CENSURFRIDNS

Thomas Steen Rasmussen
admin@censurfridns.dk

March 11th, 2012

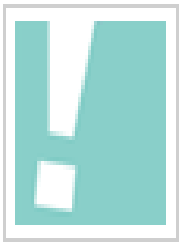
Open Source Days 2012

Agenda - Politics

- **What is censurfridns and why does it exist**
  -

What is censurfridns - and why does it exist?

- Free, open, uncensored resolvers
- Founded in 2009 due to a lack of proper resolvers in .dk (geo dns balancing)
- Proper means uncensored, dnssec enabled, ipv6 enabled, secure, fast, stable...
- The name means ”censorship free dns” in Danish. Suggestions for an additional (english language) name appreciated (see next slide).



Jack

You may or may not be able to, your best weapon is preparation. Get a DNS outside of the states, manage your own hosts file, and use proxies.

The more you know, the less they control you.

I've included a link to Censur Fri dns (a play on Semper Fi), tor, and the wiki for Hosts files.

Source(s):

http://blog.censurfridns.dk/en

http://www.torproject.org

http://en.wikipedia.org/wiki/Hosts_%28file%29

1 year ago

Report Abuse

0% 0 Votes

What is censored on the Danish ISP nameservers ?

- 2005: Pages depicting child abuse
- 2006: Copyright (allofmp3.com)
- 2008: Copyright (thepiratebay.org)
- 2011: Unlicensed gambling sites
- 2011: Illegal pharmaceutical vendors
- 2012: Copyright (grooveshark.com)
- …. ?

How come censurfridns can avoid blocking ?

- The blocking agreement between the ISPs and the police concerning child abuse pages is voluntary (or is it ? carulli.dk!). There is in other words no legal basis for this blocking.
- I am not an ISP. The court ruling against Telenor forcing them to block of thepiratebay.org only applies to ISPs. The reason has something to do with how routers and switches store and forward data packets.
- New laws or court orders may make censurfridns illegal in the future. What happens then ?
- I don't know, but the DNS servers will stay operational for as long as they are needed, one way or another.

Lies, damn lies, and politics

- One of the things that really complicates the issues surrounding DNS censorship is the variety of different content that is being blocked.
- All the different blocking has one thing in common though:
- No attempt is ever made to compare the supposed benefits versus the problems.
- Instead, FUD, lies and politics pollute any attempt at serious debate.

Won't somebody please think of the children!

- The issue of blocking pages that depict child abuse is difficult to discuss, because child abuse is perhaps the most sensitive subject there is.
- Protecting children is definitely an admirable goal, but when someone says ”blocking” it actually means ”looking away instead of acting”.
- What we are doing is not helping children in any way.
- Instead, our blocking system can actively help the criminals it is intended to fight, by providing a well-funded ”early warning system”. When a site is added to the blocklist the criminal knows the police is onto him, and he can run and hide.

Won't somebody please think of the children!

- Nothing indicates that the current blocking has any positive effects.
- With plenty of documented negative effects and no apparent positive effect, you can't help but wonder why we still have the blocking.
- Partly because the politicians are downright afraid of looking soft on child abuse.
- But the main reason is Save the Children Denmark, the primary proponent of the blocking. They receive money yearly from ”satspuljemidlerne” to operate a hotline which serves as a basis for the blocking list.
- When the media asks if the blocking is working as intended, they need to stop asking the very people getting paid to supply the blocking list. Seems like a no-brainer right ?

Won't somebody please think of the children!

- Any criticism pointing out that the filter has the opposite effect of the intention appears to be ignored entirely by Save the Children Denmark.
- Instead the whole issue is surrounded by plenty of ”think of the children” rhetoric which makes serious debate impossible
- The effect that this subject has on people has been noticed by the company NetClean. They sell products that are supposed to ”stop the spread of child abuse content in your network”

Child abuse is big business these days

- I attended a seminar which NetClean and Save the Children Denmark arranged about a year ago, right here on CBS.
- The presentation was so full of FUD and lies that I had to leave halfway through or I would have imploded.
- Among the quotes I remember are ”*10% of the data on an average companys servers is child abuse content*” and ”*the pedophiles put the illegal content on company servers because there is plenty of diskspace at work*”.

