

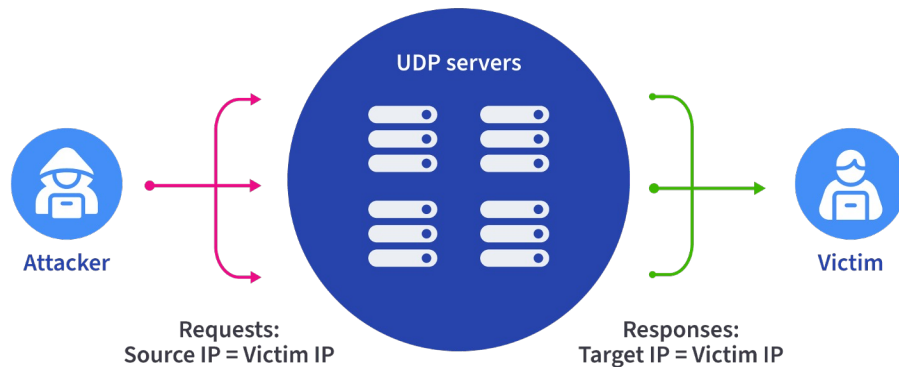
Fighting DDoS at the Source

Nina Bargisen



Fighting DDoS at the Source

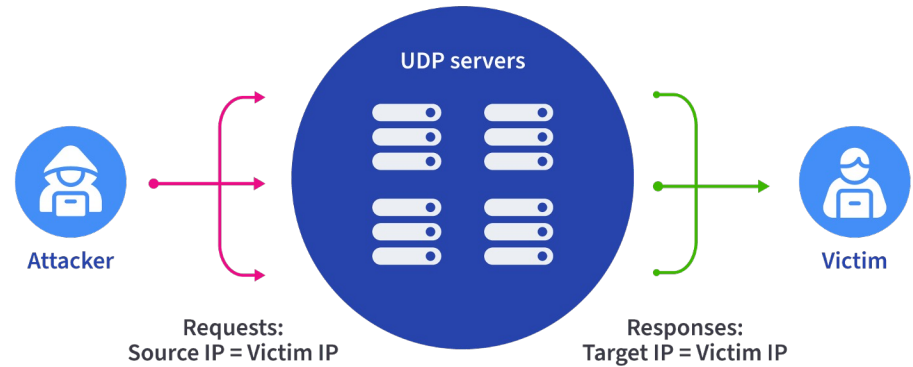
- Distributed denial of service (DDoS) attacks continue to plague the Internet.
- One of the most common forms of DDoS attack is the **reflection attack**.



Reflection attack

Reflection attacks

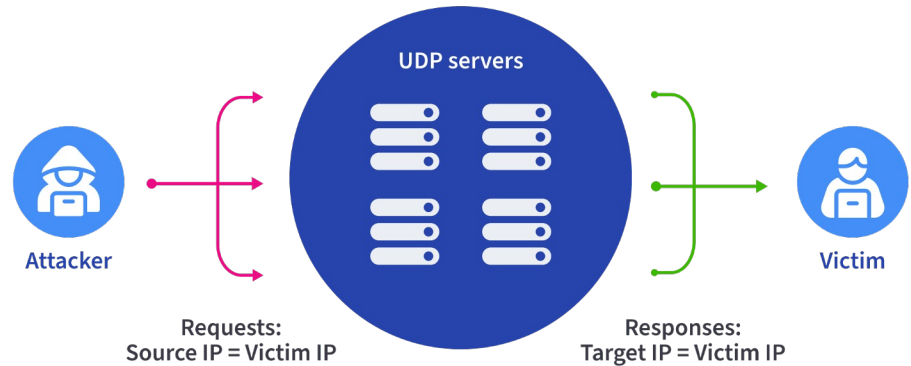
- The attacker sends thousands of requests with “spoofed” source IP addresses.
- The requests are sent to DNS, NTP etc servers who replies
- The target address is flooded with the replies
- The service becomes degraded or unavailable



