is now standardizing a mechanism by which the identity of a secure web server, and the security of the connection between a browser and that secure web server, is enhanced via DNSSEC rather than via the older and increasingly trouble-prone X.509 certificate authority network.[24]

As a result of efforts to use DNSSEC as a general infrastructure upon which secure applications will be built, it can be assumed that DNS blocking in recursive resolvers will either have a negative impact on DNSSEC deployment or become ineffective once DNSSEC sees broader implementation. The world's economy can either have secure Internet naming and therefore secure Internet applications, or have effective content blocking via Internet DNS – but not both.

8. Other Implications of DNS Blocking

DNS blocking and filtering carry potential implications beyond those discussed in previous sections. Some clear possibilities include over-blocking and bypass/circumvention by routing DNS traffic away from blocking enforcement points.

8.1 Over-Blocking

Under the assumption that DNS blocking techniques will be used, there is a risk that errors will occur in the list of entities to be blocked. This is independent of whether the blocking is based on domain names or other identifiers such as IP addresses or Uniform Resource Locators (URLs). Because of this fact, the processes used to review items to be added to a given list must be secure, trustworthy, and allow for extensive vetting. The lists used in the blocking examples described in this report derive from varied sources: private entities, cooperating law enforcement agencies, and courts or legislatures. The SSAC does not take a view on what process is best but recommends several mechanisms to promote technical stability: clear rules on what may be blocked, and a well-defined review and decision making process.

In addition, it is important to recognize that if blocking is implemented for a domain such as *example.com*, blocking using the domain name system will not only block the ability to look up the domain name when accessing content under the blocked URL *http://example.com/bad-content.html*, but also all other URLs using that same domain name; e.g., under *http://abc.example.com/* or *http://example.com/good-content.html*. DNS blocking will also block domain name lookup for all other services such as e-mail, network management, file transfer, etc. that use the same domain, and additionally, child domains of

[24] Examples of recent challenges with X.509 include the compromise of Diginotar (see http://en.wikipedia.org/wiki/DigiNotar) and multiple compromises as Comodo Registration Authorities (see http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/).

example.com (e.g., *subdomain.example.com*).[25]

Finally, in any filtering regime, whether in the DNS or elsewhere, it is vitally important to avoid errors in the generation of targets for blocking. For example a typographical error during data entry could both fail to block the intended domain name and accidentally block some unrelated domain. Internationalized domain names (IDNs) can pose special hazards since two IDNs can appear to be identical yet be distinct inside the DNS.

8.2 Routing DNS Traffic Away From a Nation That Has Imposed Blocking

Government action that results in domain blocking can encourage end users to take steps to ensure their DNS traffic is routed through name servers outside the country, for example by using VPNs or specific recursive resolvers instead of the ones operated by the access provider. This "off shore" routing of domain name queries can transfer DNS observability and control to other countries, frustrating anti-cybercrime activities within the country implementing blocking, and/or fostering increased cybercrime activities by entities outside of the country. In addition to additional latency that may be incurred, this external routing of DNS traffic can also have an impact on Internet performance within the blocking nation as many content delivery networks make decisions regarding what information to return on DNS queries based on the source IP address of the resolver making the query. The use of non-local servers can result in unexpected traffic traversing international links.

Changing to another name server, whether it is part of the common ICANN-coordinated DNS or an alternate system, can be done by straightforward rewriting of a computer's configuration, greatly facilitated by the existence of friendly graphical user interfaces on most computer systems today. Even if individuals do not have the requisite knowledge to modify their computer (or network) DNS settings, scripts and custom applications that automate DNS modification have been posted for download. An example is the MAFIAAFire plug-in posted after early stages of the U.S. Immigration and Customs Enforcement's Operation In Our Sites initiative.[26]

---

[25] See http://gigaom.com/europe/orange-censors-all-blogs/, http://www.circleid.com/posts/20120917_microsoft_takedown_of_3322_org_a_gigantic_self_goal/, and http://www.techdirt.com/articles/20110220/17533013176/ice-finally-admits-it-totally-screwed-up-next-time-perhaps-itll-try-due-process.shtml

[26] See https://addons.mozilla.org/en-US/firefox/addon/mafiaafire-redirector/ and http://en.wikipedia.org/wiki/MAFIAAFire_Redirector.

8.2.1 Impacts of Users Switching Resolvers

DNS data give ISPs an important and accurate picture of both traffic patterns and security threats on their networks. This information can allow an ISP to identify increases and shifts in traffic, which can inform business decisions. Even more importantly, monitoring DNS data supports network security, often enabling ISPs to diagnose denial-of-service attacks and identify infected hosts, compromised domains, and vulnerable users.

