

Censur på nettet i praksis (i Siminn Danmark)

- Hvad censurerer vi
- Hvorfor censurerer vi
- Hvordan censurerer vi
- Statistik

Hvad censurerer vi

- ✓ Børneporno filteret
- ✓ thepiratebay.org
- x IKKE allofmp3 - vi "blev glemt" i sin tid \o/

Hvorfor censurerer vi

- Frivillig branche aftale med politiet
- Indført “før vores tid”
- Kommercielle konsekvenser hvis Siminn trækker sig fra filteret
- thepiratebay.org lukket efter henvendelse fra IFPI og fogedretsdømme mod Telenor

Hvordan censurerer vi

Børneporno filteret fungerer således:

- 1) Script henter og formatterer listen hver time
- 2) Listen bliver kopieret til DNS serverne
- 3) Serverne reloades så de bruger seneste liste
- 4) Alle domæner i listen peger på samme zonefil
- 5) Zonefilen resolver alle A records til samme IP
- 6) Der kører Apache med STOP side på den IP
- 7) IP adresser i Apache logfiler scrambles
- 8) Logs sendes til politiet + de har awstats adgang

Hvordan censurerer vi - 1

Periodisk script henter listen hver time.
Scriptet er meget simpelt. Det henter listen
vha. SSH fra politiet og formatterer den, så
den har det rette format til indlæsning i bind.
Politiets server kender vores public SSH key.

```
----- fetchzones.sh -----  
#!/bin/sh  
DOMAINFILE=/data/www/bpstat/wwwroot/list/bp_domains  
  
for a in `ssh -b 195.184.96.117 -p 1022 siminn@w.x.y.z "cat bpfiler/bpfiler.txt" |  
    sed "s/http:\/\:\/\/"; do  
    printf "zone \"\$a\" { type master; file\"/etc/namedb/blocked/bp_zone\"; };\\n";  
done >$DOMAINFILE  
----- fetchzones.sh -----
```

Hvordan censurerer vi - 2+3

Listen hentes en gang i timen ned på DNS serverne, som herefter reloades så de bruger den seneste version af listen

```
----- bprefresh.sh -----  
#!/bin/sh  
  
#download file  
/usr/bin/fetch -qo /etc/namedb/blocked/bp_domains  
    http://censur.siminn.dk/list/bp_domains  
  
#reload bind config  
/usr/sbin/rndc reconfig  
-----
```

Hvordan blokerer vi - 4

Alle domænerne peger på samme zonefil

```
----- bp_domains -----  
....snip....  
zone "stop.politi.dk" { type master;  
  file"/etc/namedb/blocked/bp_zone"; };  
....snip....  
-----
```

Hvordan censurerer vi - 5

- Alle A records resolver til samme IP
- NS record peger på vores recursive server
- Alle andre records giver NXRRSET

----- bp_zone -----

\$TTL 43200

@ IN SOA ns.webpartner.dk. hostmaster.webpartner.dk. (

2006012001 ; serial

3600 ; refresh

3600 ; retry

3600 ; expire

3600 ; minimum

)

IN NS ns.webpartner.dk.

IN A 195.184.96.117

* IN A 195.184.96.117

Hvordan censurerer vi - 6

Apache serveren der kører STOP siden er konfigureret således (første (default) vhost!)

```
----- httpd-vhosts.conf -----  
<VirtualHost 195.184.96.117:80>  
  ServerName bp.siminn.dk  
  DocumentRoot /data/www/bp  
  RewriteEngine on  
  RewriteCond %{DOCUMENT_ROOT}%{REQUEST_FILENAME} !-s  
  RewriteRule ^.*$ /index\..html [L,R]  
  CustomLog "|/data/scripts/bp_log_scramble_ip.sh /data/www/logs/bp-access.-  
  log" bp  
  ErrorLog /data/www/logs/bp-error.log  
</VirtualHost>
```

Hvordan censurerer vi - 7

IP adressen i Apache logfilen scrambles med en “one way hash” før linien skrives i access log:

```
----- bp_log_scramble_ip.sh -----
```

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

```
while read LINE ; do
```

```
    #LINE=`awk {'print $0'}`
```

```
    IP=`echo $LINE |awk {'print $1'}`
```

```
    SIP=`echo "Whophdupan HER ER NOGET SALT $IP eittAttyie OG LIDT  
    MERE SALT I HASHEN"| md5`
```

```
    NEWLINE=`echo $LINE | sed -e "s/$IP/$SIP/"`
```

```
    echo $NEWLINE >> $1
```

```
done
```

```
-----
```

