Make the Internet safe with DNS firewall Response Policy Zones (RPZ)
Great Asean

Fastest Growing Area of Threats

Over 200 Billion devices connected worldwide by 2020.
Over 13 million active bots recorded for January 2019.
Most activity coming from countries within the ASEAN region.
Phishing & BEC

A report by the Cyber Security Agency of Singapore (CSA)

In 2018:

6,179 cybercrime cases were reported
378 business email impersonation scams

This led to businesses in Singapore suffering close to S$58 million (US$42 million) in losses.

Council of Anti-Phishing Japan
https://www.antiphishing.jp/news/alert/
Malicious Downloads

Ransomware

Malware Root Kits

Cryptojacking

Websites

Mobile Applications

 Servers
DGA Domain Generating Algorithm

93b375dd6cd9f2704d613d1016dbe0f2.info
93b375dd6cd9f2704d613d1016dbe0f2.tk
afcc0c1f4b9fd590a61balc24b49b525.ga
afcc0c1f4b9fd590a61balc24b49b525.info
afcc0c1f4b9fd590a61balc24b49b525.ml
afcc0c1f4b9fd590a61balc24b49b525.online
bbcl6e2659b9b9b5128c2f7e5877d29b.cf
bbcl6e2659b9b9b5128c2f7e5877d29b.ga
bbcl6e2659b9b9b5128c2f7e5877d29b.gq
f62b550a0e5e4f234fdd30c927665c91.xyz
C2 Command & Control

C2 Command & Control Servers

Infected Nodes & Devices (Bots)

- protefuq.info
- alonebist.info
- contacinformations.info
- detailsnews.info
- promational/material.info
- drivinfosproduits.info
- drivinfosproduits.info
- drivinfosproduits.info
- drivinfosproduits.info
- drivinfosproduits.info
- drivinfosproduits.info
- drivinfosproduits.info
- drivinfosproduits.info
- pubjeieuxfas.info
- srdepot.info
- udpdepot.info
- pixieinfo.info
- passpertinfo.info
Global Bots

- 2017: 8,051,914
- 2019: 12,927,176

2017 World

2019 World
Singapore Bots

2017: 96,780
2019: 181,066
2017 Singapore Bot Data
2019 Singapore Bot Data
A.K.A Light Leafon
14 Years Old

fdisk -l
busybox cat /dev/urandom >/dev/mtdblock0
busybox cat /dev/urandom >/dev/sda
busybox cat /dev/urandom >/dev/ram0
busybox cat /dev/urandom >/dev/mmc0
busybox cat /dev/urandom >/dev/mtdblock10
fdisk -C 1 -H 1 -S 1 /dev/mtd0
fdisk -C 1 -H 1 -S 1 /dev/mtd1
fdisk -C 1 -H 1 -S 1 /dev/sda
fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
illed bot process
route del default
ip route del default
ip route del default
rm -rf */dev/null
sysctl -w net.ipv4.tcp_timestamps=0
sysctl -w kernel-threads-max=1
iptables -F; iptables -t nat -F; iptables -A INPUT -j DROP; iptables -A FORWARD -j DROP
halt -n -f
reboot
What do these threats have in common?
How can you detect this type of activity across your entire network?
What is DNS Response Policy Zones (RPZ)?

Mechanism to introduce a customized policy in Domain Name System servers
A Treasure Trove of data in your DNS
How DNS works

The Internet Address Book

Where is www.google.co.jp?

DNS Resolver
Where is www.google.co.jp?

Other DNS Servers
Do you know www.google.co.jp?
Malicious activities also need DNS

Where is www.google.co.jp?

DNS Resolver
Where is www.google.co.jp?

Other DNS Servers
Do you know www.google.co.jp?

www.nttdocono.com
www.badguys.com
Dgaefcaseioweijvkajl.com

ISP

COM

.NET

.CO.JP
Malicious activities also need DNS

Many things connect to the internet

Where is www.google.co.jp?