As users increasingly turn to DNS servers other than those provided by their ISPs, those ISPs will have decreased ability to manage security threats and maintain effective network operations. The reduction of customer use of an enterprise, local network operator, or ISP's DNS service will mean that more compromised computers will go unidentified and uncorrected. Furthermore, the set of Internet configuration attributes that need to be evaluated when a customer calls an operator help desk for support will be much more extensive, and will increase both cost and debugging complexity.

The issues outlined above also will provide challenges for the governments of nations in which ISPs are located. Those governments may lose the ability to gain intelligence information through possible data sharing arrangements with network and Internet services operators, and also be without information that might be important evidence in law enforcement investigations. For example, the U.S. government might not have had sufficient evidence concerning botnet command and control structures and poisoned caches to have brought cases such as Operation Ghost Click, a significant action that shut down servers that propagated the DNSChanger malware.[27]

Law enforcement issues will be particularly acute when a user chooses a DNS server in another country. The ability of legal processes to address a problem is diminished when servers are out of the jurisdiction of a given enforcement agency.

8.2.2 Breaking CDN Localization If Users Switch Resolvers

Routing DNS traffic so that it does not match network topology, for example via DNS servers outside of a given country, also will negatively affect network performance (within the nation, per added propagation and aggregate round trip times) and increase costs for ISPs. For example, if users switch resolvers to avoid blocking the result may be that CDN localization may fail to work and the end user may be directed to content from CDN nodes hosted on servers outside of their country, rather than those located in the user's access network with direct interconnection links.

[27] See http://www.fbi.gov/news/stories/2011/november/malware_110911.

CDNs commonly localize content delivery by distributing the same content across servers on a wide range of networks globally. This localization reduces the load on any single server and minimizes network resource consumption and congestion by delivering content from servers as close to the user as possible. Many CDNs infer a user's location based on the IP address of their DNS resolver, which means users who have shifted to DNS resolvers outside their own country will appear to the CDNs to be browsing from abroad. The result will be a negative impact on performance and stability for such CDN users, and increased costs for ISPs transporting the associated traffic.

9. Conclusions and Further Reading

While blocking access to content via the DNS has become more common, both as a topic of study as well as in implementation, it carries with it a number of technical issues. Blocking at the DNS registry level (either directly or via a registrar) has the fewest technical implications and can work with DNSSEC but may run afoul of jurisdictional problems or trigger long-term balkanization of the Internet name space. Blocking at the authoritative servers has similar jurisdictional issues but cannot work with DNSSEC in the cases where the authoritative server operator does not also have the ability to correctly sign the zone containing the name(s) to be blocked. Finally, blocking at the resolver level, while common today, is at best problematic in the face of DNSSEC and at worst could impede the deployment of DNSSEC.

Governments and others should take these issues into consideration and fully understand the technical implications when developing policies that depend upon the DNS to block or otherwise filter Internet content.

Suggested further reading on this topic includes the following articles:

- *Shutdowns, Suspensions, Seizures, Oh My!*, D. Piscitello, http://securityskeptic.typepad.com/the-security-skeptic/2012/08/shutdowns-suspensions-seizures-oh-my.html.
- *Preventing Access or Removing Content – Laser Scalpel or Saw?*, D. Piscitello, http://securityskeptic.typepad.com/the-security-skeptic/2012/08/preventing-access-or-removing-content-laser-scalpel-or-saw.html.
- *A Chainsaw is a Poor Choice for Surgery and for Blocking Content*, D. Piscitello, http://securityskeptic.typepad.com/the-security-skeptic/2012/08/a-chain-saw-is-a-poor-choice-for-surgery-and-for-blocking-content.html.
- *Alignment of Interests in DNS Blocking*, P. Vixie, http://www.circleid.com/posts/20110723_alignment_of_interests_in_dns_blocking/.

10. Acknowledgments, Statements of Interests, and Objections, and Withdrawals

These sections provide the reader information on three aspects of our process. The Acknowledgments section lists the members who contributed to this particular document. The Statements of Interest section points to the biographies of the Committee members and any conflicts of interest, real, apparent or potential, that may bear on the material in this document. The Objections and Withdrawals section provides a place for individual members to disagree with the content of this document or the process for preparing it.

10.1 Acknowledgments

The committee wishes to thank the following SSAC members and other contributors for their time, contributions, and review in producing this Report.

Alain Aina
Jaap Akkerhuis
Don Blumenthal
KC Claffy
David Conrad
Patrik Fältström
James Galvin
Warren Kumari
Jason Livingood
Danny McPherson
Ram Mohan
Paul Vixie

10.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at: http://www.icann.org/en/groups/ssac/biographies-09oct12-en.htm.

10.3 Objections and Withdrawals

There were no objections or withdrawals.