Hvordan censurerer vi - 8

AWStats opdateres og logfilerne sendes til
Politiet ved midnat hver dag:

----- bp_log_stats.sh -----

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

```
# Rotate apache log
```

```
OLDLOG="/data/www/logs/`/bin/date -v -1H "+%Y%m%d"` .bp-access.log"
```

```
/bin/mv /data/www/logs/bp-access.log $OLDLOG
```

```
#restart apache
```

```
/usr/local/sbin/apachectl graceful
```

```
# wait for any current requests to be written
```

```
/bin/sleep 10
```

```
# send old log to police
```

```
/usr/bin/scp -o BindAddress=195.184.96.117 -P 1022 $OLDLOG siminn@w.x.y.z:logs/
```

```
# run AwStats
```

```
/usr/local/bin/perl /usr/local/www/awstats/cgi-bin/awstats.pl -config=bp.siminn.dk -update
```

```
/usr/local/bin/perl /usr/local/www/awstats/cgi-bin/awstats.pl -config=bp.siminn.dk -output -staticlinks >
```

```
/data/www/bpstat/wwwroot/index.html
```

Statistik

Statistik for børneporno filteret

Statistik

Jeg har af interesse gemt lidt tal for børneporno filteret. Der er desværre et hul i tallene grundet en config fejl, fra starten af december til 18. marts.

I perioden hvor jeg ikke har tal for filteret er der blevet ryddet kraftigt op i de blokerede domæner – cirka 60% er forsvundet fra listen. Jeg ved ikke nøjagtigt hvornår det er sket, men indenfor de sidste 3-4 måneder.

Statistik - useragents

Crawlere og robotter er talt med i statistikken, men de udgør en særdeles lille del af de samlede hits. Langt størstedelen af useragents er MSIE, Firefox og Opera. Når følgende useragents fjernes er der meget få hits tilbage, blandt andet et par fra Alexa:

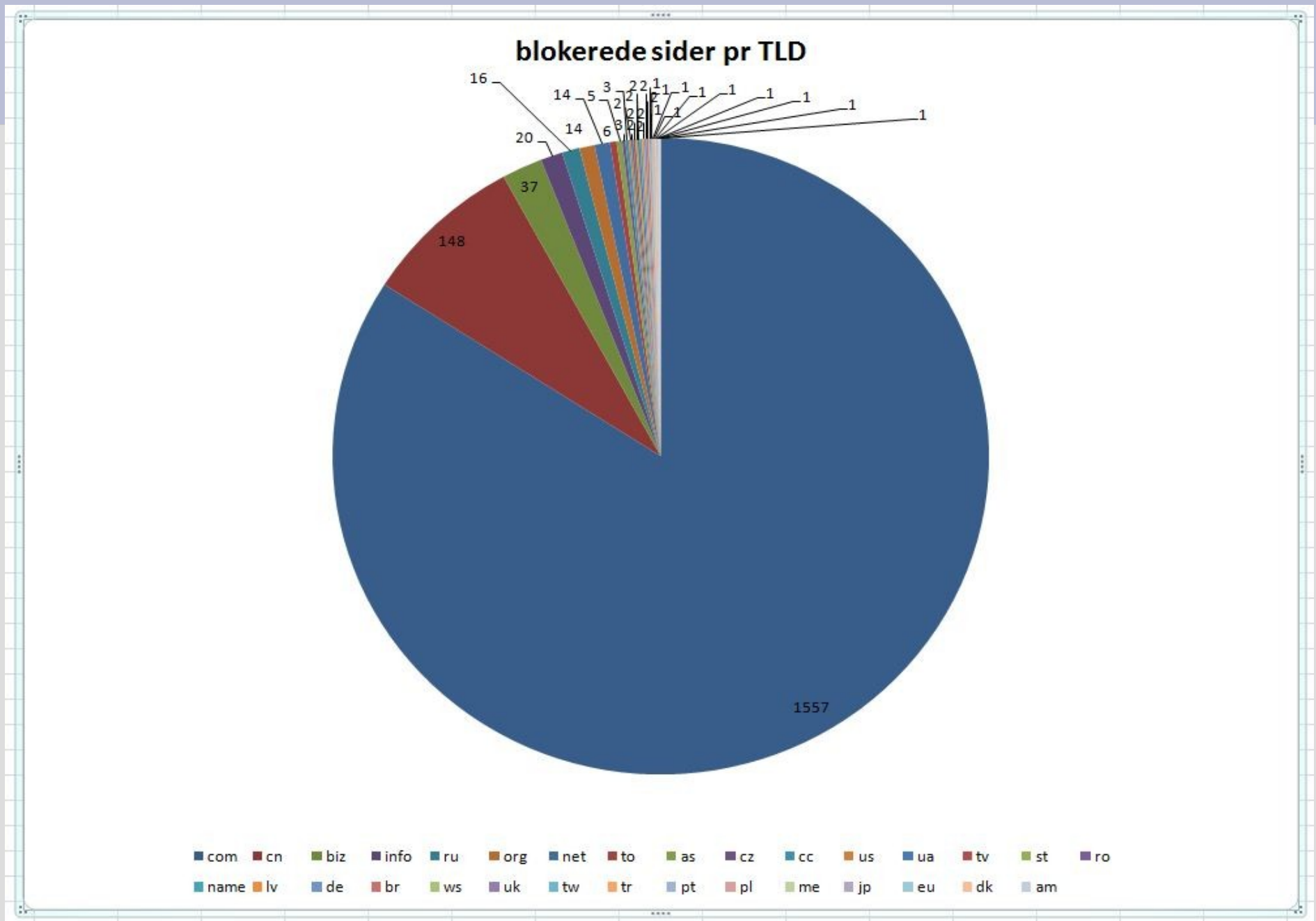
- Gecko, MSIE, Opera, Mozilla, -, Privoxy, Netscape, Konqueror, ., My-UA-String, Lynx, Site Sniper Pro, Webcollage, Rome client, porn_viewer larbin2.6.3, 12345, rrrrrrrr

