DDoS Never Dies?
An IXP Perspective on DDoS Amplification Attacks

Photo by Josep Castells

D. Kopp[1], C. Dietzel[1,3], O. Hohlfeld[2]

DE-CIX[1], BTU[2], MPI[3]

Why more Reseach on DDoS?

Victims can’t defend themselves

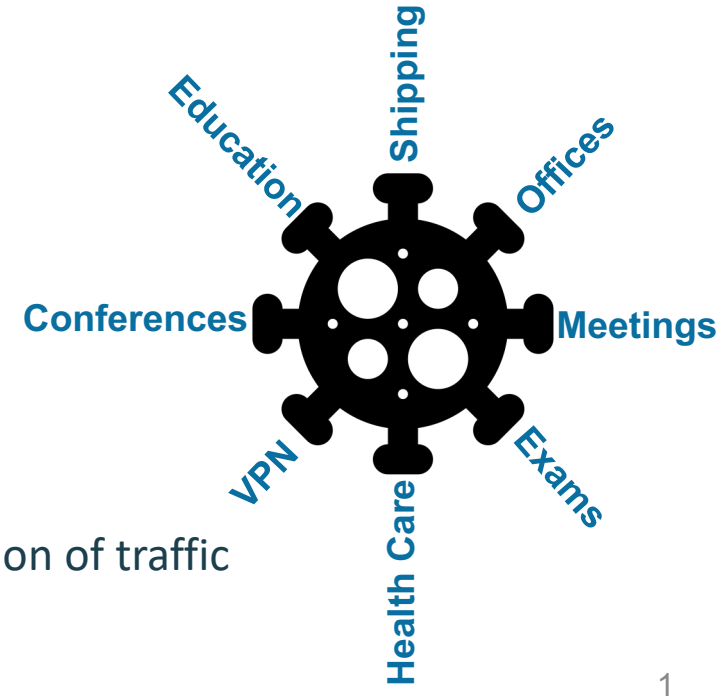
- Victims are mostly end users of the Internet → low bandwidth
- Limited view into the Internet

Targets at risk

- Gaming, e-sports, online businesses
- Finance, stock market
- Political targets and critical infrastructures

Unsolved Problems

- IP-Spoofing and security flaws → amplification of traffic



Contributions

DDoS attacks seen at a large IXP

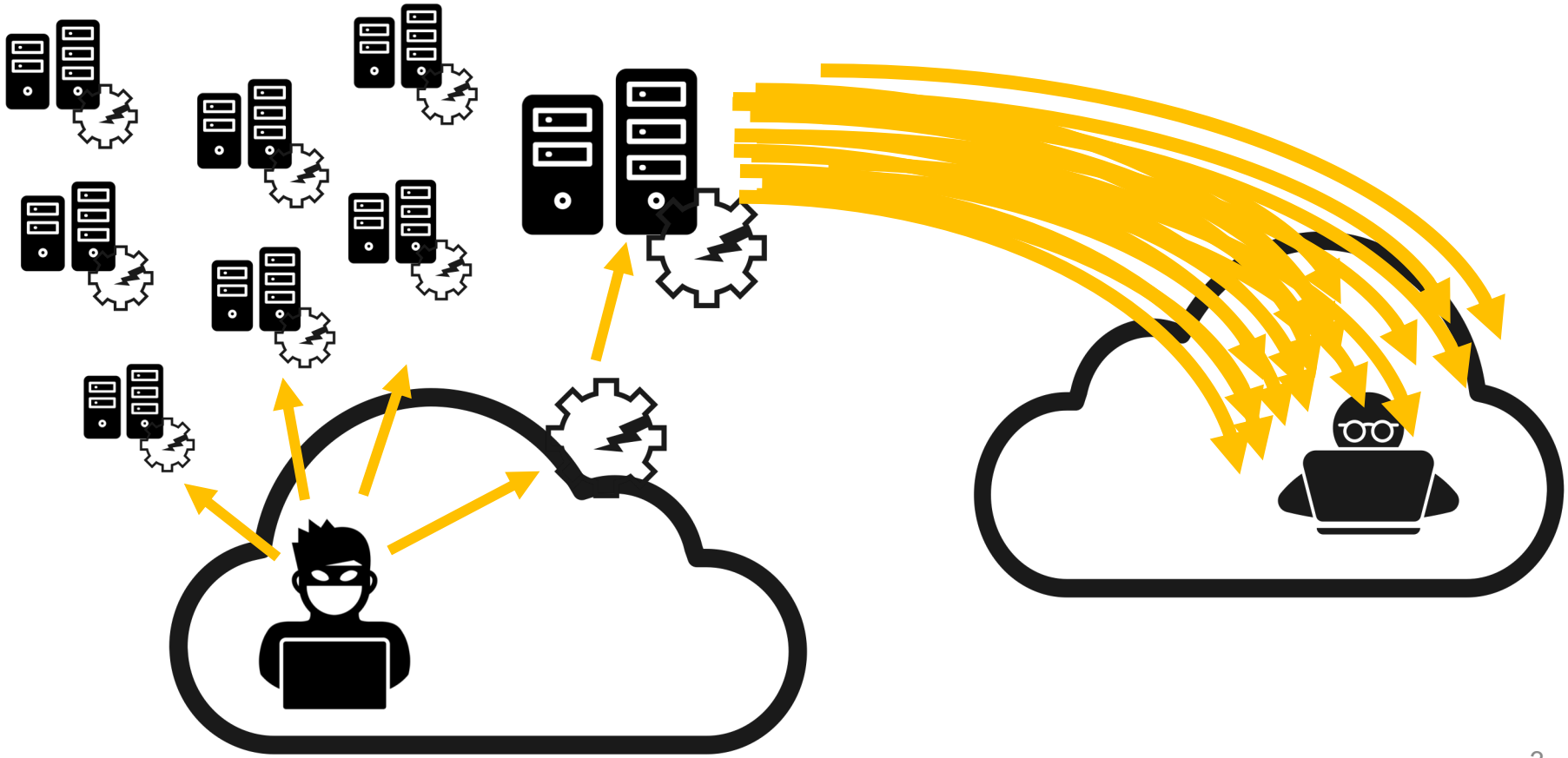
- Global visibility, focus central Europe
- > 900 connected networks

