Selecting a DNSBL

eco Competence Group E-Mail

Table of contents

Authors: Tobias Herkula (Cyren GmbH), Gunther Nitzsche (NetCologne Gesellschaft für Telekommunikation mbH), Andreas Schulze (DATEV eG), Kerstin Espey (HeLi NET Telekommunikation GmbH & Co. KG), Sven Krohlas (BFK edv-consulting GmbH), Florian Kunkel (Deutsche Telekom AG), Carsten Kühn (empaction GmbH), Olaf Petry (Hornetsecurity GmbH), Alexander Schaefer (Host Europe GmbH), Florian Vierke (Mapp Digital Germany GmbH)

Editors: André Görmer (Mapp Digital Germany GmbH)
Patrick Ben Kötter ([*] sys4 AG)
Michael Weirich (eco – Association of the Internet Industry)

Abstract

The Competence Group (CG) E-Mail of the eco Association provides advice for mail server administrators on selecting suitable blocklists.

CG E-Mail prefers to use terms that are as neutral as possible, as we consider the former use of blacklists vs whitelists to be problematic. There are better alternatives such as “blocklist” or “denylist”. We use the terms “**blocklist**” and “**allowlist**” in this document. Other good options are “denylist” vs “allowlist”, but these involve the challenge of introducing two new abbreviations.

TL;DR
The document shows why blocklists and allowlists should be used, names the different types of lists, and discusses selection criteria.
The appendix includes recommended lists and defines their purpose.

Motivation

In addition to desired messages, a multitude of unsolicited messages of all kinds now reach most mailboxes. When checking their inboxes, recipients can expect to find a mixture of malware spread by email, unsolicited advertising, sometimes newsletters sent on an irregular basis, as well as business and private correspondence.

Users and ISPs are trying their hand at spam detection and filtering. However, differentiating between desired ham messages and unsolicited spam is time-consuming and tedious. In addition to the time required for this, there are costs for storage space, bandwidth and computing capacity for the transmission and processing of spam messages. They thus represent a not inconsiderable cost factor for the receiving side. Depending on the success of the filters, desired messages still get lost among the spam, mistakenly disappear into the spam folder, or are deleted, while unsolicited messages may get classified as legitimate.

Therefore, most postmasters additionally rely on DNS-based blocklists (DNS Based Realtime Blocklists; DNSBL) of IP addresses, entire networks or domains, which are maintained in real-time. They do not accept messages from these in the first place, or they allow the information from a listing to flow into the spam scoring. These procedures are also technically described by the IETF https://tools.ietf.org/html/rfc5782
DNSBLs are generally the first line of defence against spam.

In the meantime, there are a large number of blocklists from various operators that use different criteria to list IP addresses or domains.

IP-based blocklists:
Real-time Block Lists (RBL) and Domain Name Server Block Lists (DNSBL) are blocklists based on the dispatch IP address that enable real-time querying. Mailbox providers use these lists to determine whether the mail server allows other servers to connect to it to send spam (a so-called open mail relay) or whether they are known spammers or ISPs that allow spammers to use their infrastructure.

Domain-based blocklists:
These include domains contained in the email header and email body. These blocklists check, for example, the links contained in an email to see if any of the links are known to be a source of spam. Not only the link itself is checked, but also any redirects that may have been set up.

Discussions among the members of the eco CG E-Mail have shown that it is difficult for postmasters to select the most suitable lists simply because of the large number of list providers available. This gave rise to the idea of collecting criteria for the use of blocklists and clearly explaining their consequences. We hope that this will help the administrators of mail systems and make the selection easier.

Nevertheless, the postmasters and not the list operators are solely responsible for the decision to accept, reject or deliver an email marked as spam. For this reason, many postmasters supplement their filtering concept with the use of allowlists to ensure the delivery of messages from known reputable senders and, while doing so, to avoid automated blocking by blocklists.

For a more detailed discussion of the criteria for serious blocklists, please see https://tools.ietf.org/html/rfc6471.

Selection criteria

When selecting a suitable blocklist, the mail server administrator should ask themselves at least the following questions:

How good is the quality of the list under consideration?

A good DNSBL has both a high hit rate for IP addresses submitting spam and – even more importantly – a very low error rate for ham messages. DNSBLs that more often list wrong or too large IP ranges are, of course, discussed in the usual forums. A quick search with the search engine of your choice will give you a few clues.

How widespread is the list?

A DNSBL that is largely unknown is difficult to justify to blocked senders. An increased support effort is, therefore, to be expected to explain the procedure to blocked senders.

How reputable is the list?

A reputable DNSBL does not take money for delisting (conflict of interest) and has comprehensible listing and delisting criteria.
A structured website on the DNSBL, which describes the respective criteria as well as the intended use and any restrictions on use, should be taken into account in the selection process. Contact details for the respective DNSBL should also be provided on the website. The DNSBL information pages should also not serve as a “honeypot” for further listing activities.

