CASE STUDY

XS4ALL

XS4ALL protecting customers with Response Policy Zones service to block malicious DNS traffic and botnets

Netherlands-based ISP XS4ALL is using Response Policy Zone (RPZ) threat intelligence from Deteque as a DNS firewall to provide an improved customer security service.

The Challenge

Cyber criminals are keen to abuse someone else's well-equipped network, so ISP and hosting environments are targeted by malicious actors keen to insert malware and botnets that can infect across a network.

Email filtering and anti-spam measures can block most phishing attempts but there is always the risk that a customer will unwittingly respond and allow access to malware. So there is always a risk of getting infected, or have infections that might spread to others.

The challenge for XS4ALL is to provide protection without impacting the demand for high-volume, high-speed connectivity and give customers a choice of the security profile that's right for them.

The Solution

XS4ALL runs PowerDNS Recursor for its DNS resolution because it has a native implementation to receive an AXFR/IXFR data feed for RPZ handling. With the release of version 4.0 of PowerDNS Recursor, XS4ALL was able to configure Response Policy Zones into the resolution process for the first time.

The new 4.0 version has an extra feature which enables active lookup of a configuration for the client that queries the resolvers. This enabled XS4ALL to make RPZ malware filtering optional, with each customer able to chose it as an added security service.

Implementation of RPZ was straightforward given the version of PowerDNS Recursor, the main volume of work required was to configure XS4ALL's systems to provide this as a customer option.

The Results

After a careful checking of a PowerDNS setup with mirrored traffic and reviewing the volumes of suspicious queries, RPZ was made operational as an option to customers. When enabled, customers drastically cut down on malware traffic from links in already downloaded email messages that they clicked on accidentally.

Command & Control beaconing traffic from botnets is also greatly reduced. Even though each beaconing message is very small, a compromised end-user can consume massive amounts of bandwidth when it is used to mount DDoS attacks.

About XS4ALL

XS4ALL is a medium-sized ISP based in the Netherlands. The company was one of the first ISPs in the Netherlands, and provides internet access to more than 200,000 broadband customers, and offers co-location and hosting services.
www.xs4all.nl

About PowerDNS

The PowerDNS Recursor is a high-performance DNS recursor with built-in scripting capabilities. It powers the resolving needs of over 150 million internet connections.
www.powerdns.com

> **"With RPZ acting as our DNS firewall, we are able to block thousands of malicious connections everyday. And as it can be configured on demand, it's a great option to offer our customers."**
>
> KAI S, SYSTEM ENGINEER, XS4ALL

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 Deteque-listed domains.

This constantly updated stream of data can be delivered as a data query service, effectively acting as a DNS firewall on your behalf or for organizations operating larger commercial operations serving more than 50,000 users, Deteque domain-based reputation data is available via rsync.

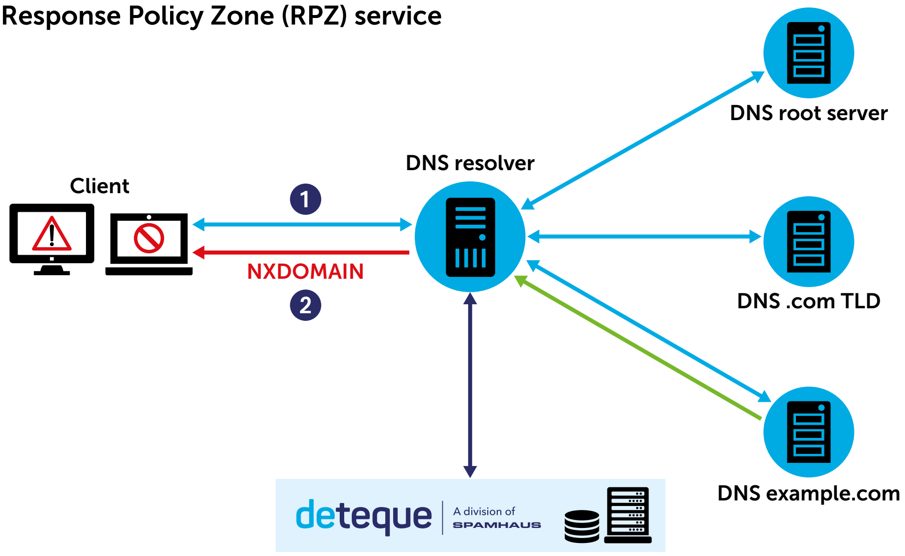
RPZ as a DNS Firewall is a highly effective layer to mitigate and prevent access to known malicious sites. RPZ updates every minute, delivering the most up-to-date Threat Intelligence to enhance your security to prevent access to known malicious sites.

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.

Response Policy Zone (RPZ) service



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

Benefits and features

- **Quick to implement**
  No extra hardware needed
- **Fast and accurate**
  Updated every 2 minutes for near real-time intelligence
- **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 customisation required

How to obtain

Deteque is a division of Spamhaus so existing Spamhaus users can enable RPZ by contacting their usual local re-seller.

New users can sign up for a 30-day free trial: Contact us at **www.deteque.com**

Follow Deteque:
@deteque-llc
@deteque
'Deteque' channel

www.deteque.com

Your contact:

deteque A division of SPAMHAUS