Details on amplification protocols used in the wild

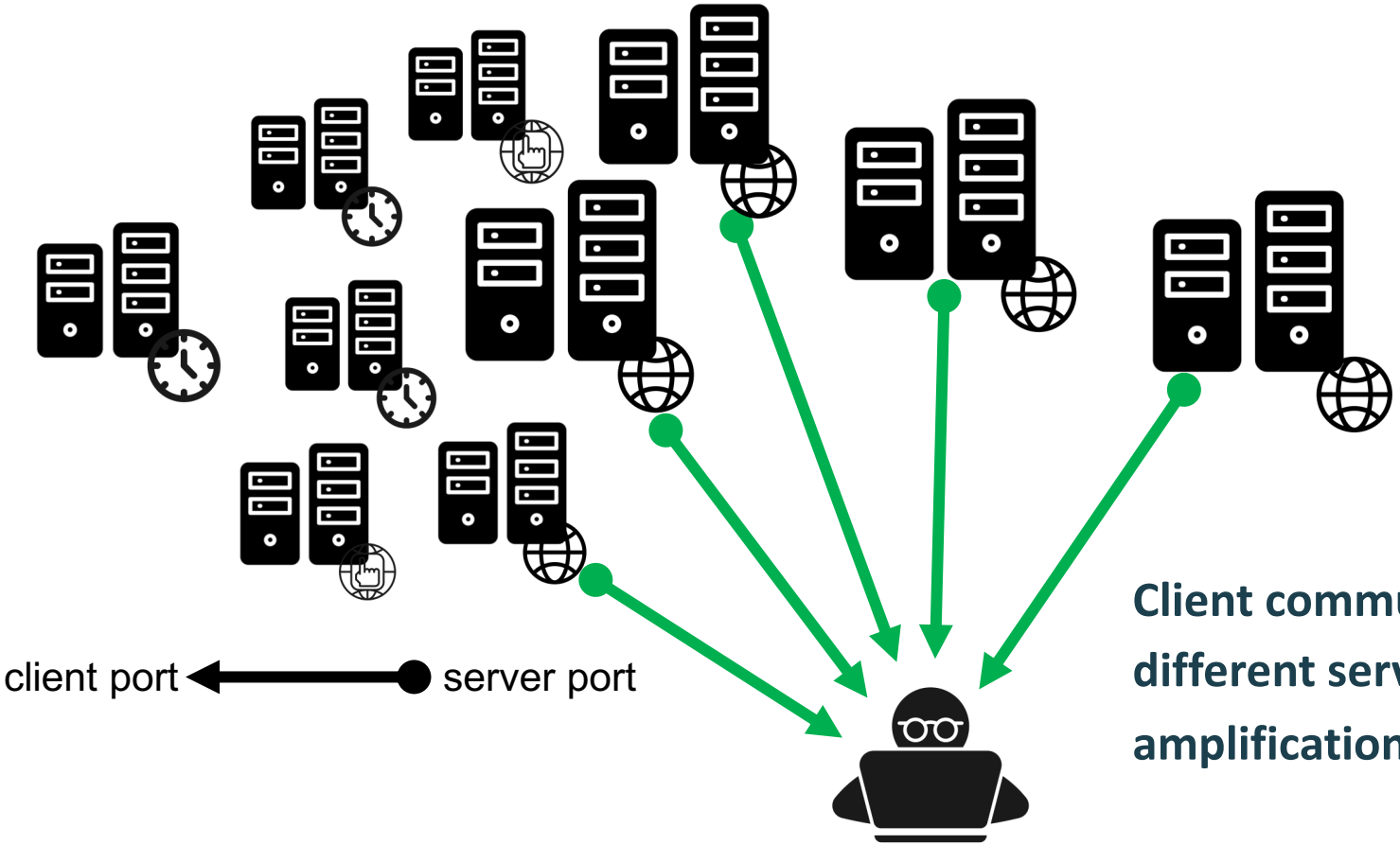
The study provides

- Infrastructure perspective
- View on targets and attack patterns
- Brief comparison of attacks seen by a honeypot
- The full paper gives more details → Table 1

