A DNS DDOS Experience

@Worldlink
dated - Dec 2014

Abhishek Singh Okheda
Sr. System Administrator
Worldlink Communications Pvt. Ltd.

One World. One Link.

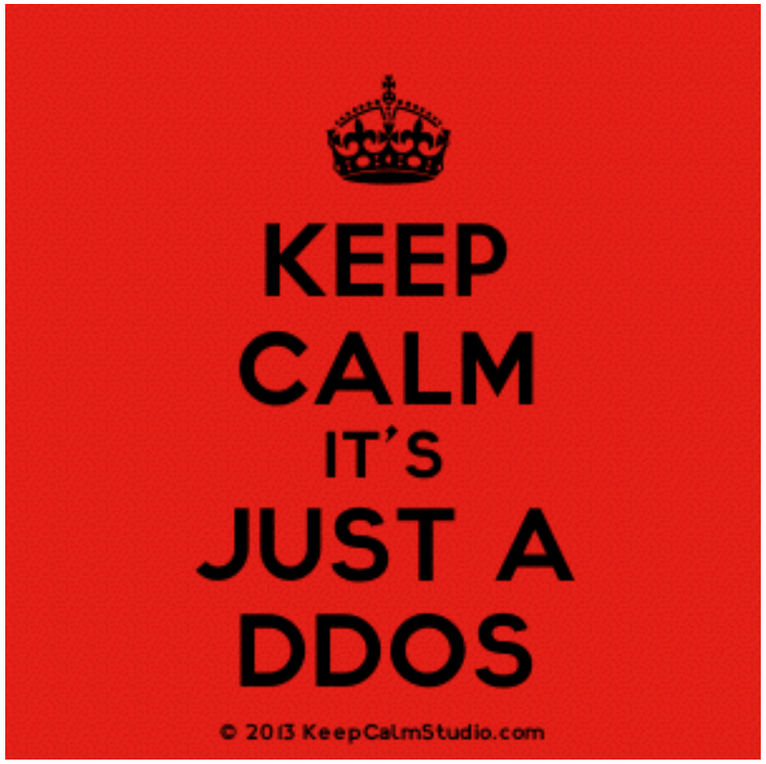
What not to expect

- Technical granularity

What to expect

- A brief overview of the experience

Software Interface Start



They Say

BUT We were not and we could not be

Because It Was

DNS

The heart of all our Infra

And it was under attack **DDOS Attack**

The Discovery

Phase 1

Discovery, obvious reasons

- DNS responses were slow
- CPU/Memory usage started increasing
- DNS service started being unresponsive now and then

Obvious Temporary Solution

- Restart DNS Services time and again 😊
- Which was not enough finally, so we had to find a way to mitigate it

arkhamnetwork

Our DNS servers were receiving a large illegitimate queries for (arkhamnetwork.org/com).

03:05:13.849579 IP 27.34.4.129.1175 > 202.79.32.4.53: 27310+ A? fZAxiQI1.**arkhamnetwork.org.** (44)
03:05:13.849583 IP 27.34.27.81.1109 > 202.79.32.4.53: 41535+ A? sqLjJ09s.arkhamnetwork.org. (44)
03:05:13.849619 IP 27.34.6.117.1115 > 202.79.32.4.53: 47685+ A? P9pAMYOD.arkhamnetwork.org. (44)
03:05:13.849669 IP 27.34.66.99.1202 > 202.79.32.4.53: 29479+ A? zb0OjZTC.arkhamnetwork.org. (44)
03:05:13.849673 IP 27.34.2.85.1161 > 202.79.32.4.53: 49730+ A? IDHksOvB.arkhamnetwork.org. (44)
03:05:13.849676 IP 27.34.6.99.1180 > 202.79.32.4.53: 65393+ A? 8B356M2e.arkhamnetwork.org. (44)
03:05:13.849718 IP 202.166.217.5.1084 > 202.79.32.4.53: 27361+ A? S0qg27rk.arkhamnetwork.org. (44)
03:05:13.849722 IP 27.34.22.85.1097 > 202.79.32.4.53: 32234+ A? Ai67nHLw.arkhamnetwork.org. (44)

And coincidentally, during the same time "Arkham (batman game)" servers were under DDOS worldwide.