Reflection attack

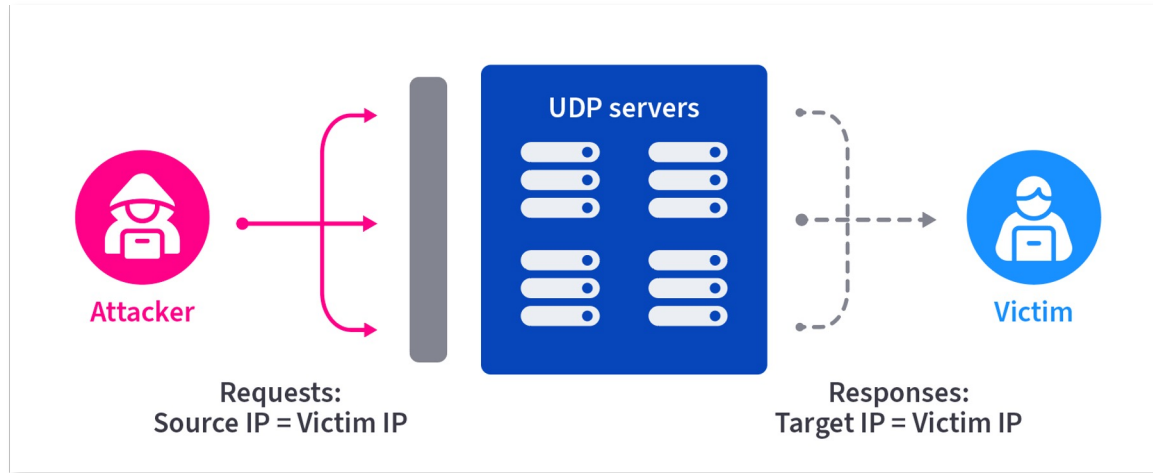
Reflection attacks

- One of the largest **reflection** attacks was targeted Google Cloud in 2017
- The attack **originated** in 4 chinese networks ((ASNs 4134, 4837, 58453, and 9394)
- The attackers used the networks to spoof **167 Mpps** (millions of packets per second) to **180,000** exposed CLDAP, DNS, and SMTP servers
- The attack peaked at **2.54 Tbps**



Reflection attack

Addressing the problem



1. Secure internet devices from responding to UDP queries from the Internet
2. Eliminate spoofed traffic via technical means (Source IP verification)
3. Identify and engage networks originating spoofed traffic

Source IP verification (BCP38)

Source IP verification

- Checks **source IPs** of packets against permitted **addresses**.

Methods of Implementation

- Strict Reverse Path Forwarding (**sRPF**):
 - Drops packets arriving on **incorrect** interface.
 - Requires **symmetric** routing
- Feasible Reverse Path Forwarding (**fRPF**):
 - Considers **all paths** to the source address.
 - Risk of **blackholing**
- Ingress Access Control Lists (**ACLs**)
 - Requires **manual** maintenance.
 - Considered bulletproof if maintained properly.
 - Best fit for **non-dynamic** configurations and **few** used prefixes.

Using NetFlow to traceback DDoS sources

A backbone provider uses a customized workflow to identify customer networks which are sending traffic in violation of BCP38.

Methodology boils down to two steps:

1

Find spikes of packets from customer networks to a large set of unique destination IP addresses using commonly abused UDP ports.

