



SPAMHAUS

THE **SPAMHAUS** PROJECT

4. MAILSERVER-KONFERENZ 2009



Welcome! In the next 75 minutes:

-➤ About Spamhaus
-➤ Spammer infrastructure
-➤ Stories from the field
-➤ All mixed with your questions



SPAMHAUS
THE SPAMHAUS PROJECT

**But first some
questions for you!**



SPAMHAUS
THE SPAMHAUS PROJECT

**Who here is doing spam
research and/or filtering?**



SPAMHAUS
THE SPAMHAUS PROJECT

**Are you using
Spamhaus data?**



SPAMHAUS
THE SPAMHAUS PROJECT

**Are you happy
with it?**



About Spamhaus

-➤ Since 1998, non-profit
-➤ Headquartered in the UK
-➤ 30+ specialists around the world
-➤ DNSBLs: SBL, XBL and PBL
-➤ ROKSO, DROP
-➤ Corporate research team



Spamhaus relations

-➤ ISPs / ESPs / xSPs
-➤ Networks and regulators
-➤ Registries and registrars
-➤ Law enforcement
-➤ Research community



Spamhaus users

-> Small, medium, large ISPs / ESPs
-> Mobile networks
-> Governments & law enforcement
-> Universities
-> Military
-> ...



SPAMHAUS
THE SPAMHAUS PROJECT

Over

1.500.000.000

mailboxes protected with our data



SPAMHAUS
THE SPAMHAUS PROJECT

**So what exactly is
our data?**



SPAMHAUS
THE SPAMHAUS PROJECT

Part one: DNSBLs



SPAMHAUS
THE SPAMHAUS PROJECT

Spamhaus SBL

Spamhaus Block List



Spamhaus SBL

-➤ 100% human input
-➤ Static spam sources
-➤ Spam webhosting / DNS
-➤ Other spam support services
-➤ Escalations if needed



Spamhaus SBL

-➤ Since the start of proxy and later botnet usage we can't manually list every emitter
-➤ Static spammers, snowshoe spam, Spammer infrastructure



Snowshoe spam

75.127.2.32	mail2.urexqsteweb.com
75.127.2.33	mail3.funexqstarts.com
75.127.2.34	mail4.myexqstearts.com
75.127.2.35	mail5.fnexqsitearts.com
75.127.2.36	mail6.myfnexqsteart.com
75.127.2.37	mail7.funexqstartz.com
75.127.2.38	mail8.exqsteartstes.com
75.127.2.39	mail9.webexqsteart.com
75.127.2.40	mail10.myexqsiteartsz.com
75.127.2.41	mail11.bestexqstartss.com
...	



Spamhaus SBL

-➤ Spammer infrastructure: DNS servers, web servers, MX, backends, C&C servers, reverse proxies, payment gateways, etc.
-➤ SpamAssassin URIBL_SBL



Spamhaus SBL

→ Spam URL `storemedstthank.com`

```
storemedstthank.com. 2D IN NS ns1.wooddoes.in.  
storemedstthank.com. 2D IN NS ns2.wooddoes.in.
```

```
ns2.wooddoes.in has address 60.191.239.153  
ns2.wooddoes.in has address 61.191.191.241  
ns2.wooddoes.in has address 218.75.144.6  
ns2.wooddoes.in has address 119.39.238.2  
ns2.wooddoes.in has address 203.93.208.86
```



Spamhaus DROP

-➤ Don't Route Or Peer list
-➤ Known rogue networks / IP ranges / ASNs, 100% under spammer control
-➤ Excellent for no-traffic policies and router/firewall usage



Spamhaus DROP

-➤ Using DROP makes lots of Botnet C&Cs, rogue DNS servers and web-based exploits ‘drop off the net’



SPAMHAUS
THE SPAMHAUS PROJECT

Spamhaus XBL

Spamhaus eXploits Block List



Spamhaus XBL

-➤ 100% automated input
-➤ Lists illegal 3rd party exploits
-➤ Only /32 listings
-➤ No-questions-asked (but limited) removals