Statistik - domæner

Børneporno filteret 25. marts 2010:

- 1853 domæner (i forhold til ~5000 i november 2009, der er blevet ryddet kraftigt op i listen)
- 720 af de 1853 er subdomæner under det samme .com domæne ?!
- Ialt 1557 .com domæner eller ~84% af alle
- Ingen .dk domæner (pånær test domæne stop.politi.dk (som iøvrigt kun resolver til en IP på censurerede resolvere))

Statistik - Domæner



Statistik - hits

Før oprydning, tilfældig dag i december 2009:

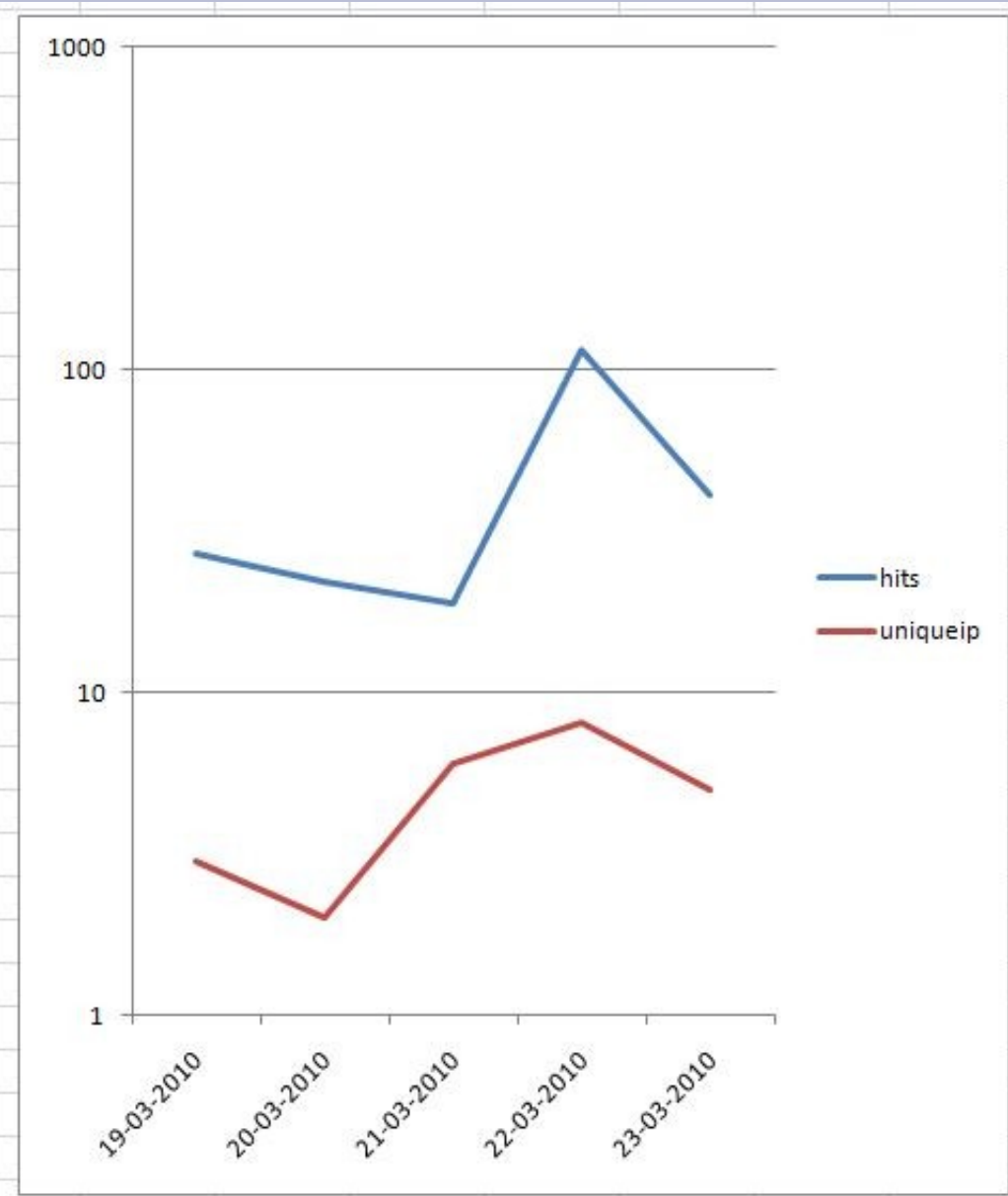
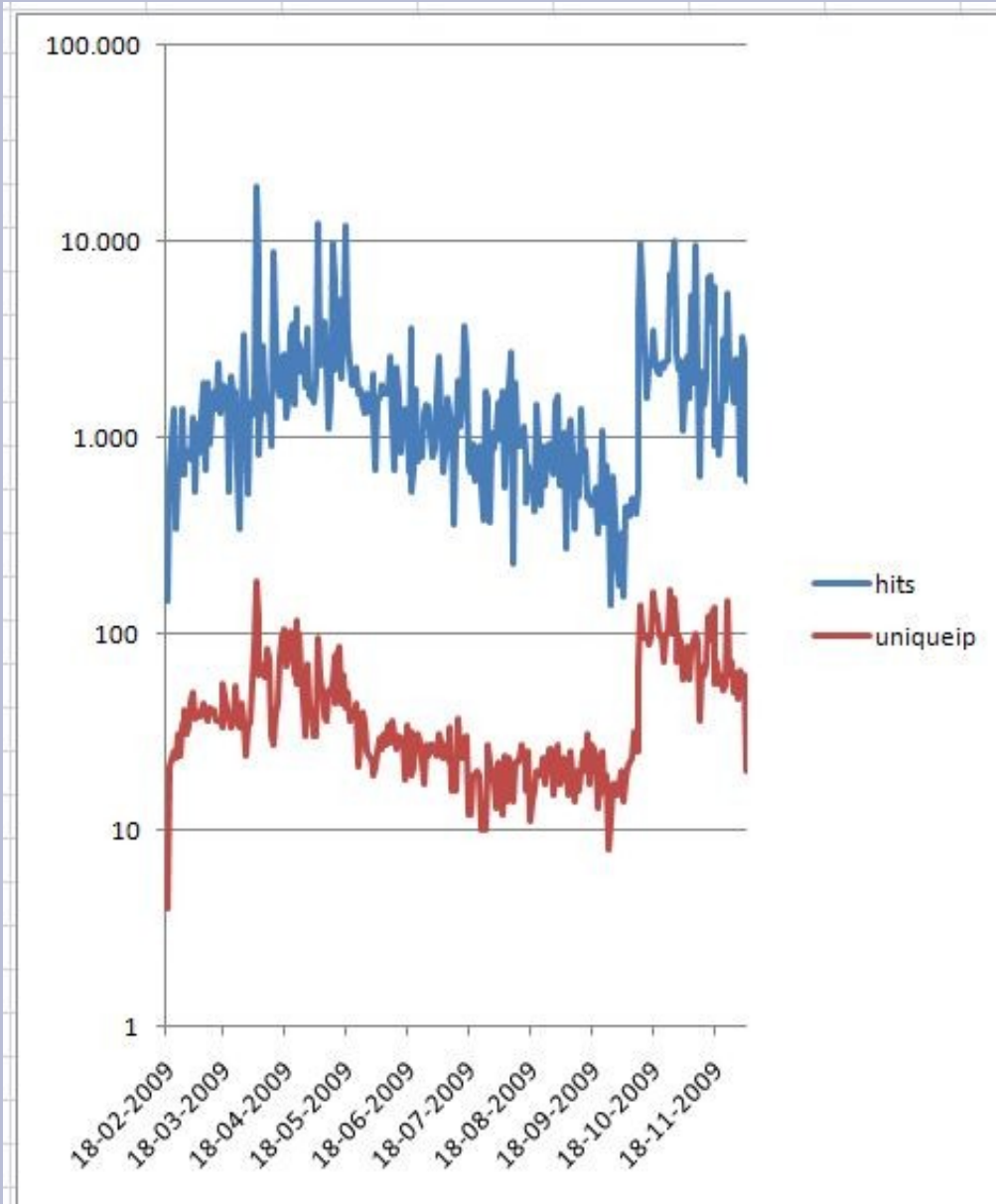
- 3270 hits på stop siden, 50 unikke IP adresser, 6 af de 50 IP har mere end 100 hits. 38 IP har under 10 hits.