2

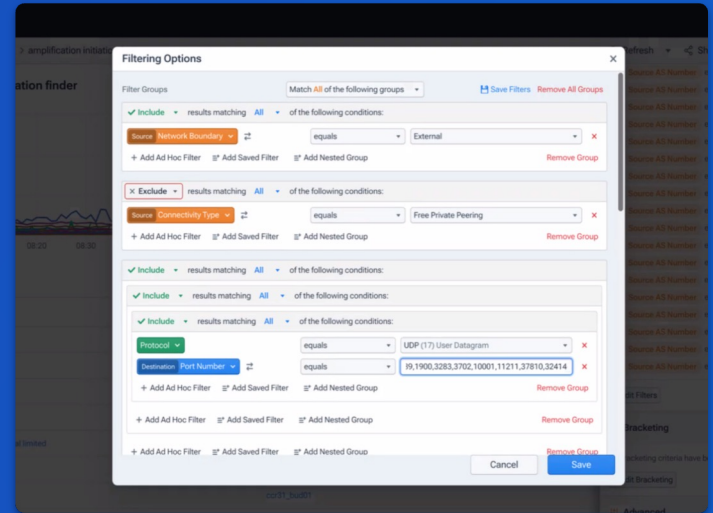
For any suspicious spikes in packets to those selected UDP ports, investigate the source IPs of these packets coming from that customer.

Using NetFlow to traceback DDoS sources

1

Run a query that captures the following:

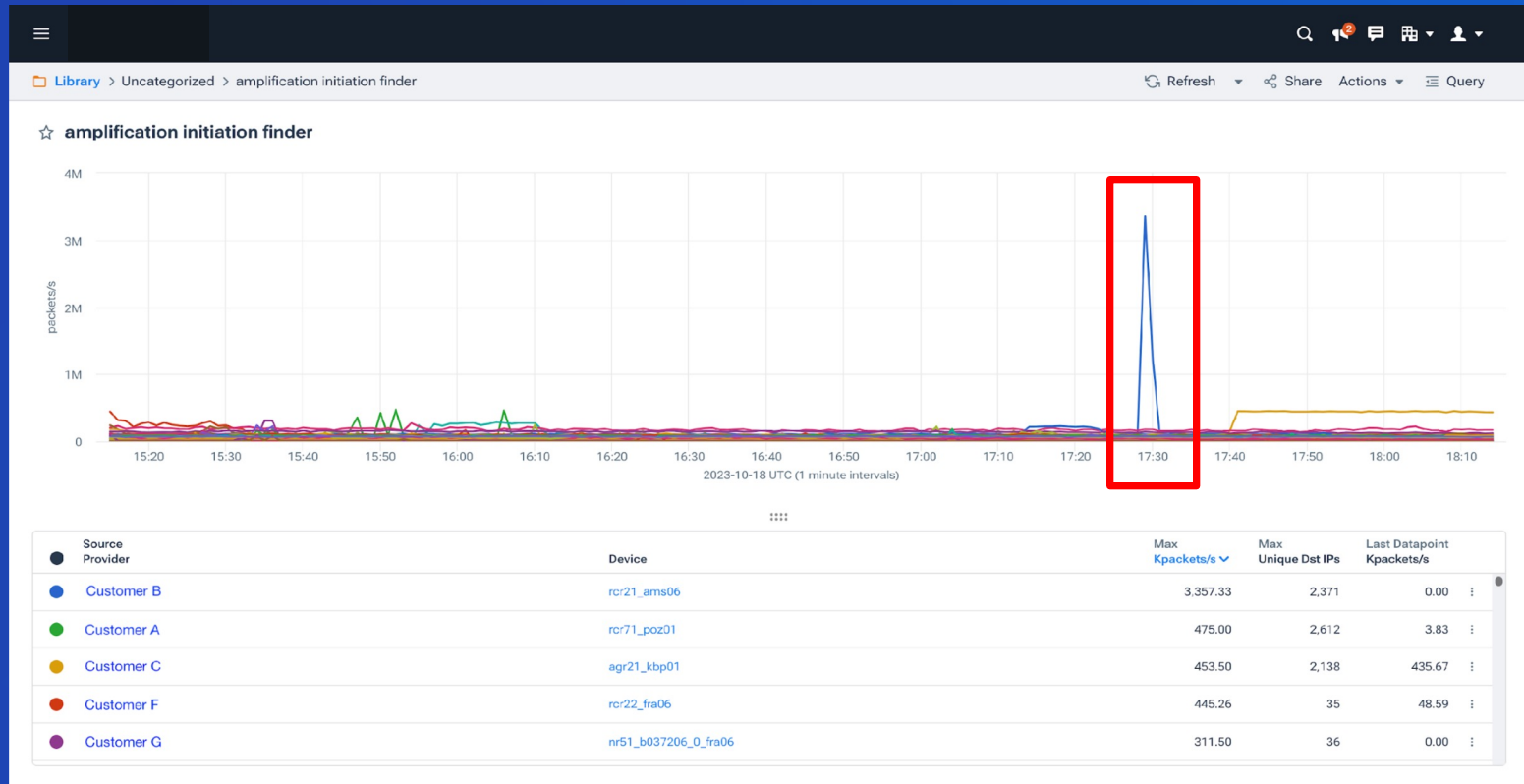
- Only traffic from an external source
- Only packets directed to commonly abused reflection ports.*
- Set metrics to
 - Packets/sec (not bps)
 - Unique number of destination IPs
- Group by customer and device



