M3AAWG
Messaging Malware Mobile Anti-Abuse Working Group

The Community and Operation of DNSWL

Matthias Leisi

Oct 5 2017

Toronto, Canada

What is dnswl.org?

...and why should you care?

Code of Conduct

M^{3}AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

M^{3}AAWG is dedicated to making our meetings and business open to all members and guests and to making it a safe place for all. We do not tolerate harassment of any kind.

We insist that all participants, attendees and meeting staff adhere to a civil demeanor at all times. This includes refraining from inappropriate language, comments and behavior, in person or by electronic communications and/or public or semi-public social media. In accordance with applicable law, M^{3}AAWG prohibits sexual harassment and harassment because of race, color, gender, age, religion, disability, sexual orientation or any other basis protected by federal, state or local law.

Participants, attendees and meeting staff who are being harassed, intimidated, or are dealing with otherwise improper behavior are encouraged to report it immediately to the Executive Director or a Board member without fear of repercussion.

Alternate methods of reporting issues include: contacts listed on the back of your badge, email to the Executive Director, jerry.upton@m3aawg.org, or if needed, calling the local police department.

Anyone who is found to be in violation of this policy may be handled in any one or more of these methods, depending on the offense: Warning, Expulsion, Contacting of employer, or Contacting the police or other legal authorities. Actions stronger than a warning will be taken at the discretion of the M^{3}AAWG Board of Directors.

M^{3}AAWG reserves the right to remove any participant or attendee at any time for any reason.

The policy also extends outside of the meeting rooms to include all areas of the meeting hotel and social gatherings sponsored by M^{3}AAWG or M^{3}AAWG member organizations.

Note: You can download this file at https://www.m3aawg.org/conduct-policy

dnswl.org in numbers

Positive reputation about 500‘000 IP addresses

30‘000 DNSWL Ids, 47‘000 domains

20 mio items of history information on the above

12‘500 Self Service users who maintain their information

100‘000 organisations using our list

250 mio DNS queries per day

Since 2006

dnswl.org in a nutshell

- We publish a list of IP addresses in typical RBL format
  - with four trust levels (none, low, medium, high)
  - “dig –t any 2.0.0.127.list.dnswl.org“
- Receivers use this information to improve the reliability of their filters
  - Exmple SpamAssassin: RCVD_IN_DNSWL* rules with negative scores
- We maintain the data by a mix of automation, user self service, and editorial oversight
  - Some default values apply based on the type of sender
  - Scores change up and down within certain limits automatically

What is dnswl.org?

dnswl.org for the ...

- Mail Receiver
- Community
- Subscribers

- Mail Sender

dnswl.org evolves

- IPv6
- Domain-based trust

dnswl.org for the Mail Receiver

- Weighted DNSxL response in MTA
  - postscreen_dnsbl_sites
- No greylisting for listed IPs
- Content filter / rule set adjustments
- Mail forwarded through whitelisted servers
  - trusted_networks
- Highlight in mail clients
- Take more risk with filtering rules, if you have solid whitelisting

postscreen_dnsbl_sites Example

```
postscreen_dnsbl_sites = zen.spamhaus.org*3
        b.barracudacentral.org*2
        bl.spameatingmonkey.net*2
        bl.spamcop.net
        dnsbl.sorbs.net
        psbl.surriel.com
        bl.mailspike.net
        list.dnswl.org=127.0.[0..255].0*-2
        list.dnswl.org=127.0.[0..255].1*-3
        list.dnswl.org=127.0.[0..255].[2..3]*-4
### This is the killer feature of Postfix 2.11 and later, which
### removes most of the pain associated with the after-220 tests, q.v.
### When a connecting host is at or below this score, the after-220
### tests are bypassed.
postscreen_dnsbl_whitelist_threshold = -1
```

Source: http://rob0.nodns4.us/postscreen.html

dnswl.org for the Community

- Contribute ☺

- Open to collaboration proposals
- Share your reputation data
- Increase the diversity of contributors - help with editing data

dnswl.org for the Subscribers

- Rsync or Query access

- Nameserver formats (bind, rbldnsd)
- Spamassassin trusted_networks files

- Community subscription

dnswl.org for the Mail Sender

- About 20 signals of trust
  - Automated response to positive and negative trust signals
  - IP, whois, domain, category, past history, changes in sending volume, correlations, aggregation (eg on AS or on /24)
  - Editorial decisions and overruling of automation
  - We. Are. Slow. On. Purpose.
  - none, low, medium, hi?

- Use Self Service

  ... and keep data up to date

- Special issue: “warming up” IPs
- Special issue: Third party sending / ESPs

Self Service In Depth

- Users „claim“ a DNSWL Id
  - like Domain Verification for SSL certs
- Users issue change requests on meta data and on IPs
  - Change requests are manually reviewed
- Users are asked to review and confirm their data after six months
- We send some notifications about noteworthy events
  - abuse messages, DNS gone missing/inconsistent, ...
  - not yet well structured, improvements over the coming months

Where do we take the project from here?

dnswl.org and IPv6

- Fully supported in our database since mid 2013.
- 1.5% of the IP ranges in our database are IPv6.
- Actual IPv6 traffic is only 0.15%.

- Standardisation of another query format?

- Why is the email ecosystem so reluctant to move to IPv6?

dnswl.org and domain names

- Attach trust to domains

- We need a verifiable domain name – likely DKIM-based
  - But which domain? d=, From:, ...
  - Strict alignment?
  - First- and third-party signatures

- We need to clarify the semantics.

Thank you!