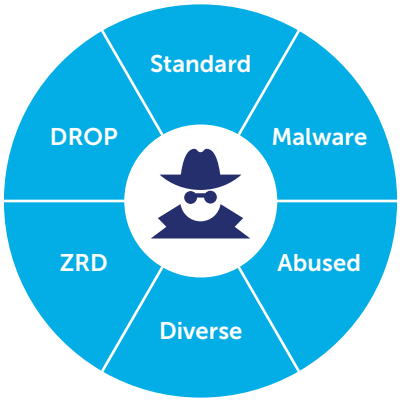
DATASHEET

Deteque RPZ Service: Zones Overview

Online fraud, disruption and exploitation take many forms so Deteque Zones are always evolving to take into account new types of threats and new ways cyber criminals abuse the DNS process.



Standard

Deteque's global research team works on your behalf to bring you the most comprehensive set of malicious domains on the internet. Don't just rely on user training and vigilance for protection: RPZ provides automated protection from visiting malicious websites and domains (particularly useful as a defence against phishing).

dbl.zone (~ 3,900,000 entries)

Domains used as malware dropper sites, malware hosting sites, malicious redirectors, domains used by botnets, botnet command and control servers and other malicious activity. It includes domains used as spam sources and senders, known spammers and spam gangs, phishing, virus and malware-related sites.

Includes 'Slow Release' segment which holds domains for longer in case bad actors try to recycle domains.

bad-nameservers.zone (~ 5,000 entries)

Lists name servers which are known to resolve malicious domains.

Malware

Don't let cyber criminals abuse or hijack your network – these Malware zones block domains that are used specifically to abuse your systems.

botnetcc.zone (~ 1,200,000 entries)

This zone contains IPs of known botnet C&C servers so it is highly likely that any machine resolving domains pointing to an IP listed in this zone has been compromised and is hosting malware.

Includes segment of domains generated by Domain Generation Algorithms, created from sandboxed malware and lists domains that the malware might use to contact C&C servers.

malware.zone (~ 67,000 entries)

A subset of DBL.zone containing just those domains associated with malware. (Spam sources, phish sources and redirectors are excluded from this dataset.)

malware-aggressive.zone (~ 4,000 entries)

An extension to malware.zone containing domains which are known to be associated with malware but scoring mechanisms have not included them in the main listing. Due to the 'aggressive' nature of this list, it has a slightly greater chance of false positives.

malware-adware.zone (~ 1,000 entries)

Domains revealed from running adware in sandboxes. Helps you to identify which of your machines need to be cleaned up.

Abused

Even the best run networks can be abused occasionally – Deteque keeps track of those that should be temporarily avoided.

abused-legit.zone (~ 35,000 entries)

Contains legitimate servers and/or services which have been (temporarily) compromised. False positives are possible as the servers are mostly legitimate but being used to distribute malware. Risk averse organizations may consider the tradeoff to be acceptable.

bogon.zone (~ 6,000 entries)

IP ranges from an area of the IP address space reserved, but not yet allocated or delegated, by the Internet Assigned Numbers Authority (IANA) or a delegated Regional Internet Registry (RIR). Frequently used to target specific organizations.

Diverse

Cyber criminals change their methods constantly – this zone contains the datasets of varying and evolving threats.

cryptominer.zone (~ 10,000 to 15,000 entries)

Blocks crypto mining networks using browser-based code to hijack processing power.

sbl.zone (~ 550,000 entries)

Known spam sources (IP) Based on the Deteque Block List.

tor-exit-nodes.zone (~ 1,000 entries)

TOR exit nodes.

ZRD

ZRD.zone (~ variable)

Blocks connections to newly-registered and previously dormant domains for 24 hours. Domains are removed after 24 hours or transferred to another zone feed based on reputation assessment.

DROP

There are some domains that you should not connect to under any circumstances – Deteque has compiled a list of the 'worst of the worst'.

drop.zone (~ 1,000 entries)

An advisory 'drop all traffic' list, consisting of netblocks that are 'hijacked' or leased by professional spam or cyber-crime operations (used for dissemination of malware, trojan downloaders, botnet controllers). Designed for use by firewalls and routing equipment to filter out the malicious traffic from these net blocks.

Follow Deteque:

@deteque-llc

@deteque

'Deteque' channel

www.deteque.com

Your contact:

deteque | A division of SPAMHAUS