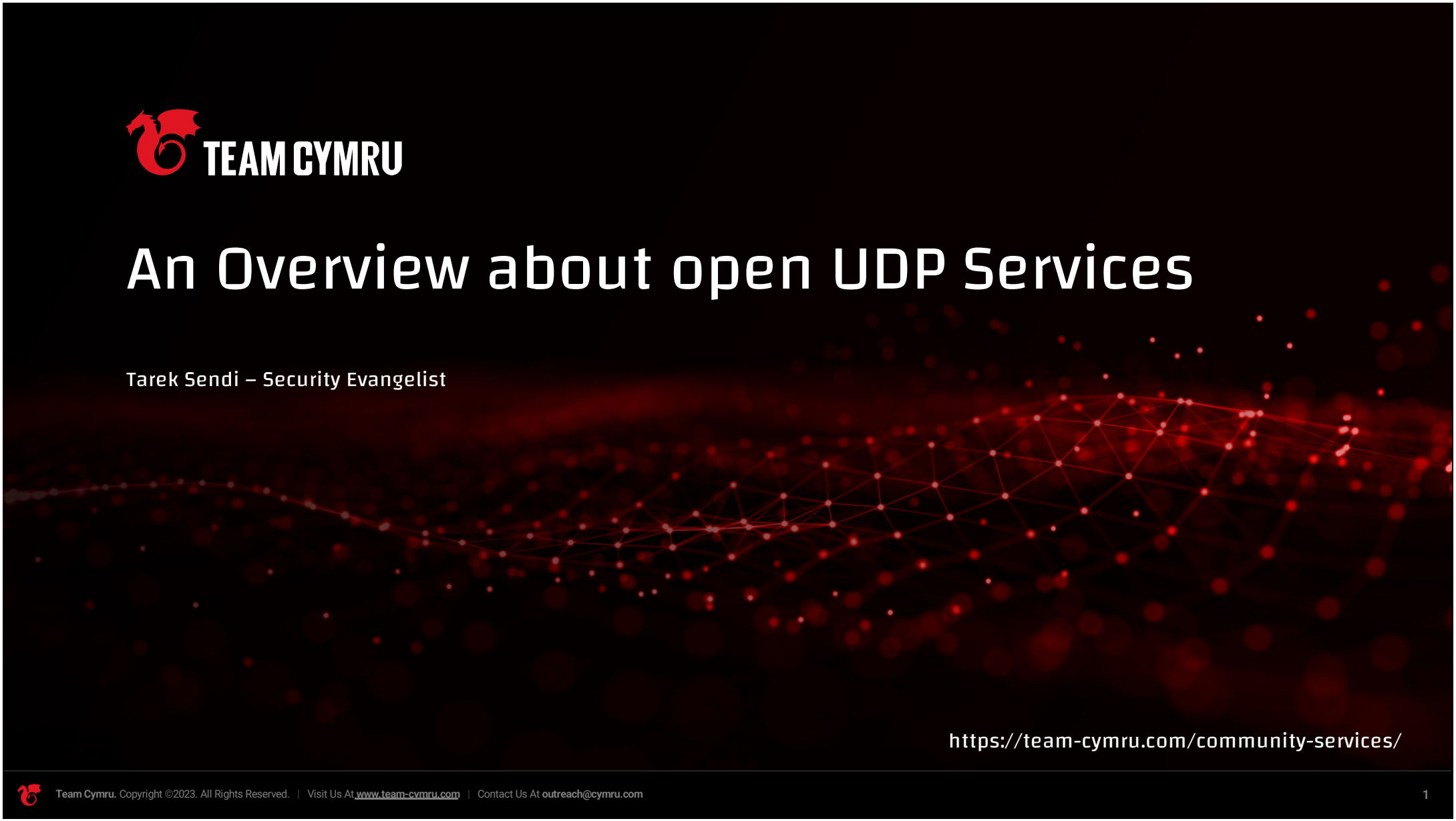


An Overview about open UDP Services

Tarek Sendi – Security Evangelist

https://team-cymru.com/community-services/

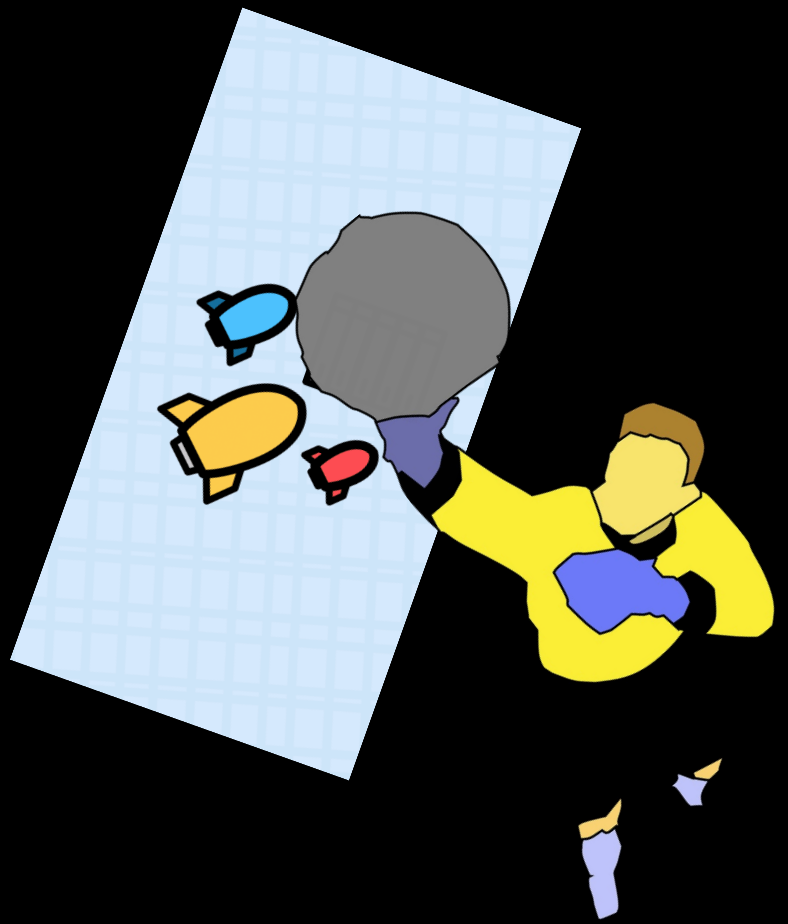
Contents

- Introduction
- Amplification DDOS Attacks
- Reflection DDOS Attacks
- SANOG Stats
- Approaches to reduce open UDP services
- Goal for SANOG ISPs
- Conclusion & Questions

https://team-cymru.com/community-services/