We found it

So, “arkhamnetwork.org" queries were the cause

Oh!! So, we are one of the pivot points for that DDOS

Solution clicked

Drop such requests with firewall

At first we opted for a vendor-firewall

Called them at night, and they arrived with a product

Condition was: drop DNS queries for arkhamnetwork

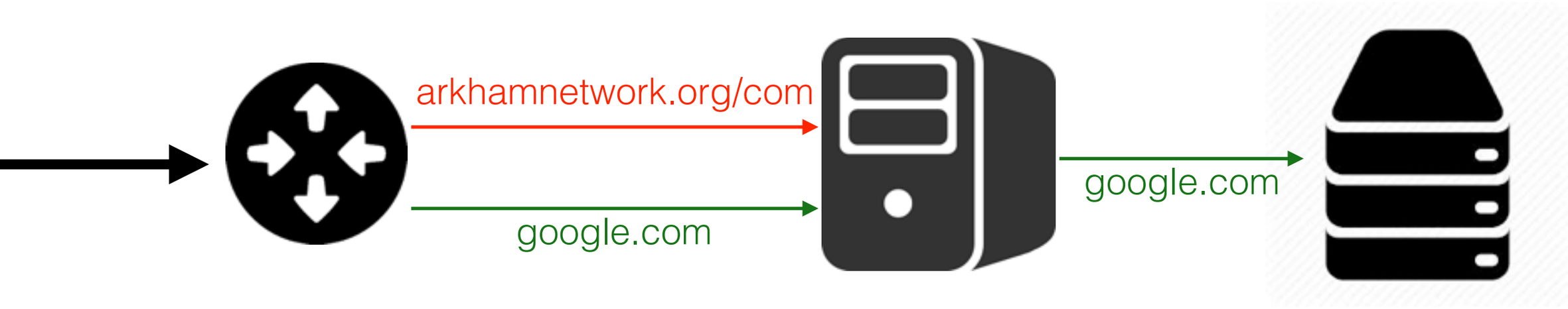
They gave their effort and tried their best

Unluckily, we were out of luck

The vendor proprietary firewall product
did not have the flexibility we required

Finally we switched to

our favorite OS - **Linux**
and
our best friend - **iptables**



Block arkhamnetwork

arkhamnetwork.com/.org DDos Attack
iptables -A INPUT -p udp --dport 53 -m string --from 40 --to 80 --string 'arkhamnetwork' --algo bm -j DROP

As an extra precaution - ratelimit PPPoE DNS Queries

####DNS rate limit to pppoe
iptables -v -A FORWARD -p udp --dport 53 -m recent --set --name dnsanyquery
iptables -v -A FORWARD -p udp --dport 53 --dst <dnsserver> --src <pppoe_pool> -m recent --name dnsanyquery --rcheck --seconds 1 --hitcount 10 -j DROP

Also, we limited the bandwidth of DNS traffic in our BRAS on per user basis (according to their subscribed bandwidth)

For example, 64k DNS traffic limit for a user who has subscribed 1M bandwidth, and 128k for 2M

The Discovery

Phase 2

- The next day, back to office, no more expecting any issues in DNS.
- But unfortunately, some other domains had started hitting the servers
  - betsjoy.com
  - nirvanmc.com
  - www.hrcp88.com
  - riotgames.com
  - 99cai.info
  - asus.com
  - laidianqp.net
  - www.ganne499.xyz
  - www.9222hh.com
  - …..

