DDoS In South Asia

A lesson on introspection

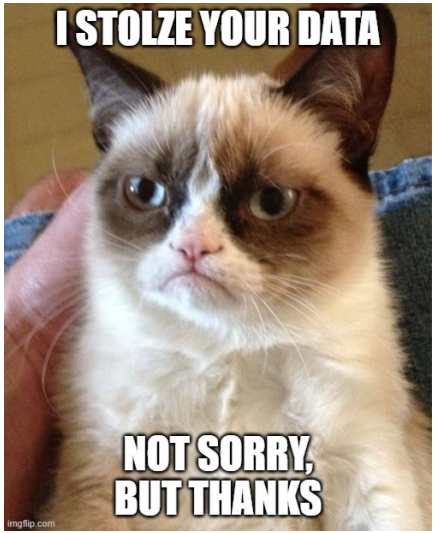
Dave Phelan - APNIC

Who Am I?

- Dave Phelan
  - Network and Infrastructure engineer for a LONG time
  - Trainer at APNIC
  - Parent to 2 Human children and 3 Fur Children
  - Likes Cat memes

Acknowledgments

- Jamie Gilespie and Adli Wahid for some of their Sec content
- Shodan.io for running a great internet scanning tool
- Cloudflare - Cloudflare Radar



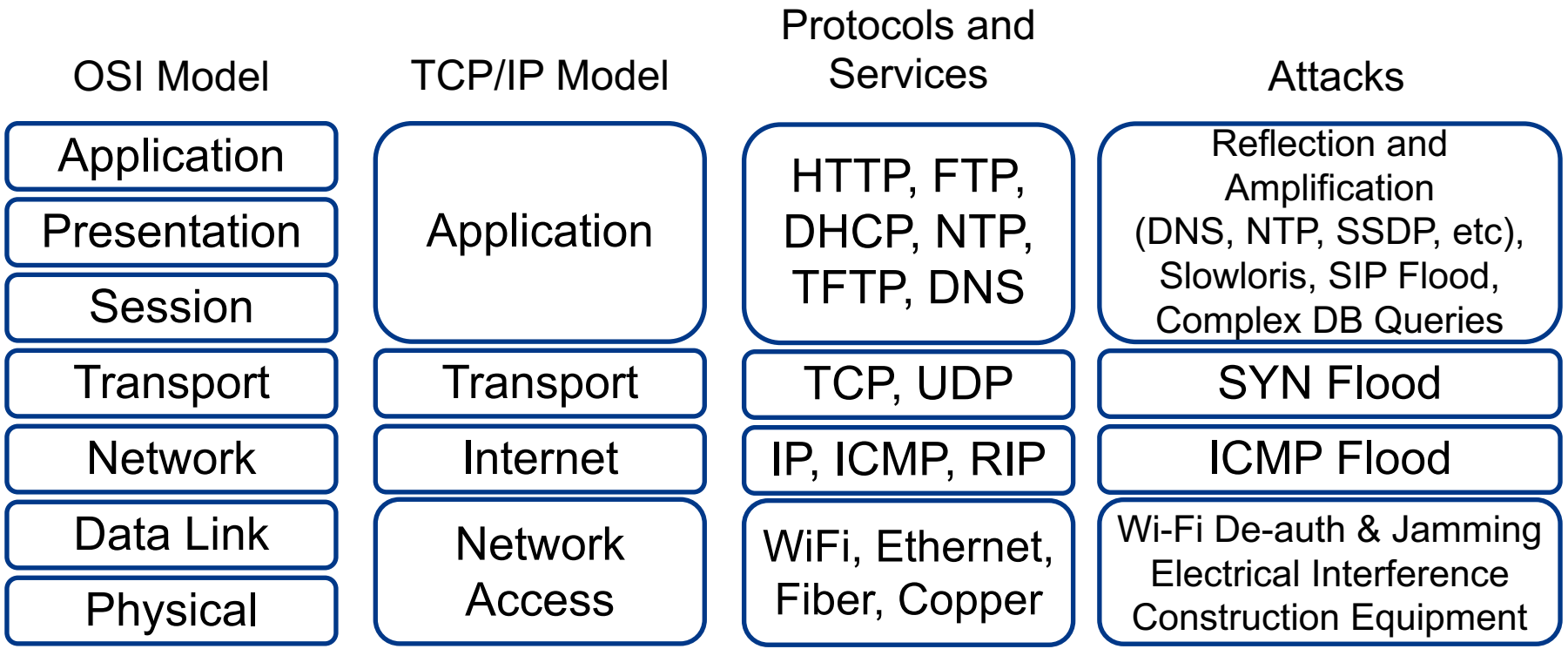
What are we going to talk about?

- What is a DDoS
- Look at some stats around DDoS Globally and Per Sub Region
- What do we need to fix?
- How can we mitigate and not contribute to the problem?

What is DoS and DDoS?

- In general, a denial of service is an attack against availability of a service
  - A service can be a network, or a specific service such as a web site
- DoS - Denial of Service
  - Usually from only one source
- DDoS - Distributed Denial of Service
  - Attack originates from multiple sources
  - This is caused through resource exhaustion

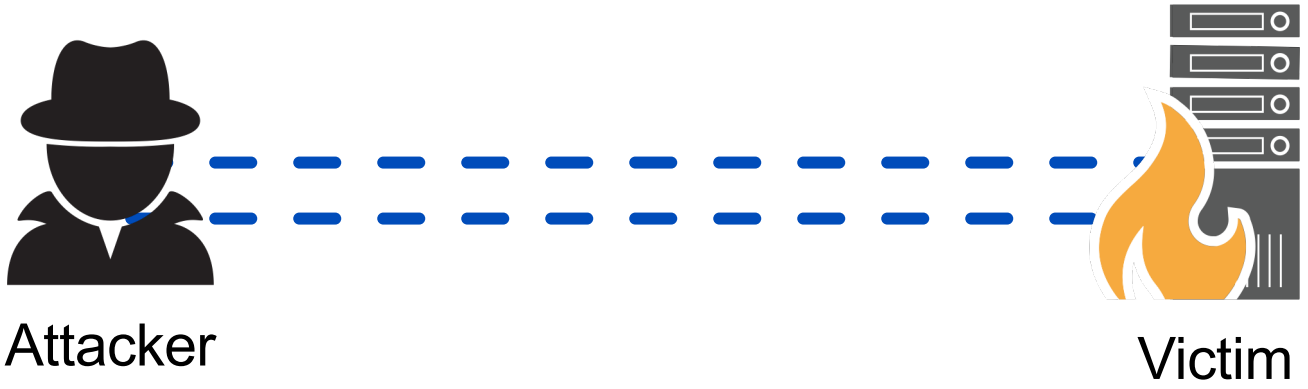
DoS by Layers



* Colour animated slide

Simple DoS

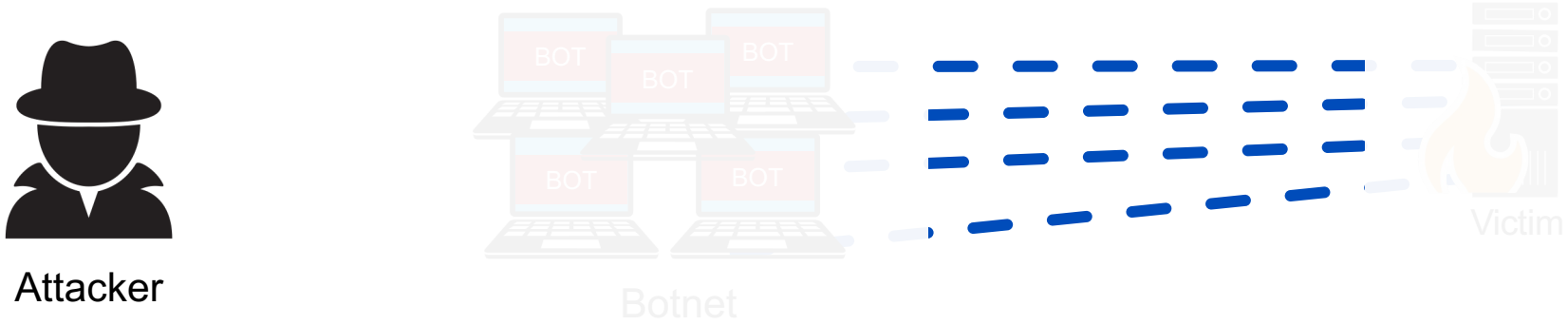
1 Attacker sends any valid or invalid traffic to the victim