Introduction

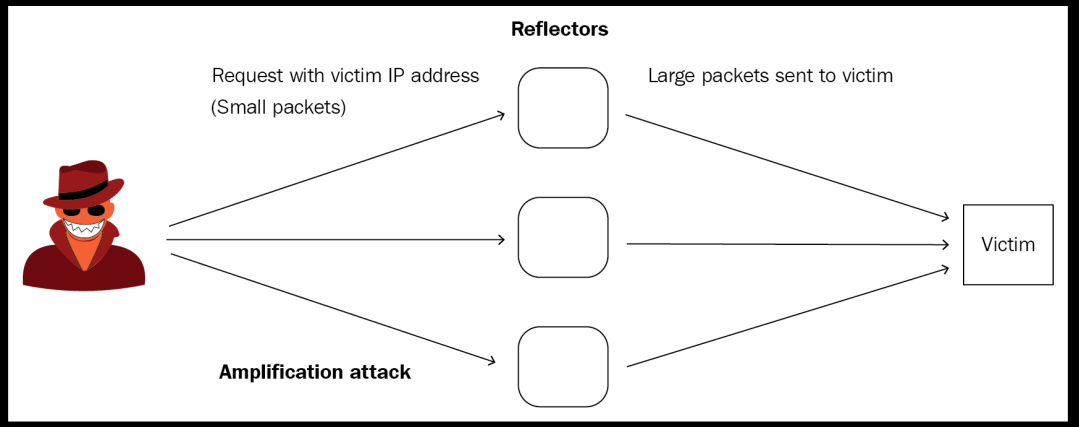
Tarek originally trained in Cyber Security as an Event Handler at the Tunisian CERT and became a Team Lead for R&D.At "Team Cymru", Tarek works daily to connect with users, partners and the wider community. When Tarek isn't glued to the computer screen, he spends his time working in the garden and trying his best not to miss a goal in soccer matches.