Efter oprydning, tilfældig dag i marts 2010:

- 115 hits på stop siden, 8 unikke IP, 2 IP har 100 hits, resten har under fem hits hver.

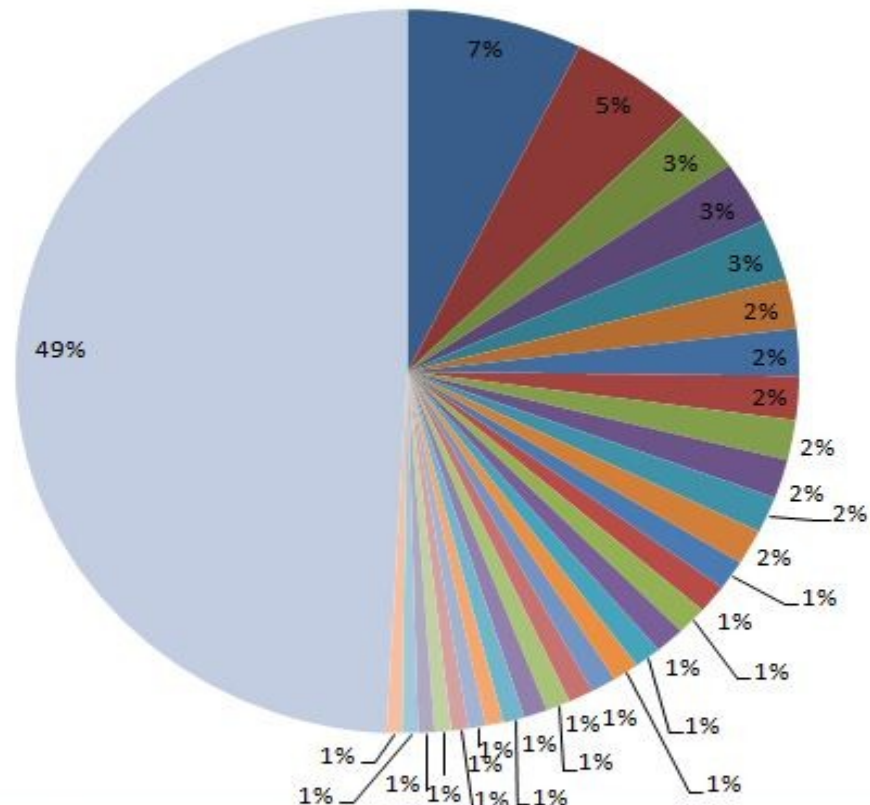
BEMÆRK: Antal hits skal altid divideres med to grundet favicon.ico requests!

