

# DDOS Attacks: How small networks can defend

---

Practical case of protecting an Faculty/University from DDOS



# Size of FCSE/UKIM

---

- University of Ss Cyril and Methodius (UKIM) – Skopje, biggest University in North Macedonia
- Faculty of Computer Science and Engineering (FCSE) – Biggest Faculty with 5000+ active students
- Our systems are Electronically First
- We run our own Data Center (Both UKIM & FCSE / one DC each)
- We run IXP.mk – official name of project: **High Availability Internet Connection Research Platform (testbed)**

# Size of FCSE/UKIM Network

---

- UKIM – announces one /19 (at least /24 for each Faculty)
- Internet access – 2 x 10Gbit from GEANT
- Peering @ IXP.mk – 10 Gbit
- Backup internet via FCSE (cold backup)
- Limited set of services hosted
  
- FCSE – announces 4 x /24 from UKIM /19 & 4 x /24 directly
- Internet access – 1 x 10Gbit from UKIM, 1 x 1 Gbit from ISP #1, 1 x 10 Gbit from ISP#2 (was not active)
- Peering @ IXP.mk – 10 Gbit
- Hosting: UKIM wide systems (student records system, LMS, etc.), FCSE services (including our own LMS + Video platform), ccTLD for .mk, National health system, Ministry of education systems,...

# Attack history

---

- Lot of IP space, many different user types (Faculty, Students, Governmental, Research) – attacks are daily/weekly usually handled but IPS/FW or Manual NOC intervention
- DDOS protection from GEANT for traffic coming from that Uplink
  
- In the last 10+ years nothing serious – generally we said: “We are not interesting target so this will not happen to US”

# Attack #1 / #2 – June/July 2022

---

- FCSE LMS (based on Moodle) gets attacked several times a day at the end of the semester;
- FCSE LMS for exams (based on Moodle) gets attacked several times a day at the end of the semester;
- FCSE website gets attacked several times a day at the end of the semester;
  
- Exams are fully online (because of Covid19)
- Attacks are usually UDP lasting 30-59 minutes – the network starts to brake since Uplink between UKIM/MARNET (which was 1 Gbit gets filled up)
- FCC makes some network changes making most of the services for exams to be available only via IXP.mk
- We need to improve visibility in order to locate the problem faster

# Attack #3 – August 2022

---

- FCSE LMS (based on Moodle) gets attacked several times a day at the end of the semester;
  - FCSE LMS for exams (based on Moodle) gets attacked several times a day at the end of the semester;
  - FCSE website gets attacked several times a day at the end of the semester;
  - We see random targets attacked
- 
- Exams are fully online (because of Covid19)
  - Attacks are usually UDP lasting 30-120 minutes – the network brakes, FCC enters “panic mode”
  - We use IXP.mk for exclusive access to systems



# Attack #3 – August 2022 (2)

- We start to improve visibility based on Netflow (we reinstalled Ntopng, installed Fastnetmon)
- We got GEANT OC on board
- We had to limit outside traffic
- Traffic levels are doubled every attack
- GEANT OC switched the DDOS protection to “always on mode”
- Attacks are developing (not only usual UDP volumetric)

