



Rackspace® deploys Response Policy Zone service from Spamhaus to improve security against malicious sites and augment DDoS protection

CASE STUDY

Global managed cloud provider Rackspace is protecting customers and improving connectivity by using the Response Policy Zone (RPZ) data service from Spamhaus to block malicious domain traffic and botnet activity.

The challenge

As the leading provider of managed cloud services, Rackspace is always looking for ways to augment its multi-layered approach to security and stay ahead of the threats from Distributed Denial of Service (DDoS) attackers looking to exploit its global infrastructure and highly connected customer base.

High volumes of domain queries across the company's infrastructure are an integral part of usual operations but Rackspace was looking for ways to reduce traffic related to malicious domains and help ensure the infrastructure isn't used by botnets to mount DDoS attacks.

In addition to security concerns, DDoS attacks are also parasites on an infrastructure, stealing bandwidth to carry out their malicious attacks.

The solution

After a market analysis of different options, Rackspace worked with Spamhaus's local value-added delivery partner to fully deploy RPZ. This included developing a pilot to ensure technical compatibility and delivery requirements with the monitoring of results prior to full implementation. Rackspace chose to have RPZ delivered as a zone transfer feed to ensure domain queries are filtered on their own DNS servers to reduce latency and because they had the skills available to implement directly.

Rackspace uses industry standard BIND servers for DNS resolution and the zone transfer feed was test integrated and was soon delivering results, blocking malicious domains, without the installation of any extra hardware.

The results

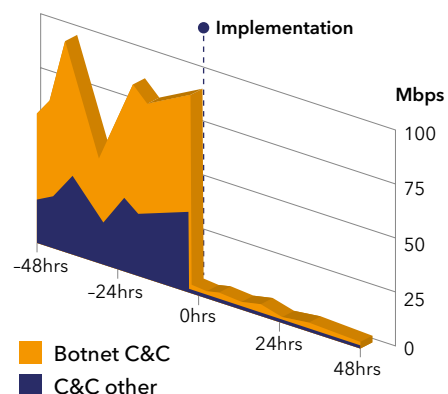
Rackspace's customers rely on their users to have a seamless online experience. For eCommerce customers that means a seamless experience from advertising through to online store and final purchase. Underpinning this is multiple DNS resolution across different sites so any interruption would have an immediate business impact.

After a month installed at its data centres worldwide to check technical compatibility with BIND servers and to review volumes of alerted traffic, RPZ was made operational. The implementation drastically cut down on botnet and other malicious Command & Control beaoning traffic. Each beaoning message is very small but an active botnet can consume massive amounts of bandwidth when it is switched on to mount a DDoS attack. Rackspace was able to virtually eliminate this traffic with no impact on customers' business flows.

About Rackspace

Rackspace, the #1 managed cloud company, helps businesses tap the power of hosting and cloud computing without the complexity and cost of managing it on their own. Rackspace engineers deliver specialized expertise, easy-to-use tools, and Fanatical Support® for leading technologies including AWS, VMware, Microsoft, OpenStack and others. The company serves customers in 120 countries, including more than half of the FORTUNE 100. Rackspace was named a leader in the 2015 Gartner Magic Quadrant for Cloud-Enabled Managed Hosting, and has been honored by Fortune, Forbes, and others as one of the best companies to work for. Learn more at www.rackspace.com

Outbound botnet and other Command and Control traffic



RPZ reduced outbound beaoning traffic from approximately 80 Mbps to almost zero immediately.

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.

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 5,000 users, Spamhaus Technology domain-based reputation data is available via rsync.

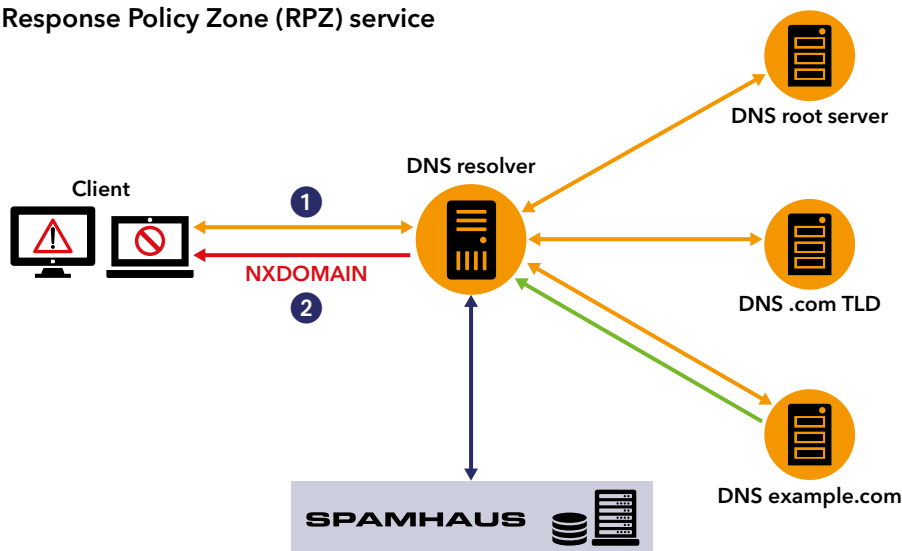
RPZ as a DNS Firewall is a highly effective layer to mitigate and prevent access to known malicious sites. RPZ updates every minute, delivering the most up-to-date Threat Intelligence to enhance your security to prevent access to known malicious sites.

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.

Response Policy Zone (RPZ) service



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



Outbound beaconing from botnets can be a precursor to DDoS attacks so we are really excited to minimize this type of traffic and interrupt a critical component of a DDoS attack. ”

JASON BRATTON, MANAGER,
SYSTEM ENGINEERING, RACKSPACE

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**
Spamhaus 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

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'



Authorized Spamhaus Reseller
sales@mxtools.com
+1.866.931.9228

SPAMTEQ

SpamTEQ is the trading name of Spamhaus Technology Ltd, London UK, company no.05078652

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'