FACTSHEET

Real-time threat intelligence from Spamhaus: Protect your mail streams from spammers, malware and malicious domains

3,000,000,000+ mailboxes protected by Spamhaus every day

Why Spamhaus?

Spam is a problem that just hasn't gone away. It's evolved from resource draining 'affiliate spam' used to send high volumes of unsolicited marketing messages to the current state where cyber criminals use email to deliver targeted malware and ransomware. They are determined to steal data, commit fraud and exploit your networks. Cyber criminals rely on volume and velocity so real-time threat intelligence from Spamhaus, drawn from live sources across the internet, is your best, first line of defence.

Our global team of security researchers has years of experience tracing connections between criminal networks, malicious domains and compromised IP addresses. This data can also be used to identify infected computers on your network by showing you which machines have tried to connect to Spamhaus-listed domains.

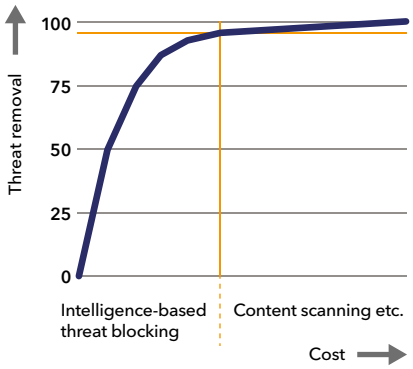
90% of all the world's email traffic is spam

Email security – the Spamhaus approach

Spamhaus block lists provide an effective, transparent mechanism for removing the vast majority of harmful email at the gateway. Emails from listed IP addresses and associated with malicious domains will be dropped as soon as the SMTP connection is made, so that bandwidth and server space are not wasted on downloading and storing spam.

Secondary filtering, using more expensive anti-spam resources, can then be used to identify unwanted emails that manage to get through this first layer of defence.

Mail server administrators can use the Zen set of block lists to block or tag connections from listed IP addresses, preventing the vast majority of spam and harmful emails from entering their networks. These databases are constantly updated by Spamhaus researchers, who work around the clock from ten worldwide locations to identify and list malicious or compromised IP addresses. This team of researchers is also responsible for delisting IP addresses that are no longer associated with malware or spam distribution.



Spamhaus is a cost effective, first line of defence

SPAMTEQ

IP Reputation intelligence

Policy Block List – PBL

What it contains

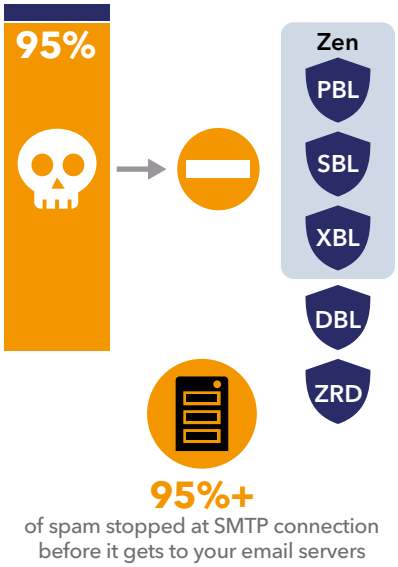
IP address ranges for end-user devices, such as home routers and smart TVs, from which email should never be sent.

The PBL lists IPs not because they are actively sending spam, but as a pre-emptive measure to prevent spam from networks that should send no email at all. Listings are manual: Either an ISP manages PBL listings for its own IP ranges or Spamhaus team members research IP ranges to determine whether the network is suitable for listing.

How it works

A mailserver that is configured to use the PBL will block a great deal of spam and almost no legitimate email. Spam sent from IP addresses in the PBL often contains embedded malware or links to malware-infected websites, so blocking this email also protects users from malware infections.

An ISP or company that lists in the PBL those IP ranges that should not send email protects other networks from any spam email that might leak from an infected or compromised computer on its network.



Spamhaus Block List – SBL

What it contains

IP addresses and networks that meet one or more of the following criteria:

- Direct spam source. Sends spam to users.
- Spam hosting. Hosts botnet command and control (C&C) servers, compromised websites, and other hosted websites and services that are advertised by spam.
- Spam services. Hosts websites that sell lists, provide email appending services, provide DNS for domains owned by spam operations, or that provide other services to spam operations.

How it works

SMTP servers. Mailservers check a delivering IP against the SBL, if it is listed the mailserver can:

- Reject delivery of the email.
- Accept delivery and then tag the email as probable spam or save in a spam folder.
- Tarpit the connection.

Spam filters. Spam filters can check IP addresses that send email and can also look up IP addresses of URI hosts or IP addresses of DNS servers that provide DNS for domains in email headers and message bodies. The filter can classify the email as spam, or can use the SBL listing as one factor in a more complex filtering process.

eXploits Block List – XBL

What it contains

The Spamhaus XBL is a list of IP addresses that host bots and malware-infected computers. The Spamhaus team uses automated tools to observe SMTP connections to an extremely large set of both spamtrap and production mailservers in near-real-time for connections that show characteristic patterns of malware or botnet-infected computers.

How it works

The XBL is designed as an anti-spam blocklist, to protect mailservers from spam. A mailserver is configured to check the XBL when another IP address attempts to deliver email. The mailserver can do one of the following things:

- Refuse the connection, rejecting delivery of the email.
- Accept the connection, but silently drop the email or save it in a system spam folder.
- Accept the connection and then tag the email as probable spam before delivering it to the recipient.
- Tarpit the connection, or engage in any other activity that the system administrator configures.