SPAMHAUS
THE SPAMHAUS PROJECT

1649318



SPAMHAUS
THE SPAMHAUS PROJECT

1649318

Zombies detected by XBL on
7th of july 2010 (unique IP addresses)



SPAMHAUS
THE SPAMHAUS PROJECT

36



36

seconds between infection and
first-spam-sent (W32/Warezov)



Spamhaus XBL

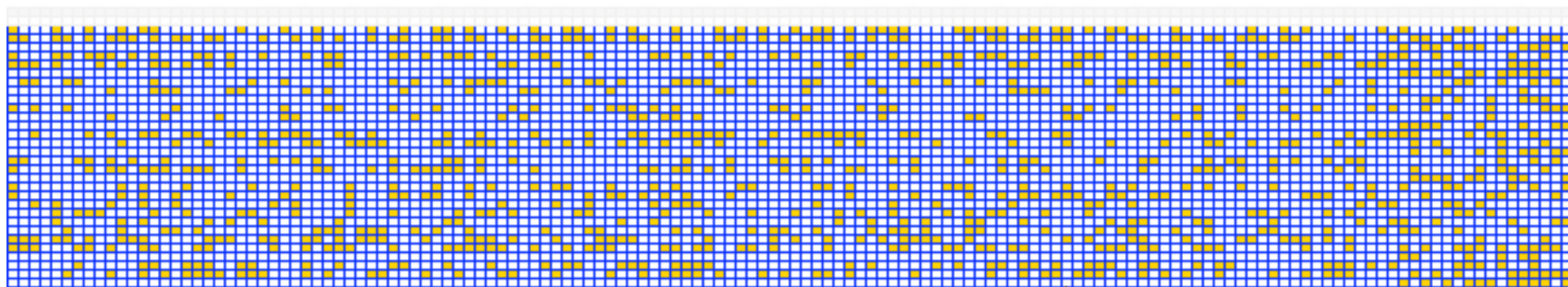
- Botnet tracking (2/3 is known)
- Stats per botnet
- ISP tracking
- Country tracking



SPAMHAUS
THE SPAMHAUS PROJECT

Spamhaus XBL

.....➤ Good ISP
(Vodacom in South Africa)



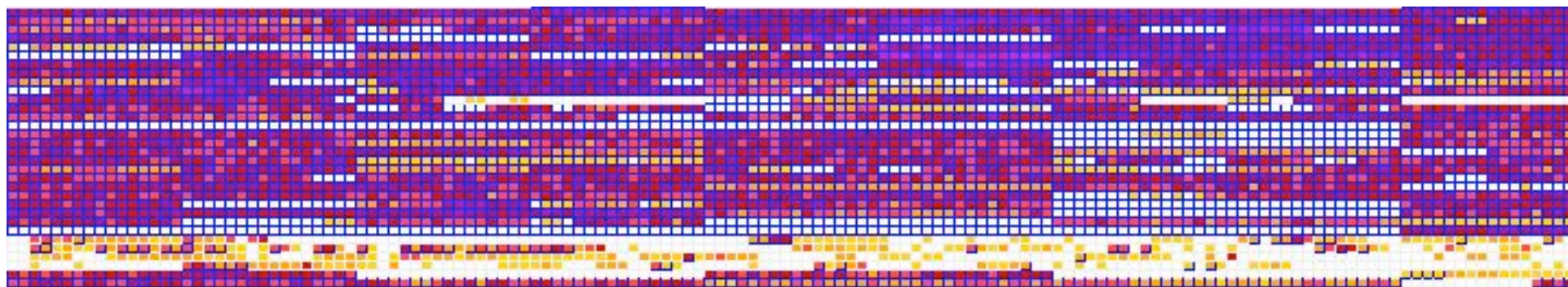


SPAMHAUS
THE SPAMHAUS PROJECT

Spamhaus XBL

.....> Bad ISP

(Vietnam Datacom Company)