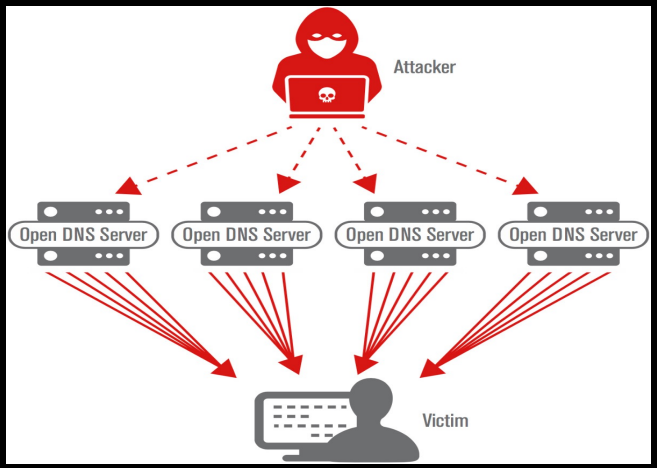


https://team-cymru.com/community-services/nimbus-threat-monitor/

Reflector and amplifier attacks

A reflection/amplification attack is a combination of the two attacks that allows the attacker to generate an enormous amount of traffic and at the same time keep its identity hidden by spoofing the victim's IP address.





https://team-cymru.com/community-services/nimbus-threat-monitor/

Reflector and amplifier attacks

Protocol	Bandwidth Amplification Factor
DNS	28 to 54
NTP	556.9
SNMPv2	6.3
SSDP	30.8
CharGEN	358.8

https://team-cymru.com/community-services/nimbus-threat-monitor/

- SANOG Stats

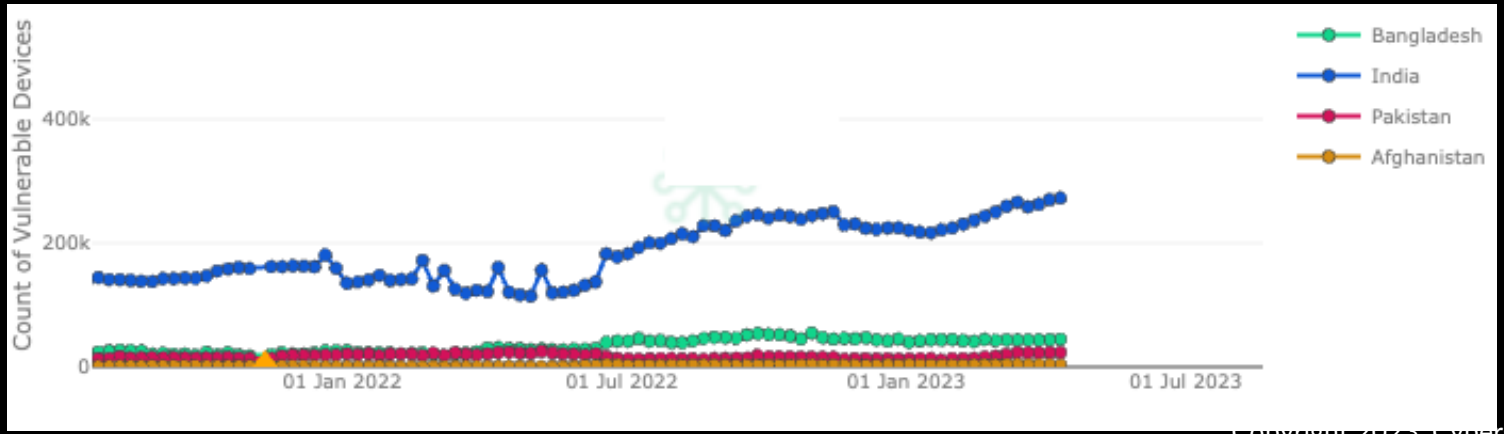
Country	Open Recursive DNS	Open NTP	Open SNMP	Open SSDP	Open CHARGEN	DDOS Potential TBit/sec	DDOS Rank
India	273,007	123,094	49,593	87,356	224	83	12
Bangladesh	44,720	29,000	13,534	52	10	18	38
Pakistan	23,305	16,729	4,448	1,321	20	10	45
Afghanistan	3,344	2,322	522	106	N/A	1	114
Nepal	1,793	5,870	827	5	5	3	77
Sri Lanka	657	3,512	177	92	3	2	102
Bhutan	146	562	N/A	13	N/A	0	154
Maldives	131	222	32	134	N/A	0	185