Simple DDoS

1 Attacker directs bots to begin attack

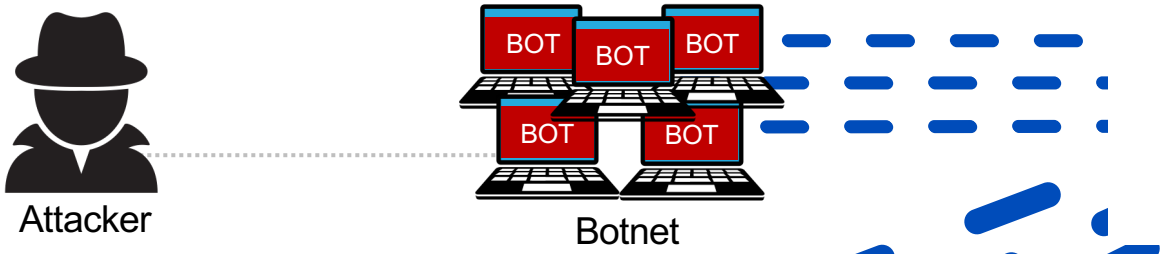
2 All bots send any valid or invalid traffic to the victim



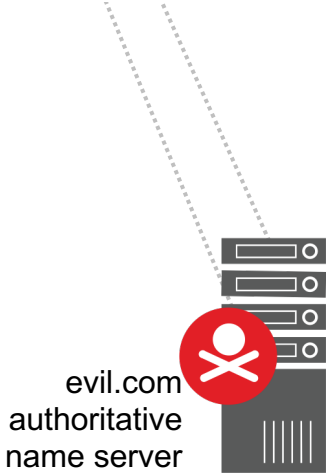
Reflected and Amplified DDoS

1 Attacker directs bots to begin attack

2 All bots send DNS queries for the TXT record in domain “evil.com” to open recursive DNS servers and fake "my IP is 10.10.1.1"



3 Open resolvers ask the authoritative name server for the TXT record “evil.com”

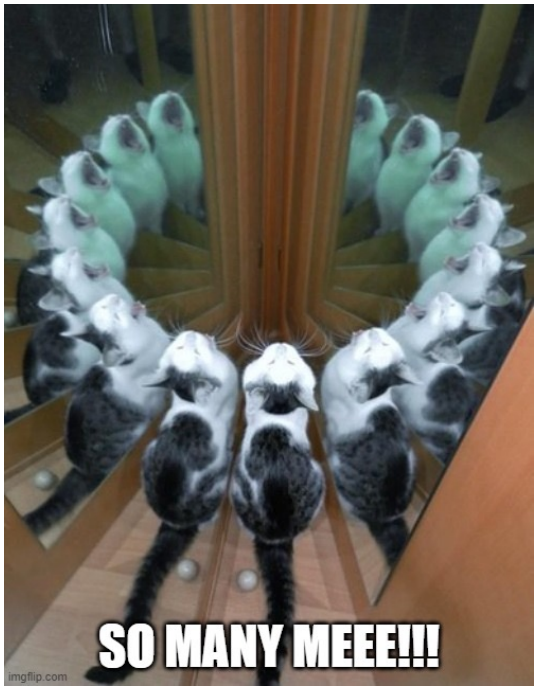


4 evil.com name server responds with 4000 byte TXT records

5 Open resolvers cache the response and send a stream of 4000 byte DNS responses to the victim

Reflection and Amplification

- What makes for good reflection?
  - UDP
    - Spoofable / forged source IP addresses
    - Connectionless (no 3-way handshake)
- What makes for good amplification?
  - Small command results in a larger reply
    - This creates a Bandwidth Amplification Factor (BAF)
    - Reply Length / Request Length = BAF
      - Example: 3223 bytes / 64 bytes = BAF of 50.4
    - Chart on next slide created with data from https://www.us-cert.gov/ncas/alerts/TA14-017A



Amplification Factors

Protocol	Bandwidth Amplification Factor
Multicast DNS (mDNS)	2-10
BitTorrent	3.8
NetBIOS	3.8
Steam Protocol	5.5
SNMPv2	6.3
Portmap (RPCbind)	7 to 28
DNS	**28 to 54**
SSDP	**30.8**

Protocol	Bandwidth Amplification Factor
LDAP	46 to 55
TFTP	60
Quake Network Protocol	63.9
RIPv1	131.24
QOTD	140.3
CHARGEN	358.8
NTP	**556.9**
Memcached	**up to 51,000**

So why are you telling me this?

- Operators Complain about DoS/DDoS
- Do the minimum to ensure they are not contributing

- But How bad is it really?
  - (Hint: It's not good….)

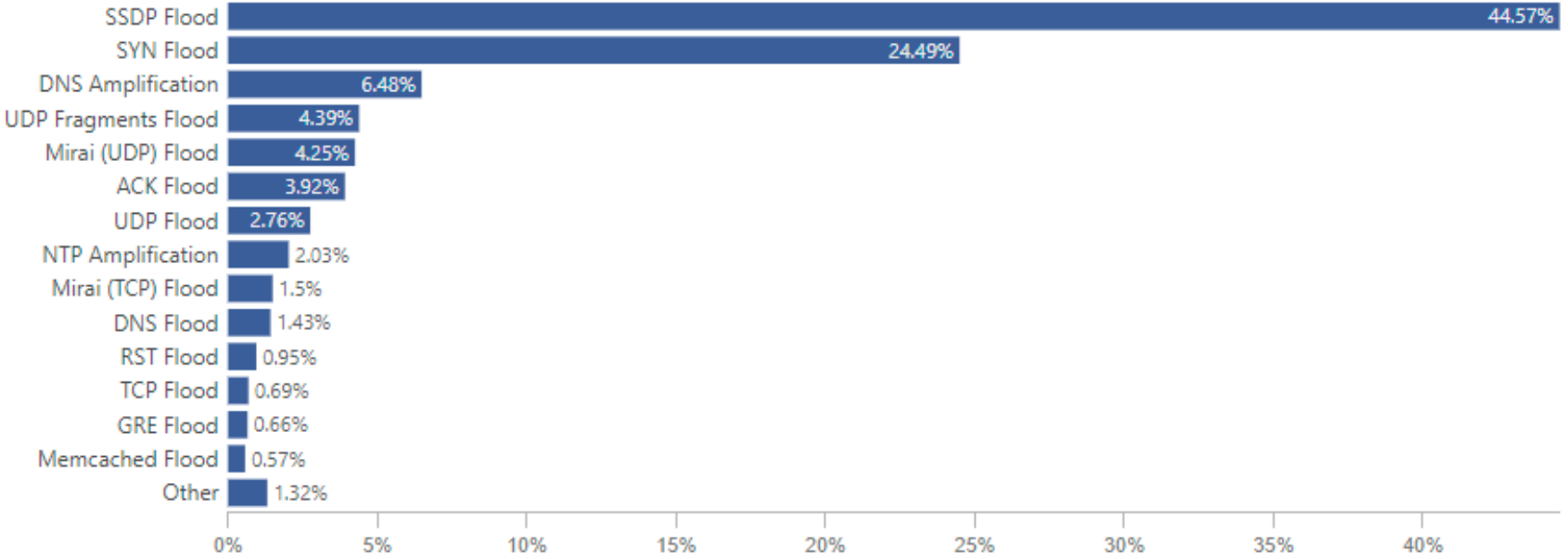
Global Numbers

- Most data sourced from
  - Cloudflare Radar
  - Shodan.io
- Top 5 Countries DDoS Sources
  - USA - 31%
  - **India – 9.2%**
  - Germany – 5.4%
  - Brazil – 5.2%
  - China – 3.3%

https://radar.cloudflare.com/security-and-attacks

Global Numbers

Attack Types



https://radar.cloudflare.com/security-and-attacks

India

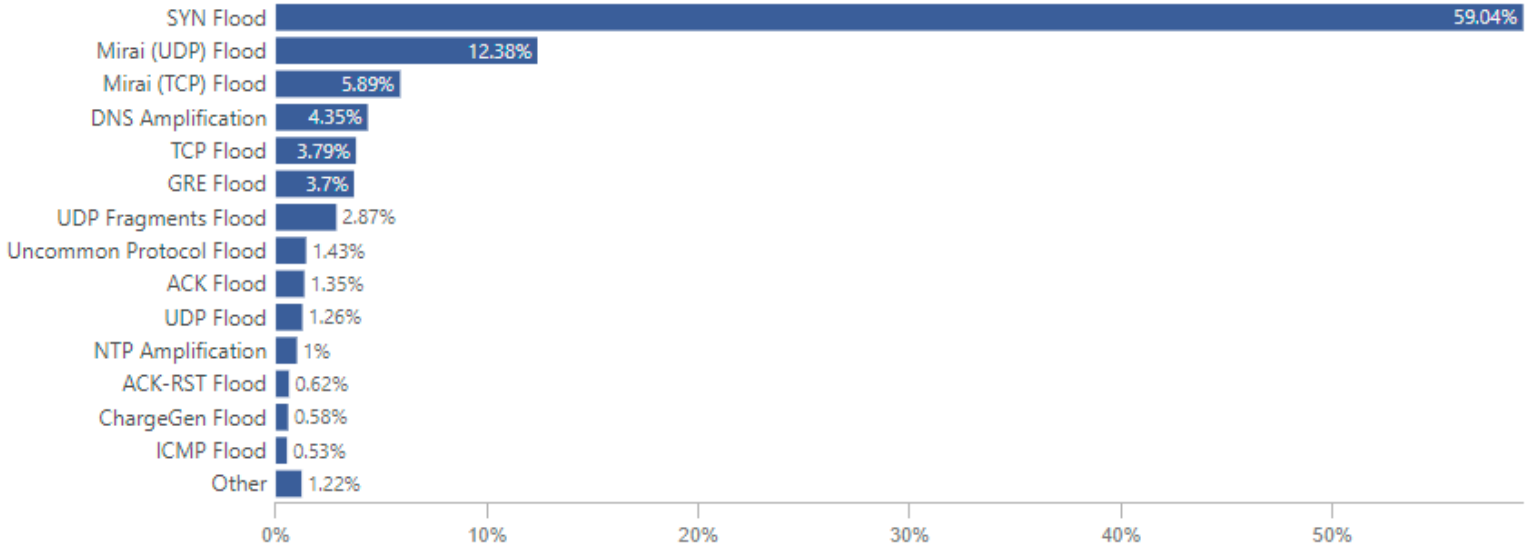
Top Source Networks:

