CENTR vzw/asbl, Belliardstraat 20, 1040 Brussels, Belgium Tel +32 2 627 5550, Fax +32 2 627 5559
Tel +32 2 627 5550, Fax +32 2 627 5559, secretariat@centr.org http://www.centr.org

Analysis of blocking and redirection of domain names as tools to restrict access to content

Recently the discussion on preventing access to illegal and harmful content has hit the headlines again.

Legislative initiatives such as SOPA[1], HADOPI 1 & 2[2] in France or the changes to the Irish Copyright Act have led to a wide range of comments and protests. In addition there have been several court cases in Europe targeting The Pirate Bay which raised the question on how best to protect legitimate interests to the attention of the broader public.

In the reports of draft laws and legal cases, the authors mention 'blocking' as a key element in the discussions.
In this issue paper, CENTR analyses the impact of techniques that aim to restrict access to content via changes to the Domain Name System (DNS). This paper does not deal with the technical nor legal effects of the (temporary) removal of domain names from the zone file.

We will look at the two different aspects of 'blocking and redirection': the technical aspects and the impact it has on the end user.

DOMAIN-NAME-BLOCKING 01

Blocking is a form of filtering. It attempts to suppress the domain name resolution, i.e., the mapping of a domain name to an IP address, by either dropping the response, substituting it by an error message of one or more possible types or even by substituting the result. The latter is often called redirection.

Domain Name blocking is an action undertaken by an intermediary[3] by changing the records which are associated with a domain name on its recursive resolvers.
When a user types in a domain name (or clicks a web link) the name is resolved by the DNS server of the network he uses to access the internet. This server is called a recursive server (or resolver) and its purpose is to match the domain name with the correct IP address[4] of the requested service.

In order to be able to do this, the recursive server consults a table that is updated on a regular basis by checking authoritative name servers. Authoritative name servers store definitive versions of all records in that zone.

The process of referring to an authoritative server can be manually overridden. In that case, the entries in the table are changed to achieve the required effect. If the correct IP address is changed to an alternative address, this is called redirection. One example comes from Belgium. Instead of referring to the correct IP address, the DNS servers of 2 Belgian ISPs are required to refer any end user trying to access the website www.piratebay.org to a webpage hosted by the Federal Police following a recent court order[5].

1 http://judiciary.house.gov/hearings/pdf/112%20HR%203261.pdf The DNS related provisions have since then been pulled from the Bill.
2 http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021208046
3 This intermediary is typically an Internet Service Provider, but the same action could take place on a local level, e.g. by the administrator of a company network.
4 For more information on how the Domain Names System works, please refer to https://www.centr.org/dns-explained/domain-name-system
5 http://nurpa.be/files/20111004_BAF-Belgacom-Telenet-DNS-blocking.pdf (Dutch)

TECHNICAL-ASPECTS.02

DNS has two essential functions. One function is high-level, user enabling, and provides humans a way to access services without memorizing IP addresses. The prominent use for this aspect of the protocol is web surfing, but basically DNS is involved whenever an internet user has to access a service. The second function is on a lower level, and puts DNS closer to the infrastructure: most services rely on DNS for their own needs: email delivery, instant messaging, internet telephony ... all require the DNS. From an architectural point of view, interfering with services close to the infrastructure and thus remote to the actual target of blocking (i.e. content on websites) is dangerous due to unquantifiable risks to dependant services.

From a technical perspective, for any filtering to be efficient and proportionate it should happen technically as close as possible to the target (content) or to the consumer. Any additional distance increases the risk of impacting more than just the specific service and hence reduces the effectiveness of the measures taken.

DNS lookups and thus any filtering attempt based on those, are service agnostic. In other words, when resolving a domain name to an IP address, it is not visible from the request whether the subsequent action is sending an email, accessing a web page, making a VOIP call or tuning into an Internet radio station. Sometimes the domain names give a clue (such as those starting with "www"), but this is not necessarily the case.

Specific side effects include that blocking example.com via DNS would prohibit email communication with '@example.com' addresses. Additional unrelated parties can be affected.

If 'example.com' hosts several websites (e.g. 'example.com/goodsite' and 'example.com/badsite'), any blocking of 'example.com' would impact all those websites.
In the cases the domain name also provides DNS service to other domain names, all those could be blocked as well. For instance the blocking of 'europa.eu' would block 'ec.europa.eu' and 'enisa.europa.eu' as well.

The most problematic aspect of the inter-dependencies is that the actual impact of a block cannot be assessed accurately beforehand because these relationships are not centrally documented.

Considering the architectural importance of DNS, a lot of work has been put into securing DNS, specifically into DNS Security Extensions, also known as DNSSEC. It consists of signing cryptographically DNS messages and thus enabling the recipient to verify their authenticity. DNSSEC is generally considered to offer an important increase in the trustworthiness of DNS, with large benefits to relying services. In particular the U.S. government has mandated the use of DNSSEC for federal .gov domain names. In Europe many ccTLD registries offer signed registrations directly or via accredited registrars. The large gTLDs have enabled DNSSEC as well. One fundamental purpose of DNSSEC is to detect tampering with DNS messages. Blocking or redirecting DNS messages is viewed as just that; an interference, and is thus indistinguishable from a malicious attack for a validating client.
The confusion created by mixing the effects of real security threats and policy based interference is likely to erode the trust DNSSEC is trying to foster.

