3-2-4
DNS Rate Limiting
a Hard Lesson

First Symptoms

- I was in a boring meeting and dealing with email
- Service to my email server was suddenly unusable
- The PoP in trouble also contained my MRTG and other measurement <blush>
- But I could log into the 'outside' IP address of one of the border routers

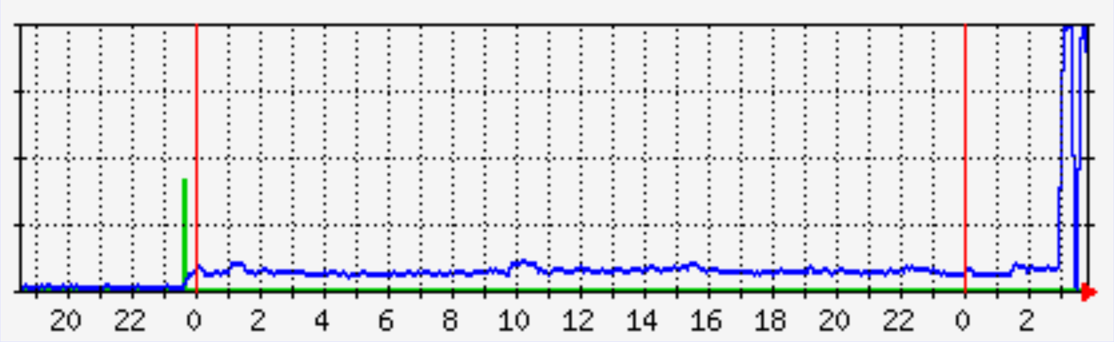
I am the Attacker?

5 minute input rate 720000 bits/sec, 210 packets/sec

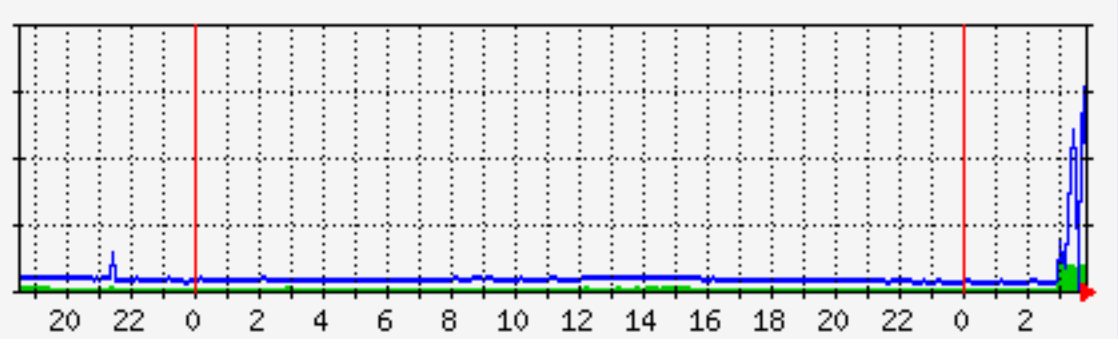
5 minute output rate **740230000** bits/sec, **72520** packets/sec

But it was Very Hard to reach MRTG and Other Tools

MRTG for Router



and a DNS Server



Really My Server?

- Managed to get to APC Power Bar which supplied server
- Shut the Server Down
- Problem Went Away!!!
- Powered Server Back Up
- OK for a Minute, but Then Back to Bad

SSH To Server - Took Three Tries Over 15 Minutes

tcpdump

```
06:28:26.448024 IP rip.psg.com.domain > 108.178.55.192.9463: 54533*- 19/0/14 SOA,
RRSIG, RRSIG, Type51, RRSIG, RRSIG, RRSIG, RRSIG, RRSIG, DNSKEY[|domain]
06:28:26.448026 IP rip.psg.com > 108.178.55.192: udp
06:28:26.448071 IP rip.psg.com.domain > 108.178.55.192.9463: 54533*- 19/0/14 SOA,
RRSIG, RRSIG, Type51, RRSIG, RRSIG, RRSIG, RRSIG, RRSIG, DNSKEY[|domain]
06:28:26.448072 IP rip.psg.com > 108.178.55.192: udp
06:28:26.448168 IP rip.psg.com.domain > 108.178.55.192.9463: 54533*- 19/0/14 SOA,
RRSIG, RRSIG, Type51, RRSIG, RRSIG, RRSIG, RRSIG, RRSIG, DNSKEY[|domain]
06:28:26.448171 IP rip.psg.com > 108.178.55.192: udp
06:28:26.448174 IP rip.psg.com.domain > 108.178.55.192.9463: 54533*- 19/0/14 SOA,
RRSIG, RRSIG, Type51, RRSIG, RRSIG, RRSIG, RRSIG, RRSIG, DNSKEY[|domain]
06:28:26.448176 IP rip.psg.com > 108.178.55.192: udp
06:28:26.448234 IP rip.psg.com.domain > 108.178.55.192.9463: 54533*- 19/0/14 SOA,
RRSIG, RRSIG, Type51, RRSIG, RRSIG, RRSIG, RRSIG, RRSIG, DNSKEY[|domain]
06:28:26.448237 IP rip.psg.com > 108.178.55.192: udp
06:28:26.448247 IP rip.psg.com.domain > 108.178.55.192.9463: 54533*- 19/0/14 SOA,
RRSIG, RRSIG, Type51, RRSIG, RRSIG, RRSIG, RRSIG, RRSIG, DNSKEY[|domain]
```

So It Was a DNS Reflector Attack!