Statistik – hits vs. unikke IP adresser



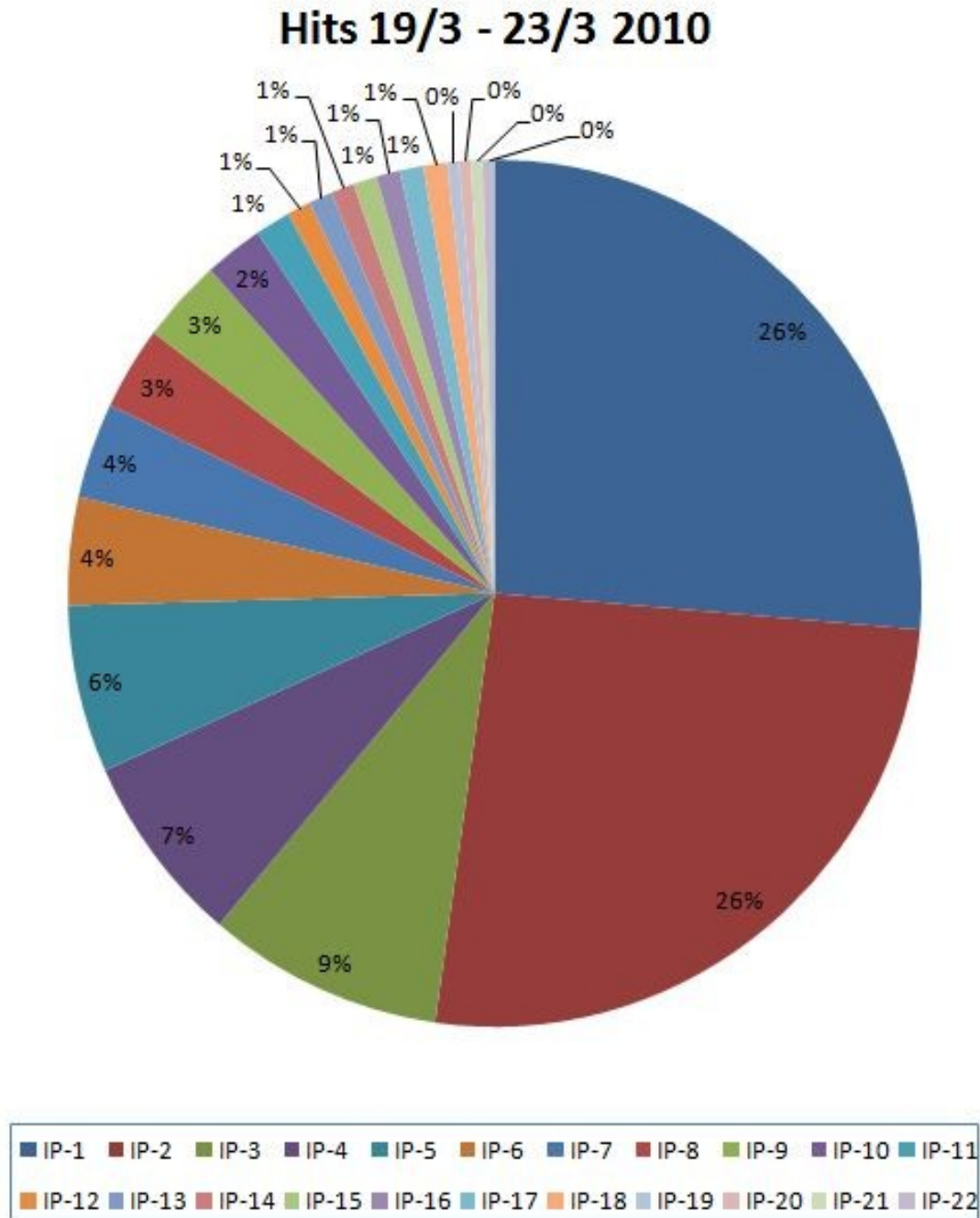
Statistik – hits vs. unikke IP adresser

Hits 18/2 - 3/12 2009



IP-1	IP-2	IP-3	IP-4	IP-5	IP-6	IP-7
IP-8	IP-9	IP-10	IP-11	IP-12	IP-13	IP-14
IP-15	IP-16	IP-17	IP-18	IP-19	IP-20	IP-21
IP-22	IP-23	IP-24	IP-25	IP-26	IP-27	IP-28
IP-29	IP-30	3.046 IP adresser				

Statistik – hits vs. unikke IP adresser



Statistik – andre protokoller

Jeg har ladet daemonlogger køre på blokerings serveren i 48 timer for at se hvad der bliver blokeret som ikke er HTTP trafik. Næsten alle applikationer bruger DNS og vil ramme blokerings serveren, men der er kun taget højde for HTTP trafik mht. STOP siden.