The Domain Name System was developed 30 years ago. It was invented to enable access to content. It is not the proper tool to enforce access restrictions.

BLOCKING-IS-INEFFECTIVE.03

Restricting access to content by requiring an intermediary to block the domain name is ineffective.
As the content remains online, it can be reached through different means:

1. In many cases the content can be reached by typing in the IP address. E.g. the website of DENIC, the registry for .de can be reached by typing in the IP address 81.91.170.12 in the address bar.

2. When a site is blocked through a court order, the owners of the site often replace the domain name swiftly with an alternative. E.g. in case of The Pirate Bay, the press mentioned in the same articles in which the court case was reported that the content could still be reached through http://www.depiraatbaai.be and http://www.baiedespirates.be[6][7].

6 The Court Case dates from 26 September 2011. The alternative domain names were registered on October 5th 2011 and December 9th 2011.
7 In just over three months time http://www.depiraatbaai.be has reached rank 118 on the alexa.com list of popular sites in Belgium. The original site http://www.thepiratebay.org was and still is on rank 207.

3. Anonymous proxy servers give end users – often for free – the opportunity to reach blocked content. The content gets repackaged to the extent that the original destination is not visible any longer for the ISP that is required to block the content. Zend2.com is an example of such a service.

4. Sites that archive web content typically provide access to recent material8. As they are never included in a blocking order the content can be freely accessed through one of these sites.[8]

5. Virtual Private Network (VPN) services allow end users to conceal their location and appear to have a different nationality.

6. Users can easily switch their DNS resolver to one that doesn't take into account national legislation or court orders (or privacy laws). OpenDNS or Google DNS are just two examples of a wide range of services that are freely available.

7. Changing Internet Service Provider will often circumvent the effects of a blocking order as typically court orders name individual ISPs that are required to abide by it.

8. Organisational networks (enterprises, but also universities and schools) are likely to run their own recursive resolver for performance and trust reasons, thus circumventing any ISP based blocking without specifically intending to do so.

While it is correct to say that not everyone will use one of these techniques to circumvent the access restrictions, it does show that restricting access to harmful or illegal content through blocking or redirection is ineffective.

It should also be stressed that circumventing blocking it not necessarily driven by criminal intend. Reasons may range from specific local requirements, via security concerns[9] to ideological human right principles (e.g. opposing all kind of censorship).

AFFECTING-SAVE-USER-BEHAVIOUR.04

The fundamental principle underlying the DNS is that the user obtains the information he seeks and reaches the destination he intends to reach. This principle is the reason why users have been educated for years to check the URL before entering any personal details. Blocking and redirection undermine that principle. The user will learn that he can no longer rely on the domain name to make sure he is looking at the right website or that his email reaches the intendend recipient.

As users discover that content they try to reach is not actually off-line, but that only the ways in which he can access it have changed, they will simply change their browsing behaviour and are likely to start experimenting with some of the tools mentioned in the previous section. Such behaviour is documented and even encouraged in popular press or in thousands of blogs and online fora.

The use of some of these, in particular the popular anonymous proxy services entails risks which the users are typically unaware of.

- By using an anonymous proxy service, the user diverts his traffic to an unknown third party.
- These third parties know the user's IP address and can therefore capture a significant amount of personal information, just by building up a database of the user's online behaviour. Most of these anonymisers operate outside the EU and therefore will not abide by EU privacy rules.
- However, these third parties can do something much more harmful: they have access to the data that is being sent back and forth. This would include access to usernames, passwords and account information and could lead to identity theft and other types of serious fraud.

For years ISPs and eCommerce providers alike have educated the user to behave in a secure way. By undermining the most fundamental principle of the addressing system and by unwittingly encouraging risky behaviour, blocking and redirecting will undermine the much needed consumer trust.

8 See e.g. http://www.thewaybackmachine.org or http://liveweb.archive.org/

9 e.g. dnssec-trigger, developped by NLNetlabs, is packaged DNSSEC-validating resolver bringing recursive resolving capabilities to end-hosts by simple point-and-click installation (http://nlnetlabs.nl/projects/dnssec-trigger/)

CONCLUSION.05

As we have explored in this paper, blocking and redirection DNS manipulation as means to restrict access to illegal content are ineffective and could have a negative impact on consumer trust. Especially the unintended impact on dependent services make them a blunt tool. Their use should be avoided if possible.

FURTHER-READING.06

- Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill
  http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf
  In-depth analysis of the technical aspects of DNS Filtering requirements
- 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
  http://www.icann.org/en/committees/security/sac050.pdf
  Advisory paper form the ICANN Security and Stability Committee