Stats on 12/2022

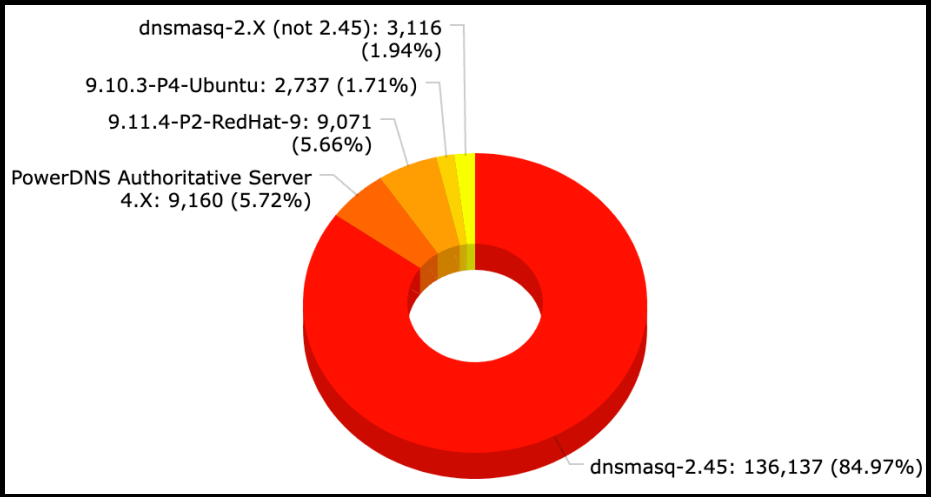
Country	Open Recursive DNS	Open NTP	Open SNMP	Open SSDP	Open CHARGEN	DDOS Potential TBit/sec	DDOS Rank
India	224,172	130,387	43,093	68,185	323	84	11
Bangladesh	47,046	25,714	12,389	53	12	16	38
Pakistan	13,394	16,457	5,330	457	28	10	50

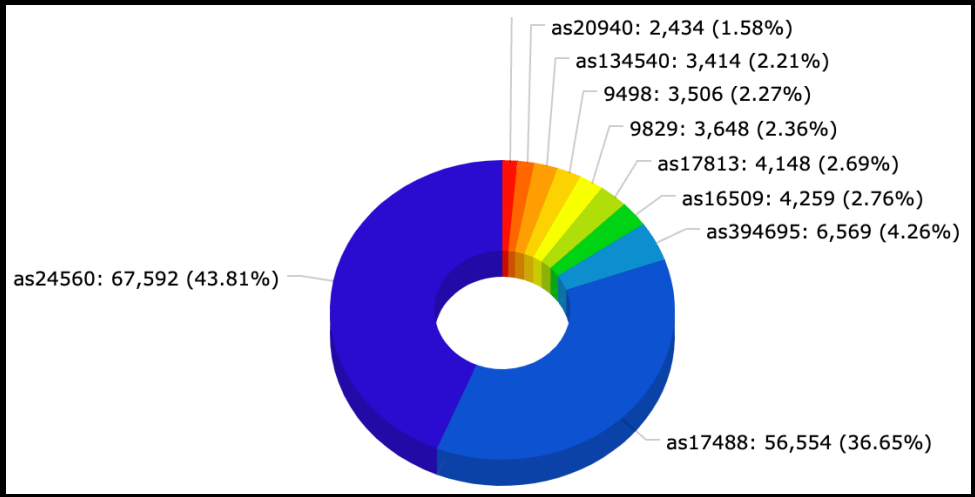
- # SANOG Stats
  - ## Open Recursive DNS

Country	Open Recursive DNS	Worldwide rank	Top ASN
India	273,007	3	AS24560 AIRTELBROADBAND-AS-AP Bharti Airtel Ltd.
Bangladesh	44,720	26	AS136732 Yellow Net & Cyber Cafe
Pakistan	23,305	37	AS17557 Pakistan Telecommunication Company Limited
Afghanistan	3,344	80	AS134134 North Telecom
Nepal	1,793	98	AS23752 Nepal Telecommunications Corporation, Internet Services
Sri Lanka	657	124	AS9329 Sri Lanka Telecom Internet
Bhutan	146	136	AS18024 Bhutan Telecom Ltd
Maldives	131	166	AS7642 DHIVEHI RAAJJEYGE GULHUN PLC



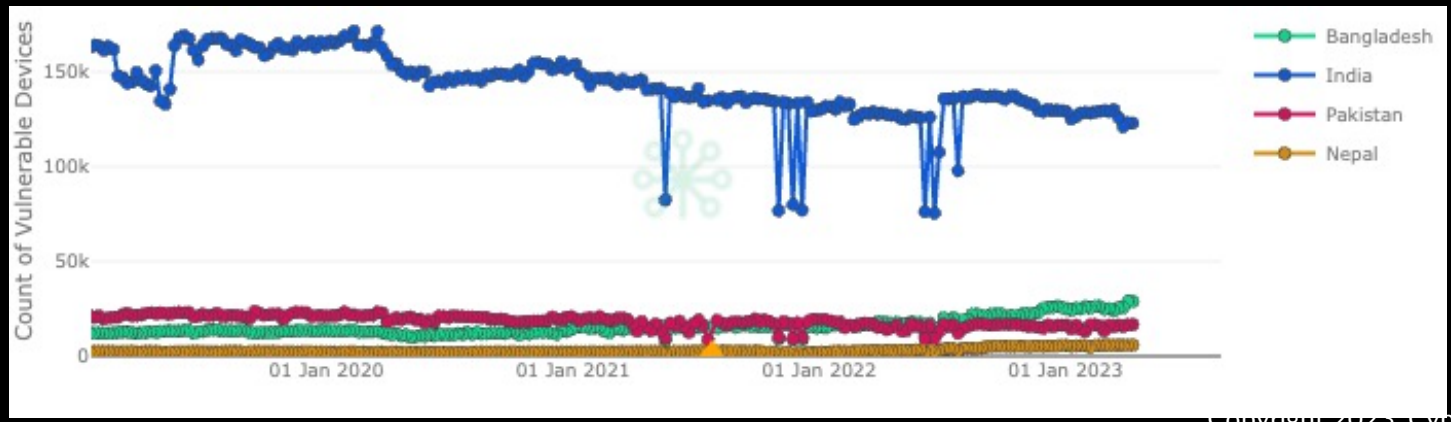
- SANOG Stats
  - **Possible Open Recursive DNS in INDIA**