En del af det blokerede trafik er SMB malware (port 139+445 scans), men der er også (så vidt jeg kan se) reelle connect-forsøg på: tcp/21, tcp/22, tcp/25, tcp/5900, tcp/6000, udp/53 og mange andre porte.

Statistik – andre protokoller

Wireshark: Summary

File
Name: c:\tr\block itpol\daemonlogger.pcap.1269272188
Length: 4250257 bytes
Format: Wireshark/tcpdump/... - libpcap
Packet size limit: 65535 bytes

Time
First packet: 2010-03-22 16:51:29
Last packet: 2010-03-25 15:00:02
Elapsed: 02 days 22:08:33

Capture
Interface: unknown
Dropped packets: unknown
Capture filter: unknown

Display
Display filter: none

Traffic	Captured	Displayed	Marked
Packets	4435	4435	0
Between first and last packet	252513,329 sec		
Avg. packets/sec	0,018		
Avg. packet size	942,339 bytes		
Bytes	4179273		
Avg. bytes/sec	16,551		
Avg. MBit/sec	0,000		

Help Close

Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00%	4435	4179273	0,000	0	0	0,000
Ethernet	100,00%	4435	4179273	0,000	0	0	0,000
Internet Protocol	100,00%	4435	4179273	0,000	0	0	0,000
Transmission Control Protocol	97,43%	4321	4168066	0,000	802	52628	0,000
Data	79,32%	3518	4114004	0,000	3518	4114004	0,000
Sinec H1 Protocol	0,02%	1	1434	0,000	0	0	0,000
Data	0,02%	1	1434	0,000	1	1434	0,000
User Datagram Protocol	1,51%	67	7635	0,000	0	0	0,000
Domain Name Service	1,15%	51	3935	0,000	51	3935	0,000
NetBIOS Name Service	0,07%	3	276	0,000	3	276	0,000
Data	0,29%	13	3424	0,000	13	3424	0,000
Internet Control Message Protocol	1,06%	47	3572	0,000	47	3572	0,000

Help Close

En usædvanlig supportsag

Fra kunde (søndag formiddag):

Hej

Jeg er meget ked af og meget flov over den email jeg har skrevet til jer.

Må sige jeg fik lidt af et chok da jeg så hvad jeg havde skrevet dagen forinden.

Havde været i byen og fået en lille kæp i øret og har ikke været helt ædru da jeg skrev til jer.

Jeg har dog oplevet mange gange at klikke på et link hvor der så derefter kommer et "politi skilt" frem på skærmen. Det syntes jeg er ret ubehageligt, da der ikke skulle ligge noget ulovligt eller andet bag links`ene. Indrømmer blankt at det ofte er sider med links til unge piger/kvinder, der fører til de "politi-skilte". Men der skulle ikke ligge noget ulovligt bag og det er det der undrer mig og virker ret irriterende.

Venlig hilsen

x x

En usædvanlig supportsag

Til kunde (mandag morgen):

Hvilken side er det, du prøver at tilgå og ikke mener bør være blokeret?

Mvh

Support

En usædvanlig supportsag

Til kunde:

Jeg beklager generne ved vores filter.

Der vil altid havne nogle reelle sider i vores filter. Hvis du mener at vi filtrerer en side eller flere sider, som ikke indeholder ulovligt materiale, så skal du blot sende os linket og en begrundelse, så kigger vi på det og får åbnet hvis alt er i orden.

En usædvanlig supportsag

Fra kunde:
Hej

Der er nogle af dem her der har ført til en spærring nogle gange. Jeg vil ikke mene at der skulle være noget forkert i nogle de links.

<links klippet ud>

Men det må der jo være alligevel, men det ser bare ikke umiddelbart sådan ud.

Venlig hilsen x x

En usædvanlig supportsag

Til kunde:

Vi har bedt politiet om at undersøge disse sider nærmere. Vi vender tilbage, når vi hører mere.

