
Getting started with a BIND DNS Firewall

December 14, 2017

with

deteque

A division of
SPAMHAUS

**SECURITY
ZONES**
REALTIME THREAT INTELLIGENCE

Logistics

- Webinar is scheduled for 1 hour
- This session will be recorded and posted at <http://www.isc.org/webinars>
- Participants are muted to improve audio quality for everyone.
- We want questions! Please enter into the WebEx Q&A tab
 - The presenter may defer some questions until the end of the presentation

Presenters



Eddy Winstead
ISC
Sr. Sales Engineer



Matt Stith
Spamhaus/Deteque
Product Manager

Agenda

- DNS firewall basics
- Case Study - Rackspace
- Getting Started
 - steps to trial RPZ
- Summary and References

Why do you need a DNS firewall?

Botnet C&C



Malware



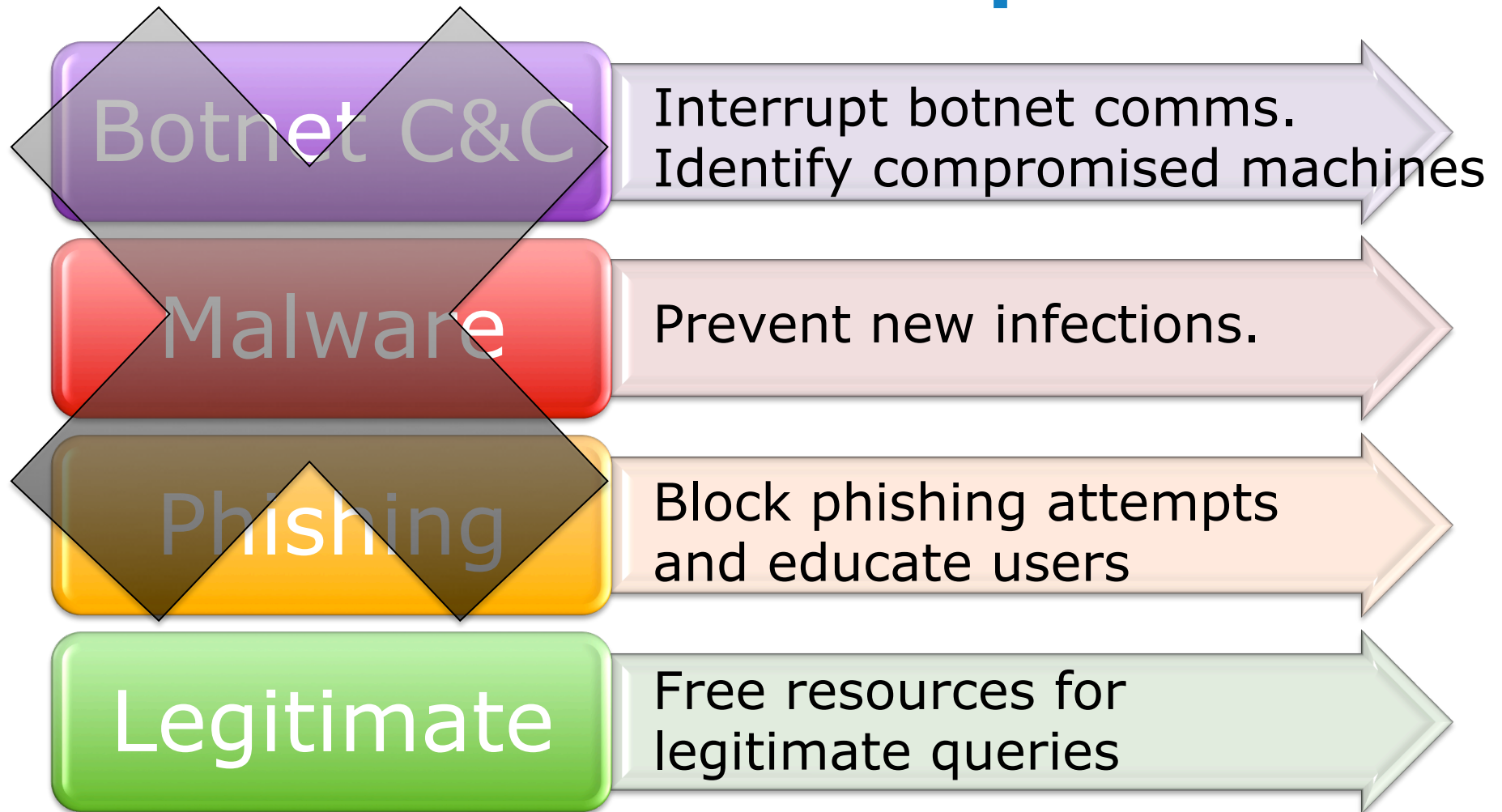
Phishing



Legitimate



Intercept and remove abuse domains from responses



Hosted services have raised the bar

Outsourced resolver services

- Google DNS
- Quad9.net (launched in late November)
- OpenDNS (commercial service from Cisco)
- Akamai appliances (recently purchased Nominum)