* 19, 53, 123, 161, 389, 427, 1900, 3283, 3702, 10001, 10074, 11211, 37810, 32414

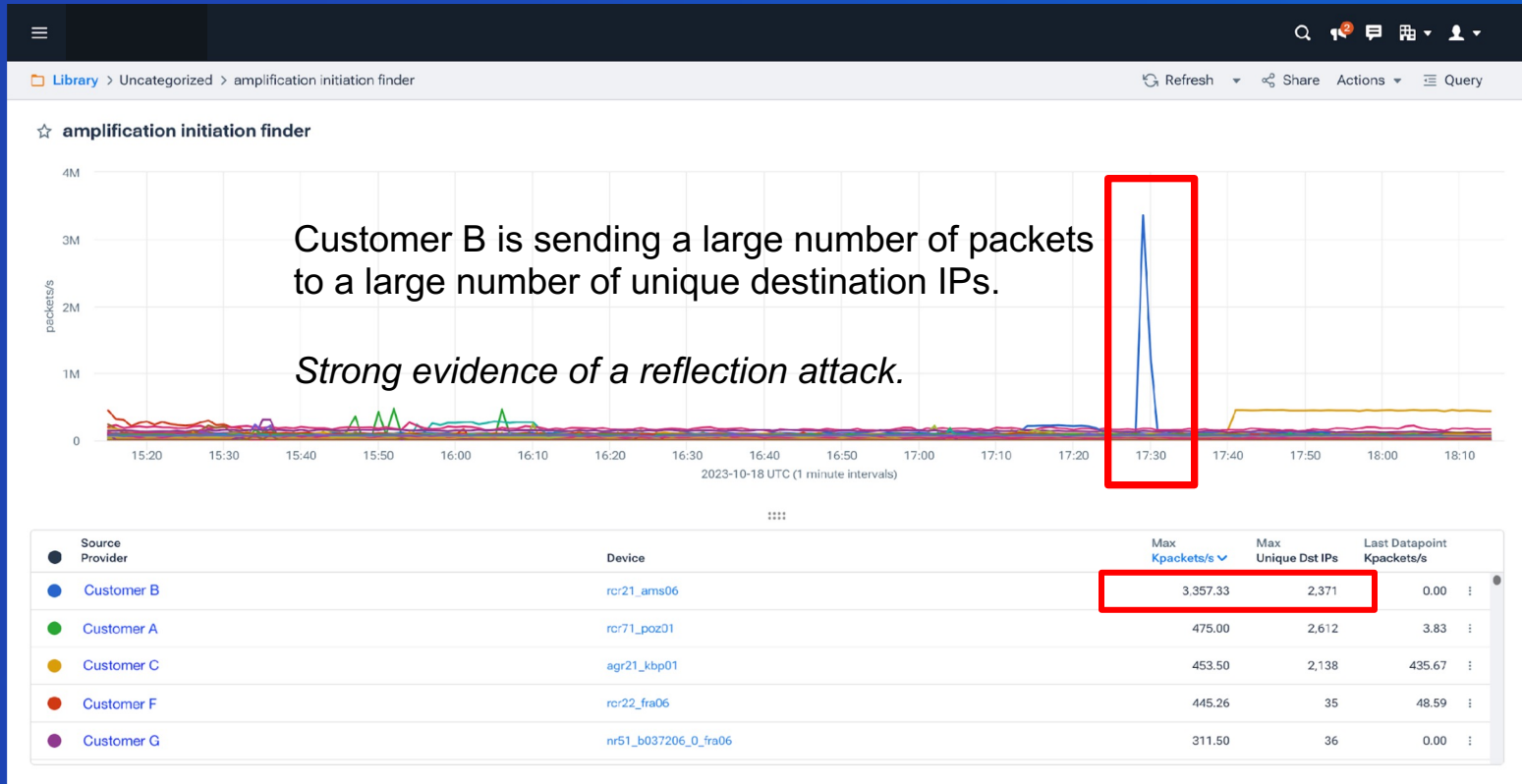
Using NetFlow to traceback DDoS sources

1



Using NetFlow to traceback DDoS sources

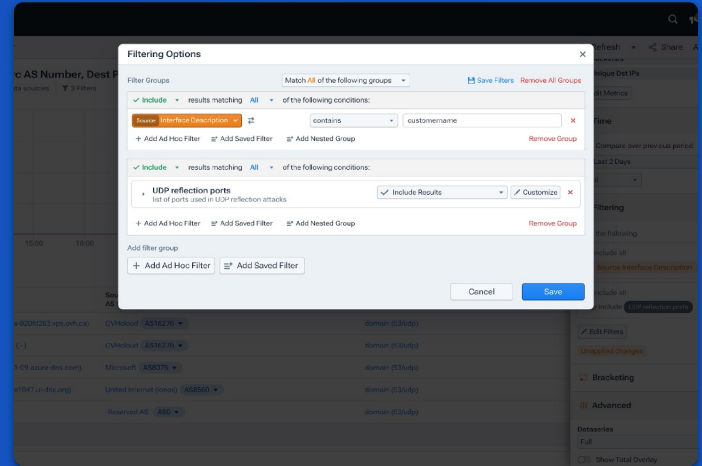
1



Using NetFlow to traceback DDoS sources 2