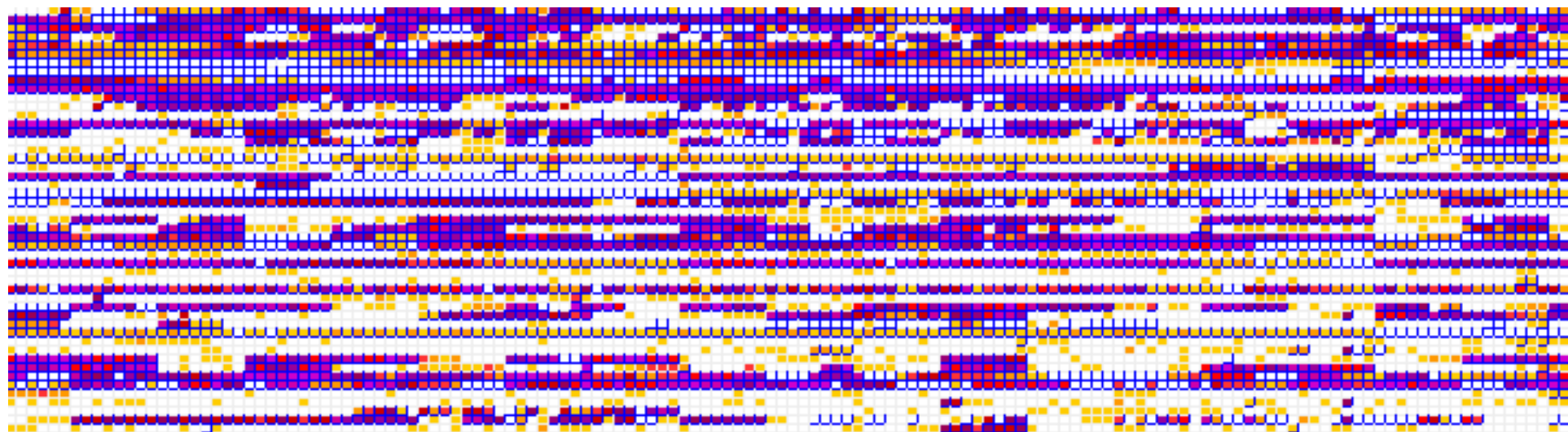




SPAMHAUS
THE SPAMHAUS PROJECT

Spamhaus XBL

.....➤ Zooming out: bad region
(South America / LACNIC)





SPAMHAUS
THE SPAMHAUS PROJECT

Spamhaus PBL

Spamhaus Policy Block List



Spamhaus PBL

-➤ Spamhaus Policy Block List
-➤ List ranges that should not do direct-to-MX
-➤ Input by Spamhaus and ISPs
-➤ No questions asked single IP removal



Spamhaus PBL

-➤ Over 600 million IP addresses listed
-➤ 1/3rd contributed by ISPs
-➤ Big German participants:
Arcor, 1&1, Netcologne
-➤ Big other ISPs:
Comcast, Roadrunner, Verizon



SPAMHAUS
THE SPAMHAUS PROJECT

Spamhaus DBL

Spamhaus Domain Blocklist



Spamhaus DBL

-➤ Provide additional protection against spam that passes IP-based DNSBLs
-➤ Shorten the usable lifespan of spammer controlled domains
-➤ Help registrars and registries protect their TLD(s)



What is the input for the DBL?

-➤ Domains, domains, domains
-➤ And some IP addresses as well
-➤ Not only bad domains!



And then?

-➤ DBL engine processes each domain to calculate reputation
-➤ Bad domains are put into the DBL zone
-➤ New zone is built and distributed to worldwide users ***every minute***



What ends up in the zone?

-➤ Domains fully under the control of cybercriminals and spammers
-➤ Used for spam, phishing or malware distribution
-➤ These domains will have either been used in spamvertized URLs or as nameservers, redirectors, reverse DNS, etc.