Does the list offer an in-house solution?

Through the (DNS) query at a DNSBL, the list operator also receives further information about the mail traffic of the query party. The use of lists intended for content filtering even reveals parts of the message content. The list operator receives this information via lists which are applied to the metadata of communication, such as IP addresses. Should list operators offer the possibility to copy their lists – for example, using Rsync – they can be used as a local copy without these data protection concerns, avoiding legal problems.

What is the purpose of the list?

Most DNSBLs provide IP address lists that can be used to reject emails. However, there are also lists that can be used for content analysis (e.g. advertised URLs) and/or act on the basis of domain names. The mail server administrator must be clear about their preferred purpose and should only use the list according to the specified purpose. Some DNSBLs are also not filled by the operator, but use messages from other ISPs who enter certain IP address ranges (such as dynamic dial-up IPs) from which no emails are to be sent directly. If, for example, your own customer addresses are listed there, you should not use this list on the customer mail servers without checking it carefully.

Note:
To comply with the German Telemedia Act (TMG), an email may no longer be rejected once the acceptance has been reported to the sender in the SMTP protocol. To send a reject based on a content check, the email acceptance must be delayed until all the checks are done and the decision weather to reject or to accept the mail is made.

Which listing criteria are applied?

Inclusion on a DNSBL is never without reason, although the length of time an entry remains on a DNSBL may itself depend on various factors, such as the reputation of the sender and the listing reason.

There are various listing reasons, e.g.:

- Evidence of infection with malware
- Spamtrap hits
- Behaviour that indicates abuse, such as the conspicuously frequent addressing of non-existent addresses
- Policy reasons: The listed IPs, networks or domains are not allowed to send emails, according to the owner or operator. This is often the case, especially with dynamically assigned address ranges. IPs or entire networks of operators which do not eliminate spam problems or do not do so promptly can also be listed by policy.
- Bot logins via open or poorly secured web login forms

This list is not exhaustive.

As a user of the list, why do I need to know the listing criteria so precisely?

If the list operator clearly communicates the reason(s) that led to a listing, support requests from users and senders will be easier and quicker to process.

The postmaster can refer directly to the listing reason (in the reject message already). The prerequisite for this is that the list operator keeps evidence of the listing reason for a

reasonable period of time. Depending on the reason for the listing, these can be, for example, samples of received spam mails or delivery statistics.

Instructions on how to remove or find any malware detected by its behavior could also be sent as a notice to the blocked user.

Evidence for the listing reason does not necessarily have to be retrievable automatically. However, if the retrieval would only be possible from the listed IP, this information can no longer be used for support requests. Also, the administrator of the listed system may not be able to access the reasoning themselves, because not every mail server is equipped with software to communicate via other protocols. The usual way is to query the DNSBL's website, indicating the IP concerned.

If a list operator offers a listing notification option, this allows the affected party to quickly analyse the incident. In addition, this can reduce support requests on the receiving side, as the consignor concerned can respond more quickly and without further queries.

How does delisting work?

The path to delisting itself should be documented in order to reduce support efforts. Care should be taken to ensure that technical hurdles are low and that it is implementable; otherwise blocked senders will not ask the list operator for help, but rather the postmaster of the receiving system.

How much does a list cost?

In the professional environment, some DNSBLs charge a fee for their services; others are free of charge. In order to be able to assess whether the desired DNSBL is worth the money, particular reference should be made to the points of quality and dissemination of the list. In individual cases, a test phase should be agreed upon with the provider.

Not only should listings be used exclusively for technically well-founded reasons, but they should also only be maintained for such reasons. Should a delisting be dependent on monetary payments, for example, this may constitute a conflict of interests. After all, the operator would benefit financially from a listing and subsequent delisting.

How can the list operators be contacted?

In Germany, business partners are usually expected to have an address at or to which a legal summons may be served. This can be problematic, especially with lists from abroad. Domestic lists should, in any case, have a summonable address. Do keep in mind:
The postmaster, not the operator of the DNSBL, is responsible for accepting incoming mails. If a sender is unable to get themselves delisted because of contact problems, they may seek legal redress against the postmaster.

A communicated support address with fast response and reaction times is advisable in any case. Contact, for example, only via certain Usenet groups with undefined contact persons, is certainly not conducive to quick and targeted support.

Is it possible to test the DNSBL?

If a DNSBL has the test entries specified in https://tools.ietf.org/html/rfc5782#section-5, administrators can check the correct functionality of their mail system as well as the DNSBL itself. This enables a quick reaction, for example, if the DNSBL is to be switched off at a later stage.

The effectiveness of blocklists for known use cases can also be checked by comparing known good and bad IP addresses on different DNSBLs.