But the Server Was NOT a Recursive Resolver

Turned off DNS

- Used /etc/ipfw.conf, IP Firwall to

```
add deny udp from any to any 53
```

- I Could Now Breathe and Think
- But the Server was Critical to DNS, serving 20 ccTLDs
- A Quick Mailing List Question Showed that this was a DNSsec-based Query Reflector Attack

With a Highly Signed
CH ccTLD
One Byte of Query
Produced > 1KB
of DNSsec Response

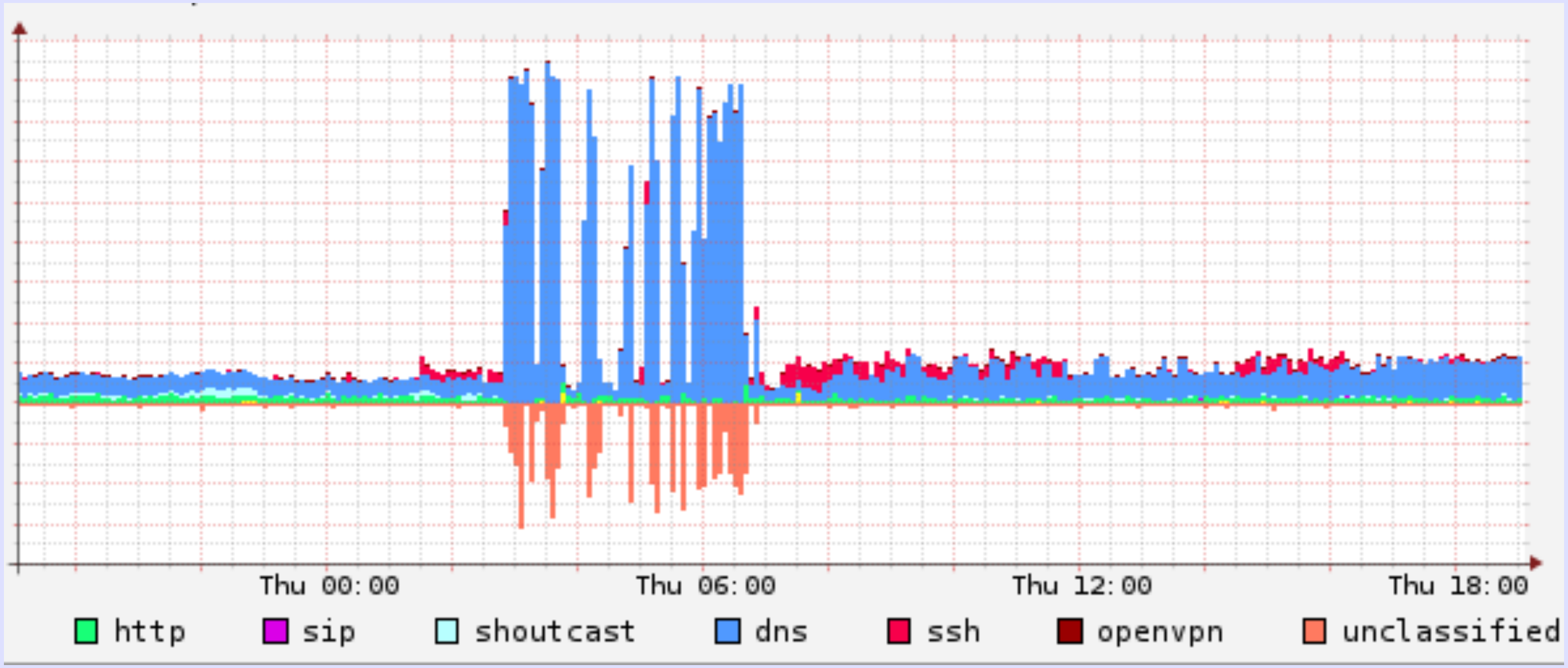
Attacker Used Spoofed Source Address, the Address of the Victim, for UDP Query

The Solution Would Be Rate-Limiting

Throttle Queries From a Single Source

Upgraded BIND to 9.9.2 with Patch rl005.12-P1

```
Options {
  rate-limit {
    responses-per-second 5;
    window 5;
    };
  };
```


Thu 00:00
Thu 06:00
Thu 12:00
Thu 18:00
http
sip
shoutcast
dns
ssh
openvpn
unclassified

The Problem Was Solved!

From: CH ccTLD Admin

As you have seen today the CH-zone got hit with a DNS ANY query storm. I assume the traffic has been sent to most CH secondary name-servers.

We saw the following kind of query towards our name-servers which resulted in an amplification factor of 75:

```
dig +edns=0 +bufsize=9000 CH. ANY
```

Lessons

- OOB Access Really Needed to Be Out Of Band <blush>
- Set Up a Second Measurement System to Measure the First?
- Install and Configure DNS Flow-Limiting Before This Happens to You!!

Unbound

Measurement of Plasma Unbound
Unconjugated Bilirubin

Monitoring changes in bilirubin concentration using diazo derivatives, and correcting for rate-limiting dissociation of bilirubin from albumin.

Google does not always work

NSD

Use the configure script option

```
./configure –enable-ratelimit
```

The default parameters are a good start