WE ARE SHAPING THE INTERNET.

Selecting a DNSBL

eco Competence Group e-mail

Table of contents

Authors: Tobias Herkula (optivo GmbH), Gunther Nitzsche (NetCologne Gesellschaft für Telekommunikation mbH), Andreas Schulze (DATEV eG), Kerstin Espey (HeLi NET Telekommunikation GmbH & Co. KG), Sven Krohlas (1&1 Mail & Media GmbH), Florian Kunkel (Deutsche Telekom AG), Carsten Kühn (empaction GmbH), Olaf Petry (antispameurope GmbH), Alexander Schäfer (Host Europe GmbH), Florian Vierke (TERADATA)

Editor: Sven Krohlas (1&1 Mail & Media GmbH)

Abstract

The competence group e-mail of the eco Association assists mail-server admins in selecting the right black lists.

Motives

It's not just expected mail but also a considerable amount of unsolicited messages that make it to the users' inboxes. When a user opens his or her e-mail program, he or she will see a mixture of messages including malware, unwanted advertising, sporadically sent newsletters, and finally business and private correspondence.

Users as well as ISPs have tried detecting and filtering spam all the time; however, telling ham and unwanted spam apart is complex and cumbersome. Not only does it take a lot of time but also involves high costs for storage, bandwidth, and computing performance required for spam-message transmission and processing. In that regard, spam is a considerable cost driver for the recipients. Moreover, depending on the filtering criteria applied, important messages might get lost among all the undesired mail, be moved to your spam folder or be deleted by mistake, or unwanted messages are classified as legitimate.

Therefore, most postmasters also rely on DNS-based realtime blacklists (DNSBLs) containing IP addresses or entire networks or domains. Messages coming from addresses on the blacklist will either be rejected right away, or postmasters will use information from the list for scoring messages. The IETF has provided a technical definition of the approach in https://tools.ietf.org/html/rfc5782.

Today, there are a large number of blacklists issued by various providers and listing IP addresses or domains based on various criteria. The exchange of practical experience within the eco e-mail expert group has shown that postmasters have problems with selecting the lists most suitable for them merely because of the massive amount of available lists. This led to the idea of collecting criteria for the use of blacklists and of clearly explaining the consequences of applying those criteria. In doing so, we hope to provide support and assistance to e-mail admins in making the right choice.

Nevertheless, it is the postmaster rather than the list operators who are responsible for accepting or rejecting a message or flagging it as spam before delivery. Therefore, many postmasters try enhancing their filtering approach by using whitelists in order to ensure delivery of mail sent by known trustworthy senders.

For an extensive discussion of criteria for reliable blacklists, refer to https://tools.ietf.org/html/rfc6471.

Selection Criteria

When trying to choose the right blacklist, the mail-server admin should try answering at least the following questions:

Is the quality of the considered list sufficient?

Of course, a good DNSBL will include a large number of IP addresses where spam messages are actually sent from; yet more importantly, the number of errors where ham is detected as spam needs to be as low as possible. In the relevant forums, people obviously talk about DNSBLs that frequently list incorrect or too large IP ranges. Launch your favorite search engine to get first clues.

Is the list well-known?

A DNSBL mostly unknown is obviously hard to justify towards blocked senders. This means that support efforts will probably increase since blocked senders will need to get informed about the procedure.

What about the trustworthiness of the list?

A respectable operator will set up comprehensible listing and delisting criteria and will delist you free of charge (as otherwise a conflict of interest will occur).

During selection, be sure to check that a well-structured webpage describing the criteria of the DNSBL, its purpose, and any usage limitations exists. The webpage should also provide contact details for that DNSBL. In addition, those DNSBL info webpages must not be used as some kind of “honeypot” for additional listing activities.

Does the list offer an in-house solution?

When a postmaster submits a (DNS) request to a DNSBL, the list operator also receives additional information on the requestor's e-mail traffic. Lists used for content filtering can even disclose parts of the message contents. The list operator gets the information by means of lists that are applied to communication metadata, for example, IP addresses. If list operators allows for copying their lists (for example, through rsync), you can safely use a local copy without privacy concerns that might even involve compliance issues.

What is the list's intended use?

The majority of DNSBLs offer IP-address lists that are used for rejecting e-mails. In addition, there are lists that can be used for content analysis (for example, advertised URLs) and/or act on the basis of domain names. The mail-server admin must be aware of the application at hand and select the list appropriately. There are also some DNSBLs that are not populated by their operators; instead, they use information submitted by other ISPs in order to add IP-address ranges that should not allow for direct e-mail reception (for example, addresses used for dynamic dial-in). For example, if addresses of your customers are on your list, you might not want to implement it on your customers' servers without prior review.

Note:

For compliance with the German Telecommunications Act (Telekommunikationsgesetz, TKG), an e-mail message must not be rejected after its acceptance has been reported to the sender through SMTP. Therefore, to be able to send a reject based on content inspection, e-mail acceptance must be delayed until the status is reported.

Which listing criteria are applied?