With
http://www.anti-abuse.org/multi-rbl-check
http://mxtoolbox.com/blacklists.aspx
http://rbl-check.org
https://hetrixtools.com/
http://multirbl.valli.org/

or other providers, it is easy to verify whether, as expected, a spam-sending IP address is listed and good IP addresses are not. By repeating the test with IP addresses of diverse current attacks, the postmaster can estimate the effectiveness of the individual lists.

A non-exhaustive selection of some DNSBLs [1]

List name	Classification	Website	Blocklist type	Comment
Abusix	*recommended*	abusix.com black.mail.abusix.zone exploit.mail.abusix.zone dynamic.mail.abusix.zone dblack.mail.abusix.zone shorthash.mail.abusix.zone diskhash.mail.abusix.zone white.mail.abusix.zone dnswl.mail.abusix.zone nod.mail.abusix.zone noip.mail-beta.abusix.zone btc-wallets.mail-beta.abusix.zone attachhash.mail-beta.abusix.zone authbl.mail.abusix.zone	IPs of trap hits IPs list by behaviour policy-based IP list IP/domain of content URLs of shortener links URLs of storage links IP Whitelist DNSWL Newly-observed domains Newly-observed IPs Crypto-currency wallets Attachment hashes Subset of exploit for auth	- Free version - >99% hit rate - Self-service delist - Live query & rsync - 14-day trial - Live support
nixspam	*recommended*	nixspam.org	IP-based	- Free of charge - High-hit rate - German list operator
spamhaus	*recommended*	spamhaus.org sbl.spamhaus.org xbl.spamhaus.org dbl.spamhaus.org zen.spamhaus.org	IP-based IP-based Domain-based Combination of all lists (includes SBL, SBLCSS, XBL and PBL lists)	- most used blocklists worldwide - Fees for larger or commercial installations - Offers lists for different categories (spam, known spammers, dynamic dial-up IPs)
CBL	*recommended*	cbl.abuseat.org	IP-based	- Is integrated in Spamhaus "CBL" (https://www.abuseat.org/cutover.html)

[1] Source: https://www.validity.com/de/leitfaden-zu-e-mail-blacklists-alles-was-sie-uber-die-schwarzen-listen-wissen-mussen/

Spamcop	*recommended*	spamcop.org	IP-based	- Cisco service
URIBL	*recommended*	uribl.com	Domain-based	- Lists domains that appear in SPAM, not the domains from which the spam mails were sent.
SURBL	*recommended*	surbl.org	Domain-based	- The SURBL Domain Blocklist captures website domains that are received in unsolicited email messages.
apews	*not recommended*	apews.org	IP-based & domain-based	- "Anonymous Postmasters Early Warning System" - High error rate, hardly any contact options
aspews	*not recommended*	aspews.org	IP-based & domain-based	- Successor to "Spews: Spam Prevention Early Warning System" - High error rate, hardly any contact options
Blocklist.de	*recommended*	blocklist.de	IP-based	- Not widely disseminated - Not a very high hit rate (small database) - Can be used well as a supplement
Return Path Reputation Network Blacklist	*restricted recommendation*	senderscore.org/rtbl/	IP-based	- Includes all those senders (or IP addresses) categorised as the "worst of the worst". - Prediction model that analyses more than 600 variables and evaluates IPs in real time.
Sorbs	*restricted recommendation*	sorbs.net	IP-based	- "Spam and Open Relay Blocking System" - Also lists larger ranges - Hardly any contact options - Offers various subcategories
UCEprotect	*not recommended*	uceprotect.net	IP-based	- High error rate - Listing of large IP address ranges - No operator address available - Delisting subject to a fee

Sources and references

DNS Blocklists and Allowlists
https://tools.ietf.org/html/rfc5782l

Overview of best practices in the operation of DNS-based email lists (DNSBL)
https://tools.ietf.org/html/rfc6471

See also, e.g., https://en. wikipedia.org/wiki/Comparison_of_DNS_blacklist
or
http://www.intra2net.com/de/support/antispam/ for a weekly comparison of the hit rate.

The latest version of this document is available online for download from the CG E-Mail.

https://www.eco.de/themen/e-mail/downloads/

About eco – Association of the Internet Industry

With more than 1,100 member companies, eco is the largest association of the Internet industry in Europe. Since 1995, we have been instrumental in shaping the development of the internet in Germany, promoting new technologies, infrastructures and markets, and shaping framework conditions. All important experts and decision-makers of the Internet industry are represented in the eco Competence Groups and drive current and future Internet topics forward, together with a team of over 60 employees.

Special eco services help to make the market more transparent for providers and users, and our seals of approval ensure quality standards. With counselling offers for members and our services for internet users, we support with questions about the legal situation, increase security and improve the protection of minors.

As an association, one of our most important tasks is to represent the interests of our members vis-à-vis politicians and in national and international bodies. In addition to our head office in Cologne, we have our own capital office in Berlin and are represented on the ground for all relevant political decision-making processes in Brussels.

You can find more information about the eco Competence Group E-Mail on the official CG pages at https://international.eco.de/topics/e-mail/.