Passive DNS: trusted real-time threat intelligence from Spamhaus

FACTSHEET

Passive DNS intelligence uncovers patterns of malicious activity from networks around the world, delivering threat data directly to you, blocking connections to malicious domains.

What it is

The internet works through a system of domain name servers (DNS) resolving queries from client machines. If a DNS resolver is unable to return a domain name from its cache, it sends a recursive request to other name servers – a situation known as a cache miss. Cache misses can be maliciously caused by DDoS traffic and cache poisoning, causing internet users to experience delays in reaching websites.

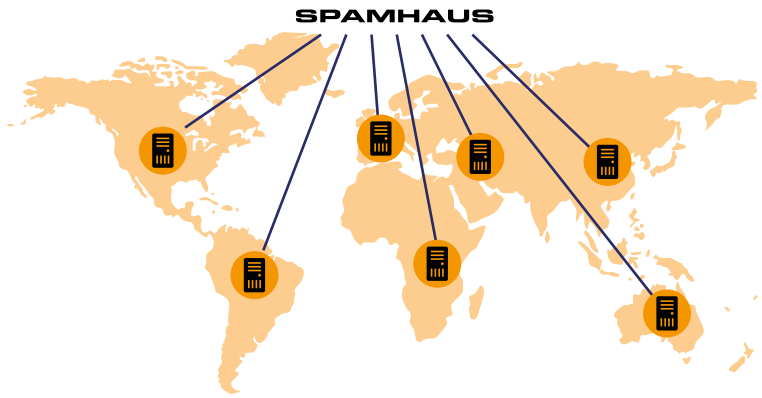
Security researchers are able to use cache misses to retrace recursive queries, map connections and identify new bad domains. This passive DNS replication reconstructs a partial view of DNS queries and resolution and can be used to reveal the internet pathways between cybercriminals and DNS servers, without capturing IP addresses of client devices, or compromising the privacy of internet users.

How it works

Created through links with service providers and a community of security researchers who are dedicated to combatting DNS abuse, Spamhaus Technology's Passive DNS datasets compile domains that are, or have been directly associated with cybercrime.

Studying passive DNS data allows researchers to track which domain names are hosted by particular name servers and which domain names point to which IP networks. They can also see where domain names used to point and which subdomains exist below a certain domain name.

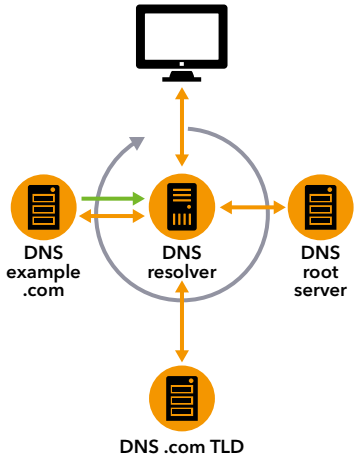
By uncovering the links between name servers and domains, Passive DNS helps to identify new bad domains as soon as they are live. Our Passive DNS datafeed can be used as a real-time threat intelligence tool; helping you to proactively protect your users' devices from connecting to bad domains.



Spamhaus operates its own Passive DNS sensor network, gathering anonymized DNS query data from thousands of recursive DNS servers around the world.

Why Spamhaus?

- **Reliable and trusted**
  Trusted track record of gathering anonymized DNS query data from thousands of recursive DNS servers around the world
- **Quick to implement**
  No extra hardware needed
- **Fast and accurate**
  Updated every 20 minutes for near real-time intelligence
- **Easy to integrate**
  Available as a data feed in industry standard formats so no special customisation required



A client queries a local DNS resolver and if the IP address for that domain is not included in its cache, it will query in turn an external root server, the Top Level Domain server and the domain server itself to get access to the site.

SPAMTEQ

Spamhaus Technology Passive DNS is available as a raw dataset

Through our web portal

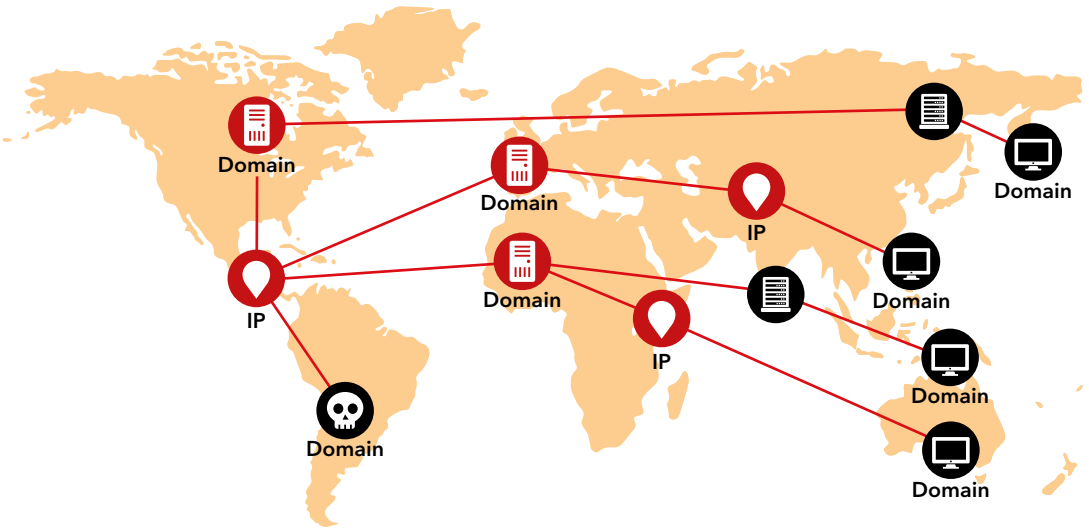
Designed for information security professionals and cyber incident response analysts who want to carry out digital forensics, and security researchers who want to investigate what sort of activity is associated with particular IP ranges, or analyse the relationships between DNS queries and responses.

Through an API

For security vendors and expert users who wish to integrate our raw datasets with their own software and security platforms.

On the wire

For security researchers and law enforcement agencies who wish to continuously monitor live recursive DNS traffic to aid the identification of new malicious domains, emerging threats or cybercriminal trends.



Domain Reputation – the Spamhaus approach

Our global team of security researchers has years of experience tracing connections between criminal networks, malicious domains and compromised IP addresses to provide blocklists of known or suspect domains. This domain-based 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.

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 three 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 cybercrime.

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

DNS-001-04.17