DNSBLv5: About and usage

- 1 Contact / Removal
- 2 DNSBL v5.0
- 3 API
  - 3.1 APIv3
  - 3.2 APIv2 is deprecated
- 4 What is a DNSBL?
- 5 Resolving
  - 5.1 RBL Bitmasking Data
    - 5.1.1 dnsbl.tornevall.org
    - 5.1.2 bl.fraudbl.org
    - 5.1.3 Coming soon
    - 5.1.4 wl.tornevall.org - whitelisting system [PLANNED ONLY]
- 6 The FraudBL Project
  - 6.1 Fraudalent/phishing-tagged e-mail
- 7 Links
- 8 Project status

Contact / Removal

Removal requests are for the moment available but manually handled. Just send a mail to dnsbl@tornevall.org (or support@tornevall.net) with the address you want to have unlisted.

DNSBL v5.0

Check the bottom of this page to get more information about migrations to version 5 or here to view the DNSBL Project dashboard.

API

APIv3

TorneAPI v3.0 is coming up with a new request interface, which is configured via the TorneAUTH Control panel. Currently, the control panel is very simple and the only purpose of it, is to create the required API key that is required to do extended requests. For example, adding and delisting spamhosts. If you only need the resolving controls, you should consider using the DNS lookup instead of the API lookup as it is much faster than API requests.

If you still think that the API is the right way to go, continue reading at the new API description docs.

> **TorneAUTH Production and Test**
>
> The current environment of TorneAUTH is pointing at v3.0 (not to be mixed with the API release). If you are willing to take the risk, the test servers for TorneAUTH (unstable) is located at https://auth.tornevall.com (version 4) and https://auth.tornevall.nu (version 3 development).

APIv2 is deprecated

See the section for ~~APIv2.0~~ (deprecated) and ~~DNSBL API~~ (deprecated)

What is a DNSBL?

A DNS-based Blackhole List (DNSBL, Real-time Blackhole List or RBL), is a means by which an Internet site may publish a list of IP addresses, in a format which can be easily queried by computer programs on the Internet. As the name suggests, the technology is built on top of the Internet DNS or Domain Name System. DNSBLs are chiefly used to publish lists of addresses linked to spamming. Most mail transport agent (mail server) software can be configured to reject or flag messages which have been sent from a site listed on one or more such lists (Source)

We are regularly scanning new proxies that are reported to us and we're also trying to keep updated with the "Tor"-network proxies, a network that forgets that anonymity can be a problem when we are speaking abuse.

Resolving

dnsbl.tornevall.org: Default zone
opm.tornevall.org: Added 1 june 2016 (Deprecation as of 30 june 2013 was reverted)
bl.fraudbl.org: Added 22 june 2016

RBL Bitmasking Data

dnsbl.tornevall.org

Mask	Description	APIv3
1	DEPRECATED **IP address has been reported (As this bit has no real actual effect and rather is a false positive, it will be deprecated in short)** Meaning: The ip has been reported from a third party application, honeypot, but may not necessarily be confirmed by our local sweepers (this is for proxies) As there may be SMTP-servers amongst our hosts, this bit value may be unsafe to use and in the case of SMTP, there is no available confirmation. **Deprecating from march 2017**	FREE_SLOT_1_PREVIOUSLY_REPORTED
2	CONFIRMED PROXY IP has been confirmed as working proxy.	IP_CONFIRMED
4	PHISHING When FraudBL is used, this mask confirms the host as fraudible (Servers used for phishing, fraud, etc) **Active since June 2016**	IP_PHISHING
8	CHANGING **Will update soon** As this bitvalue has no meaning (since it only flags that nothing happens while trying to connect to it, this will change shape soon (Deprecated: timeout)	FREE_SLOT_8_PREVIOUSLY_PROXYTIMEOUT
16	EMAIL SPAM **June 2016:** E-Mail spammer *This is the former field for failed connections, which there is no interest in* **Active since June 2016**	IP_MAILSERVER_SPAM
32	HAS SECOND ENTRY IP is tested and is fully functional but there is a second entry point (meaning this ip is not the same as the one that has been used by the user"), *or the address is an exit node in TOR-network*	IP_SECOND_EXIT
64	ABUSE IP is marked as "abusive". Primary used to point out spam or attacks through webforms, forum, telnet, etc. **Updated since June 2016:** When FraudBL is used, this mask are also added, which means that - for example - if there is a phishing case (mail) the bit will be set to over 64 (4+16+64).	IP_ABUSE_NO_SMTP
128	ANONYMOUS IP has a different anonymous-state (web-based proxies, like anonymouse, etc)	IP_ANONYMOUS

bl.fraudbl.org

Follows all bitmasks as dnsbl.tornevall.org generates.

Coming soon

Special bitmasking in the fraudbl zone is upcoming

wl.tornevall.org - whitelisting system [PLANNED ONLY]

1	INTERNAL WHITELISTING SYSTEM STANDARD This status is set by the auto whitelisting system, after manual inspections
2	REMOVED VIA WEBSITE This status is set by the webservice removal system
4	SUPPORT MAIL SERVED This status is set when removal has been made manually, through support

The FraudBL Project

Fraudalent/phishing-tagged e-mail

FraudBL has just been started as a separate project - for the moment you can reach the site at https://fraudbl.org. FraudBL - Explained has been added here at the docs (from fraudbl.org), for your convenience.

tornevall.org covers both

FraudBL is a separate project, which lists mail that contains all kinds of phising. However, dnsbl.tornevall.org is covering FraudBL too so you actually don't need to resolve against both domains unless you don't want another scoring on the FraudBL content. Since dnsbl.tornevall.org collects all kinds of spam, the scoring is normally lower rated than the phising mail.

More information about the scoring can be found at DNSBL for Spamfilters.

Links

API References

Project status

We are currently working on a complete migration to a new system. Here, you can find the status of that project.
Older versions from 2006 are following TornevallWEB versioning (1.x-4.x).

Check out our project pages here!