Amplification DDoS Attack

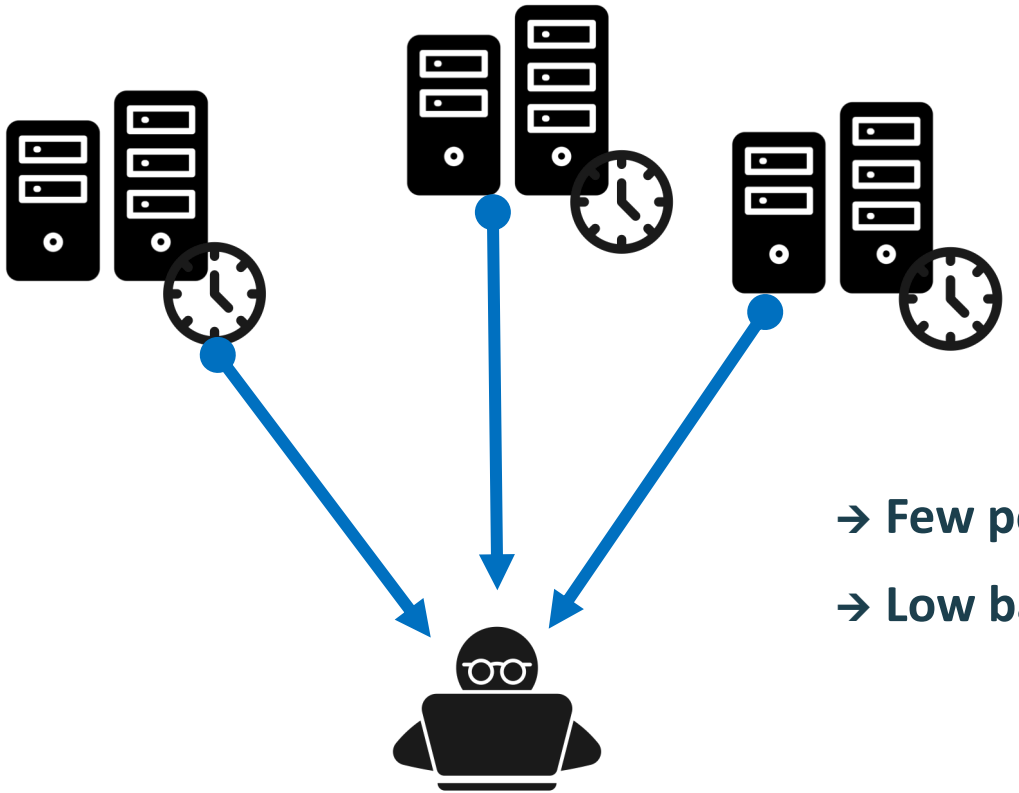


Normal Client Traffic



Client communication to different servers with non amplification protocols

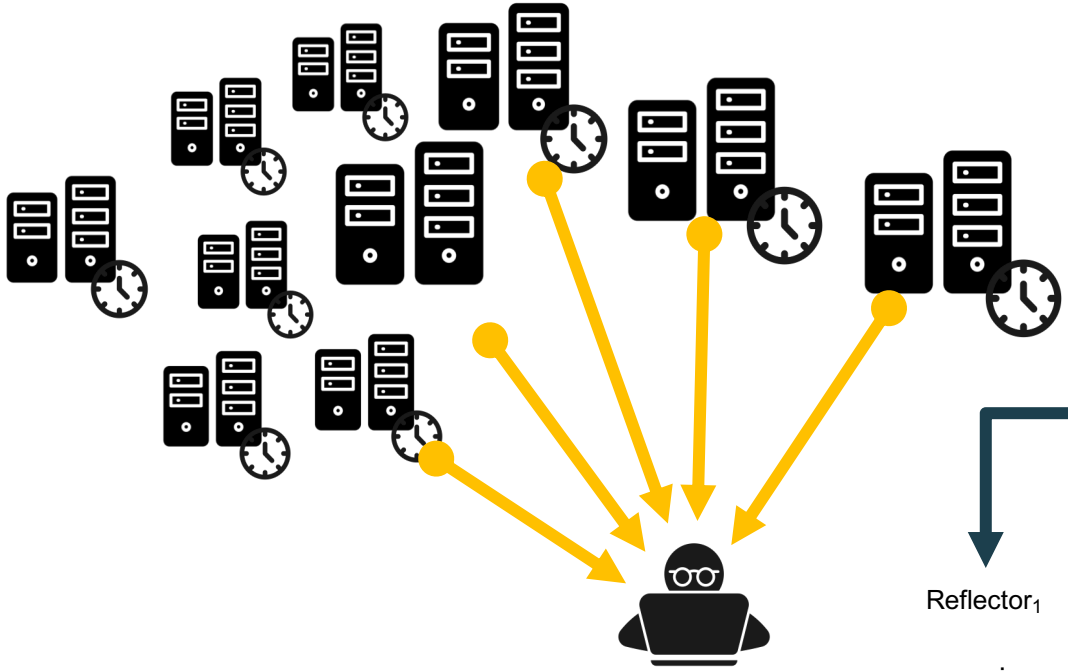
Normal NTP Traffic



→ Few potential amplification servers

→ Low bandwidth

DDoS Classification



Source port = amplification protocol

More than 10 sources

Traffic > 1 Gbps

UDP flows with src port *x* (e.g. NTP, OpenVPN, ...)