Child abuse is big business these days

Child abuse is big business these days

- Not once during the presentation did they talk about actually doing something about the problem, like contacting hosting providers.
- In fact, their entire business model is based on the continued availability of illegal materials. Ironic, huh ?
- The knowledge that someone, somewhere is getting rich off of child abuse concerns me. But to abuse the fear people have of the subject of child abuse to turn a profit is something that really pisses me off.
- As we know, blocking websites (whether it is in ISP DNS servers or using one of NetCleans solutions) does nothing to solve the actual problem. It appears the saying is true: **If you are not part of the solution, there is good money to be made in prolonging the problem.**

Child abuse wrap-up

- I could rant about this subject for days, but we have limited time
- Read https://blog.censurfridns.dk and http://ak-zensur.de/2010/09/looking-away.html which describes the takedown case I talked about
- Quote from the ak-zensur.de link: *Internet blocking does not fight abuse, in practice it only serves to conceal the failures of politics and police. Websites can remain on blocking lists for years even though they have either been deleted or could be deleted easily and quickly.*


STOP
Stop believing that hiding
a problem will somehow
help to solve it

Count to 10

Protecting content owners (allofmp3, thepiratebay.org etc)

- Only a year after the beginning of DNS censorship in DK, we saw the first Danish court order to DNS block a site due to copyright infringement.
- The site was allofmp3.com and more sites soon followed.
- There was actually an increase in traffic to thepiratebay.org from Danish IP addresses right after the block, because of all the media attention. If anyone still thinks DNS blocking has any effect, they are not paying attention.
- The latest site to be blocked due to copyright infringement is grooveshark.com a couple of months ago. More on this in a little while.

Protecting content owners (allofmp3, thepiratebay.org etc)

- There is a powerful lobby (paid for by the content owners) putting pressure on the government, asking for more blocking and more legislation
- Yes, even in Denmark
- Why do we permit this ? You do _not_ get to destroy the internet because it doesn't fit your outdated business model.
- Complain to your politician – and join itpol.dk

Protecting content owners

- Rettighedsalliancen claims they picked a random Danish ISP for the grooveshark.com case (they picked '3').
- But '3' is a mobile provider. All mobile providers have equipment to do DPI, it is an integral part of how mobile networks work.
- Furthermore, the nature of '3' means they likely share nameservers between Danish and Swedish customers.
- These two facts combined make it likely that any court order against '3' to block a site would result in DPI blocking, not DNS blocking.
- With this in mind, you have to be pretty naive to believe that '3' was a random choice. Nothing they do is random, be *very* careful not to underestimate them.

Count to 10

Censorship for profit (unlicensed gambling sites)

- In 2011 we got a new type of DNS blocking in our legislation: unlicensed gambling sites
- The Lottery Funds is the large (1.6 billion DKK last year) amount that Danske Spil makes after expenses and paying prizes to winners.
- The money is distributed anually to various Danish ministries according to the distribution specified in the Danish national budget (finansloven).
- Each Minister then distributes money to the charities he/she feels appropriate.

Censorship for profit (unlicensed gambling sites)

- The politicians have been worried for a while about the Internet introducing new gambling providers that do not pay tax to the Danish market, affecting the size of the Lottery Funds.
- They are worried because handing out money makes them look nice - and who doesn't want to look nice ? (especially politicians)
- They have decided to use DNS blocking to solve this problem (is anyone seeing a pattern here ?)
- This is the first Danish case of censorship for government profit: using DNS blocking for the single, stated purpose of protecting the size of the Lottery funds.

Count to 10

Protecting consumers from themselves (blocking illegal pharma sites)

- One of the newest types of blocking we have in Denmark is of illegal pharmaceutical vendors. 24hdiet.com was the first.
- People are apparently buying diet pills online from questionable vendors, instead of buying them in a Danish pharmacy (the claim is that they don't know it is illegal?)
- Like other types of blocking, it is highly doubtful whether the blocking will have the intended effect. People are pretty good at procuring illegal drugs. Always have been, always will be.
- This blocking illustrates well how the politicians see DNS censorship as ”just another tool in the toolbox” these days.
- Gradual censorship is not a theory, these days it is fact.

