rackspace
the #1 managed cloud company

Rackspace DDoS protection augmented with Response Policy Zone service from Spamhaus

CASE STUDY

Global 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 one of the world's leading provider of 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 cut traffic related to malicious domains and 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 value-added delivery partner, SecurityZones, 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 zone transfer feed to ensure domain queries are filtered on their own DNS servers to ensure minimum 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 clients 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.

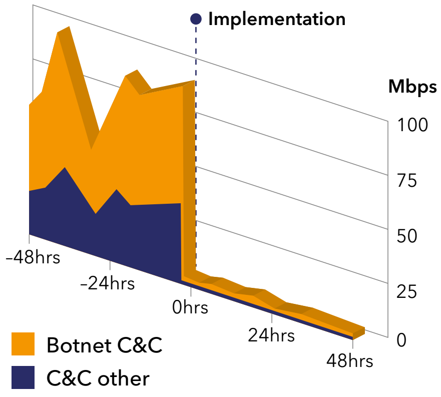
After a month installed at its data centres worldwide to check technical compatibility with BIND servers and to review volumes of alerted traffic, RPZ was made operational. The implementation drastically cut down on botnet and other malicious Command & Control beaconing traffic. Each beaconing message 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 clients' business flows.

About Rackspace

Rackspace® (NYSE: RAX) is a global leader in hybrid cloud and founder of OpenStack®, the open-source operating system for the cloud. The company has been delivering enterprise-level hosting services to businesses of all sizes and kinds around the world since 1998 and has grown to serve more than 205,000 customers operating from four continents.

Gartner positions Rackspace as a leader in their Magic Quadrant for Managed Hosting, North America and Europe and for Managed Hybrid Cloud Hosting, Europe.

Outbound botnet and other Command and Control traffic



RPZ reduced outbound beaconing traffic from approximately 80 Mbs 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.

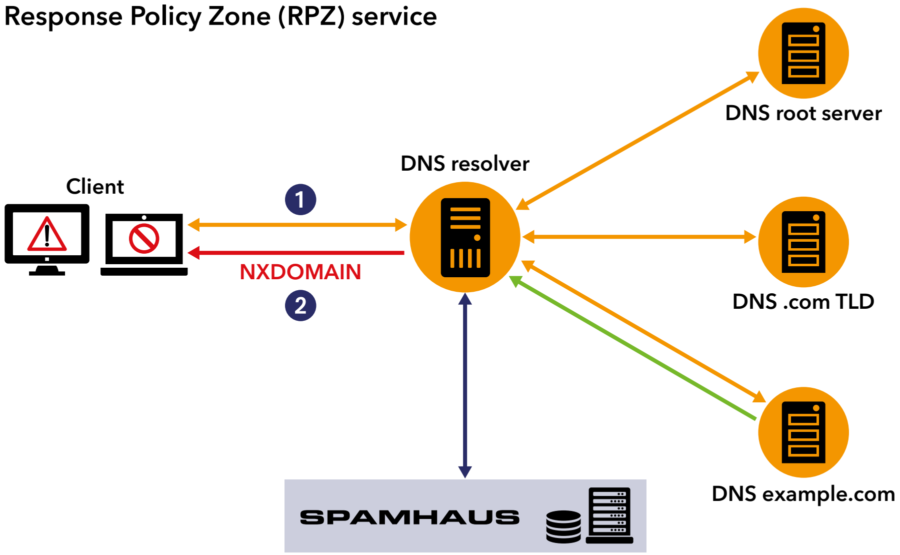
This constantly updated stream of data can be delivered as a data query service, effectively acting as a DNS firewall on your behalf or for organizations operating larger commercial operations serving more than 5,000 users, Spamhaus Technology domain-based reputation data is available via rsync.

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 3 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 is a precursor to enable a DDoS attack so we are really excited to minimise this type of traffic and choke DDoS attacks before they can begin.”
>
> RACKSPACE

Benefits and features

- **Quick to implement**
  No extra hardware needed
- **Fast and accurate**
  Updated every 20 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’

SECURITY ZONES
Realtime Threat Intelli gence

securityZONES is a Platinum Reseller of Spamhaus. **securityZONES** provides sales, technical support, and customer service to leading ISP’s, Enterprises, Universities, and Governments worldwide.

Contact us at **www.securityzones.net; support@securityzones.net; or +44 (0) 20 8133 9344**

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

SPAMTEQ™