Reflector$_1$

⋮

Reflector$_k$

⋮

Reflector$_n$

∑flows > *t* Gbit/s

flow$_1$

flow$_k$

flow$_n$

Target IP

Criteria: DDoS if min *k* reflectors with > *t* Gbit/s traffic

Amplification Protocols

WS-Discovery

CLDAP

NTP

SSDP

OpenVPN

DNS

SNMP

Chargen

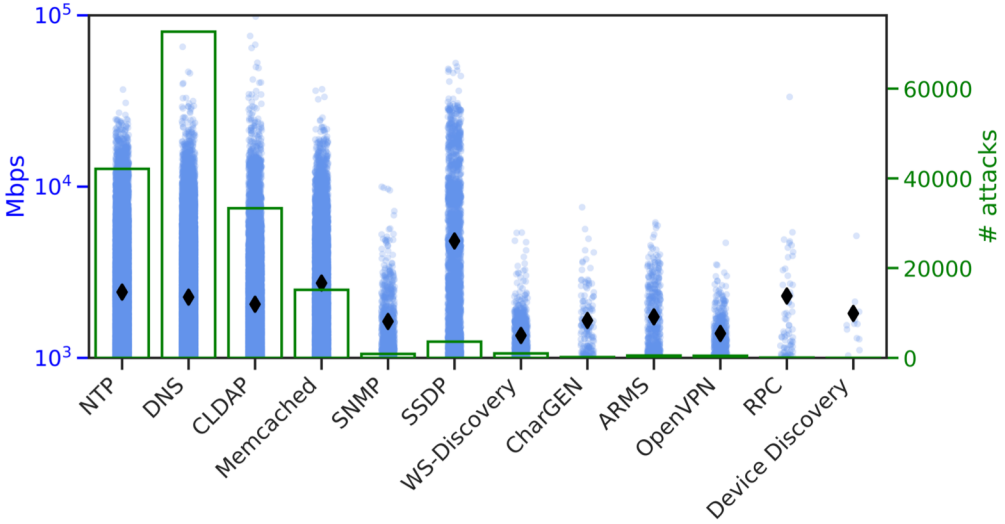
RPC

Memcached

ARMS

Device Discovery

Dataset and Results



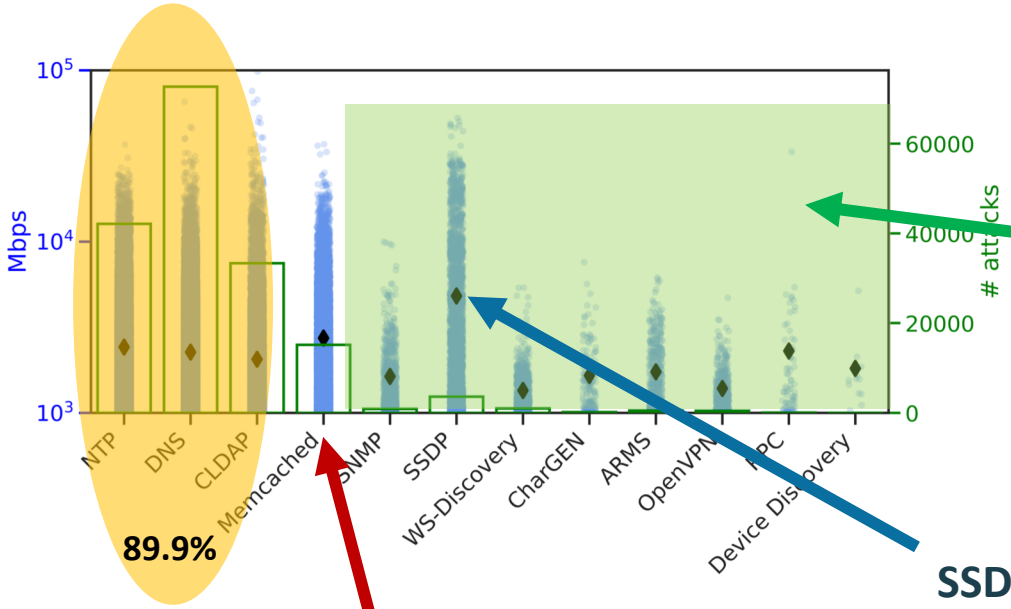
DDoS Dataset

- 58,000 attacks with at least 1 Gbps over 6 months

Validation

- Including non amplification protocols
- Potential false-positives (root DNS)
- Inspection of DDoS events with IXP

Dataset and Results



Less frequent and new protocols

- Not to be underestimated
- Generate severe traffic rates

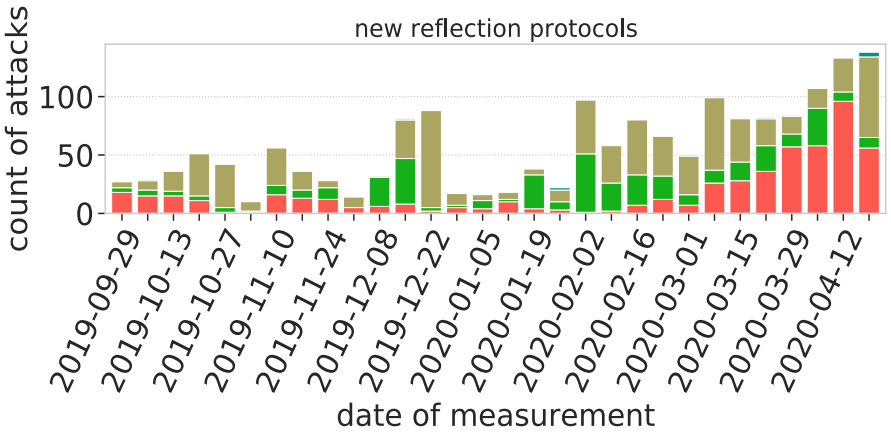
SSDP

- Used for sophisticated, long duration attacks
- High packet rates and traffic volume