#	ASN	Percentage
1	55836 - RELIANCEJIO-IN Reliance Jio Infocomm Limited	40.30%
2	45609 - BHARTI-MOBILITY-AS-AP Bharti Airtel Ltd. AS for GPRS Service	24.20%
3	38266 - VIL-AS-AP Vodafone Idea Ltd	3.90%
4	24560 - AIRTELBROADBAND-AS-AP Bharti Airtel Ltd., Telemedia Services	3.80%
5	16509 - AMAZON-02	3.30%

https://radar.cloudflare.com/security-and-attacks/in?dateRange=12w

India

Attack Types



https://radar.cloudflare.com/security-and-attacks/in?dateRange=12w

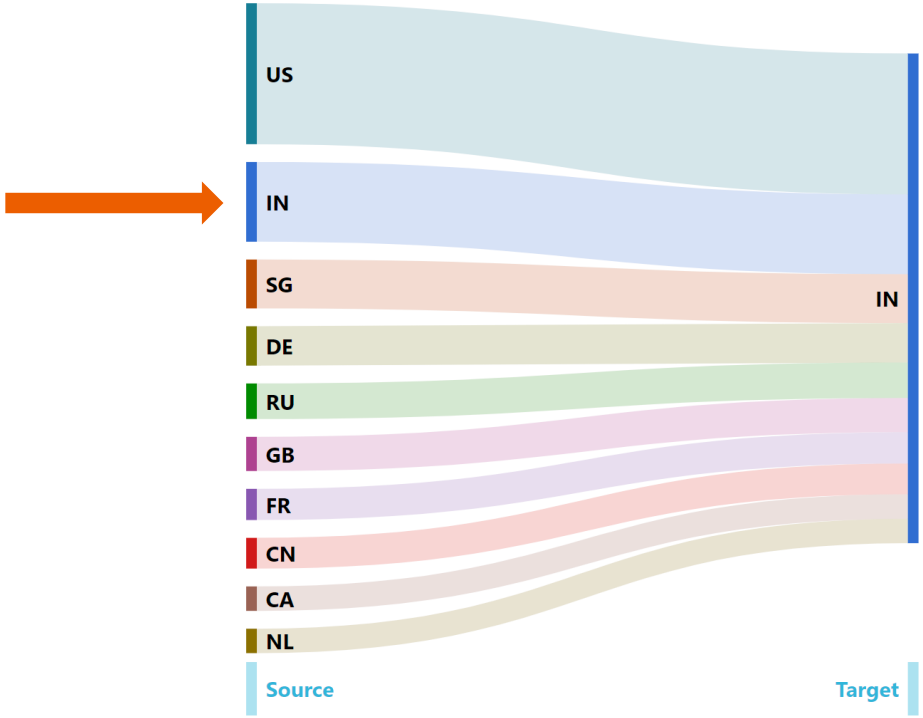
India

- Open Ports

DNS	330,983
NTP	121,750
SSDP	198,091
MemcacheD	2,125
Telnet	37,503

https://www.shodan.io/search?query=country%3Ain

India



https://radar.cloudflare.com/security-and-attacks/in?dateRange=12w

Sri Lanka

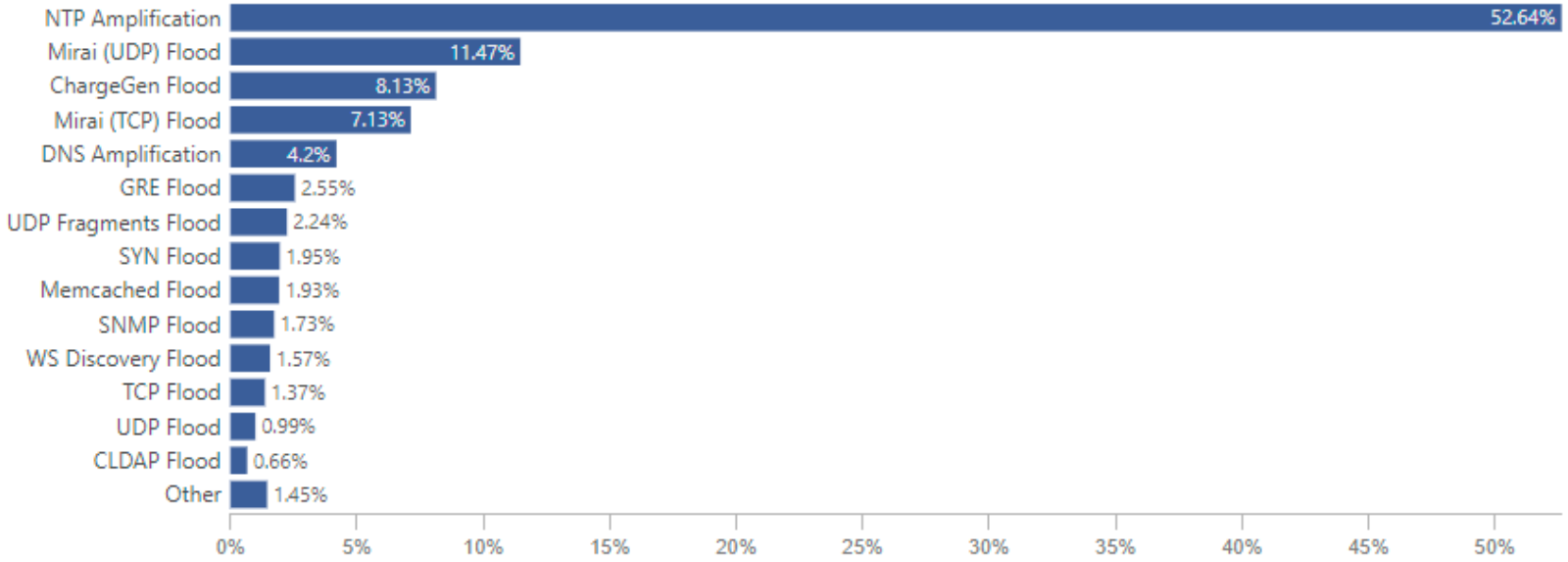
Top Source Networks:

#	ASN	Percentage
1	18001 - DIALOG-AS Dialog Axiata PLC.	**40.00%**
2	9329 - SLTINT-AS-AP Sri Lanka Telecom Internet	**30.30%**
3	45356 - MOBITEL-LK Mobitel Pvt Ltd	**10.40%**
4	132045 - AIRTEL-AS-ISP Bharti Airtel Lanka Pvt. Limited	**5.70%**
5	17470 - HUTCHISON-LK Hutchison Telecommunications Lanka Private Limited	**3.50%**

