FACTSHEET

Response Policy Zone service: improve security against malicious and compromised sites

Threat Intelligence updated every two minutes to block domains used by cyber criminals to steal data, carry out fraud and exploit legitimate systems. RPZ blocks malicious domains and is a powerful tool in developing best practices across any enterprise.

What it is

Every day, millions of users, machine-to-machine updates and IoT devices rely on the Domain Name System and associated infrastructure to connect seamlessly to websites, cloud applications, eCommerce sites and other online services.

With connections taking place in a fraction of a second, you run the risk of connecting to domains that are used to install malware, ransomware, botnets or have been compromised by cyber criminals.

Security professionals can mitigate this risk by using Response Policy Zones (RPZ) to block access to malicious sites by preventing the DNS process from resolving to malicious domains and IP addresses.

Deteque researchers and automated systems gather information from across the internet to identify actively malicious domains, low reputation domains before they become active and compromised IP addresses to provide threat intelligence.

How it works

Without RPZ, 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. The process will return both legitimate and malicious sites as there is no check in the process to exclude malicious domains.

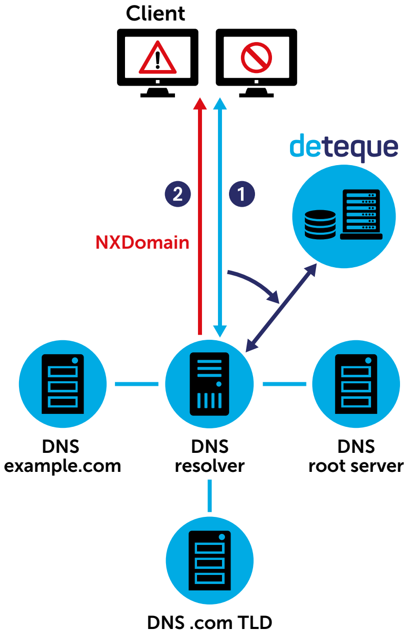
When a client initiates a query on an RPZ enabled nameserver, each step of the recursive DNS lookup process is analyzed to identify known bad domains, addresses and nameservers. If RPZ identifies a security risk the DNS server returns a 'does not exist' type answer which prevents access to the threat.

Each organization can customize the user warning page to include security awareness and best practice training messages. It's an essential step to make sure everyone across an organization contributes to online security.

RPZ can be delivered as a data query service, effectively acting as a DNS firewall on your behalf. For organizations operating larger commercial operations serving more than 5,000 users, Deteque domain-based reputation data is available via IXFR.

Benefits and features

- **Quick to implement**
  No extra hardware needed
- **Fast and accurate**
  Continuously monitored, delivered every 2 minutes
- **Reliable and trusted**
  Deteque 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



1. Client queries local DNS resolver, which queries Deteque RPZ first
2. Deteque RPZ identifies malicious domain, allowing local DNS resolver to block domain query and also send warning to user

Threat Intelligence includes:

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

DROP – Do not Route Or Peer

IP address ranges known to have been hijacked by professional spammers and cybercriminals, or have been directly allocated to criminal organizations by a regional internet registry (RIR). It also includes a list of IP ranges that cyber criminals have leased from ISPs.

Standard

Deteque's security researchers use automated systems to constantly monitor newly-registered domains and identify links to cybercriminal activity, allowing us to rapidly list suspect domains.

Malware

The Deteque global team of security researchers traces connections between criminal networks, malicious domains and compromised IP addresses. RPZ data can be used to help prevent DDoS attacks by choking botnet beaconing communications which are usually a precursor to an attack. Our researchers reverse engineer malware to reveal Domain Generation Algorithms domains and the times that they are due to be used, allowing us to block them before criminals start using them as contact points for botnet command & control servers.

Abused

Domains which are generally legitimate but are abused by spammers through exploits/hacking. Referred to as 'abused legit' to signify that the domain owners are legitimate operators whose servers have been hacked.

Diverse

This includes miscellaneous threat types including Tor exit node blocking to restrict unwanted use of your network by anonymised traffic. Also included are IP addresses listed on the Spamhaus Block List because they appear to be under the control of, or made available for the use of, senders of unsolicited bulk email.

Domain Reputation – the Deteque approach

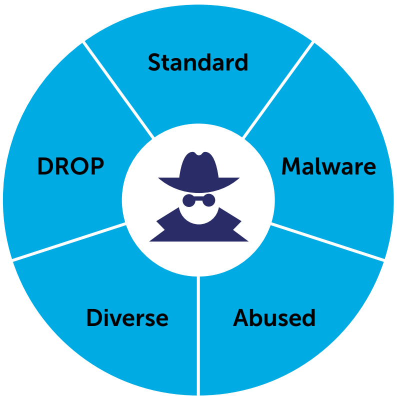
Our global team of security researchers has years of experience tracing connections between criminal networks, malicious domains and compromised IP addresses to provide blocklists of known or suspect domains. This domain-based data can also be used to identify infected computers on your network by showing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

RPZ as a DNS Firewall is a highly effective layer to mitigate and prevent access to known malicious sites. RPZ updates every 2 minutes, delivering the most up-to-date Threat Intelligence to enhance your security to prevent access to known malicious sites.

Deteque – a division of Spamhaus

Deteque is a division of Spamhaus and integrated with a global network of service providers and a community of security researchers who are dedicated to combating DNS abuse.

Since 2008, Deteque has been at the forefront of securing networks by collecting, collating and delivering DNS-related threat intelligence to protect organizations in real-time.



Deteque's RPZ service evolves to stay ahead of the threats

Employee security awareness

Stopping connections to malicious domains is essential. Making employees aware of the risks they have been taking is even better. RPZ doesn't just block bad domains, you can also use a blocked return to send a warning message immediately that's customized to your security training and awareness programme.

Follow Deteque:

@deteque-llc

@deteque

'Deteque' channel

www.deteque.com

Your contact:

deteque | A division of SPAMHAUS