ISP

Query: www.google.co.jp

Cname: www.google.co.jp

DNS Resolver

Where is www.google.co.jp?

Other DNS Servers

Do you know www.google.co.jp?

Malicious activities also need DNS

wWw.nttdocono.com
wWw.badguys.com
Dgaefcaseiwoweijvkajl.com

DNS LOGS?

www.google.co.jp
DNS Logs + ELK Stack

Where is www.google.co.jp?

DNS Resolver
Where is www.google.co.jp?

Log Report
Who accessed google.co.jp?

Malicious Activity

ISP

Query: www.google.co.jp

Cname: www.google.co.jp

NXDomain

Cname

Sinkhole

ISP

RPZ Data

Level | Source | Threat Type
--- | --- | ---
Critical | 10.24.31.13 | C2 Comm
Critical | 131.31.23.13 | Malware Domain
High | 34.123.22.4 | Ransomware
High | 51.1.31.44 | DGA Domain
IoT and Infected Devices

Where is Ccdomains.co.jp?

Query: Ccdomains.co.jp
Cname: Ccdomains.co.jp

ISP

RPZ Data

DNS Resolver
Where is Ccdomains.co.jp?

Log Report
Who accessed Ccdomains.co.jp?

<table>
<thead>
<tr>
<th>Level</th>
<th>Source</th>
<th>Threat Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>10.24.31.13</td>
<td>C2 Comm</td>
</tr>
<tr>
<td>Critical</td>
<td>131.31.23.13</td>
<td>Malware Domain</td>
</tr>
<tr>
<td>High</td>
<td>34.123.22.41</td>
<td>Ransomware</td>
</tr>
<tr>
<td>High</td>
<td>51.1.31.44</td>
<td>DGA Domain</td>
</tr>
</tbody>
</table>
Internal Malicious Activity

Malicious User

Query: Corporate AD

DNS

Active Directory

Mail Server

Where is company AD server?

DNS Resolver
Scan for AD or other Internal Servers

Log Report
Who accessed AD Server?

<table>
<thead>
<tr>
<th>Level</th>
<th>Source</th>
<th>Threat Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>10.13.22.31</td>
<td>Active Directory</td>
</tr>
<tr>
<td>Critical</td>
<td>10.13.22.31</td>
<td>Active Directory</td>
</tr>
<tr>
<td>High</td>
<td>10.13.22.31</td>
<td>MS Exchange</td>
</tr>
<tr>
<td>Low</td>
<td>51.1.31.44</td>
<td>Other AD</td>
</tr>
</tbody>
</table>
We already have a firewall.

We have a proxy/web filter.

We use endpoint security.

We have a SIEM.
DNS RPZ - Detect, protect, and, analyze

- Due to HTTPs filtering on proxy is almost no point of use.
- DNS Firewall works on recursive DNS servers
- Its easy to classify threats based on threat intelligence
- Over 91% percent malware uses DNS (As Cisco 2016 Annual Cyber security report)
- Use Of DNS Firewalls Could Reduce 33% Of All Cybersecurity Breaches, New Global Cyber Alliance Research Finds. According to the study, DNS firewalls might have prevented $10 billion in data breach losses from the 11,000 incidents in the past five years. https://finance.yahoo.com/news/dns-firewalls-could-reduce-33-140000777.html
- No new instrustruce needed to implement
- All open source tools used
- Easy to handle false positive
Use Case: Implementation at a major ISP

One Recursive DNS server for Bind: LXD Container with Ubuntu 18.04, vCPU: 8 cores, Memory: 8GB, Storage: 100GB.

We used Bind, Unbound, PowerDNS recursor also support RPZ for DNS firewall.

Second server ELK stack for data visualization.

LXD Container with Ubuntu 18.04, vCPU: 4 cores, Memory: 4GB, Storage: 100GB

RPZ zones Data feed from RPZ feed provider
Any feed provider.
You can also test for 1 month with trial.
Using Open Source Tools to Monitor Your DNS Activity

The ELK stack is a collection of three open source tools -

Elasticsearch + Logstash + Kibana along with log shipper
Classified Threats and Policy Zones

Following RPZ zones were added at the end of the /etc/bind/named.conf.options using the response-policy. Bind currently has a 32 zone limit.