Now we want to investigate the source IPs of these packets coming from that customer by running a query that captures the following:

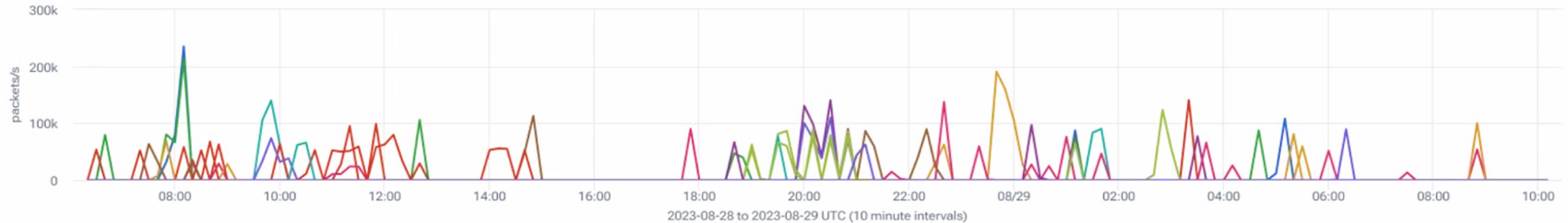
- Only packets to abused UDP ports from the customer interface.
 - Group by source IP/ASN
 - Group by destination port
- Still set metrics to
 - Packets/sec (not bps)
 - Unique number of destination IPs