https://radar.cloudflare.com/security-and-attacks/lk?dateRange=12w

Sri Lanka

Attack Types



https://radar.cloudflare.com/security-and-attacks/lk?dateRange=12w

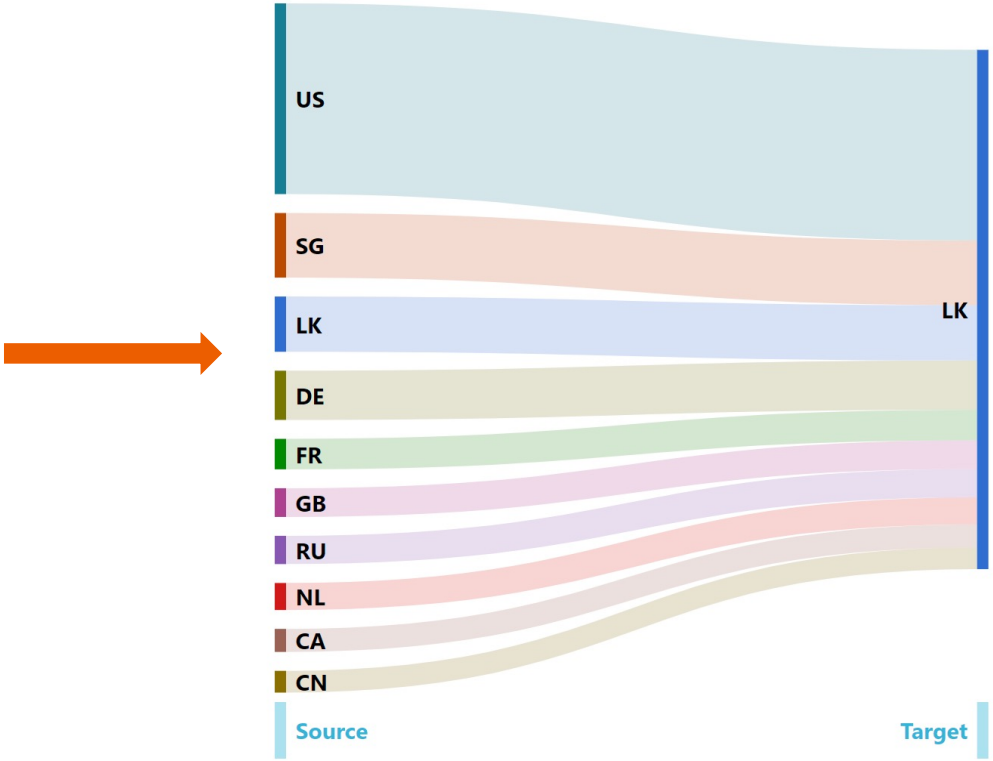
Sri Lanka

- Open Ports

DNS	138
NTP	3958
SSDP	204
MemcacheD	93
Telnet	1636

https://www.shodan.io/search?query=country%3Alk

Sri Lanka



https://radar.cloudflare.com/security-and-attacks/lk?dateRange=12w

Nepal

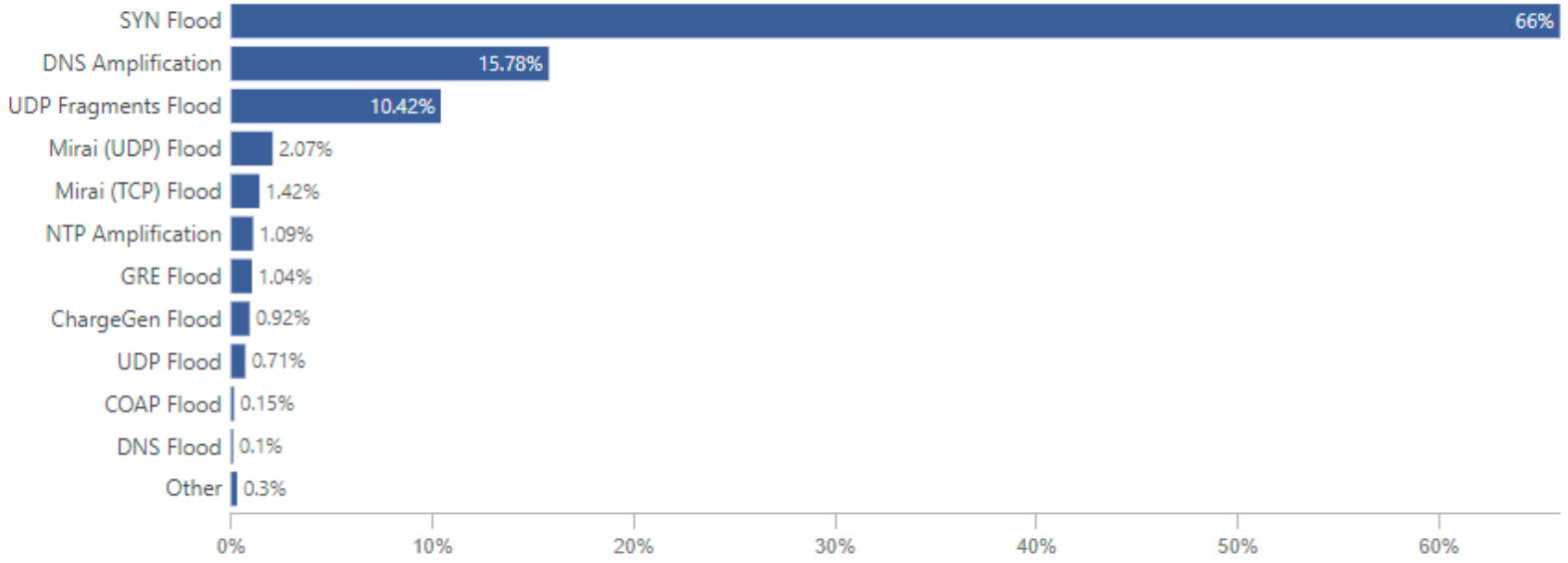
Top Source Networks:

#	ASN	Percentage
1	17501 - WLINK-NEPAL-AS-AP WorldLink Communications Pvt Ltd	**33.90%**
2	4007 - SUBISU-CABLENET-AS-AP Subisu Cablenet Pvt Ltd, Baluwatar, Kathmandu, Nepal	**19.50%**
3	45650 - VIANET-NP Vianet Communications Pvt. Ltd.	**6.30%**
4	139922 - DMNPL-AS-AP DISH MEDIA NETWORK PUBLIC LIMITED	**5.10%**
5	23752 - NPTELECOM-NP-AS Nepal Telecommunications Corporation, Internet Services	**4.90%**