Extremely easy to setup.

Classified threats include.

- Phishing
- Malware
- Criminal Networks
- Bad Nameservers
- Malicious Adware
- Cryptominer
- CryptJacker
- And more.

Sample Configuration

5 Min Install

```plaintext
response-policy {
    zone "rpz.local";
    ### 11 Standard Feeds
    zone "adware.host.dtq";
    zone "badrep.host.dtq";
    zone "bad-nameservers.ip.dtq";
    zone "bad-nameservers.host.dtq";
    zone "bogons.ip.dtq";
    zone "botnetcc.host.dtq";
    zone "botnet.host.dtq";
    zone "botnetcc.ip.dtq";
    zone "dga.host.dtq";
    zone "malware.host.dtq";
    zone "phish.host.dtq";
}
```
Simple Configuration: Get RPZ data from Masters and Generating RPZ logs

RPZ zones will be downloaded from feed provided as a slave zone.

```plaintext
zone "malware.edit.host.dtq" {
    type slave;
    file "dbx.malware.edit.host.dtq";
    masters {199.168.xx.xx;199.168.xx.xx;199.168.xx.xx; }
    allow-transfer { none; }
}
```

Bind RPZ Logging:

```plaintext
channel rpzlog {
    file "rpz.log" versions unlimited size 1000m; print-time yes;
    print-category yes; print-severity yes;
    severity info;
}
category rpz { rpzlog; }
```
How to parse/filter logs with Logstash...

```ruby
filter {
  if [source] == "/var/cache/bind/rpz.log" {
    grok {
      match => [ "message", "%{DATA:NC_timestamp} %{DATA} %{GREEDYDATA}info: %{DATA:X_client} %{GREEDYDATA:X_step2}" ]
    }
    date {
      match => [ "timestamp", "MMM dd HH:mm:ss", "MMM dd HH:mm:ss" ]
    }
  }
}

#### drop unneeded events by X_client

  if [X_client] != "client"{
    drop {
    }
  }
  mutate {
    remove_field => "X_client"
  }

#### Filter X_step2

  grok {
    match => [ "X_step2", "%{DATA} %{DATA:NC_srpip}#%{GREEDYDATA}(%{DATA:NC_hostname}): %{DATA:X_rpz} %{GREEDYDATA:X_step3}" ]
  }
```
How to parse/filter logs with Logstash

#### drop unneeded events by X_rpz

```plaintext
if [X_rpz] != "rpz"{
  drop {} 
}
mutate {
  remove_field => [ "X_rpz", "X_step2" ]
}

#### Filter X_step3

```plaintext
grok {
  match => [ "X_step3", "%{GREEDYDATA} via %{GREEDYDATA:X_type}" ]
}
mutate {
  remove_field => [ "X_step3" ]
}
```
How to parse/filter logs with Logstash..3

```ruby
#### RPZ-Type
if [X_type] =~ "rpz.local" {
    mutate {
        add_field => [ "NC_rpz_type", "rpz.local" ]
    }
} else if [X_type] =~ "adware.host.dtq" {
    mutate {
        add_field => [ "NC_rpz_type", "adware.host.dtq" ]
    }
} else if [X_type] =~ "badrep.host.dtq" {
    mutate {
        add_field => [ "NC_rpz_type", "badrep.host.dtq" ]
    }
} else if [X_type] =~ "bad-nameservers.ip.dtq" {
    mutate {
        add_field => [ "NC_rpz_type", "bad-nameservers.ip.dtq" ]
    }
}
```
DNS Firewall Use Case
DNS Firewall Use Case
DNS Firewall Use Case
DNS Firewall Use Case
DNS Firewall Use Case

https://www.joesandbox.com/analysis/37219/0/executive
Thank you!

For more info:
www.pipelinesecurity.net
https://dmsrpz.info/