CASE STUDY

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

Global managed cloud provider Rackspace is protecting customers and improving connectivity by using the Response Policy Zone (RPZ) data service from Deteque 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 Deteque'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 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

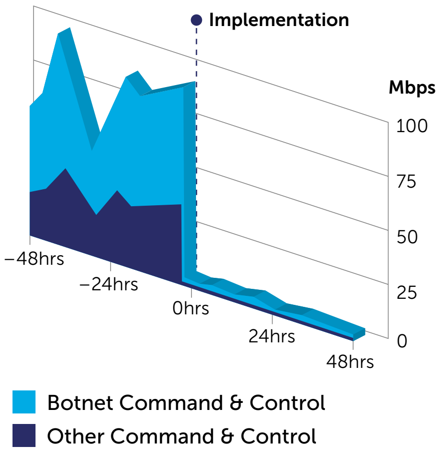
Rackspace's customers rely on their users to have a seamless online experience. For eCommerce customers that means a seamless experience from advertising through to online store and final purchase. Underpinning this is multiple DNS resolution across different sites so any interruption would have an immediate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

After a month installed at its data centers 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 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 & Control traffic



RPZ reduced outbound beaconing traffic from approximately 80 Mbs to almost zero immediately.

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

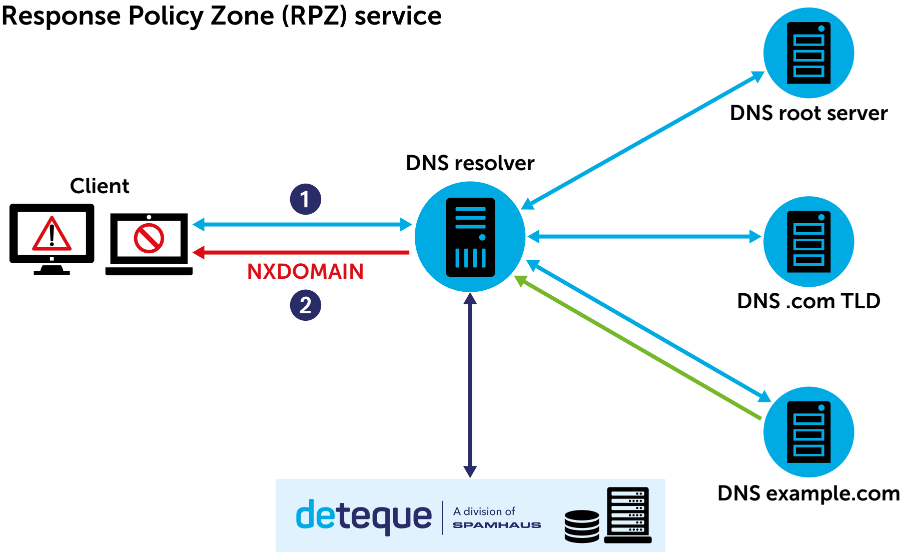
RPZ as a DNS Firewall is a highly effective layer to mitigate and prevent access to known malicious sites. RPZ updates every minute, delivering the most up-to-date Threat Intelligence to enhance your security to prevent access to known malicious sites.

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

> **"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**
  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