Memcached

- Still a popular attack vector

Well Known Amplification Protocols

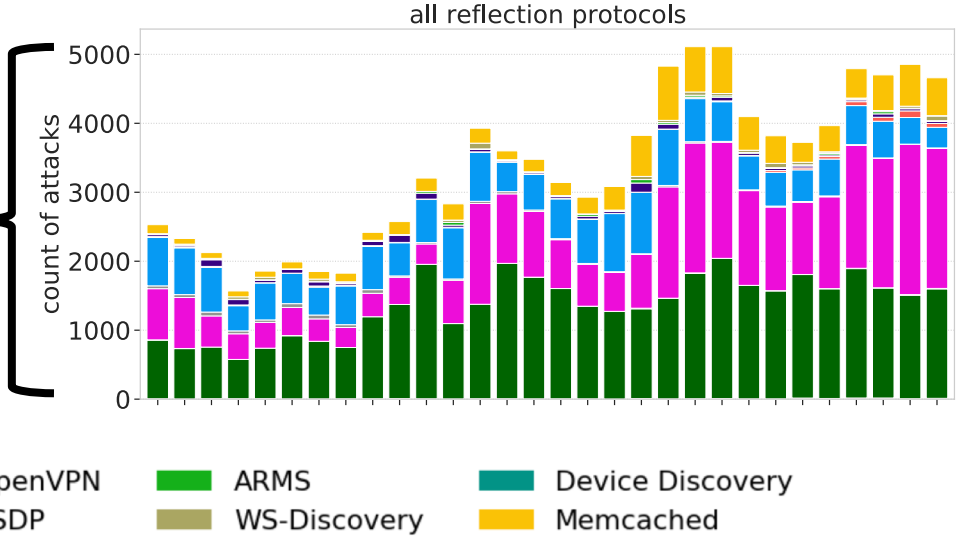


OpenVPN rose by 500%

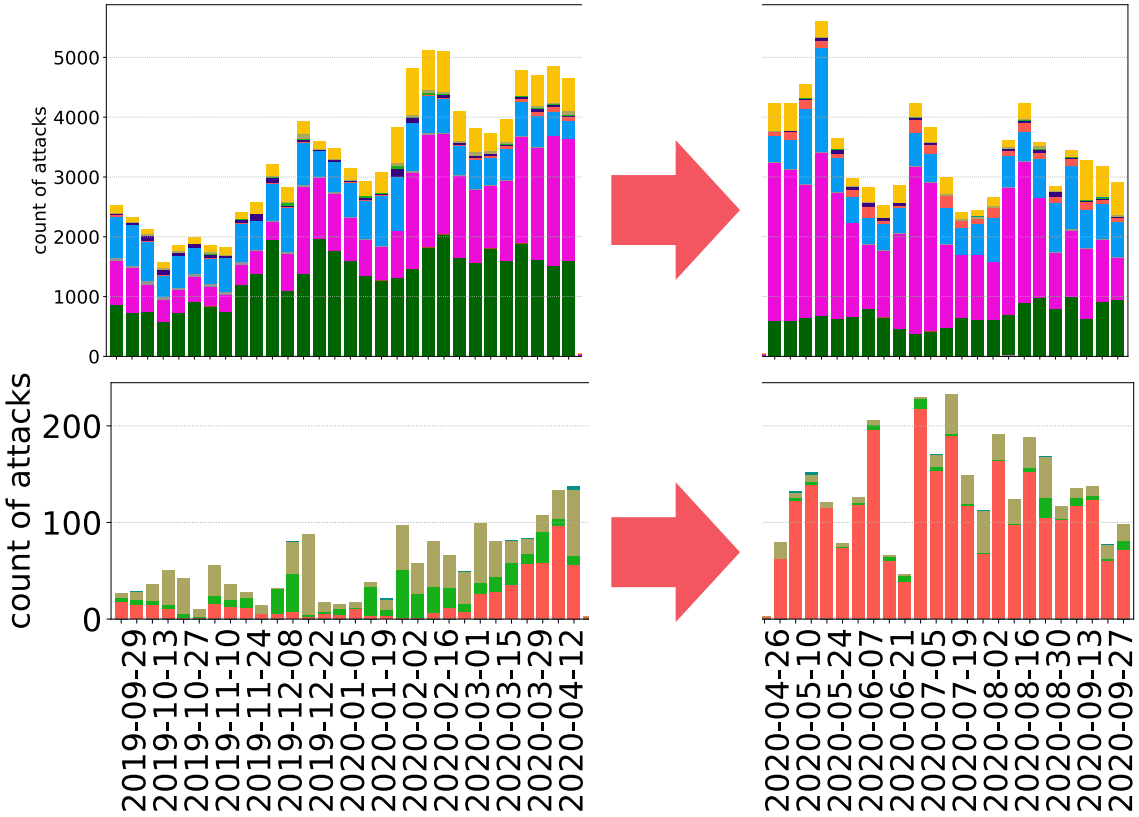
(starting from a low level)

well known protocols

weekly attacks



Amplification Protocols - Update



Traffic Volume & Packet Rate – Poll

What is of more interest to you with DDoS attacks, packet rate, traffic volume or both?