En usædvanlig supportsag

Til kunde (14 dage senere):

Det er nu muligt at tilgå ovenstående sites igen.

thepiratebay.org

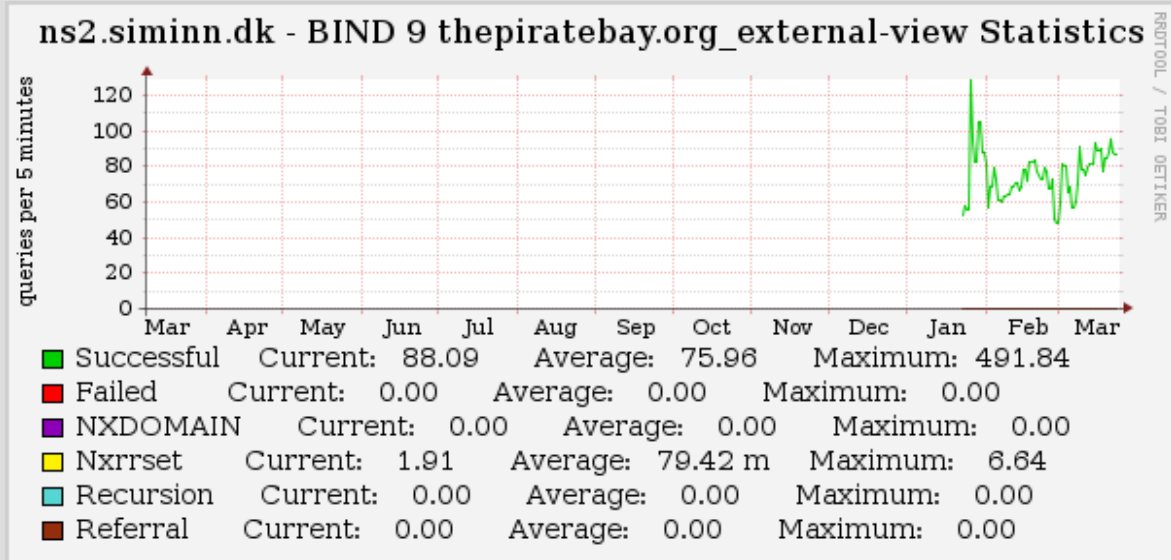
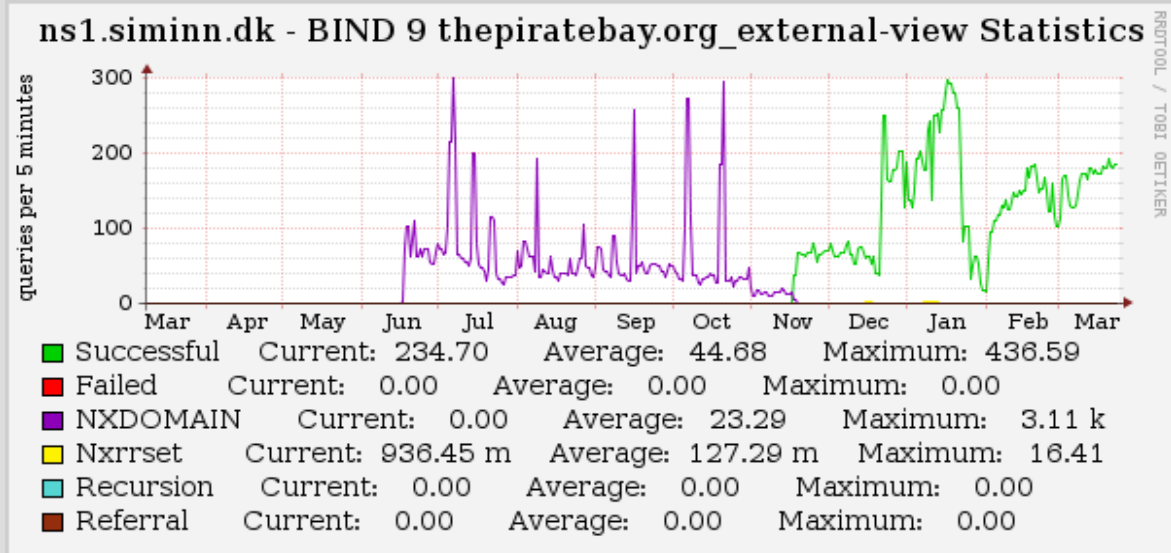
Statistik for thepiratebay.org blokeringen

Statistik - thepiratebay.org

thepiratebay.org blokeringen er implementeret på samme måde som børneporno filteret, dog uden opdatering, webstatistik og logfiler.

- Lidt over 50 DNS opslag i minuttet tilsammen på begge servere i thepiratebay.org zonen
- Niveaulet lader ikke til at falde (sandsynlig årsag: torrents indeholder også andre trackere end TPBs så folk får stadig deres data, og bemærker derfor ikke blokeringen, og skifter derfor ikke DNS server.)

Statistik - thepiratebay.org



Censur på nettet i praksis

Spørgsmål ?