Traditional In-house resolver

- Keep your data in-house
- Lower cost
- Greater control
- Improve network security by adding well-maintained RPZs from security experts

DNS Filtering with RPZ

- Reputation data is packaged into Response Policy Zones (RPZs)
- RPZ's update frequently via IXFR/AXFR
- RPZs include both the filter criteria, and a 'response policy' action
- BIND evaluates whether its response matches a filter in the RPZ and applies the policy specified

RPZ re-writes Responses



could be:
Passthrough
NXDOMAIN
NODATA
local-data
DROP





- 1) Check response vs RPZ zone files
- 2) Match on clientIP, Server IP, NSDNAME, etc
- 3) Apply policy, re-write response
- 4) Send response
- 5) write log

BIND RPZ support

Triggers (Filter index)

- **Qname** (FQD)
- **Client-IP** (.rpz-client-ip)
- **IP** (.rpz-ip)
- **NSDNAME** (.rpz-nsdname)
- **NS-IP** (rpz-nsip)

Actions

- **NXDomain** 
- **NODATA**
- **Passthru** 
- **TCP-Only**
- **DROP** 
- **Local-Data** 

RACKSPACE CASE STUDY

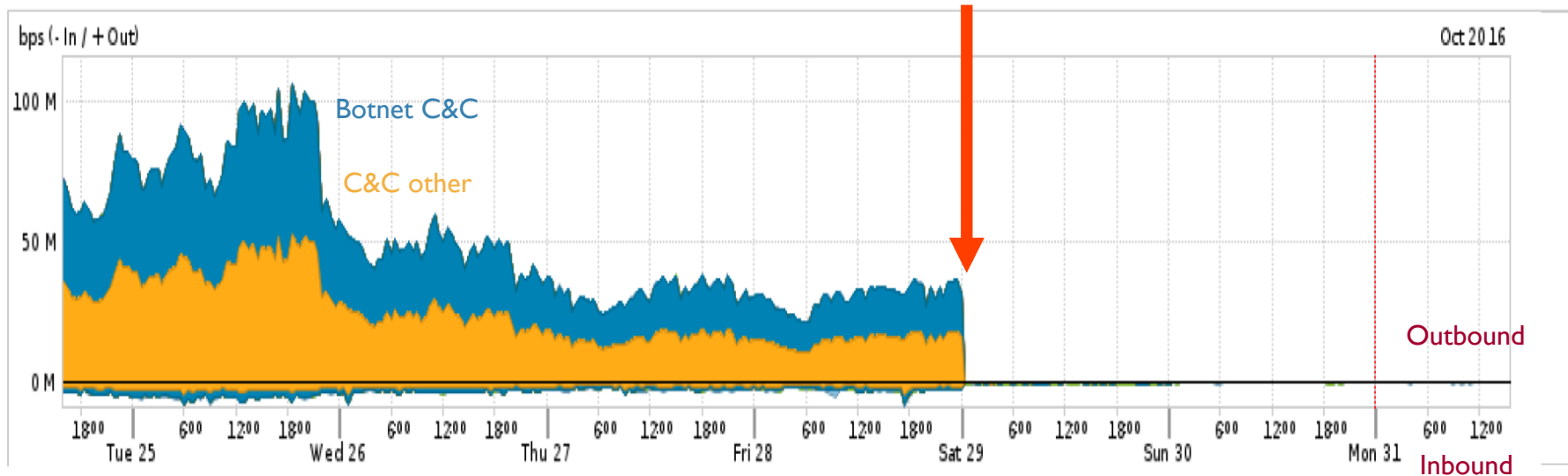
Matt Stith, Product Manager, deteque-Spamhaus