Agenda - technical

- How does the Danish blocking work
- Technical description of the censurfridns.dk service and infrastructure
- Security and stability considerations when running nameservers (especially open recursive ones)
  - Cache poisoning
  - Redundancy
  - The sad story of OS resolvers failover fail
- How I discovered I was participating in a DDOS
- The conflict between security and freedom online

How does the Danish blocking work

- Each ISP sends a public key to the police, who adds it to the server holding the current list
- The ISP uses scp to fetch the list file regularly, like once per hour
- The list is just a list of http://domain.tld lines so it is reformatted to fit bind config syntax with standard unix tools like sed and cut.
- The list is then copied to the nameservers and loaded there.
- All domains in the list point at the same zone file

Example zone file

```
------------------------------------------
$TTL 43200
@  IN SOA      ns.example.com. hostmaster.example.com. (
              2006012001      ; serial
              3600            ; refresh
              3600            ; retry
              3600            ; expire
              3600            ; minimum
              )
              IN      NS      ns.example.com.
              IN      A       192.0.2.117
*             IN      A       192.0.2.117
------------------------------------------
```

- In this example the webserver hosting the STOP page is at 192.0.2.117 and all queries return this IP (wildcard record)

The server hosting the STOP pages

- The webserver logfile for the child abuse stop page is sent to the police every night.
- But first, the IP of the clients is concealed in the fortress of security known as md5 using a script similar to the one below:

```
-------------------------------------------
#!/bin/sh

while read LINE ; do
        #LINE=`awk {'print $0'}`
        IP=`echo $LINE |awk {'print $1'}`
        SIP=`echo "halløjsa HER ER NOGET SALT $IP jow tak OG LIDT MERE SALT I
    HASHEN"| md5`
        NEWLINE=`echo $LINE | sed -e "s/$IP/$SIP/"`
        echo $NEWLINE >> $1
done
-------------------------------------------
```

Technical description of censurfridns.dk

- Originally two nameservers, ns1.censurfridns.dk and ns2.censurfridns.dk
- The servers always had ipv6 support using 6to4, native IPv6 coming soon for ns1, no current plans on ns2 (provider related)
- The servers always had DNSSEC support, although it was using DLV before the root was signed
- Recently ns1 was upgraded to new hardware, and replicated so there are two physical servers handling queries for ns1 now. If one goes down, the other takes over. This is done with CARP and scripts on the servers to monitor DNS functionality.

Technical description of censurfridns.dk

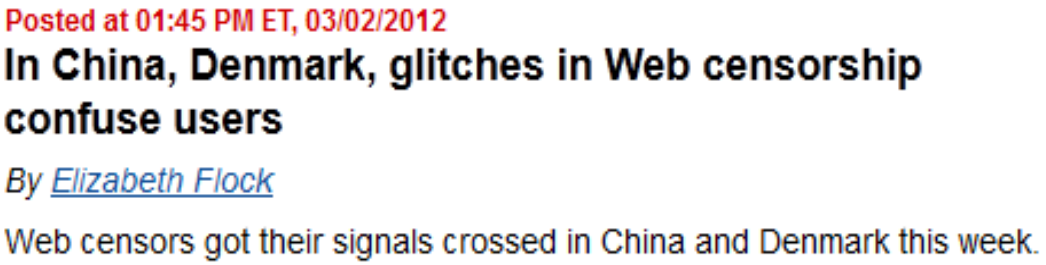
- In front of ns1 there is a couple of redundant CARP firewalls (it's been like that since the start)
- All of these servers run FreeBSD (surprise)
- ns1 and ns2 are placed in different datacenters, different cities, with different providers providing the upstream link.
- The monitoring system runs from a third place, nothing special about it, it works pretty well.
- I get SMS notifications when anything is wrong.

What are the technical problems with blocking in DNS

- First of all the blocking system we have in Denmark is based on some weird idea that the Internet equals HTTP and nothing else
- The STOP page gives a message explaining why stuff doesn't work as expected if you use a webbrowser
- But what if you were trying to send a mail to one of the blocked domains ? Only the HTTP protocol is handled. You would get a bounce four days later.

What are the technical problems with blocking in DNS

- The Danish blocking system for child abuse pages introduces a single point of failure into the DNS
- This was demonstrated better than I could have asked for a couple of weeks ago:



Posted at 01:45 PM ET, 03/02/2012

In China, Denmark, glitches in Web censorship confuse users

By Elizabeth Flock

Web censors got their signals crossed in China and Denmark this week.