The addition of an IP address to a DNSBL is never without a good reason; however, various factors such as the reputation of the reporting entity or the reason for the addition affect how long an entry will stay on the list.

Among others, reasons for an addition to a DNSBL include the following:

- Evidence of malware infection.
- Spamtrap hits.
- Behavior suggesting abuse — for example, conspicuously frequent use of non-existing recipient addresses.
- Policy-based prevention: According to the respective owners or operators, e-mail cannot be sent from the listed IP addresses, networks, and domains. This is particularly true with dynamically assigned address ranges. IP addresses or entire networks of operators who do not resolve spam issues timely (or not at all) might be added based on policies.

Note that this list is not exhaustive.

Why do I as a simple list user have to know so well about the criteria?

A list operator clearly communicating the reasons that lead to the listing will speed up and simplify the processing of support inquiries from users and senders.

In this case, the postmaster can refer to the reason right away (i.e. in the reject message). This requires the list operator to retain relevant evidence for a reasonable time. Depending on the reason for listing, this may include, for example, samples of received spam or delivery statistics.

Another possibility would be to provide instructions to the blocked user for finding or removing malware detected by its characteristic behavior.

Processing requests regarding such evidence does not necessarily need to be automated; however, if those requests can be submitted only from the listed IP address, the information cannot be accessed through support requests. In addition, the admin of a listed system may not access those reasons as there are mail servers that do not allow for communicating through other protocols. Typically, admins will send an inquiry indicating the affected IP address on the webpage of the DNSBL in question.

If the list operator offers notification of listed entities, the affected senders can quickly analyze the incident. This also reduces the amount of support inquiries on the receiving side as the affected sender can respond more quickly and without repeat calls.

How does delisting work?

The actual delisting steps should be clearly documented in order to reduce support efforts. While doing so, it should be ensured that the process is technically simple and easy to implement—otherwise, blocked senders will ask the postmaster of the receiving server rather than the list operator for assistance.

How much is the list?

In the professional area, there is a number of DNSBLs available at a fee while others are free of charge. To evaluate whether your chosen DNSBL is worth the money, you might want to specifically check its quality and distribution. If unsure, you should ask the operator for a trial period.

New entries should be added to the list and maintained on the basis of a technical justification. For example, requiring a delisting fee might constitute a conflict of interests — after all, the operator would obtain a financial benefit from delisting.

How to contact the list operators?

In Germany, business partners typically expect to be provided with an address of service. This can become a problem, in particular, with lists from abroad. In any case, domestic lists should be able to provide an address of service. Always remember: The postmaster rather than the DNSBL operator is responsible for accepting incoming e-mail. If a sender cannot ask for a delisting just because of missing contact information, he or she may even decide to take legal action against the postmaster.

Setting up a publicly available support address with short response times is always recommendable; in contrast, offering a point of contact, for example, only through specific Usenet groups without specifying a contact name might not be helpful if you want to provide fast and targeted support.

Is there a test option?

If a DNSBL includes the test entries specified at https://tools.ietf.org/html/rfc5782#section-5, administrators can test the functionality of their e-mail system and the DNSBL itself. This ensures a speedy response, for example, when the DNSBL is taken off-line someday.

To evaluate the effectiveness of a blacklist for known use cases, you might check eligible DNSBLs for entries for IP addresses that are known to be good or bad. If you simply want to verify whether an IP address that sends spam is listed in a DNSBL (or a good IP address is not listed), check out http://www.anti-abuse.org/multi-rbl-check/, http://mxtoolbox.com/blacklists.aspx, http://rbl-check.org/ or the website of any other qualified vendor. By repeating the test with IP addresses used for several recent attacks, the postmaster can evaluate the effectiveness of the various lists.

Sources and References

DNS Blacklists and Whitelists

https://tools.ietf.org/html/rfc5782l

Overview of Best Email DNS-Based List (DNSBL) Operational Practices

https://tools.ietf.org/html/rfc6471

The most recent version of this document is available for download on the Competence Group e-mail blog.

https://e-mail.eco.de/downloads.html

About eco – Association of the Internet Industry

eco, with more than 800 member organizations, is the largest Internet industry association in Europe. Since 1995, the eco Association has been instrumental in the development of the Internet in Germany, fostering new technologies, infrastructures and markets, and forming framework conditions. In the Competence Groups, all important specialists and decision makers of the Internet industry are represented, and current and future Internet themes are driven forward.

Special eco services help to make the market more transparent for providers and users. The eco seal of approval ensures quality standards; eco consultations for members and services for users provide support in questions of legality, security and youth protection.

As an association, one of eco's most important tasks is to represent the interests of its members in politics, and in national and international committees. As well as having headquarters in Cologne, eco has an office in the German capital Berlin, and is represented at all relevant political decision-making processes in Brussels.

eco is a founding member of EuroISPA, the umbrella organization for European Internet associations. eco also represents the German industry with a seat on the Council of the Generic Names Supporting Organization (GNSO) at ICANN, and is a driving force behind the Internet Governance Forum.

More information about the eco Competence Group e-mail can be found on the official blog https://e-mail.eco.de/