Results RIPE 82 Meeting:

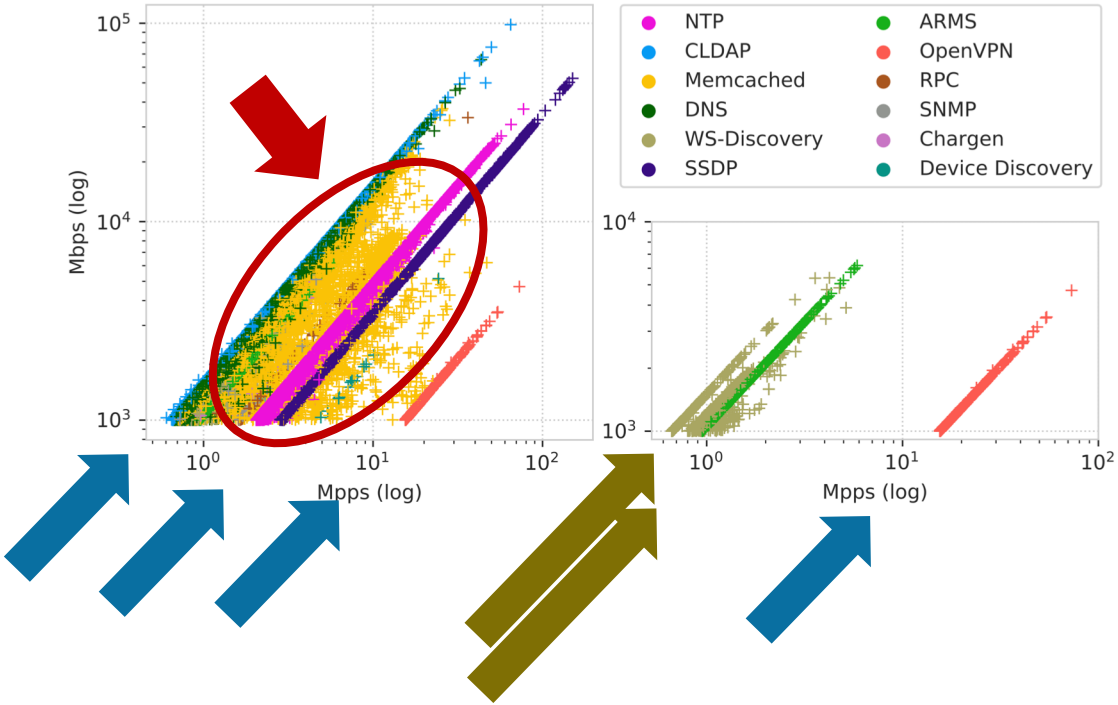
BOTH 47% (22)

TRAFFIC VOLUME 17% (8)

PACKET RATE 13% (6)

NO EXPERIENCE WITH DDoS ATTACKS 21% (10)

