DNS Procedures for removals

Document content

This page covers some information about how removals are actually handled internally.

Automatic Removals

This DNSBL have an automatic removal procedure, as blacklisted ip-addresses tend to get old and move around. The basic rule is to keep a host alive until it stops spamming, and if nothing happens with it in a year, it will be clean again. One year is quite long for a host, but some of the listed hosts has also long life and normally, they keep themselves in the list by continuing the spam. The same is also for, for example, TOR exit nodes and some proxies. However, TOR exit nodes has a shorter lifetime in the list - they are only kept for a half year. The rules are shown below:

- Mail spam: 365 days
- TOR Exit nodes: 183 days

APIv3 - Removal procedures are about to change

Read more here: Endpoint: dnsbl - DNSBL v5 with API v3

This project is under construction.

Support and SLA

Please see the section for Support and service levels for more information.

Why am I listed?

With our current database, no reasons of the blacklisting are stored anywhere. If your host is reported, it will only be registered and that's it. In our upcoming version of DNSBL version 5, we will also try to create referers of why and when it got blacklisted. Data will only be held until your address are removed.

Your address may be registered by a few different reasons (and it does not necessarily needs to be you that caused the blacklisting):

- Someone abused a service back in time when another Internet Service Providers owned the ip range and the address never got removed afterwards
- Someone reported your address as a webspammer
- Your address got stuck in a honeypot that registered the address as an active spammer
- Your address was listed as a receiver connected to active e-mail spam
- Your address has been scanned as "working" from open proxy lists

> ⚠ **GDPR NOTICE**
>
> We used to snapshot the that rendered the blacklist reason.
>
> However, as of 25th may 2018, when the data protection law changed the history of personal integrity, we no longer store this kind of content. It might sound strange that we do not store spam that works like a proof for why e-mail has been blacklisted. It also normally helps system administrators (especially those who administers email services) to trace the source of spam. But to protect the receivers part data, the mail spam storage project has been abandoned.

Removal

Find self helping tools at https://dnsbl.tornevall.org/removal/.

Service Level Agreement for DNSBL - Notice

As of august 2016 there are tools available for helping self (e.g. DNSBL), meaning the SLA state has been changed to normal.

Before contacting us, make sure you have tried to use the tools first.

Read more at Support and service levels

Penalties

As of 1 september 2016, we are implementing a penalty system, meaning the more times we have to delist the same ip address from the database, the longer it will take to get it removed. This has to be implemented since there are a few site owners out there, that apparently tries to get their hosts removed each time they get blacklisted due to phishing spam and similar. Hosts that is registered as tor exit nodes are not included in this penalty system.

Practical example of penalties

From **DNSBL-36** - Getting issue details... STATUS :

The first beta of PenaltiesBL is based on the average interval between each delisting and kicks in when more than two removals of same ip has been requested.

Release state for PenaltyBL is ***DNSBL-39*** *- Getting issue details...* ***STATUS***

Example:

If someone requesting removal and the requests has an average of 6 days (it goes 6 days between the requests, since the hosts are gets blacklisted once per week), the penalty time will be 60 days before next removal.
If someone requesting for removal after two weeks, the penalty time till be 30 days and so one.
Primarily removal requests has to be sent more than twice before the rules kicks in.

Request interval (days)	Penalty time
0-10	60 days
11-20	30 days
21-30	15 days
31-60	10 days
Over 60	5 days
Over 180 days	Counter will reset

The API response will also give the requester this information, when the host will be delisted from the system.


```
{
  "response": {
    "ipResponse": {
      "delete": {
        "[redacted]": "1"
      },
      "penalties": {
        "[redacted]": {
          "avgRemovalIntervals": "8.0000",
          "removalCount": "5",
          "penaltyTime": "30",
          "removalTime": "2016-10-02 10:27:58"
        }
      }
    }
  },
  "errors": {
    "success": "1",
    "faultstring": "",
    "action": "",
    "code": "0"
  },
  "api": {
    "endPoint": "dnsbl",
    "verb": "ip"
  },
  "request": [],
  "client": []
}
```

PenaltyBL 1.0.0-Integrated status

key	summary	type	created	updated	due	assignee	reporter	priority	status	resolution

Jira project doesn't exist or you don't have permission to view it.

View these issues in Jira

How do I check my host?

If your ip address is 255.255.255.252, you could do a lookup like this:

Linux

```
host 255.255.255.252.opm.tornevall.org
host 255.255.255.252.dnsbl.tornevall.org
host 255.255.255.252.fraudbl.org
```

Windows

```
nslookup 255.255.255.252.opm.tornevall.org
nslookup 255.255.255.252.opm.tornevall.org
nslookup 255.255.255.252.fraudbl.org
```

How do you collect the data?

Primary data collecting is being made from e-mail honeypots, webscraping, TOR network lists, reporting sites like StopForumSpam.com, etc.

I'm still listed even if I've sent a delist request [Rendered zone files]

The zone file for tornevall.org are re-rendered once per hour, but the default TTL for each host in all zones we are hosting are only five minutes, so if your host is uncached in a global DNS it will disappear in only a few minutes after the render. We used to say that removal may take up to 24-48 hours, since updating world DNSes may take different amount of time depending on how low hostnames are cached.

If you're using the API instead of the DNS request, the answer if you're listed will be instant - however, this does not mean DNS data is synchronized yet.

With a short description, after the removal has been confirmed your host should disappear from the master DNS within an hour.

Project information

key	summary	type	created	updated	due	assignee	reporter	priority	status	resolution

Jira project doesn't exist or you don't have permission to view it.

View these issues in Jira

Unknown macro: 'viewtracker'