- from http://www.washingtonpost.com/blogs/blogpost/post/in-china-denmark-glitches-in-web-censorship-confuse-users/2012/03/02/gIQATFwzmR_blog.html

Security and stability considerations when running nameservers (especially open recursive ones)

Cache poisoning

- Since Kaminsky published his DNS cache poisoning bug there has been default source port randomization in bind. But stuff like firewalls/NAT and default source port ranges in the operating system can complicate the issue.
- **sysctl net.inet.ip.portrange.hifirst=1025**
- Never assume it is OK without testing it:

```
$ dig @ns1.censurfridns.dk +short porttest.dns-oarc.net TXT
porttest.y.x.w.v.u.t.s.r.q.p.o.n.m.l.k.j.i.h.g.f.e.d.c.b.a.pt.dns-oarc.net.
"89.233.43.72 is GREAT: 26 queries in 4.2 seconds from 26 ports with std dev 16518"
$ dig @ns2.censurfridns.dk +short porttest.dns-oarc.net TXT
porttest.y.x.w.v.u.t.s.r.q.p.o.n.m.l.k.j.i.h.g.f.e.d.c.b.a.pt.dns-oarc.net.
"89.104.194.142 is GREAT: 26 queries in 4.2 seconds from 26 ports with std dev 19388"
$ dig @ns1a.censurfridns.dk +short porttest.dns-oarc.net TXT
porttest.y.x.w.v.u.t.s.r.q.p.o.n.m.l.k.j.i.h.g.f.e.d.c.b.a.pt.dns-oarc.net.
"89.233.43.72 is GREAT: 26 queries in 4.2 seconds from 26 ports with std dev 16518"
$ dig @ns1b.censurfridns.dk +short porttest.dns-oarc.net TXT
porttest.y.x.w.v.u.t.s.r.q.p.o.n.m.l.k.j.i.h.g.f.e.d.c.b.a.pt.dns-oarc.net.
"89.233.43.73 is GREAT: 26 queries in 4.2 seconds from 26 ports with std dev 17295"
```

Redundancy

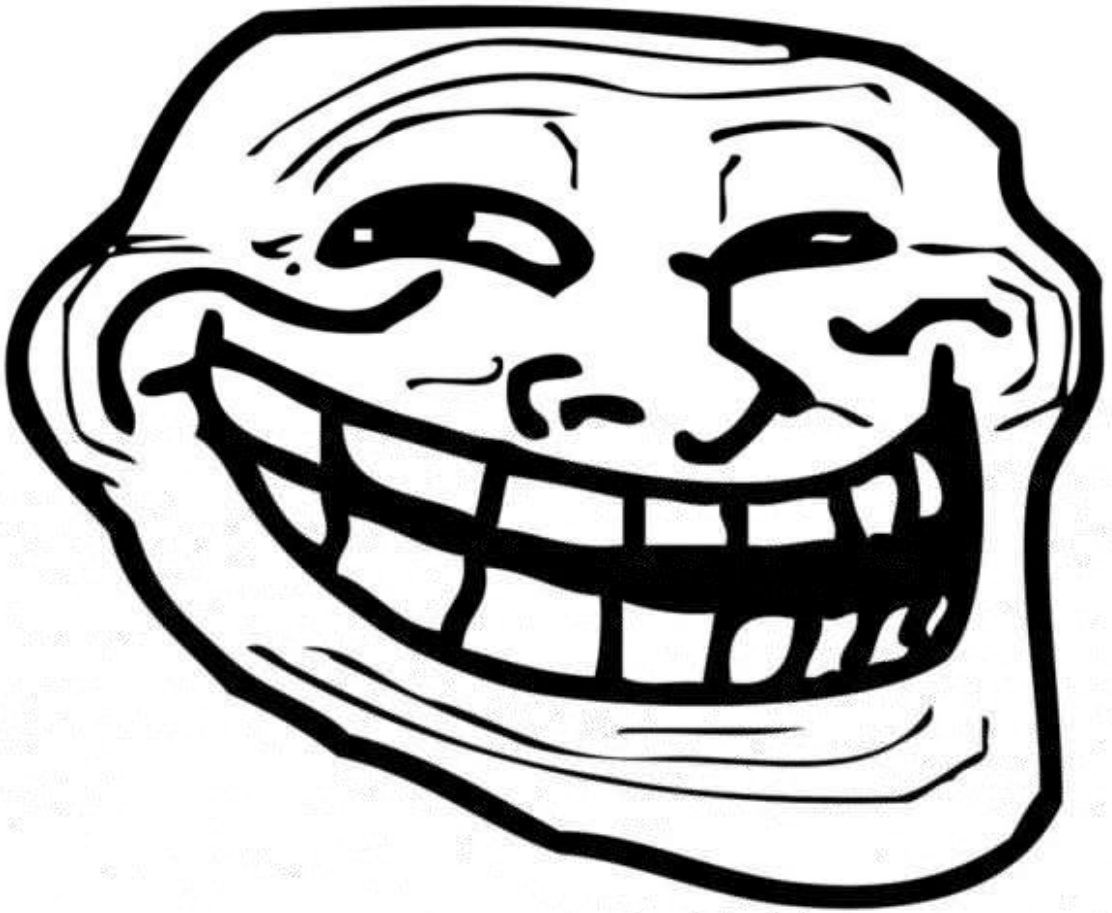
- When operating recursive nameservers it is important to consider what happens when one goes down (since the users REALLY notice when DNS doesn't work).
- I went through the redundancy of ns1 and the firewalls in front of it.
- There is a good reason I have more redundancy on ns1 than on ns2.
- Most people put ns1 first and ns2 second in their OS/router resolver configs (easy to see from the load on the two servers)
- The order the servers are configured in shouldn't matter, but it does