<http://www.securityzones.net/images/downloads/Rackspace-RPZ-Case-Study.pdf>

Case Study - Rackspace

- Provides DNS resolution for hosted applications
- Wanted to protect customers and the network from Botnets responsible for DDOS
- Implemented RPZ company wide October 2016 after extensive testing and evaluation

Case Study - Rackspace - Blocked Abuse

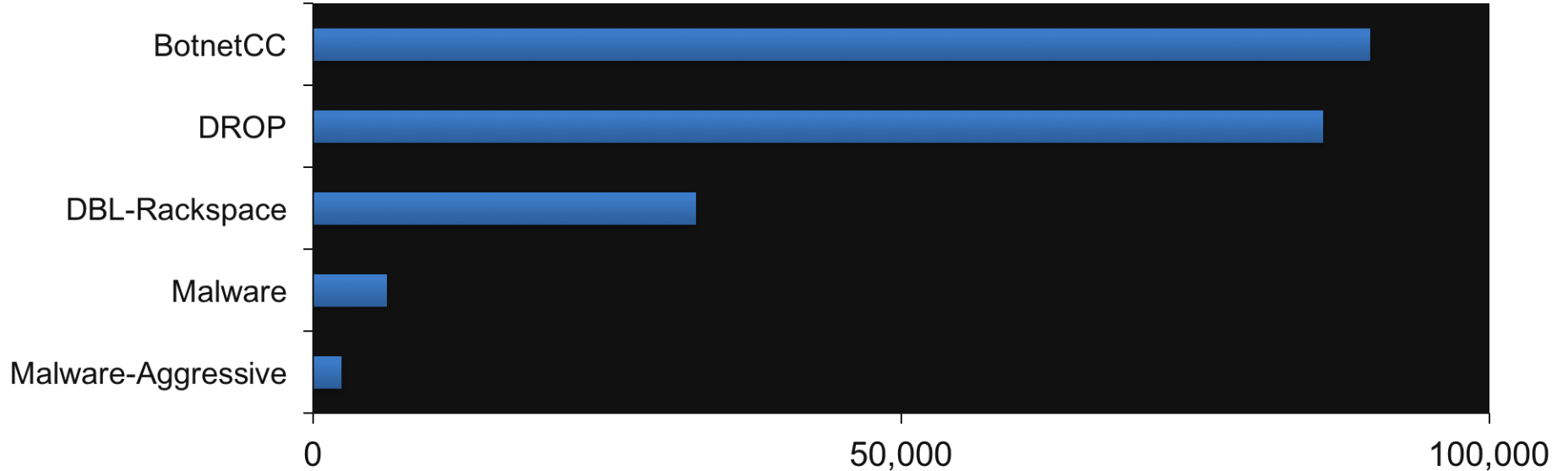


Outbound beaconing traffic reduced from ~ 80 MBPS to near zero

Case Study - Rackspace

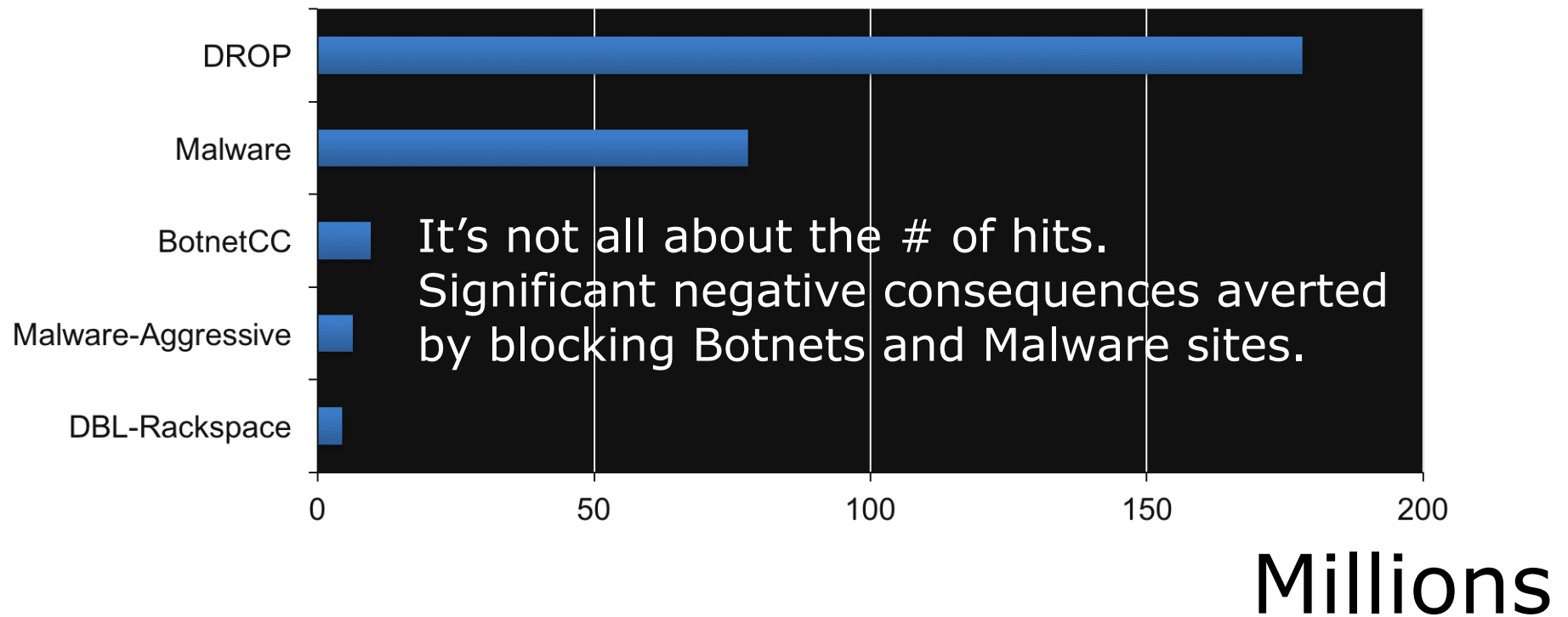
Domains Blocked by Spamhaus RPZ lists

Blocked Domains per Policy List



Case Study - Rackspace - 'Hits' at Rackspace for Spamhaus zones

Policy List Hit Count



Rackspace Experience

Domains Blocked	217,708
RPZ Hits	275,000,000
Devices Protected	8,734

Rackspace experience

- Able to mitigate infected clients upon activation of RPZ
- Notified other users who potentially had the same issues
- Prevented large bills / extended downtime for customers who were infected
- Support and abuse teams more aware of potential large scale infections
- A 20-30 percent drop in complaints for the Abuse Team

GETTING STARTED WITH RPZ

For a detailed tutorial, with example configuration files, see the BIND Installation Guide at

[http://www.securityzones.net/images/downloads/
BIND_RPZ_Installation_Guide.pdf](http://www.securityzones.net/images/downloads/BIND_RPZ_Installation_Guide.pdf)

How to enable DNS RPZ and use Spamhaus' free DROP zone

1. Enabling RPZ logging
2. Creating a local RPZ zone
3. Defining Master and Slave zones
4. Enabling RPZ

1) Enabling RPZ Logging

```
logging {  
    channel rpzlog {  
        file"rpz.log" versions unlimited size 1000m;  
        print-time yes;  
        print-category yes;  
        print-severity yes;  
        severity info;  
    };  
    category rpz { rpzlog; };  
};
```