11:24:19.454425 IP 202.79.56.247.46000 > 202.79.32.4.53: 15603+ A? **jgzffeq.www.8777hh.com**. (40)
11:24:19.465507 IP 202.79.56.247.58923 > 202.79.32.4.53: 15370+ A? mqvaqsv.www.8777hh.com. (40)
11:24:19.468848 IP 202.79.44.228.38165 > 202.79.32.4.53: 45497+ A? tjlmgzlxjpiqjku.www.8777hh.com. (48)
11:24:19.481068 IP 202.166.217.108.2075 > 202.79.32.98.53: 31620+ A? ivaryvotyvgtonir.www.8777hh.com. (49)
11:24:19.493897 IP 202.166.198.81.55150 > 202.79.32.4.53: 22817+ A? csq.www.8777hh.com. (36)
11:24:19.494332 IP 202.166.198.81.54243 > 202.79.32.4.53: 15337+ A? eci.www.8777hh.com. (36)
11:24:19.507191 IP 202.166.221.118.40118 > 202.79.32.98.53: 12180+ A? ttsynwcui.www.8777hh.com. (42)
11:24:19.512773 IP 202.166.205.201.39246 > 202.79.32.4.53: 40617+ A? sdqhufcxyferchqn.www.8777hh.com. (49)
11:24:19.513524 IP 202.166.205.201.36968 > 202.79.32.4.53: 22008+ A? kbujihydkfqlmtqb.www.8777hh.com. (49)
11:24:19.516131 IP 202.166.217.47.54784 > 202.79.32.4.53: 62135+ A? bufclywyxvyrwae.www.8777hh.com. (48)
11:24:19.525956 IP 202.166.217.47.39361 > 202.79.32.4.53: 6887+ A? fhshbqaktlvrjcl.www.8777hh.com. (48)
11:24:19.528708 IP 202.79.51.206.49870 > 202.79.32.4.53: 60993+ A? mnb.www.8777hh.com. (36)
11:24:19.529668 IP 202.79.51.206.49353 > 202.79.32.4.53: 26801+ A? idh.www.8777hh.com. (36)
11:24:19.536093 IP 202.166.198.81.57950 > 202.79.32.4.53: 26746+ A? aocqesguvjxlm.www.8777hh.com. (46)
14:39:18.787549 IP 202.166.198.81.58092 > 202.79.32.4.53: 64183+ A? **uoauzlbtact.betsjoy.com**. (41)
14:39:18.789046 IP 202.166.206.99.59879 > 202.79.32.4.53: 44783+ A? cnizsbcxazelah.betsjoy.com. (44)
14:39:18.789096 IP 202.79.48.218.35815 > 202.79.32.4.53: 53089+ A? ixul.betsjoy.com. (34)
14:39:18.790544 IP 202.166.206.61.45025 > 202.79.32.4.53: 24729+ A? opcvifin.betsjoy.com. (38)
14:39:18.790793 IP 202.79.41.114.58368 > 202.79.32.4.53: 52052+ A? xplnjwgsopl.betsjoy.com. (41)
14:39:18.791742 IP 202.79.45.53.60677 > 202.79.32.4.53: 58826+ A? qj.betsjoy.com. (32)
14:39:18.793421 IP 202.166.205.64.58700 > 202.79.32.4.53: 44+ A? mtazujitmdsd.betsjoy.com. (42)
14:39:18.794088 IP 202.166.205.212.39615 > 202.79.32.4.53: 27525+ A? ntltonmyrhz.betsjoy.com. (41)
14:39:18.799784 IP 202.166.206.99.58679 > 202.79.32.4.53: 32000+ A? sdqhgnixwdyz.betsjoy.com. (42)
14:39:18.799929 IP 202.79.48.218.53500 > 202.79.32.4.53: 49405+ A? gdmdsrgzan.betsjoy.com. (40)
14:39:18.801227 IP 202.166.206.61.51074 > 202.79.32.4.53: 19713+ A? er.betsjoy.com. (32)
14:39:18.804373 IP 202.79.57.84.51219 > 202.79.32.4.53: 42882+ A? orqn.betsjoy.com. (34)
14:39:18.804771 IP 202.166.221.109.54911 > 202.79.32.4.53: 2590+ A? abchklmziz.betsjoy.com. (40)
14:39:18.805070 IP 202.79.58.252.53595 > 202.79.32.4.53: 30017+ A? onar.betsjoy.com. (34)
14:39:18.805077 IP 202.79.58.252.58049 > 202.79.32.4.53: 53259+ A? ufilylixgpepylkf.betsjoy.com. (46)
14:39:18.806722 IP 202.79.57.84.50606 > 202.79.32.4.53: 5722+ A? mbgpitcvwlwfad.betsjoy.com. (44)
14:39:18.807367 IP 202.79.41.114.32929 > 202.79.32.4.53: 13422+ A? id.betsjoy.com. (32)
14:39:18.810262 IP 202.79.48.223.37209 > 202.79.32.4.53: 45894+ A? kpijyfqzwxwb.betsjoy.com. (42)
14:39:18.811312 IP 202.166.205.201.56430 > 202.79.32.4.53: 45361+ A? cdwjehavkxev.betsjoy.com. (42)
14:39:18.812363 IP 202.166.205.218.57904 > 202.79.32.4.53: 21418+ A? pejdvpvddbh.betsjoy.com. (41)