https://radar.cloudflare.com/security-and-attacks/np?dateRange=12w

Nepal

Attack Types



https://radar.cloudflare.com/security-and-attacks/np?dateRange=12w

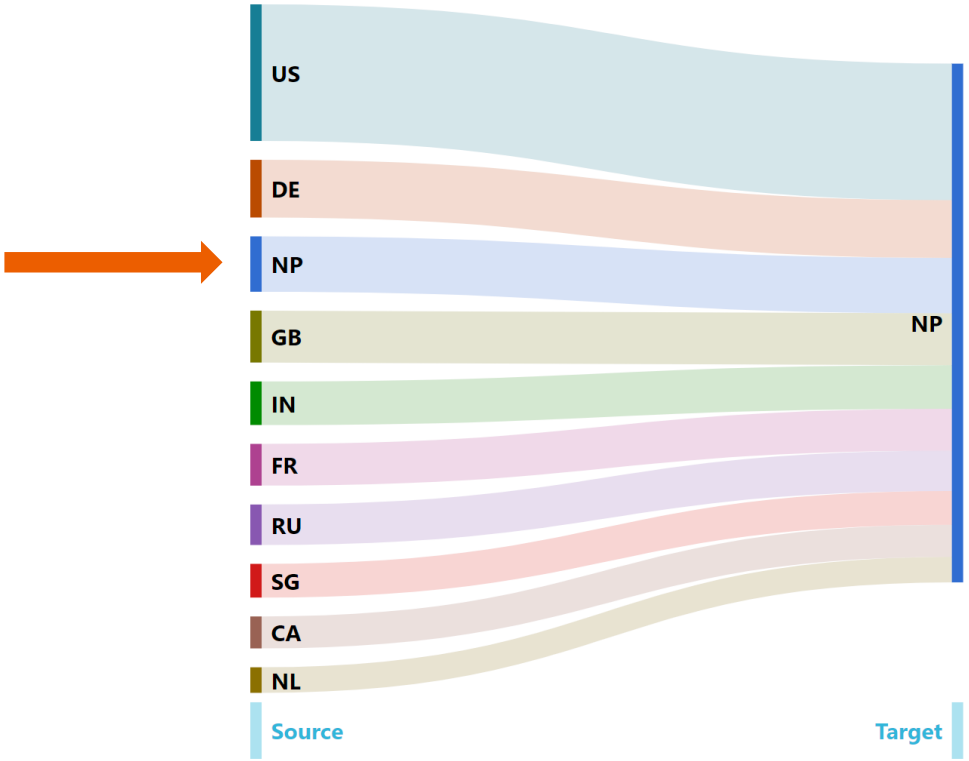
Nepal

- Open Ports

DNS	868
NTP	5540
SSDP	16
MemcacheD	19
Telnet	974

https://www.shodan.io/search?query=country%3Anp

Nepal



https://radar.cloudflare.com/security-and-attacks/np?dateRange=12w

Bhutan

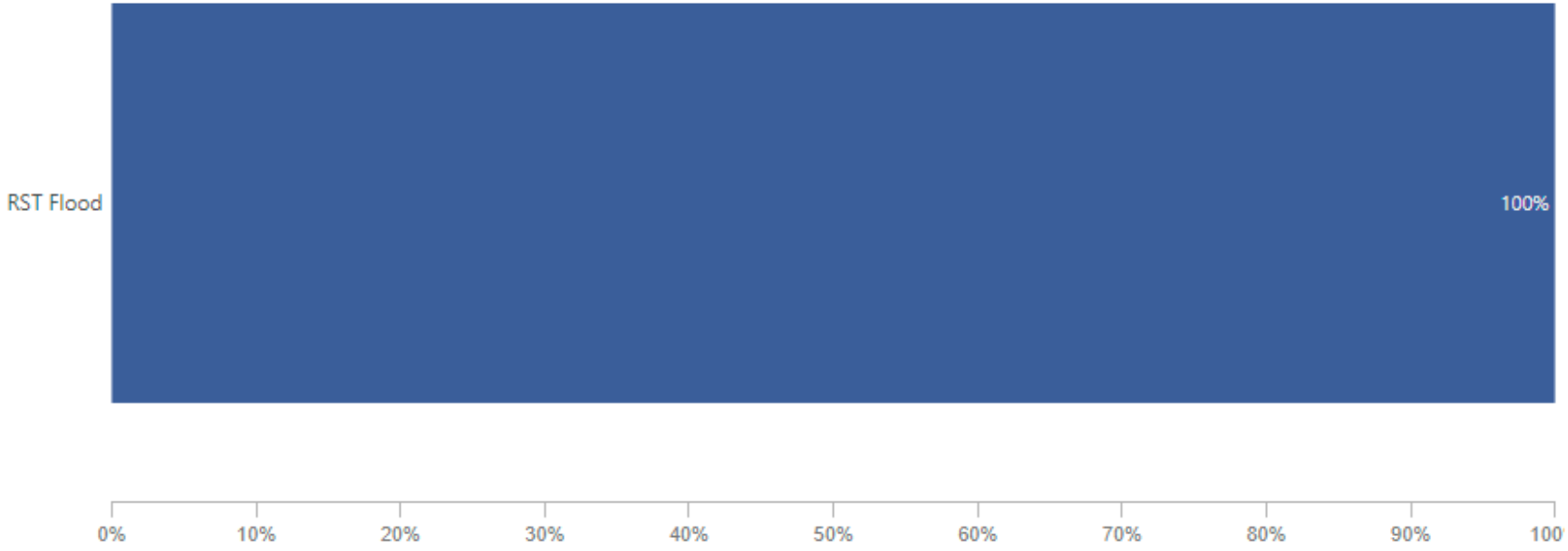
Top Source Networks:

#	ASN	Percentage
1	18024 - BTTELECOM-AS-AP Bhutan Telecom Ltd	**82.00%**
2	23955 - TASHICELL-DOMESTIC-AS Tashi InfoComm Limited	**6.70%**
3	137412 - TASHICELL-MOBILE-AS Tashicell Domestic AS Thimphu Bhutan	**4.10%**
4	134715 - GTA-AS-AP Government Technology Agency	**3.40%**
5	136039 - NANO-AS-AP NANO, Bhutan	**1.30%**

https://radar.cloudflare.com/security-and-attacks/bt?dateRange=12w

Bhutan

Attack Types



https://radar.cloudflare.com/security-and-attacks/bt?dateRange=12w

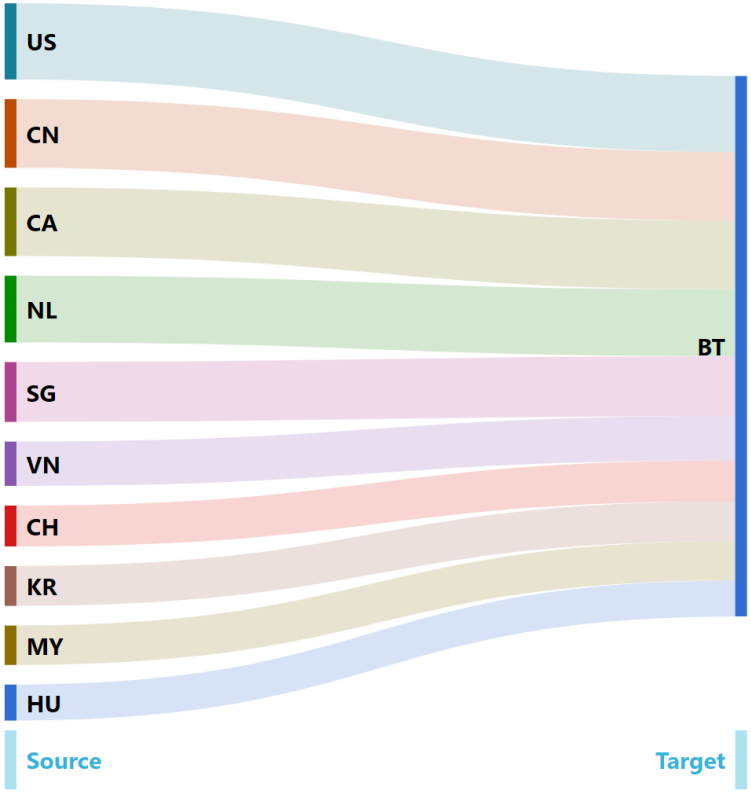
Bhutan

- Open Ports

DNS	56
NTP	548
SSDP	5
MemcacheD	0
Telnet	88

https://www.shodan.io/search?query=country%3Abt

Bhutan



https://radar.cloudflare.com/security-and-attacks/bt?dateRange=12w

Bangladesh

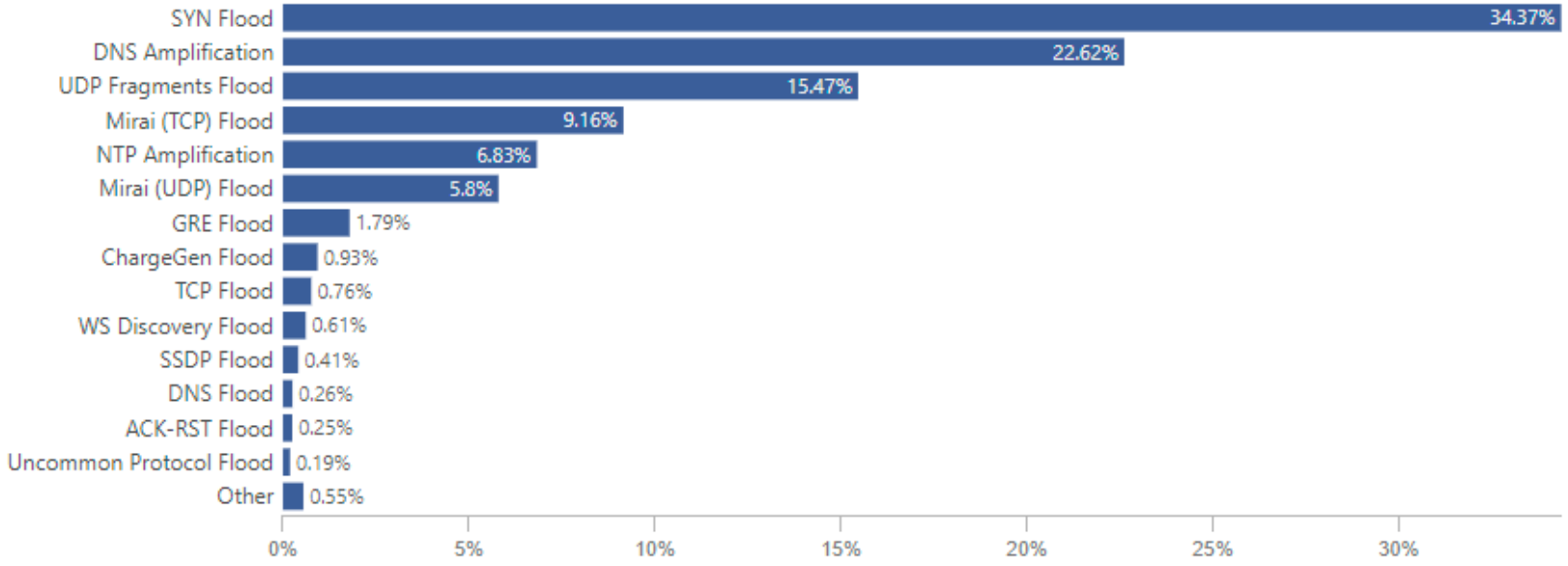
Top Source Networks:

#	ASN	Percentage
1	24389 - GRAMEENPHONE-AS-AP GrameenPhone Ltd.	**5.80%**
2	24342 - BRAC-BDMAIL-AS-BD BRACNet Limited	**5.50%**
3	24432 - AXIATA-ROBI-AS-AP TM International Bangladesh Ltd.Internet service Provider,Gulshan-1,Dhaka-1212	**4.50%**
4	45245 - BANGLALINK-AS Banglalink Digital Communications Ltd	**3.20%**
5	23688 - LINK3-TECH-AS-BD-AP Link3 Technologies Ltd.	**2.40%**

https://radar.cloudflare.com/security-and-attacks/bd?dateRange=12w

Bangladesh

Attack Types



https://radar.cloudflare.com/security-and-attacks/bd?dateRange=12w

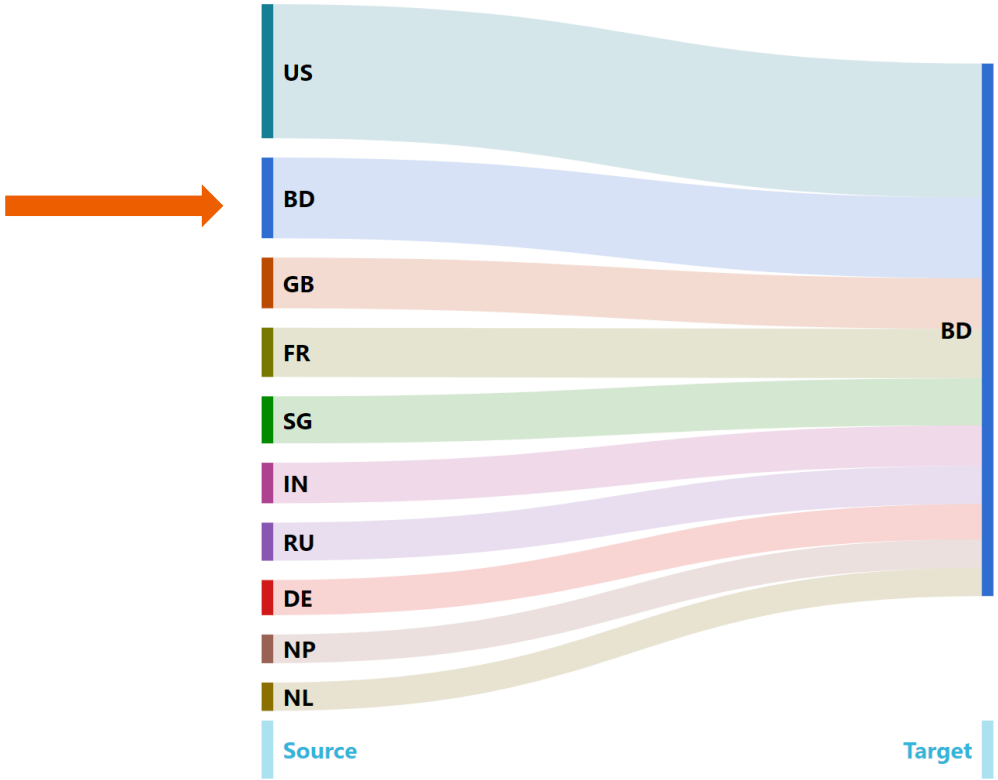
Bangladesh

- Open Ports

DNS	62,002
NTP	27369
SSDP	104
MemcacheD	158
Telnet	5472

https://www.shodan.io/search?query=country%3Abd

Bangladesh



https://radar.cloudflare.com/security-and-attacks/bd?dateRange=12w

Pakistan

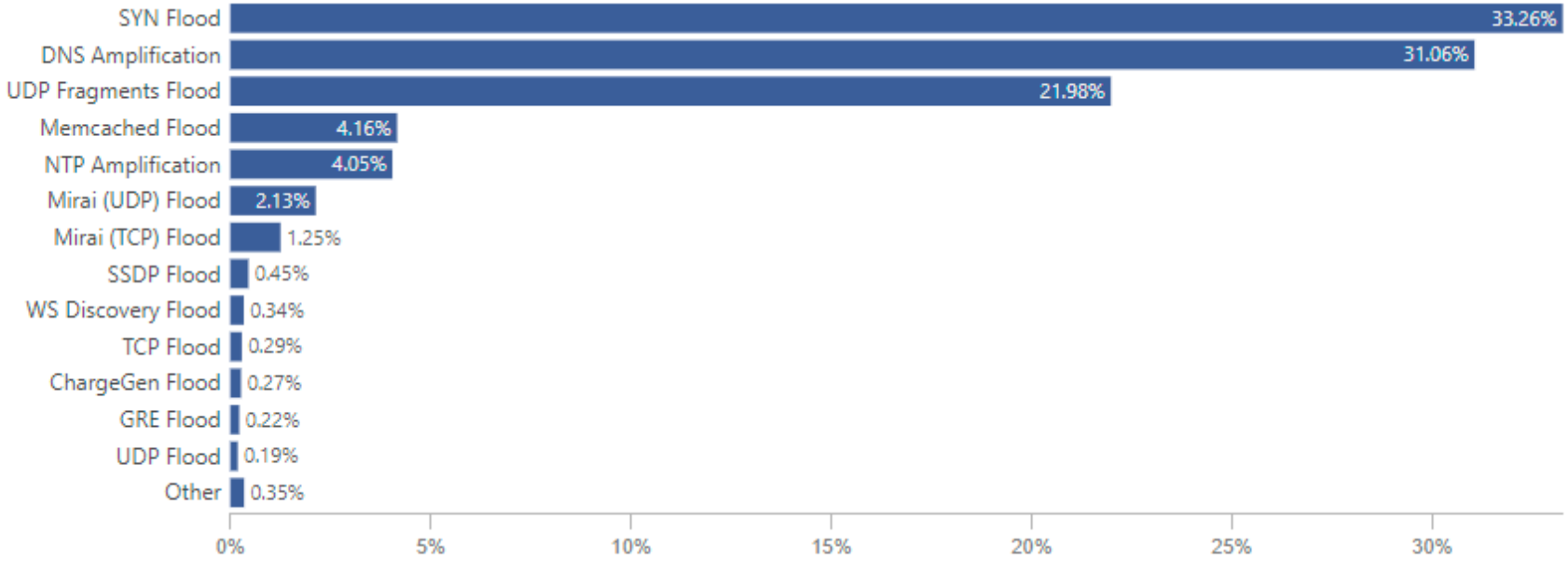
Top Source Networks:

#	ASN	Percentage
1	136384 - OPTIX-AS-AP Optix Pakistan Pvt. Limited	**33.40%**
2	17557 - PKTELECOM-AS-PK Pakistan Telecommunication Company Limited	**10.90%**
3	45669 - MOBILINK-AS-PK PMCL LDI IP TRANSIT	**9.50%**
4	59257 - CMPAKLIMITED-AS-AP CMPak Limited	**8.20%**
5	9541 - CYBERNET-AP Cyber Internet Services Pvt Ltd.	**6.20%**

https://radar.cloudflare.com/security-and-attacks/pk?dateRange=12w

Pakistan

Attack Types



https://radar.cloudflare.com/security-and-attacks/pk?dateRange=12w

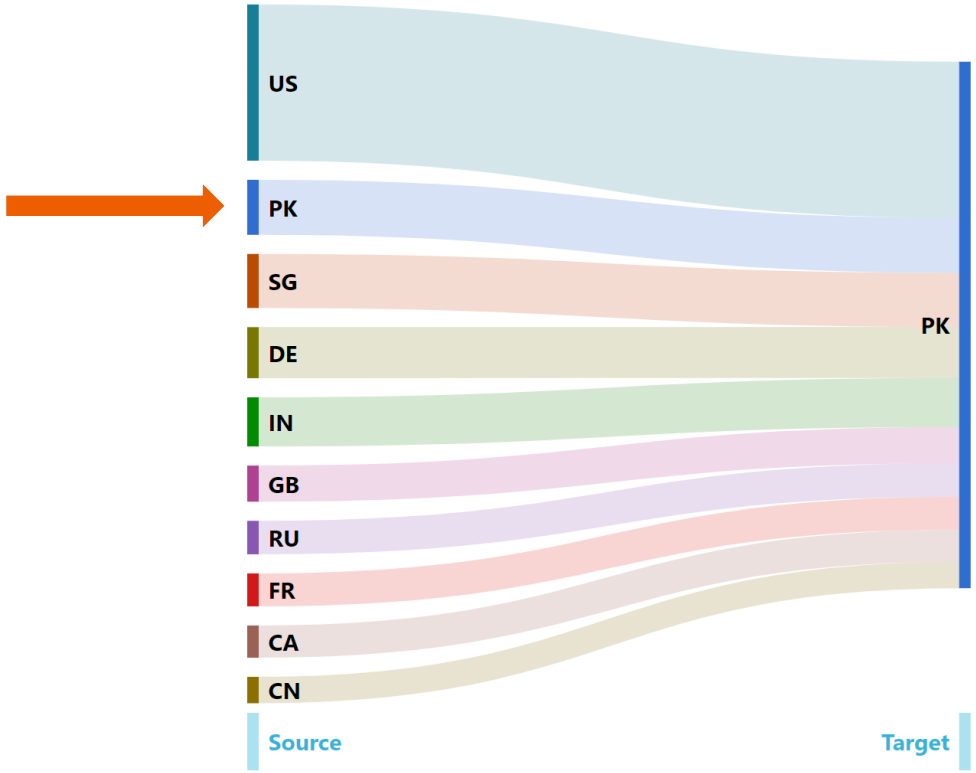
Pakistan

- Open Ports

DNS	41380
NTP	15546
SSDP	103
MemcacheD	136
Telnet	62667

https://www.shodan.io/search?query=country%3Apk

Pakistan



https://radar.cloudflare.com/security-and-attacks/pk?dateRange=12w

Afghanistan

Top Source Networks:

#	ASN	Percentage
1	55330 - GCN-DCN-AS AFGHANTELECOM GOVERNMENT COMMUNICATION NETWORK	**30.90%**
2	131284 - ETISALATAFG-AS-AP Etisalat Afghan	**23.40%**
3	38742 - AWCC-AS-AP Afghan Wireless Communication Company	**10.70%**
4	59381 - VICEGROUP-AF Vice Group	**9.30%**
5	45178 - ROSHAN-AF Main Street, House No. 13 Wazir Akbar Khan	**5.50%**

https://radar.cloudflare.com/security-and-attacks/af?dateRange=12w

Afghanistan

Attack Types

Insufficient Network Layer Attack Data!

https://radar.cloudflare.com/security-and-attacks/af?dateRange=12w

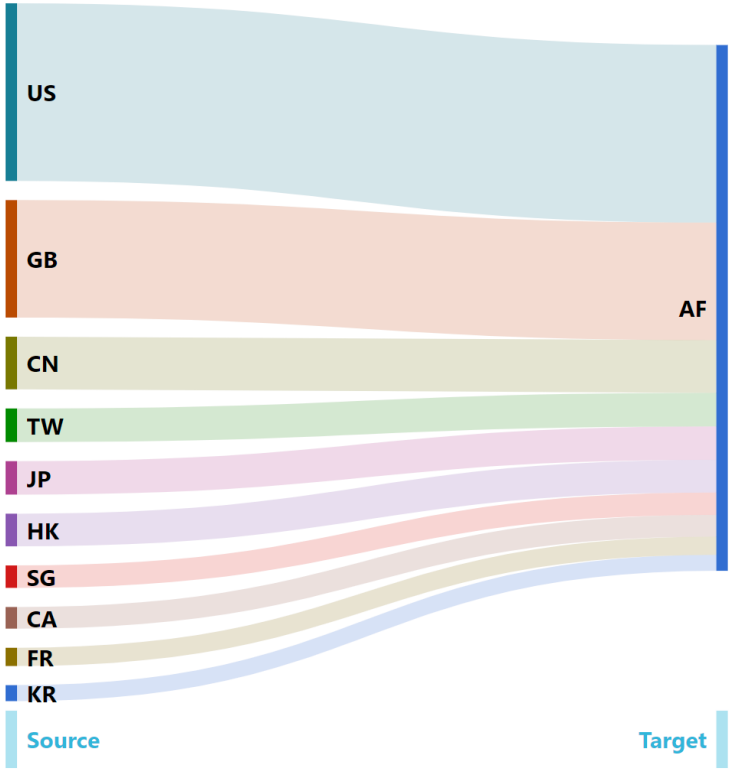
Afghanistan

- Open Ports

DNS	1974
NTP	2525
SSDP	8
MemcacheD	1
Telnet	1505

https://www.shodan.io/search?query=country%3Aaf

Afghanistan



https://radar.cloudflare.com/security-and-attacks/af?dateRange=12w

Maldives

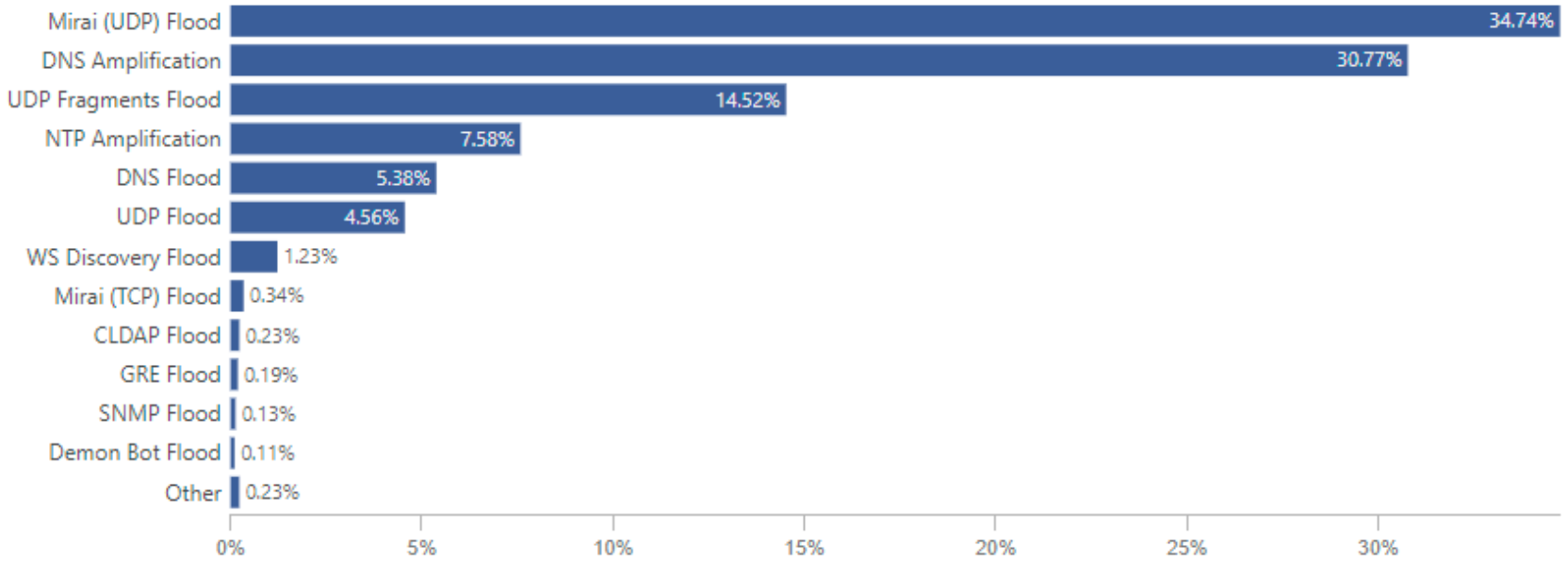
Top Source Networks:

#	ASN	Percentage
1	7642 - DHIRAAGU-MV-AP DHIVEHI RAAJJEYGE GULHUN PLC	79.30%
2	55944 - OOREDOO-MV Ooredoo Maldives Plc	17.90%
3	13335 - CLOUDFLARENET	0.90%
4	24016 - RAAJJEONLINE-AS Focus Infocom Private Limited	0.80%
5	136238 - SATLINKPVTLTD-AS-AP SatLink Pvt Ltd	0.40%