2) Create Local Zone

```
$TTL 300
@           IN SOA  localhost.rpz.local (
                20170913 ; Serial number
                60      ; Refresh every minute
                60      ; Retry every minute
                432000; Expire in 5 days
                60 )    ; negative caching ttl 1 minute
IN NS      LOCALHOST.

isc.org    IN CNAME rpz-passthru.
*.isc.org  IN CNAME rpz-passthru.
32.25.195.32.rpz-ip  IN CNAME rpz-passthru. ;whitelist 34.194.195.25/32
32.71.219.35.rpz-ip  IN CNAME rpz-passthru.      ;whitelist 35.156.219.71/32

baddomain.com    IN CNAME .                ;local block against baddomain.com
*.baddomain.com  IN CNAME .                ;local block against *.baddomain.com
```

3) Defining zones in configuration

Master Zone

```
zone "rpz.local" {  
    type master;  
    file "rpz-zone/db.rpz.local";  
    allow-transfer { none; };  
    allow-query { localhost; };  
};
```

3) Defining zones in configuration

Slave Zone

```
zone "drop.rpz.spamhaus.org" {  
    type slave;  
    file "db.drop.rpz.spamhaus.org";  
    masters { 35.156.219.71; 34.194.195.25; };  
    allow-transfer { none; };  
    allow-query { localhost; };  
};
```

4) Enabling Response Policy Zone

```
options {  
    response policy {  
        zone "rpz.local";  
        zone "drop.rpz.spamhaus.org POLICY RPZ-PASSTHRU";  
    };  
};
```

Notes to consider

- Create a backup of your named.conf
- Test first with passthru 10-14 days
- Always have your local zone listed first in priority and others by most egregious
- Customer notification (?)

Recommended tools for Assessing Results

- Splunk (Realtime)
- ELK (Elasticsearch, Logstash, Kibana) (Realtime)
- MYSQL or other DB (Report Based)

Available Response Policy Zones

» Standard

- bad-nameservers.zone ~18,000 entries
- dbl.zone ~2,900,00 entries

» Malware

- botnetcc.zone ~1,200,000 entries
- malware.zone ~67,000 entries
- malware-aggressive.zone ~4,000 entries
- malware-adware.zone ~4,000 entries

» Abused

- abused-legit.zone ~35,000 entries
- adservers.zone ~18,000 entries
- bogon.zone ~6,000 entries

» Diverse

- sbl.zone ~550,000 entries
- tor-exit-nodes.zone ~1,000 entries

» DROP ~1,000 entries

CONTACT Arnie Bjorklund, arnie@securityzones.net FOR FREE TRIAL

SUMMARY

Requirements

- BIND 9.12 has refactored (faster, non-blocking RPZ)
- BIND 9.9 or later will work
- Subscribe to one or more RPZ feeds
- RPZ feeds are available from:
Spamhaus/Deteque, SURBL,
Farsight, Switch (see dnssrpz.info)

Recommendations

- As with any blocklist, you have to be on the watch for false-positives.
- Subscribe to a well-managed list(s)
- Enable RPZ in log-only mode at first
- Establish passthrough for local zones
- Monitor RPZ logs

Don't forget

... the importance of white listing your own internal zones to prevent accidental blocking

<https://kb.isc.org/article/AA-00522/0>

To try Spamteq RPZ



To begin Free Trial:

- <http://www.securityzones.net/free-trial.html>
- Arnie Bjorklund, SecurityZONES - mention 'ISC Webinar'

Special Offer from SecurityZONES
for webinar attendees:

- 90 day Extended Trial period
- includes ALL RPZ zones
- Setup instructions, assistance, personal consultation

References

RPZ web site with data feed providers list - <https://dnssrpz.info>

Security Zones - **Rackspace Case Study**

<http://www.securityzones.net/images/downloads/Rackspace-RPZ-Case-Study.pdf>

Free Trial - <http://www.securityzones.net/free-trial.html>

Installation Guide for BIND with RPZ with links to example files:

http://www.securityzones.net/images/downloads/BIND_RPZ_Installation_Guide.pdf

ISC KB articles on RPZ: <https://kb.isc.org/article/AA-00525/110/Building-DNS-Firewalls-with-Response-Policy-Zones-RPZ.html>

Thank You!

contacts:
info@isc.org

Arnie Bjorklund
arnie@securityzones.net
www.securityzones.net

QUESTIONS

Please type your questions into the chat window