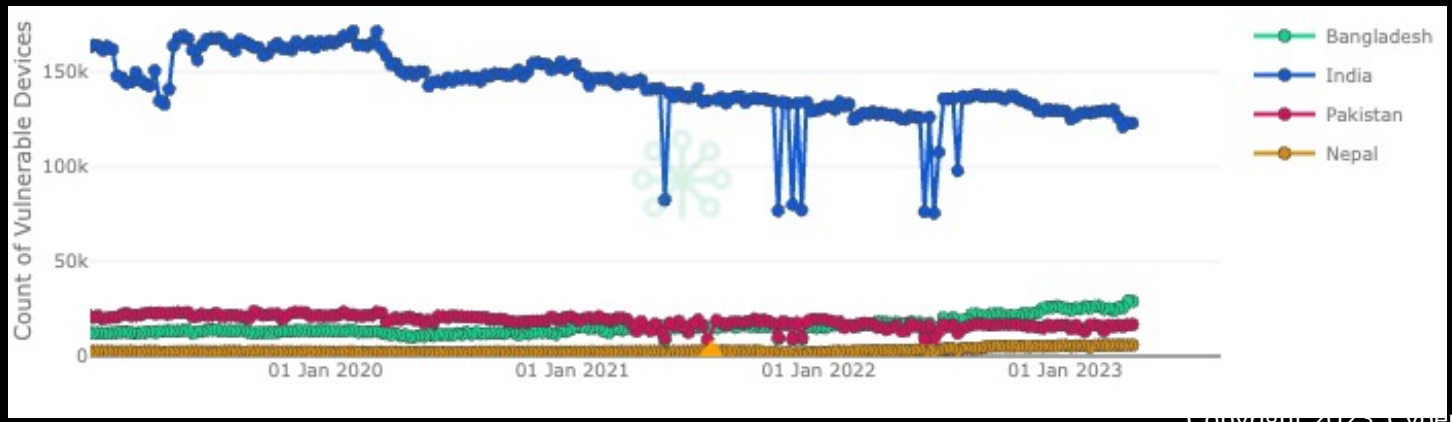
- SANOG Stats
  - **Open NTP**

Country	Open NTP	Worldwide rank	Top ASN
India	123,094	3	AS9498 BBIL-AP BHARTI Airtel Ltd.
Bangladesh	29,000	26	AS23688 Link3 Technologies Ltd.
Pakistan	16,729	46	AS38264 National WiMAX/IMS environment
Afghanistan	2,322	114	AS55330 AFGHANTELECOM GOVERNMENT COMMUNICATION NETWORK
Nepal	5,870	76	AS23752 Nepal Telecommunications Corporation, Internet Services
Sri Lanka	3,512	100	AS18001 Dialog Axiata PLC.
Bhutan	562	151	AS134715 Government Technology Agency
Maldives	222	184	AS7642 DHIVEHI RAAJJEYGE GULHUN PLC



- SANOG Stats
  - **Open SNMP**

Country	Open SNMP	Worldwide rank	Top ASN
India	49,593	7	
Bangladesh	13,534	20	AS24342 BRAC-BDMAIL-AS-BD BRACNet Limited
Pakistan	4,448	43	AS23750 GERRYS-AS-AP GERRYS INFORMATION TECHNOLOGY PVT LTD.
Afghanistan	522	111	AS17411 Io Global Services Pvt. Limited
Nepal	827	95	AS24550 WEBSURFERNP-AS-NP Websurfer Nepal Internet Service Provider
Sri Lanka	177	137	AS9329 SLTINT-AS-AP Sri Lanka Telecom Internet
Bhutan	52	182	AS134715 DRUKREN-MOIC-AS
Maldives	32	184	AS7642 DHIRAAGU-MV-AP DHIVEHI RAAJJEYGE GULHUN PLC