Some lessons learned (1)

-➤ The big 'Ruskranian' spam operations use new domains every few minutes
-➤ So, they consider domains a throw-away resource!
-➤ Makes them very different from regular customers, who tend to be in it for the long run



Some lessons learned (2)

-➤ Some spammers 'age' domains: domains are not always used directly after registration
-➤ Aging can be weeks or months, periods of over a year have been seen in the wild



Some lessons learned (3)

-➤ Who considers rogoxxywtrcwph.info to be a legit domain?
-➤ Apparently there is no need to hide
-➤ Some register domains like these in batches of thousands



Some lessons learned (4)

-➤ Speaking of hiding... whois privacy protection is still strongly associated with badness
-➤ Roughly 1 in 5 privacy protected domains we see ends up being listed in the DBL



Some lessons learned (5)

-➤ Some registrars have over 90% of their sponsored domains listed
-➤ We doubt the legitimacy of these kind of 'registrars'



Some lessons learned (6)

-➤ Domains have become a vital part of the spammer infrastructure
-➤ Resiliency is built by spreading over TLDs, registrars and nameservers



SPAMHAUS
THE SPAMHAUS PROJECT

Trends in spammer infrastructure



Current 'hot technologies' (1)

-➤ P2P botnets
-➤ Reverse proxies
-➤ VPN usage
-➤ Fast flux / bulletproof hosting



Current 'hot technologies' (2)

-➤ DNS hijacking
-➤ Malware staging
-➤ iframe exploits
-➤ Legit website compromises



SPAMHAUS
THE SPAMHAUS PROJECT

P2P

No more easy C&C shutdown



SPAMHAUS
THE SPAMHAUS PROJECT

Reverse proxies

Content is not where it seems to be



SPAMHAUS
THE SPAMHAUS PROJECT

VPN

Shady VPN providers
deliver encrypted anonymity



SPAMHAUS
THE SPAMHAUS PROJECT

Fast flux

x new locations. Every y minutes.



SPAMHAUS
THE SPAMHAUS PROJECT

DNS hijacking

Addresses are not
where they seem to be



SPAMHAUS
THE SPAMHAUS PROJECT

Malware staging

Modulized malware for specific tasks



SPAMHAUS
THE SPAMHAUS PROJECT

iframe exploits

Embed badness in any webpage



SPAMHAUS
THE SPAMHAUS PROJECT

Legit website compromises

Get infected by visiting the website
of the local soccer team



Compromise-du-jour

..... ❖ Spamvertized:

<http://emaze.gr/phenol17.html>

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML (etc)
<html><head>
<META HTTP-EQUIV="refresh"
CONTENT="0;URL=http://ersteskur.com">
    <title></title>
</head></html>
```




SPAMHAUS
THE SPAMHAUS PROJECT

Stories from the field



Storm worm web-based updates

```
server {
    listen          80;
    server_name     localhost;
    access_log      logs/host.access.log  main;

    include conf/blacklistrules;

