Stop. Outbound. Spam.
S.O.S.
About Spamhaus

- 30 researchers worldwide.
- Used daily by 1.7 billion users.
- IP, domain & URI reputation data.
- Extending to DNS with BIND RPZ.
Contrary to popular belief, Spamhaus **DOES NOT** block spam or filter any email content.
Spamhaus Mission

“To research and publish the most **accurate** internet reputation data.”

“This data enables users to make **informed** decisions on what network connections should be accepted.”
S.O.S. Recommendation #1

**Start** using XBL **today.**
Stop talking to bad guys.

Japan Net Neutrality regulations do not apply since there is Zero packet filtering.
XBL

eXploit Block List

1,500,000 bad IPs tracked worldwide

36 seconds - time to start spam (W32/Warezov)
Spamhaus XBL

- 100% automated input.
- Traps, sinkholes, prod systems.
- Botnet tracking – 66% of listings.
- IP’s with confirmed bad behavior.
- /32 listings - No question removals.
Spamhaus XBL

- Stats per botnet, ISP, country.
- Data visualization.
- Detailed intelligence available.
Good vs. Bad Netblock
Spamhaus XBL

- **Exploit intelligence:**

  128.127.46.188, IP DETECTED
  AS12871, ASN
  128.127.32.0/20, IP RANGE
  NL, COUNTRY
  concepts.nl, ISP/NETWORK
  postmaster@concepts.nl, CONTACT
  1361260266, TIMESTAMP
  s_hermes 87.255.51.229 80 1059 get-msg.org
  BOT NAME          SINKHOLE IP          DST & SRC PORT    C&C DOMAIN
S.O.S. Recommendation #2

Implement DBL.
DNS Firewall with BIND RPZ.

Protect users from getting infected.
DBL – not just for email

- “In-message” URI click filter.
- Use as DNS Firewall.
- Resolvers now re-direct users.
- Inbound and outbound mitigation.
- Shorten the lifespan of bad domains.
DBL – what URIs?

- Domains under miscreant control.
- Phishing & malware distribution.
- Spamvertized URI, redirectors, shorteners, reverse DNS botnets, C&C, etc...
- Updates every 10 seconds.
S.O.S. Recommendation #3

a) Stop C&C Botnets.
b) DROP criminal traffic.
Spamhaus C&C

- IP addresses used for botnet command/control.
- Impact C&C communications.
- Block on router level or DNS.
- Monitor own network for infection.
- Prevent outbound spam.
Spamhaus DROP

- Worst of the worst.
- IP space under control of bad guys.
- Use on router/firewall.
- Monitor own network for infection.
S.O.S. Recommendation #4

Use SBL/PBL if possible.
The foundation of your efforts.
Spamhaus SBL Data

- 100% IP Based.
- Human and automated input.
- Static Spam sources.
- Spam Webhosting / DNS.
- Other spammer support services.
SBL identifies:

- Spammer infra: DNS servers, web servers, MX Servers, C&C Server, reverse proxies, payment gateways, MITM injections, exploit pages, etc...
- Hijacked IP ranges & ASNs – used for fraud & spamming.
Use SBL to fight:

- Static spammers
- Snowshoe spam
- Spammer eco-system
Policy Block List

- Ranges with no direct-to-MX.
- Input by Spamhaus and ISPs.
- No question asked single IP removal.
- 925 million IP addresses.
- ISP can add custom policies and info.
The End.

almost...
Together we can win

- We need your help.
- Let's share knowledge/expertise.
- Can we provide tools (passive DNS).
- How about Data sharing?
- Does JPRS want to play?
Network Self-Regulation Works.

“But not if you ignore concerns from other networks, or if you do not communicate. Others will block traffic from your network.”
Thank you!