- SANOG Stats
  - **Spoofer Test Results**

Country	Client IP blocks	Spoofing IP blocks	Blocking IP blocks		Inconsistent IP blocks	Client ASNs	Spoofing ASNs
			Non-NAT	NAT			
ind (India)	565	53 (9.4%)	91 (16.1%)	420 (74.3%)	1 (0.2%)	36	13 (36.1%)
npl (Nepal)	50	18 (36.0%)	7 (14.0%)	24 (48.0%)	1 (2.0%)	9	5 (55.6%)
bgd (Bangladesh)	48	15 (31.3%)	1 (2.1%)	32 (66.7%)	0 (0.0%)	28	11 (39.3%)
pak (Pakistan)	28	2 (7.1%)	2 (7.1%)	24 (85.7%)	0 (0.0%)	11	2 (18.2%)
mdv (Maldives)	9	1 (11.1%)	2 (22.2%)	6 (66.7%)	0 (0.0%)	4	1 (25.0%)
btn (Bhutan)	3	1 (33.3%)	2 (66.7%)	0 (0.0%)	0 (0.0%)	1	1 (100.0%)
lka (Sri Lanka)	9	0 (0.0%)	0 (0.0%)	8 (88.9%)	1 (11.1%)	1	1 (100.0%)
mmr (Myanmar)	8	0 (0.0%)	0 (0.0%)	8 (100.0%)	0 (0.0%)	5	0 (0.0%)
afg (Afghanistan)	No Data	No Data	No Data	No Data	No Data	No Data	No Data

https://spoofer.caida.org/summary.php

- Approaches to reduce the impact of open UDP services

Detection

Open DNS Resolver :

- https://openresolver.com
- # dig ANY isc.org @x.x.x.x

Open NTP :

- # ntpdc –c monlist x.x.x.x
- “ntp-monlist” script is available for NMap

Open SNMP :

- #snmpget -c public -v 2c x.x.x.x 1.3.6.1.2.1.1.1.0
- #snmpget -c public -v 2c x.x.x.x 1.3.6.1.2.1.1.5.0

nmap –sU –A –PN –n –pU:53,123,161 –script=ntp-monlist,dns-recursion,snmp-sysdescr <target>

https://team-cymru.com/community-services/

- Approaches to reduce the impact of open UDP services

This is what we can do:

- Adhere and use ingress filtering to block spoofed packets (IETF BCP 38 and BCP 84 guidelines).
- Use traffic shaping on UDP service requests to ensure repeated access to over-the-Internet resources is not abusive. (rfc2475 and rfc3260)
- Disable and remove unwanted services, or deny access to local services over the internet, e.g., for NTP or DNS
- Add session handling to the protocols

