Recently registered Domains: How to reduce the risk

OVERVIEW

Zero Reputation Domain (ZRD) service from Spamhaus Technology

Blocking email traffic associated with recently registered Domains provides an extra layer of protection against malware, ransomware and spamming. The ZRD blocklist from Spamhaus is proven and easy to implement.

What it is

Research by Spamhaus has driven the development of the Zero Reputation Domain service designed to thwart cyber criminals who use newly registered domains to send spam and drive traffic to harmful websites hoping that users will fall victim before a domain has been analysed for its reputation.

Legitimate organisations 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 unknown domains until it can be firmly established that they are not associated with zero day attacks, phishing, bot-herding, spyware and ransomware campaigns.

How it works

ZRD works by preventing a customer's mail servers from accepting email from potentially malicious domains, preventing users from visiting newly-registered malware dropper sites and bad IP addresses that pose a significant risk.

ZRD complements existing Domain Name Blocklists generated by Spamhaus' global team of security researchers who maintain constantly updated domain-based blocklists using data compiled from a range of live sources.

Use case

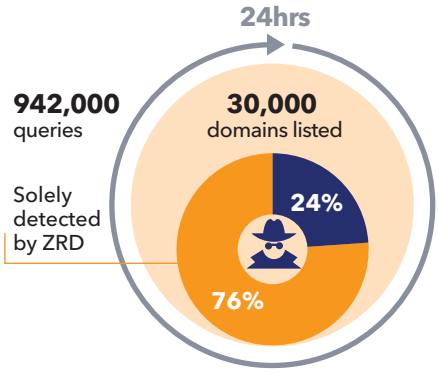
The ZRD blocklist is already proving its worth in a pilot with a UK-based email security service provider. In a regular working day in pilot for one customer, the provider's systems made almost a million queries to the ZRD blocklist, complementing existing blocklists to identify suspicious domains used for emailing or embedded in messages.

For the service provider, reducing the volume of further processing is very important to provide a fast and efficient service. Newly registered domains are particularly harmful because a single domain will be used for high-volume, high-speed email attempts by cyber criminals exploiting its unknown reputation.

In the pilot, the ZRD identified 30,000 domains of which 23,000 were solely detected by the ZRD and so could be blocked immediately, without the need for further expensive content scanning.

Benefits and features

- **Quick to implement**
  No extra hardware needed when using a data query service
- **Fast and accurate**
  Updated every minute for near real-time intelligence
- **Reliable and trusted**
  Spamhaus researchers work constantly to update threat intelligence on your behalf
- **Easy to integrate**
  Available as a DNS lookup, so no special customisation required



Pilot result

SPAMHAUS TECHNOLOGY

Domain Reputation – the Spamhaus approach

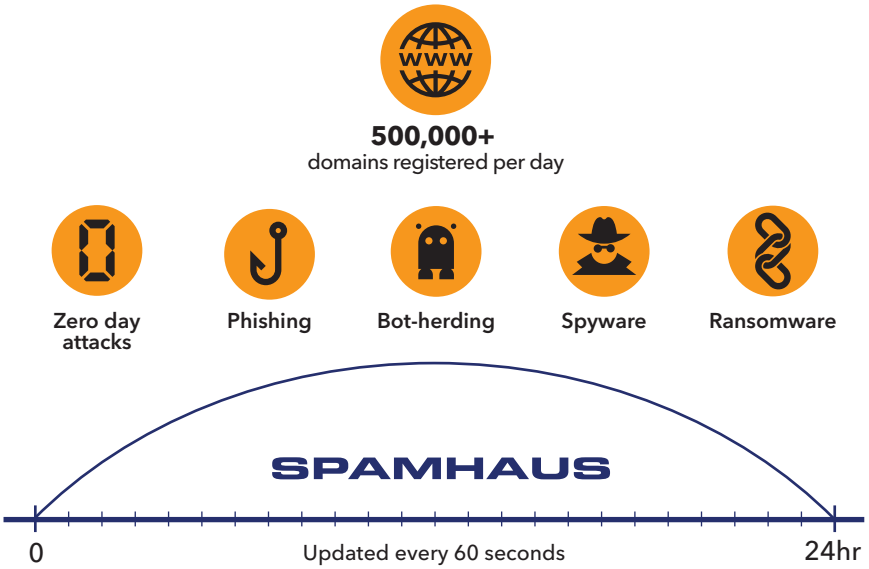
ZRD augments Spamhaus's existing, proven approach to establishing domain reputation. Our global team of security researchers has years of experience tracing connections between criminal networks, malicious domains and compromised IP addresses to provide blocklists of known or suspect domains.

The ZRD adds a new layer of protection to email filtering, allowing you by default to block domains whose reputations have yet to be established. This constantly updated stream of data can be delivered as a data query service, to provide efficient, on-demand referencing against the live ZRD list.

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.



Zero Reputation Domain (ZRD)

Protection from newly-registered domains, until it is established that they are not malicious

Feedback from the pilot project

> **"Generally, anything that gives me a 10% non-overlap would get me pretty excited, so consistently achieving over 50% is amazing and it's hitting exactly the kind of domains that I hoped it would."**

DEVELOPMENT DIRECTOR,
EMAIL SECURITY PROVIDER

How to obtain

Existing Spamhaus users can add ZRD as a Data Query Service to complement current services.

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

Follow Spamhaus Technology:

@SpamhausTech
Search Groups for 'Spamhaus Technology'
'Spamhaus Technology' channel

Your contact:

ZRD-002-08.19

SPAMHAUS TECHNOLOGY