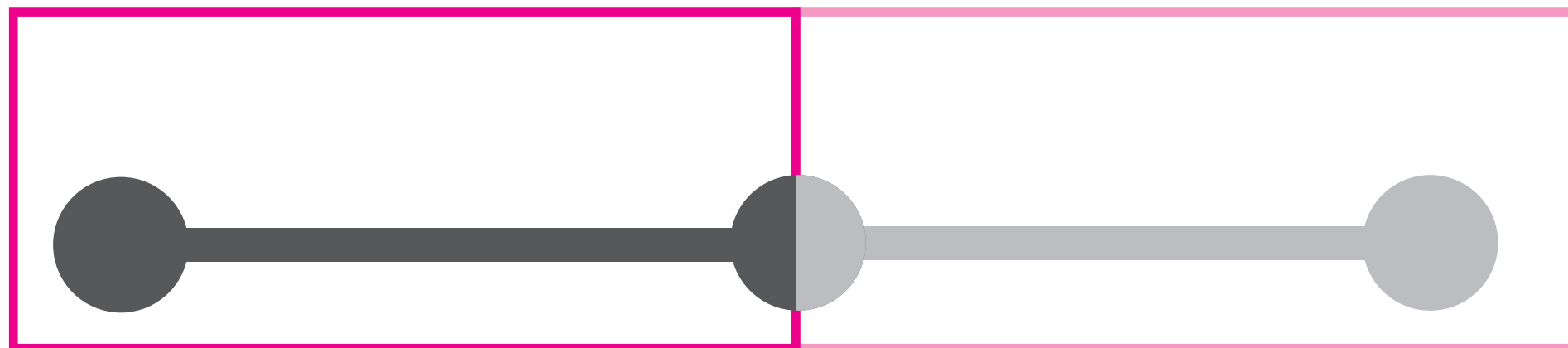
    location ~ /aff/.* {
        proxy_pass      http://216.255.187.146:80;
        proxy_set_header X-Real-IP  $remote_addr;
    }
}
```



Storm worm web-based updates

Visible with packetlogging

Only visible at ISP!



Storm
infectee

nginx
server

real server
containing
the malware



Custom proxies

-> *nix binary for web and DNS
-> Built in list of good guys
-> Good guys (us!) firewalled with iptables
-> Deletes itself from disk on startup



Back-end zonefile

-➤ Administrative domain for spammer infrastructure found with passive DNS
-➤ Due to config error whole zone was found



Back-end zonefile

- 241 DNS records pointing to over 100 servers
- Hosted at 25 ISPs
- In 11 countries



Back-end zonefile

001	1H	IN	A	195.128.
agava1	1H	IN	A	89.108.7
anyy	1H	IN	A	192.168.
backup	1H	IN	A	208.43.6
backup2	1H	IN	A	75.126.2
chat	1H	IN	A	195.128.
china100	1H	IN	A	211.91.2
china105	1H	IN	A	111.67.2
china106	1H	IN	A	60.191.2
china111	1H	IN	A	119.18.2
china113	1H	IN	A	59.63.15
china119	1H	IN	A	111.67.2
china121	1H	IN	A	218.10.1



Back-end zonefile

china122	1H	IN	A	61.235.1
china125	1H	IN	A	61.191.6
china127	1H	IN	A	61.191.1
china128	1H	IN	A	60.172.2
china129	1H	IN	A	61.191.1
china130	1H	IN	A	222.172.
china132	1H	IN	A	222.241.
china133	1H	IN	A	221.12.8
china134	1H	IN	A	218.93.2
china135	1H	IN	A	219.72.2
china136	1H	IN	A	202.111.
china137	1H	IN	A	121.14.1
china138	1H	IN	A	60.172.2





Back-end zonefile

china139	1H	IN	A	61.158.1
china140	1H	IN	A	218.75.1
china141	1H	IN	A	59.53.88
china142	1H	IN	A	218.75.1
china143	1H	IN	A	58.218.2
china144	1H	IN	A	121.170.
china145	1H	IN	A	61.191.1
china146	1H	IN	A	222.138.
china147	1H	IN	A	59.53.91
china148	1H	IN	A	222.241.
china149	1H	IN	A	60.172.2
china150	1H	IN	A	60.172.2