https://team-cymru.com/community-services/

- Approaches to reduce the impact of open UDP services

NTP secure Templates

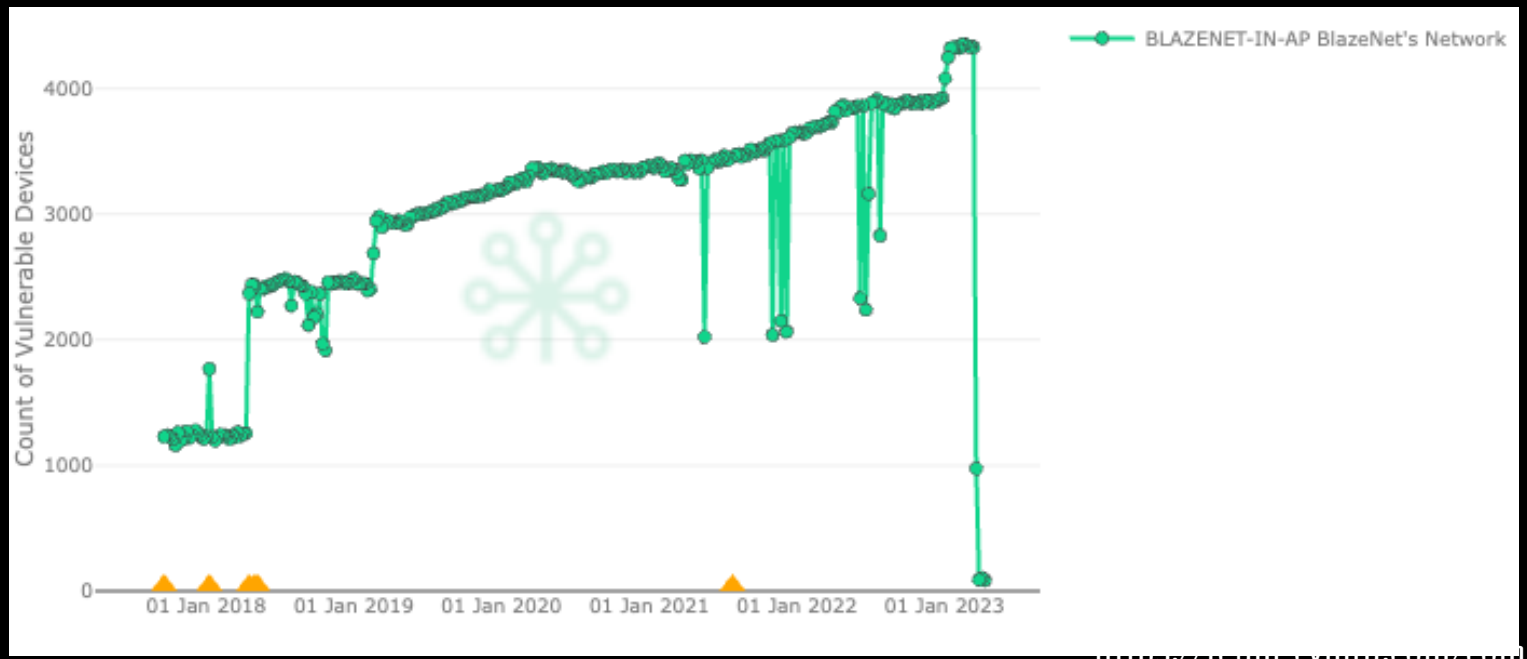
- Cisco IOS
- Juniper
- UNIX ntpd

https://team-cymru.com/community-services/

- Goal for SANOG ISPs

  - We hope to reduce the number of open UDP services

Below an example of partnership to reduce the number of open UDP services

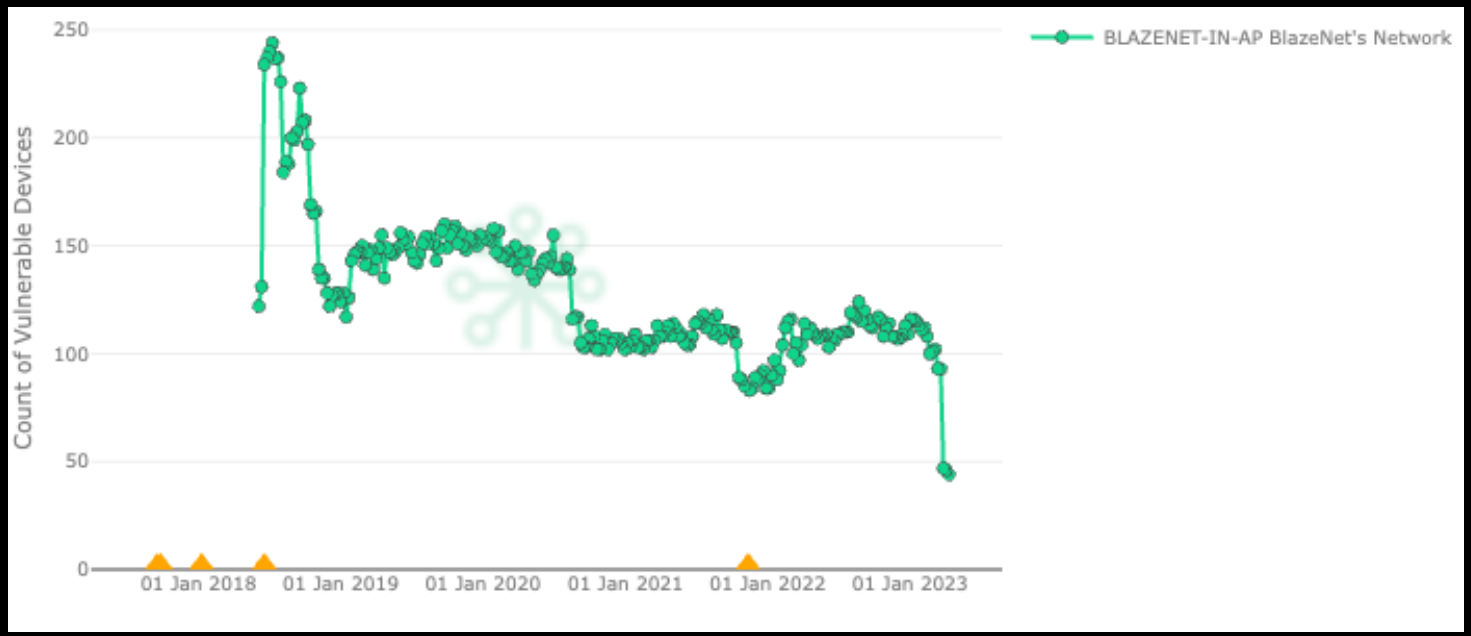