Using NetFlow to traceback DDoS sources 2

Top Src IP/CIDR, Src AS Number, Dest Protocol:IP Port by Max packets/s

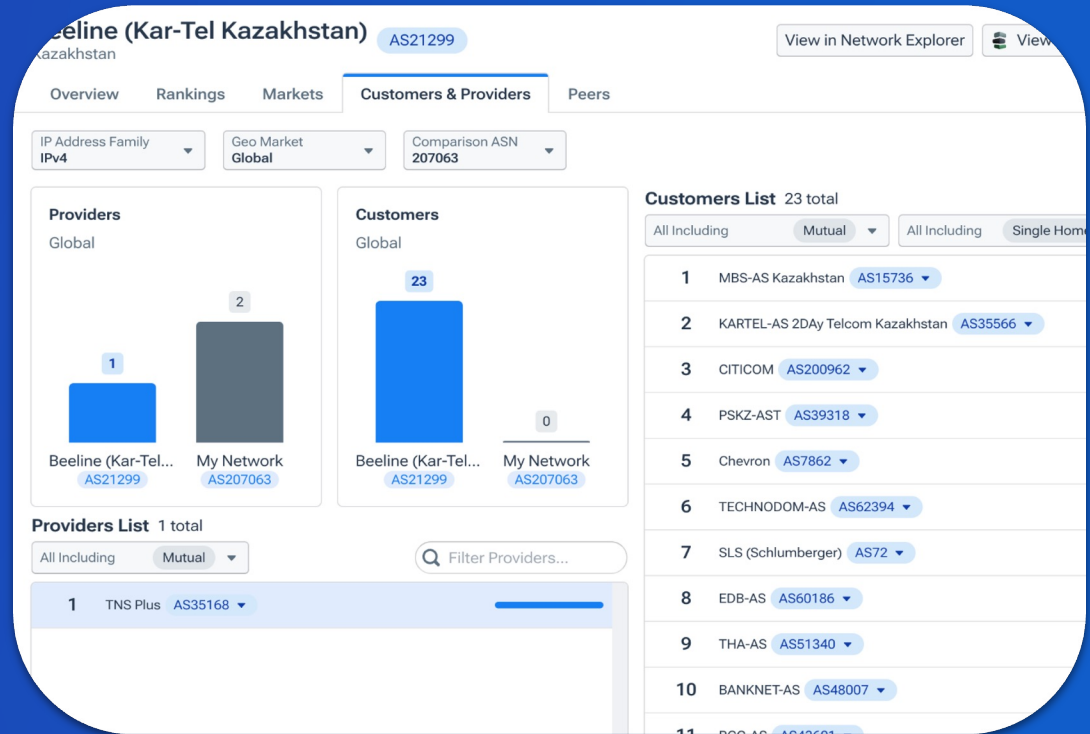
Aug 28, 2023 06:20 to Aug 29, 2023 10:20 (1 day and 4 hours) 1 of 903 data sources 2 Filters



Source IP/CIDR	Source AS Number	Destination Service (Port+Proto)	Max Kpackets/s	Max Unique Dst IPs	Last Datapoint Kpackets/s
193.45.120/32	Beeline (Kar-Tel Kazakhstan) AS21299	snmp (161/udp)	235.10	13,842	0.00
193.45.120/32	Beeline (Kar-Tel Kazakhstan) AS21299	domain (53/udp)	212.45	11,616	0.00
193.97.25/32	OVHcloud AS16276	ws-discovery (3702/udp)	190.78	7,626	0.00
193.105.196/32 (-)	Microsoft AS8075	domain (53/udp)	140.78	8,019	0.00
193.71.233/32	Verizon AS701	snmp (161/udp)	140.55	8,294	0.00
193.127.195/32 (-)	VISL-IE AS201071	domain (53/udp)	139.73	8,139	0.00
193.46.21/32	OVHcloud AS16276	domain (53/udp)	137.50	8,233	0.00