- Eventually we had realized we were **self-mislead** by the worldwide “arkhamnetwork” DDOS attack news. It was not the actual cause.

- Also, we were no more stable with the “string-match” iptables rules

- We had to find the root cause now

we needed to buckle up

- Reviewing again, we realized that most (almost all) of the source IPs of the DDOS causing traffics were of our customer's Mikrotik routers.

But why were the Mikrotik routers sending such queries

The Discovery

Phase 3

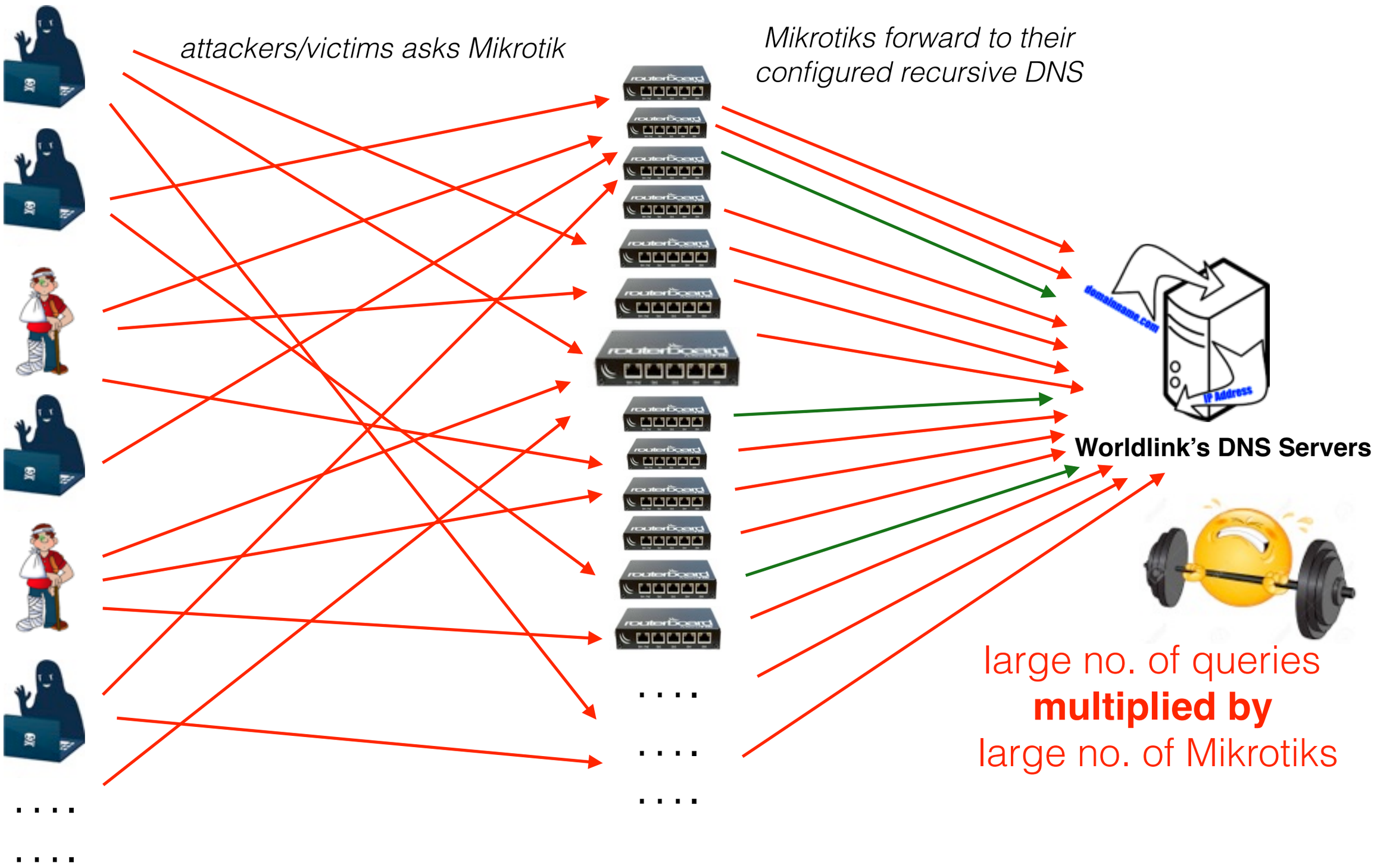
- We viewed the live traffic dump of some of the suspected Mikrotik routers
- Luckily Mikrotik supports TZSP (TaZmen Sniffer Protocol) which made it easy for us to remotely view the traffic flow in Wireshark