https://team-cymru.com/community-services/

- Goal for SANOG ISPs

  - We hope to reduce the number of open UDP services

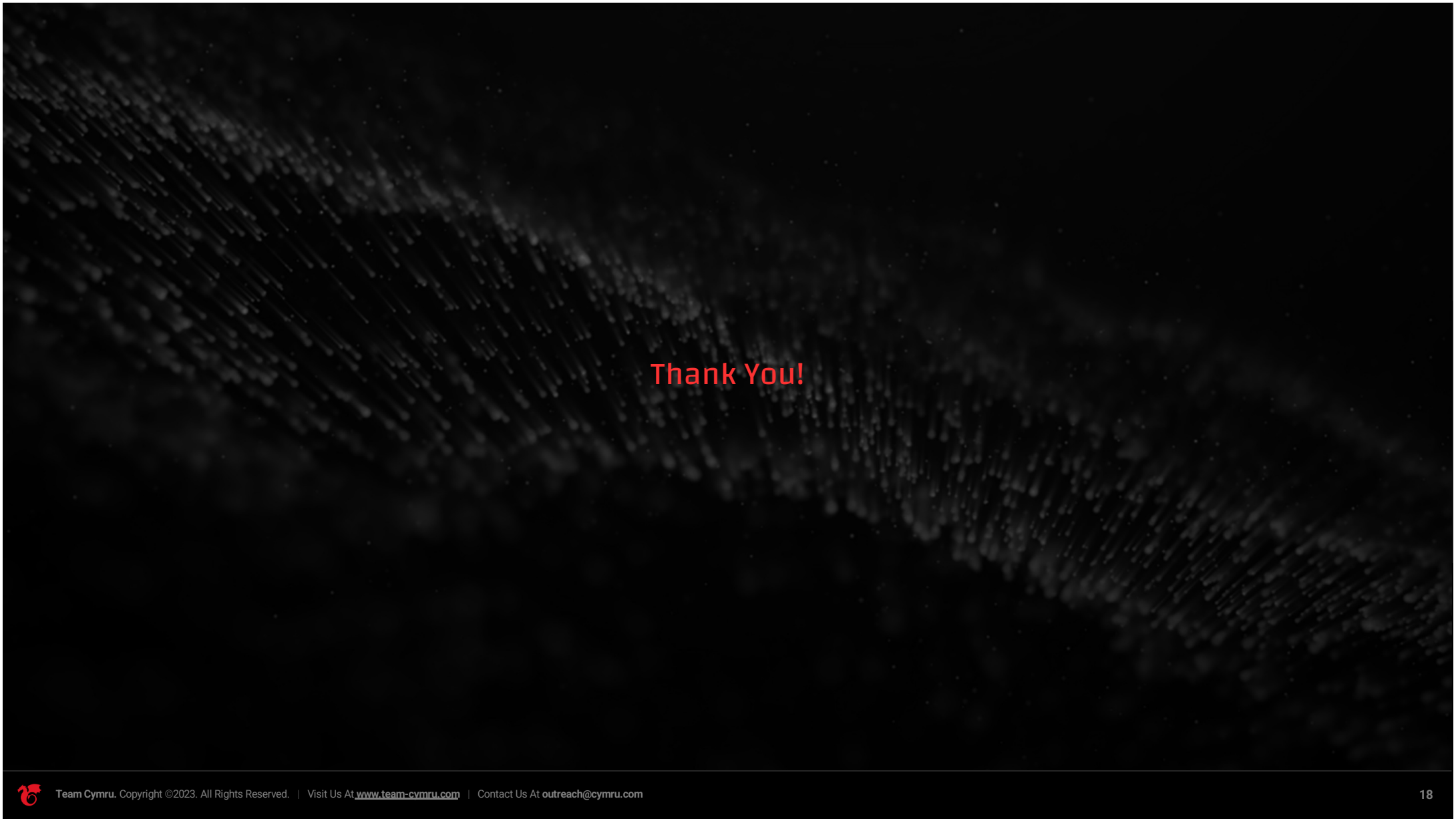
  Below an example of partnership to reduce the number of open UDP services



https://team-cymru.com/community-services/

Conclusion
&
Questions?

https://team-cymru.com/community-services/



 | Visit Us At **www.team-cymru.com** | Contact Us At **outreach@cymru.com**