china151	1H	IN	A	58.17.36





Back-end zonefile

china152	1H	IN	A	218.10.1
china153	1H	IN	A	117.41.1
china154	1H	IN	A	61.191.1
china155	1H	IN	A	218.10.1
china156	1H	IN	A	61.191.1
china157	1H	IN	A	60.172.2
china158	1H	IN	A	60.172.2
china159	1H	IN	A	222.138.
china160	1H	IN	A	220.181.
china161	1H	IN	A	61.191.1
china162	1H	IN	A	121.11.8
china163	1H	IN	A	218.61.1
china164	1H	IN	A	58.218.1





Back-end zonefile

china165	1H	IN	A	121.10.1
china166	1H	IN	A	123.164.
china167	1H	IN	A	211.234.
china168	1H	IN	A	218.61.1
china169	1H	IN	A	61.235.1
china170	1H	IN	A	222.162.
china171	1H	IN	A	124.248.
china172	1H	IN	A	58.218.1
china173	1H	IN	A	60.172.2
china174	1H	IN	A	61.191.1
china175	1H	IN	A	59.34.19
china176	1H	IN	A	61.158.1
china177	1H	IN	A	218.93.2





Back-end zonefile

china178	1H	IN	A	219.129.
china79	1H	IN	A	222.241.
china95	1H	IN	A	59.53.88
clock	1H	IN	A	195.128.
clock	1H	IN	A	195.128.
cvs	1H	IN	A	80.93.56
czech1	1H	IN	A	193.104.
de	1H	IN	A	195.95.1
dev	1H	IN	A	195.128.
dim	1H	IN	A	80.250.2
egor1	1H	IN	A	89.149.1
eurovps1	1H	IN	A	77.235.4
gera2	1H	IN	A	195.190.



Back-end zonefile

gera3	1H	IN	A	91.207.4
german1	1H	IN	A	89.149.2
glavmedvds	1H	IN	A	92.63.11
holland1	1H	IN	A	85.12.25
hongkong1	1H	IN	A	119.42.1
hop1	1H	IN	A	217.65.9
hop2	1H	IN	A	217.65.9
hop2mf	1H	IN	A	217.65.9
hop3	1H	IN	A	217.65.9
hop4	1H	IN	A	89.188.1
icq	1H	IN	A	195.128.
incom-mail	1H	IN	A	82.146.4
ipserver3	1H	IN	A	91.193.1



Back-end zonefile

ipserver6	1H	IN	A	95.211.1
isps	1H	IN	A	82.146.5
isps-nss	1H	IN	A	82.146.3
isps10	1H	IN	A	78.24.21
isps11	1H	IN	A	92.63.11
isps12	1H	IN	A	82.146.4
isps2	1H	IN	A	82.146.4
isps3	1H	IN	A	82.146.3
isps4	1H	IN	A	82.146.5
isps5	1H	IN	A	82.146.4
isps6	1H	IN	A	82.146.4
isps7	1H	IN	A	82.146.4
isps8	1H	IN	A	82.146.3



Back-end zonefile