And then we came to realize that the Mikrotik routers were acting as **vectors (victims)** for the DDOS attack

They were **Open DNS Resolver** by default.

No firewall for it in place, so they were open to all the rest of the world

And our recursive DNS Servers are open to them and are also their configured DNS server.

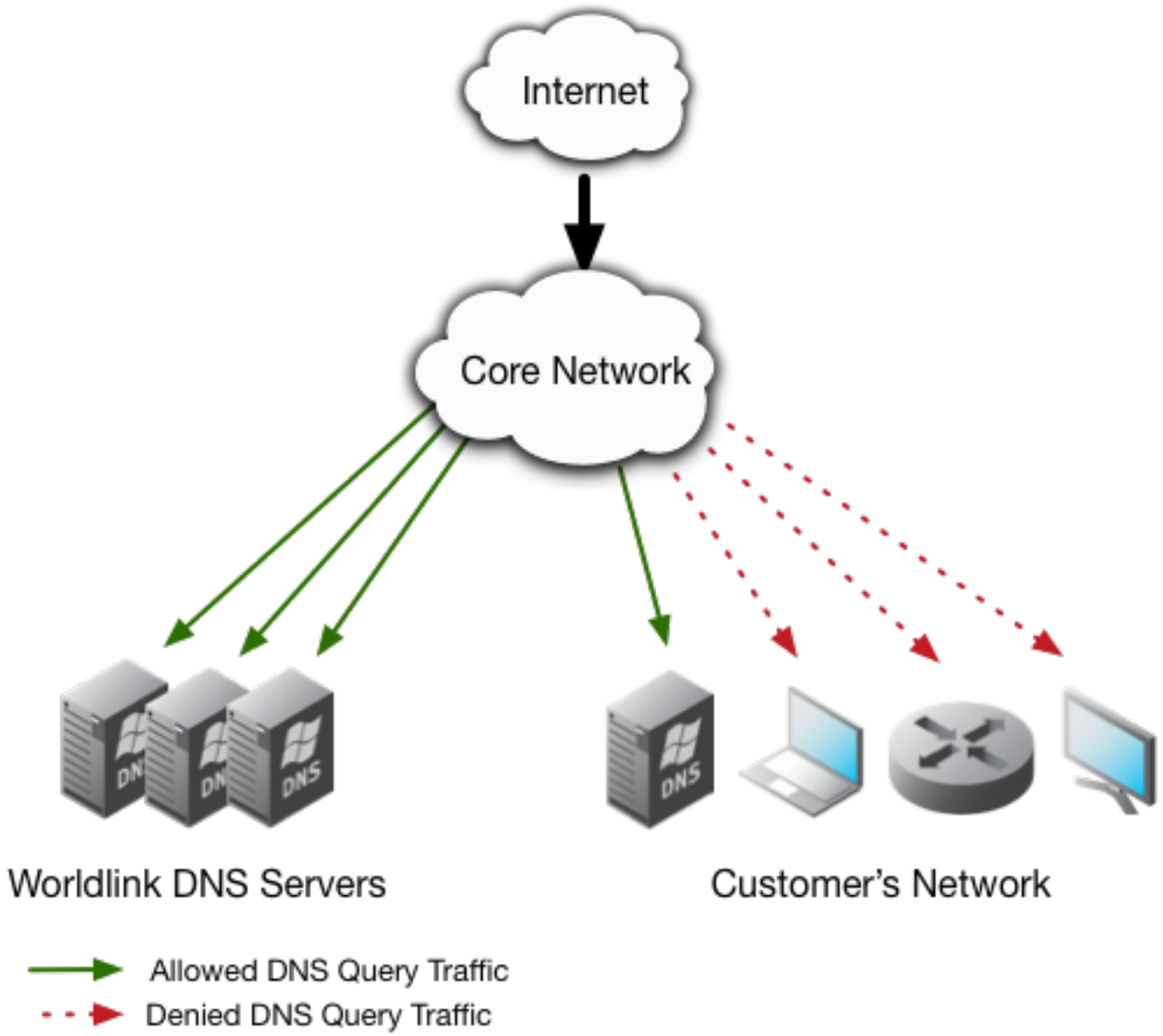


The attack illustration