Do Not Route or Peer DROP and extended DROP

What it contains

The Spamhaus Do not Route Or Peer (DROP) list includes IP ranges that are known to have been hijacked by spammers and cyber criminals, or have been directly allocated to criminal organizations by a regional internet registry (RIR).

These networks are controlled by criminal organizations and send zero legitimate traffic. They are solely used for spamming, hosting malware-infected sites, phishing emails, hosting botnet command & control servers and launching DDoS attacks.

The extended DROP list (eDROP) is a list of IP ranges that cyber criminals have leased from ISPs for the same purposes.

How it works

Both DROP and eDROP can be loaded into your router, BGP gateway, IDS or firewall and used to block malicious email and traffic at your network edge.

By blocking connections from a listed range, you can avoid wasting bandwidth and protect your users from being exposed to phishing links and malware embedded in spam.

Spamhaus updates the DROP and eDROP lists every few minutes. However, these lists generally remain stable because criminals tend to control IP address blocks for an extended period.

100 spam operations are behind 80% of spam in Europe and North America

Domain Reputation intelligence

In addition to IP-based reputation data, Spamhaus researchers maintain constantly updated domain-based blocklists. These use multiple sources to define whether domains are involved in malicious activity or hosting harmful content.

Domain-based reputation data is compiled from a range of live sources including information on bad domain neighbourhoods, DNS glue records, WhoIs records, domains on hold and short-term expiry dates, Alexa web traffic activity data, and temporal data showing brand new domain registrations and new senders of web and email traffic.

Cyber criminals use spam to steal data, hijack networks, extort money and commit fraud

Domain Block List

What it contains

Spam domains. Domains owned by spammers and used only for spam or other malicious purposes.

Legitimate domains used in spam operations: Domains owned by non-spammers, used for legitimate purposes, and abused by spammers. Also called an *abused-legit* domain.

Both spam domains and legitimate domains are subdivided by type of abuse, including simple spam, phishing, malware, botnet C&C and redirector domains.

How it works

Configure your mailserver or your spam filtering system to check the DBL to see if a domain in the header or body of an email is listed. Configure the mailserver or spam filters to reject or filter email appropriately.

Zero Reputation Domain

What it contains

Cyber criminals use newly registered and active domains to send spam and drive traffic to harmful websites hoping that users will fall victim before a domain has been analyzed for its reputation.

Legitimate organizations will rarely activate a domain and start using it immediately after registration so the ZRD automatically adds newly-registered and previously dormant domains to a blocklist for 24 hours. This protects users from clicking on links and visiting domains until it can be firmly established that they are not associated with malicious activities.

How it works

Configure your mailserver or your spam filtering system to check the ZRD list to see if a domain in the header or body of an email is listed. Configure the mailserver or spam filters to reject or filter email appropriately. ZRD allows you finer control as it can be configured to block domains which are anywhere from 2 hours to 24 hours old.

How to obtain

	Free Public Mirror	Data Query Service	rsync
SBL, PBL, XBL, DBL	✓	✓	✓
Known false positives due to escalation listings	✓	✗	✗
ZRD	✗	✓	✗ (See PassiveDNS)
Continuously updated	✗	✓	✓
Support available	✗	✓	✓
High Volume	✗	✓	✓✓
Online reports available (coming soon)	✗	✓	✗
Custom license options, typically for creation of derivative products	✗	✗	✓

How to use Zen

The Spamhaus IP-based block list contains live data on IP addresses that have been observed to be involved in sending or hosting spam, including hijacked servers and computers infected with botnet malware.

To speed the IP address query process, Spamhaus Zen combines all IP-based block lists into a single block list comprising SBL, XBL and PBL (zen.spamhaus.org).

- **Quick to implement**
  No extra hardware needed
- **Fast and accurate**
  Continuously monitored, with delivery updates to suit your set-up
- **Reliable and trusted**
  Spamhaus researchers work constantly to update threat intelligence on your behalf
- **Easy to integrate**
  Available as a data feed in industry standard formats so no special customization required

About us

Founded in London in 2004, Spamhaus Technology provides commercial data distribution and synchronization services for the real-time datastreams, raw datasets and security technologies developed by the non-profit organization The Spamhaus Project including IP-based and domain-based reputational data, response policy zones (RPZ managed services and RPZ transfer) and Border Gateway Protocol Feeds and blocklists, which are used to protect more than 3 billion mailboxes worldwide from spam, phishing emails and malware.

From the proceeds of selling these services and data, Spamhaus Technology helps to provide a pool of worldwide public servers that provide Spamhaus data to the public, funds research into anti-spam technologies and contributes research and equipment to the global fight against cyber crime.

How to obtain

Existing Spamhaus users can enable by contacting their usual local re-seller.

Users who are new to Spamhaus can sign up for a free 30-day trial:
www.spamhaustech.com/free-trial

Follow Spamhaus Technology:

@spamteq

Search Groups for 'Spamhaus Technology'

SPAMTEQ™

SpamTEQ is the trading name of Spamhaus Technology Ltd, London UK, company no.05078652

ZEN-001-03.17