```
isps9          1H IN A      82.146.3
israel2        1H IN A      82.166.4
israel3        1H IN A      212.150.
jabb           1H IN A      67.228.8
jail-mail      1H IN A      91.209.1
jail1          1H IN A      195.95.1
jail2          1H IN A      195.95.1
jail3          1H IN A      91.208.1
knock-test     1H IN A      195.128.
knock-welcome  1H IN A      174.36.2
kvm            1H IN A      195.128.
livechat       1H IN A      195.128.
localhost     1H IN A      127.0.0.
```



Back-end zonefile (highlights)

backup	1H	IN	A	208.43.6
backup2	1H	IN	A	75.126.2
chat	1H	IN	A	195.128.
cvs	1H	IN	A	80.93.56
icq	1H	IN	A	195.128.
incom-mail	1H	IN	A	82.146.4
livechat	1H	IN	A	195.128.
nagios	1H	IN	A	74.86.30
mysql.otrs	1H	IN	A	89.188.1
send-mail	1H	IN	A	82.146.4
support-wiki	1H	IN	A	195.128.
vpn-node	1H	IN	A	67.228.9
wiki	1H	IN	A	174.37.1



SPAMHAUS
THE SPAMHAUS PROJECT

Funnies

Stories from the field



Babblefish or?

How are you.

Me as the Min-ho, Jeong which is in Korea it does. The SBL the bedspread where the mail server child blood of our company is register in list.

The IP Block the substitute actor which is to the IDC and we among the rest are in the process of using one IP.



Happy ISP

Thank you for great help! How about your last weekend? Do you feel happy? Today is Monday. Your efficient reply gives me so much encouragement. Therefore, I won the praises for my job this morning. Personally this praise should be given to you honestly. Furthermore, I hope more efficient cooperation between Spamhaus and [elided] will proceed.



An invitation...

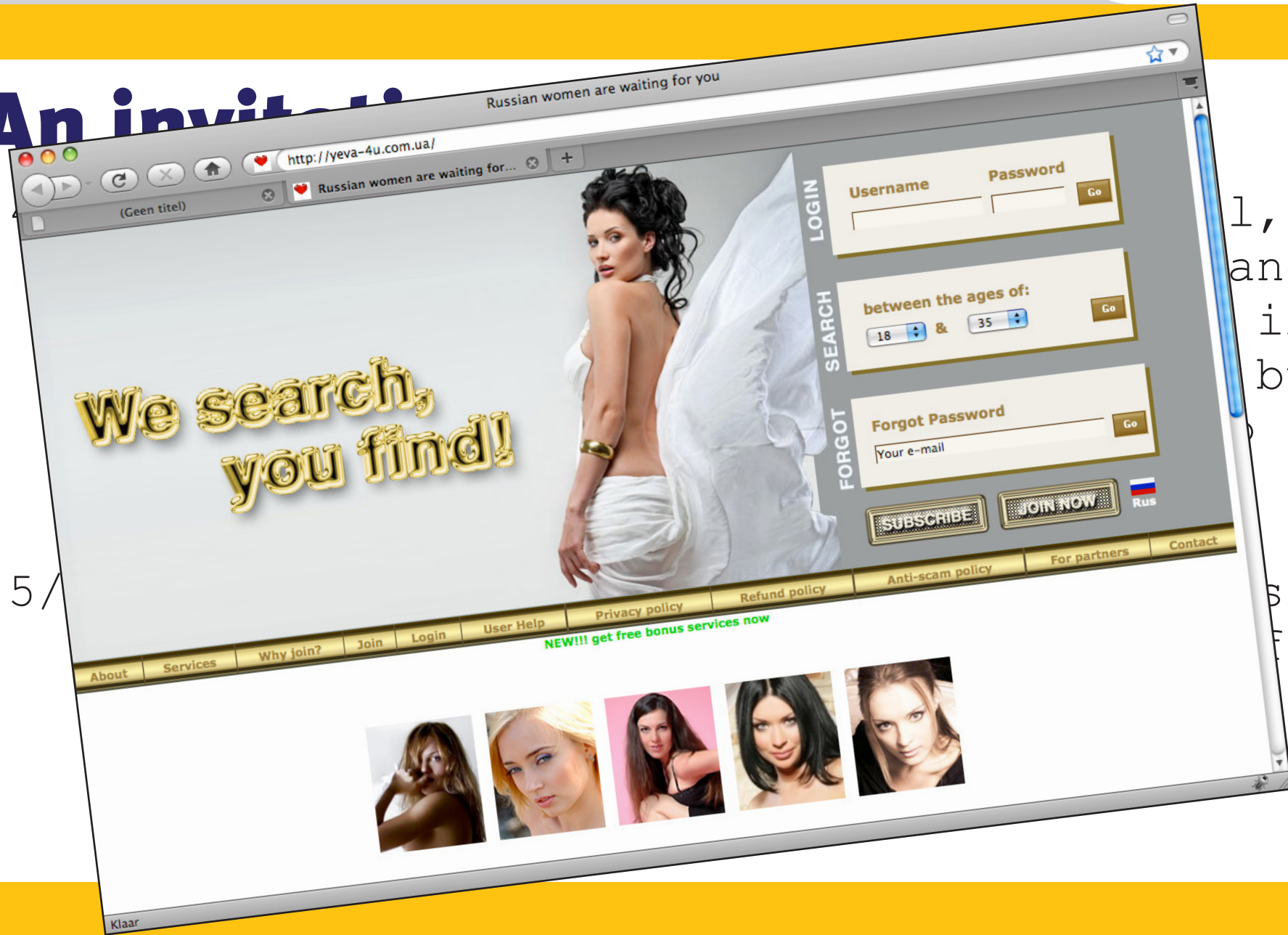
- 4/ it is not our main business, we have oil, real estate businesses here, in Moscow and Saint-Petersburg. so we are not so good in Internet business, sure we can mistake, but we wish to work well, to have friendship with you.

- 5/ we are willing to invite you to visit Russia, we will organize it for free everything for you here for high class. you can see that we are good comapny with good people and we are not spammers and scammers at all.



SPAMHAUS
THE SPAMHAUS PROJECT

An invitation



1,
and
in
but

ssia,
for
we
are

5/



SPAMHAUS
THE SPAMHAUS PROJECT

Closing up...



Closing up...

-➤ Thank you! But...
-➤ We must try harder. Problems are getting more serious and harder to solve.