Does this list of source ASNs make sense? ②

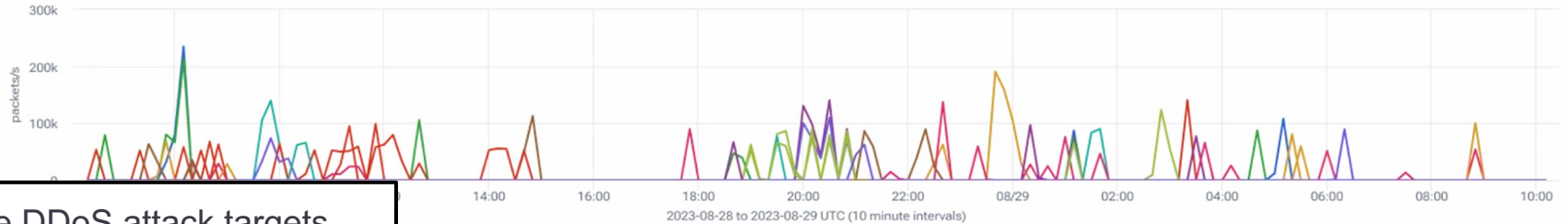
- Common sense
- Looking glass
- Tools like bgp.he.net or Kentiks KMI can help



Using NetFlow to traceback DDoS sources 2

Top Src IP/CIDR, Src AS Number, Dest Protocol:IP Port by Max packets/s

Aug 28, 2023 06:20 to Aug 29, 2023 10:20 (1 day and 4 hours) 1 of 903 data sources 2 Filters



The DDoS attack targets

Source IP/CIDR	Source AS Number	Destination Service (Port+Proto)	Max Kpackets/s	Max Unique Dst IPs	Last Datapoint Kpackets/s
203.45.120/32	Beeline (Kar-Tel Kazakhstan) AS21299	snmp (161/udp)	235.10	13,842	0.00
203.45.120/32	Beeline (Kar-Tel Kazakhstan) AS21299	domain (53/udp)	212.45	11,616	0.00
104.97.25/32	OVHcloud AS16276	ws-discovery (3702/udp)	190.78	7,626	0.00
105.196/32 (-)	Microsoft AS8075	domain (53/udp)	140.78	8,019	0.00
71.233/32	Verizon AS701	snmp (161/udp)	140.55	8,294	0.00
127.195/32 (-)	VISL-IE AS201071	domain (53/udp)	139.73	8,139	0.00
146.21/32	OVHcloud AS16276	domain (53/udp)	137.50	8,233	0.00

Now the fun begins — contacting customers!

- Service providers could simply refer the traffic to the abuse team to take action (e.g. disconnect).
- Customer would just continue activity with another provider.
- A service provider's objective should be to get the customer's netops team to understand the issue and address it.

A very time-consuming process:

1. Language barriers
2. Network engineers who are either overworked or poorly trained
3. Unfortunately, networking teams who are simply uninterested in fixing the problem
4. Other reasons...

Anti-Spoofing Reflection / Amplification Peer Response

BINGO

That's not our IP	Okay, we blocked those UDP ports on the customer	Misinterprets the data and claims you sent it	Our routers can't do ACLs or uRPF	Asks what destination IPs are being attacked
NetFlow tool screenshot looking for desination IPs	We only have NetFlow on our internet edge	I can't find the traffic	We're a transit provider; we can't do this	Shares link to an internal tool I can't access
Due to privacy, we don't collect NetFlow data	Insults	FREE	Those IPs you reported are yours	We notified the customer
"show route" output of the IP in question	Using the wrong timezone	cc's 15 other people on the email thread who can't help	Customer is multi-homed; can't BCP38	Includes novice security team on thread
We put a policer to limit the pps	We don't know what server generated this	No response from peer	We don't have NetFlow	Promotes buying DDoS protection service

Source: a certain cat at a cloud provider

Call to action



If your network is allowing spoofed traffic, someone is probably using your infrastructure to launch DDoS attacks against victims around the world.



If you run a network that operates as a service provider, you have a responsibility to the rest of the Internet to actively look for and eliminate spoofed traffic.



If contacted, you need tools in place to investigate and address the claims. Don't want to be the one to complete someone's ***anti-spoofing response bingo card***.

Thank you!

Your name

nina@kentic.com

 @nissen333

 in/ninabargisen

 [Join Kentik on Slack](#)