Traffic Volume & Packet Rate



Linear

- Stable amplification factor

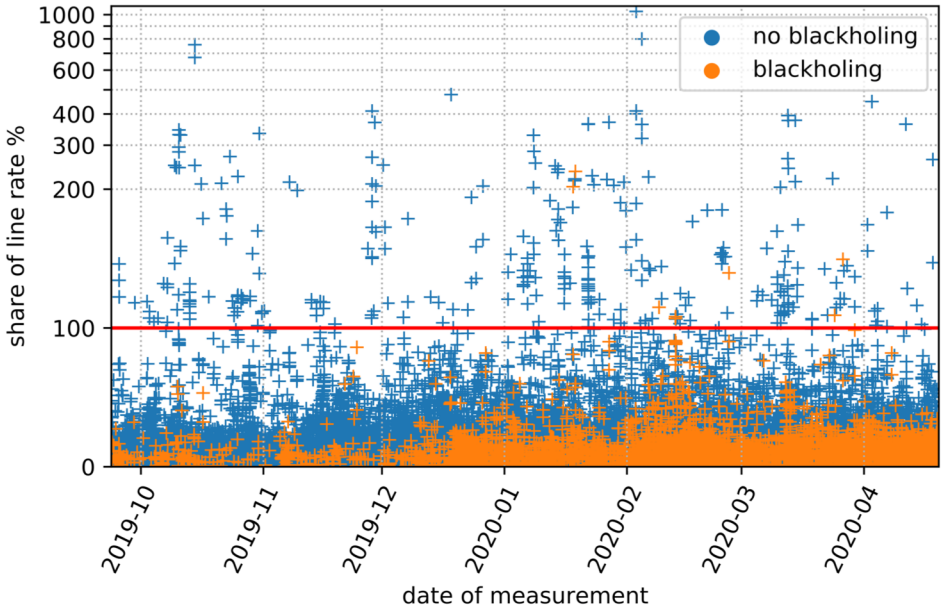
Multi linear

- Multiple amplification flaws

Non linear

- Payload of variable size

Infrastructure Perspective



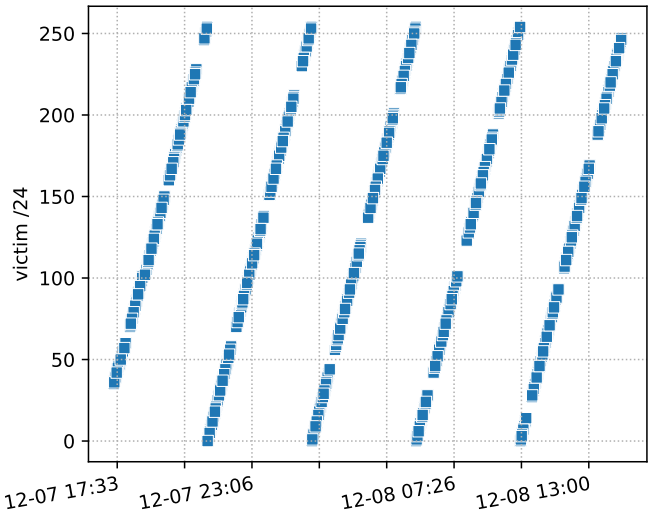
0.18% of attacks exceeded port capacity

26% of attacks at 50% of port capacity

IXP perspective

- Combined DDoS traffic was 3.6% of IXPs peak traffic

View on Targets



Temporal attack pattern

- Attach traversed /24 1 min each IP
- Probably to evade mitigation

High profile attacks

- Target 28% - 10% of announced IP space

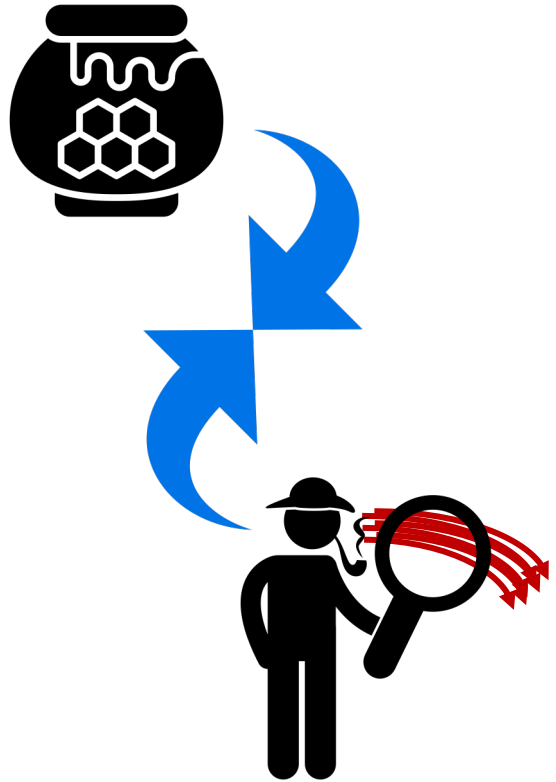
Attacks on VPN infrastructure

- 1.2M unique VPN endpoints in DNS dataset
- 39 Targets in 30 ASes

Comparison to a Honeypot

Divergent view of honeypot and IXP