The Mitigation

Firewall of course

Firewall Implementation



Firewall Rules for DST Port 53

Lesson Learnt

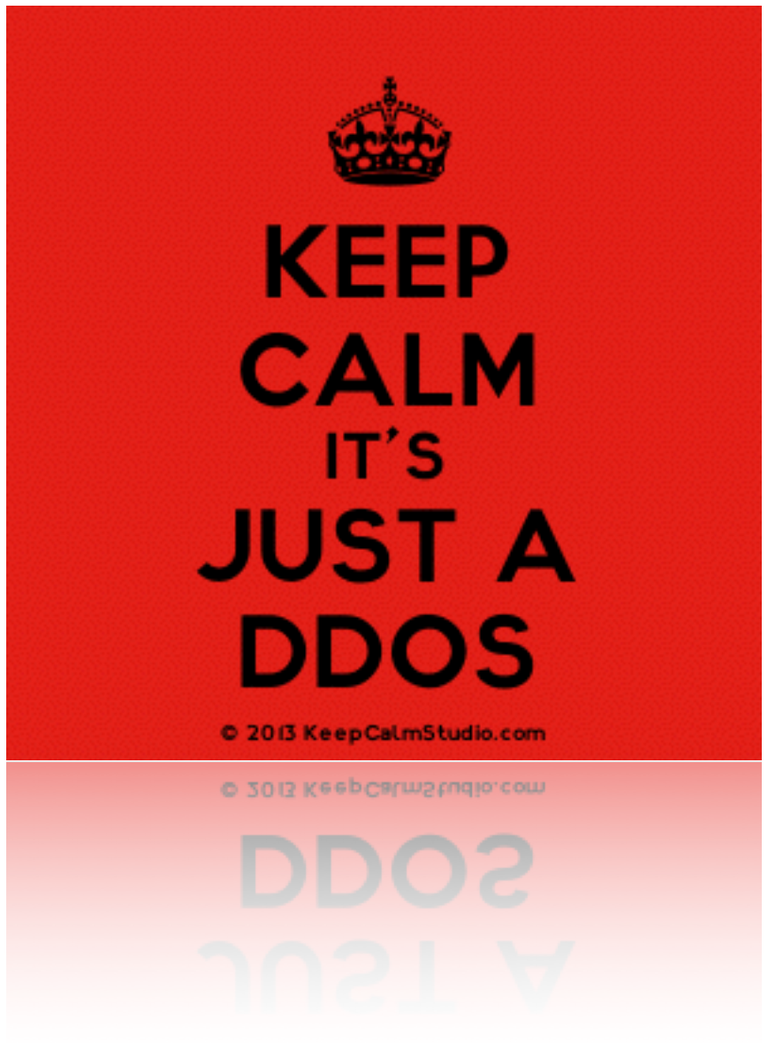
नजिकको तिर्थ हेला नगरौ !!

Internal Network Security is important

We started out with external attack mitigation and did not even notice the major **AMPLIFIERS** of the DDOS

Our own **INTERNAL NETWORK**

I would like to end by saying



The End

Thank You