https://radar.cloudflare.com/security-and-attacks/mv?dateRange=12w

Maldives

Attack Types



https://radar.cloudflare.com/security-and-attacks/mv?dateRange=12w

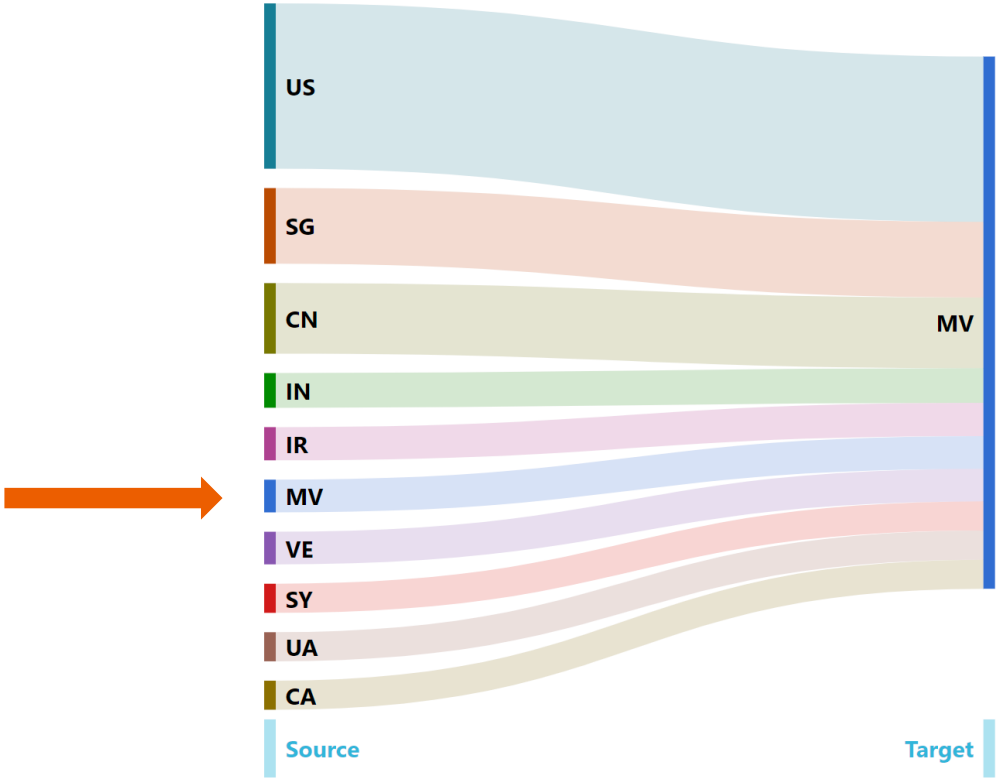
Maldives

- Open Ports

DNS	155
NTP	254
SSDP	10
MemcacheD	10
Telnet	74

https://www.shodan.io/search?query=country%3Amv

Maldives



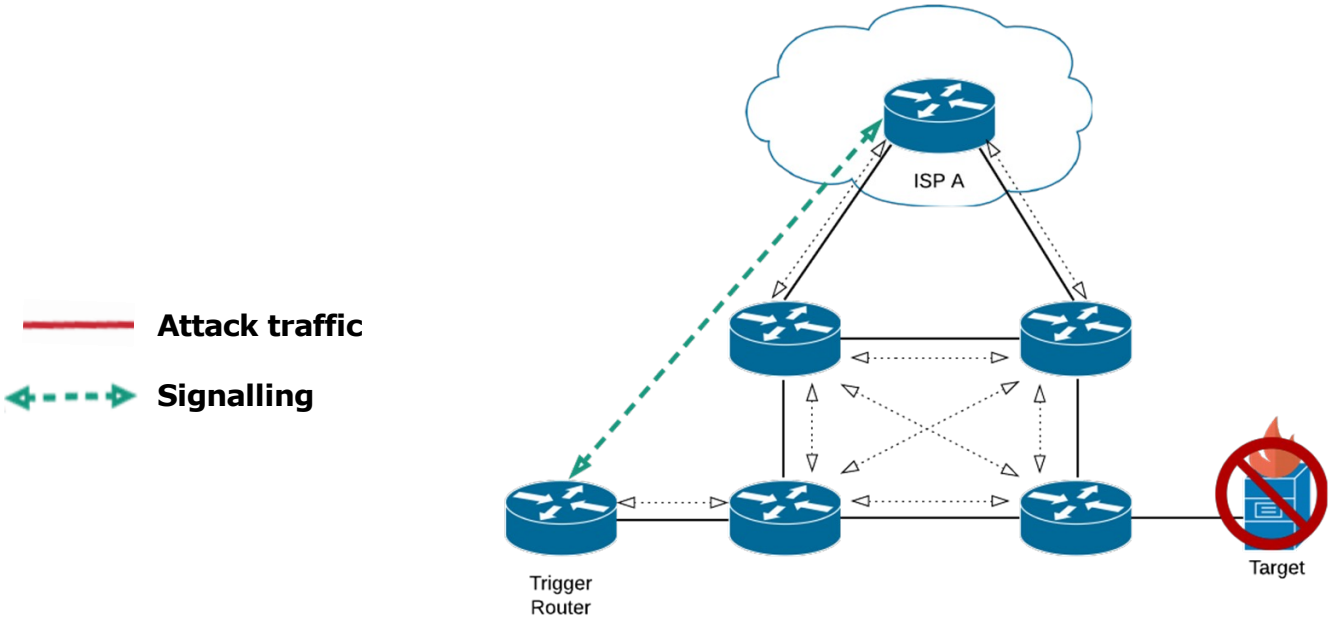
https://radar.cloudflare.com/security-and-attacks/mv?dateRange=12w

Mitigation Strategies

- Protect your services from attack
  - Anycast
  - IPS / DDoS protection
  - Overall network architecture
- Prevent your services from attacking others
  - Rate-limiting
  - BCP38 (outbound filtering) source address validation
  - Securely configured DNS, NTP and SNMP servers
  - **No open resolvers!**
    Only allow owned or authorised IP addresses to connect

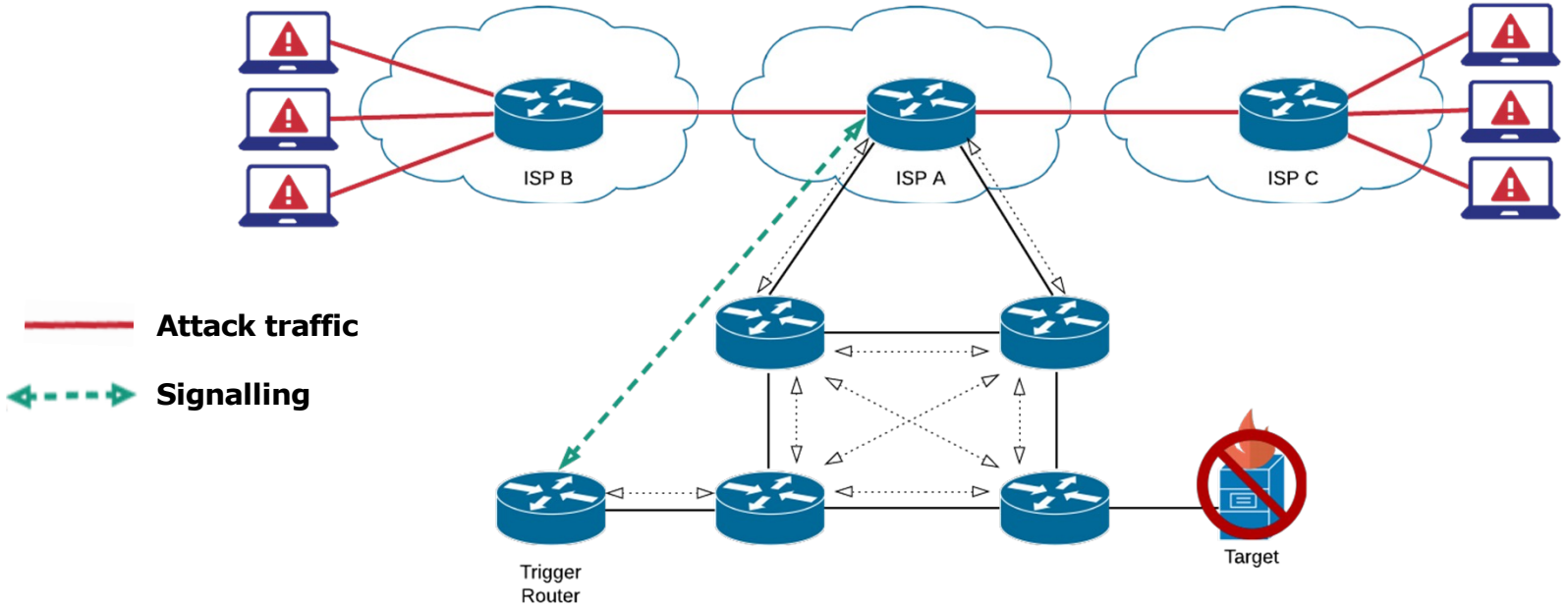
Mitigation Strategies

- Remote Triggered Black Hole (RTBH) filtering
  - With your ISP



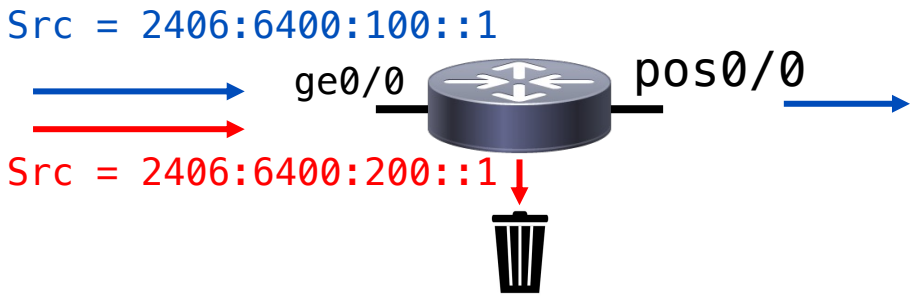
Mitigation Strategies

- Remote Triggered Black Hole (RTBH) filtering
  - With your ISP



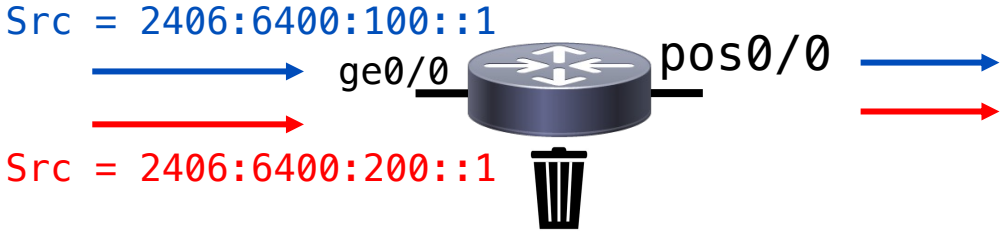
Mitigation Strategies

- uRPF
  - Strict: verifies both source address and incoming interface with entries in the forwarding table




```
Forwarding Table:
2406:6400:100::/48   ge0/0
2406:6400:200::/48   fa0/0
```

  - Loose: verifies existence of route to source address



Mitigation Strategies

- Source Remote Triggered Black Hole (sRTBH) filtering
  - RTBH with uRPF (Unicast Reverse Path Forwarding)
    - RFC5635
  - Basic Operation
    - Setup a RTBH Sinkhole (routing to a Null Interface)
    - Enable uRPF in loose mode
    - Create an appropriate community to NH traffic to your Sinkhole
    - When a source is identified
      - Tag with appropriate community to send to the Sink
      - uRPF check will fail (as it is routed to a Null)
      - Traffic Dropped

http://www.cisco.com/web/about/security/intelligence/blackhole.pdf

Questions?