- Only 8% attacks (33% targets) visible by honeypot
- 0.95% of the targets visible in IXP dataset
- High IXP threshold > 1Gbps
- Scanning events in honeypot data
- Likelihood of attack choosing honeypot
- Visibility of vantage points on the Internet



Conclusion

Updated view on amplification protocols and DDoS attacks

- Legacy protocols still heavily used
- New protocols are effective, pose an emerging threat
  - OpenVPN 500% incline (but on a low level compared to other DDoS amplification protocols)

No severe impact at core Internet infrastructures

Divergent picture of attacks observed from different sources

DDoS Never Dies?
An IXP Perspective on DDoS Amplification Attacks

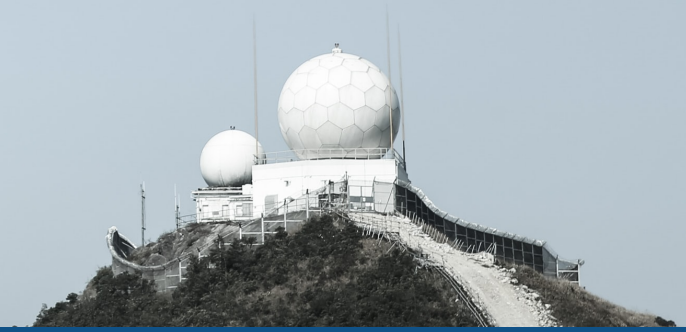


Photo by Samuel Wong on Unsplash

D. Kopp[1], C. Dietzel[1,3], O. Hohlfeld[2] DE-CIX[1], BTU[2], MPI[3]