The sad story of OS resolvers failover fail

- At some point a while back there was downtime on ns1 (before it was redundant) due to a raid controller fail
- If it wasn't because I'd tried the same thing at work a few years earlier I would have been thoroughly surprised at the amount of emails and calls I got, complaning about DNS not working. Even though ns2 was up and answering queries just fine.
- The fact is that our operating systems (even FreeBSD) are horribly bad at switching between the configured resolvers if one is down.

The sad story of OS resolvers failover fail

- I haven't looked into it further (but I will, watch the blog) – but there is definitely something wrong.
- It may seem obvious, but: when the resolver doesn't get a reply from the nameserver it is asking, it should switch to the next one in the list.
- It should then keep using that nameserver until that fails, and then take the next one on the list, and so on.
- Instead, it seems like it tries the first nameserver in the list for (nearly) every query, which effectively means that you have to wait for your resolvers timeout delay again and again, as it keeps asking the server that is down.
- It is like this on all operating systems I know of



problem?

How I discovered I was participating in a DDOS

- Background: ns1a and ns1b are located on a subnet: 89.233.43.64/28
- I was getting lots of weird error messages on the nameservers saying ”Connect to address: 89.233.43.64: Permission denied” and ”Connect to address: 89.233.43.79: Permission denied”
- Some of you probably guessed by now what was going on ?

Spoofed traffic

- Someone was spoofing queries with source IP addresses in the same /24 as the nameserver was in
- This is probably because most nameservers today are limited to the ISP they run at (like, only TDC customers can use TDCs nameservers)
- The attacker has no way of knowing my subnet layout
- When my nameserver received queries from its own network address and broadcast address, and tried to send a response, the firewall said ”no thanks”
- The target of the attack was a Chinese DNS hosting company, the domains being queried were all hosted on the same nameservers, which were likely very busy at the time.

The conflict between security and freedom online

- On some level, there is a basic conflict between security on the internet, and online freedom
- My nameservers can certainly be used to resolve domains with illegal content
- They may also be used in a DDOS again some day
- The same could be said for things like TOR and Bitcoin. They can be (ab)used for illegal purposes – but at the same time they enhance our freedom online.

A relevant quote

The trouble with fighting for human freedom is that one spends most of one's time defending scoundrels. For it is against scoundrels that oppressive laws are first aimed, and oppression must be stopped at the beginning if it is to be stopped at all.

H. L. Mencken, (1880 - 1956) US editor

The end

- This is the end of the presentation. I have more to say, but not quite enough time to do it. The political aspects of DNS blocking is a huge subject, and the technical aspects of DNS are always interesting
- If you have any questions then ask away – or find me in the BSD-DK booth, or send me an email at admin@censurfridns.dk
- Follow the twitter feed @censurfridns and read the blog at https://blog.censurfridns.dk (self-signed certificate, the broken CA system is not getting any of my money, but that's for another talk)
- Buy a t-shirt or a coffee mug, to help spread the word! The webshop is at http://censurfridns.spreadshirt.dk - I do not get any money from the sales.