We have detected a DDoS attack event affecting your network which we automatically started to scrub (unless the "Event Type below is \*Ended\*"). All the information pertaining to it can be found below:

```
=====
Segment: DST MARnet (subnets:)
Time: 2022-08-16 22:16:31 UTC
Event type: Attack details
Triggered detection methods: UDP
Attack ID: 6581
```

```
Attack signature: (protocol 17 AND source 103.192.0.0/10 AND destination 185.153.48.10/32) OR (protocol 17 AND source 103.147.6.109/32 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 103.176.0.0/13 AND destination 185.153.48.10/32) OR (protocol 17 AND source 103.145.0.0/18 AND destination 185.153.48.10/32) OR (protocol 17 AND source 64.0.0.0/3 AND destination 185.153.48.10/32) OR (protocol 17 AND source 45.192.0.0/10 AND destination 185.153.48.10/32) OR (protocol 17 AND source 45.76.187.184/32 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 45.116.156.224/27 AND destination 185.153.48.10/32) OR (protocol 17 AND source 196.0.0.0/6 AND destination 185.153.48.10/32) OR (protocol 17 AND source 128.0.0.0/2 AND destination 185.153.48.10/32) OR (protocol 17 AND source 45.153.165.118/32 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 208.0.0.0/4 AND destination 185.153.48.10/32) OR (protocol 17 AND source 38.0.0.0/8 AND destination 185.153.48.10/32) OR (protocol 17 AND source 45.143.30.59/32 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 0.0.0.0/5 AND destination 185.153.48.10/32) OR (protocol 17 AND source 103.0.0.0/9 AND destination 185.153.48.10/32) OR (protocol 17 AND source 100.36.238.42/32 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 40.0.0.0/6 AND destination 185.153.48.10/32) OR (protocol 17 AND source 193.0.0.0/8 AND destination 185.153.48.10/32) OR (protocol 17 AND source 101.0.0.0/10 AND destination 185.153.48.10/32) OR (protocol 17 AND source 12.0.0.0/6 AND destination 185.153.48.10/32) OR (protocol 17 AND source 101.255.0.0/16 AND destination 185.153.48.10/32) OR (protocol 17 AND source 103.145.247.18/32 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 103.189.206.42/32 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 39.62.59.74/32 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 23.128.0.0/10 AND destination 185.153.48.10/32) OR (protocol 17 AND source 104.0.0.0/5 AND destination 185.153.48.10/32) OR (protocol 17 AND source 103.146.128.0/17 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 112.0.0.0/4 AND destination 185.153.48.10/32) OR (protocol 17 AND source 46.0.0.0/7 AND destination 185.153.48.10/32) OR (protocol 17 AND source 45.65.139.226/32 AND destination 185.153.48.10/32) OR (protocol 17 AND source 103.128.0.0/12 AND destination 185.153.48.10/32) OR (protocol 17 AND source 24.0.0.0/5 AND destination 185.153.48.10/32) OR (protocol 17 AND source 103.160.0.0/12 AND destination 185.153.48.10/32) OR (protocol 17 AND source 45.126.252.169/32 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 103.144.0.0/16 AND destination 185.153.48.10/32) OR (protocol 17 AND source 45.137.98.31/32 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 200.0.0.0/5 AND destination 185.153.48.10/32) OR (protocol 17 AND source 98.175.87.243/32 AND destination 185.153.48.10/32) OR (protocol 17 AND source 100.6.67.52/32 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 102.0.0.0/8 AND destination 185.153.48.10/32) OR (protocol 17 AND source 101.168.176.0/21 AND destination 185.153.48.10/32) OR (protocol 17 AND source 96.0.0.0/7 AND destination 185.153.48.10/32) OR (protocol 17 AND source 45.130.0.0/15 AND destination 185.153.48.10/32) OR (protocol 17 AND source 45.153.50.137/32 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 45.0.0.0/11 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 103.147.246.64/26 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 103.148.0.0/14 AND destination 185.153.48.10/32) OR (protocol 17 AND source 45.65.232.139/32 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 45.128.68.16/28 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 103.188.236.110/32 AND destination 185.153.48.10/32) OR (protocol 17 AND source 101.79.73.105/32 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 36.0.0.0/7 AND destination 185.153.48.10/32) OR (protocol 17 AND source 101.96.0.0/12 AND destination 185.153.48.10/32) OR (protocol 17 AND source 32.0.0.0/6 AND destination 185.153.48.10/32) OR (protocol 17 AND source 103.147.218.34/32 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 101.75.158.2/32 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 103.145.128.0/19 AND destination 185.153.48.10/32) OR (protocol 17 AND source 45.127.134.27/32 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 194.0.0.0/7 AND destination 185.153.48.10/32) OR (protocol 17 AND source 39.152.0.0/14 AND destination 185.153.48.10/32) OR (protocol 17 AND source 8.0.0.0/10 AND destination 185.153.48.10/32) OR (protocol 17 AND source 103.184.0.0/14 AND destination 185.153.48.10/32) OR (protocol 17 AND source 45.137.121.38/32 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 103.152.0.0/13 AND destination 185.153.48.10/32) OR (protocol 17 AND source 45.80.0.0/12 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 45.70.0.0/15 AND destination 185.153.48.10/32) OR (protocol 17 AND source 103.145.180.67/32 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 48.0.0.0/4 AND destination 185.153.48.10/32) OR (protocol 17 AND source 192.0.0.0/8 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 45.146.0.0/15 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 45.160.0.0/11 AND destination 185.153.48.10/32) OR (protocol 17 AND source 8.242.0.0/15 AND destination 185.153.48.10/32) OR (protocol 17 AND source 45.127.121.182/32 AND destination 185.153.48.10/32 AND destination-port =80)
```

Mitigation status: Auto-mitigation selected by the customer

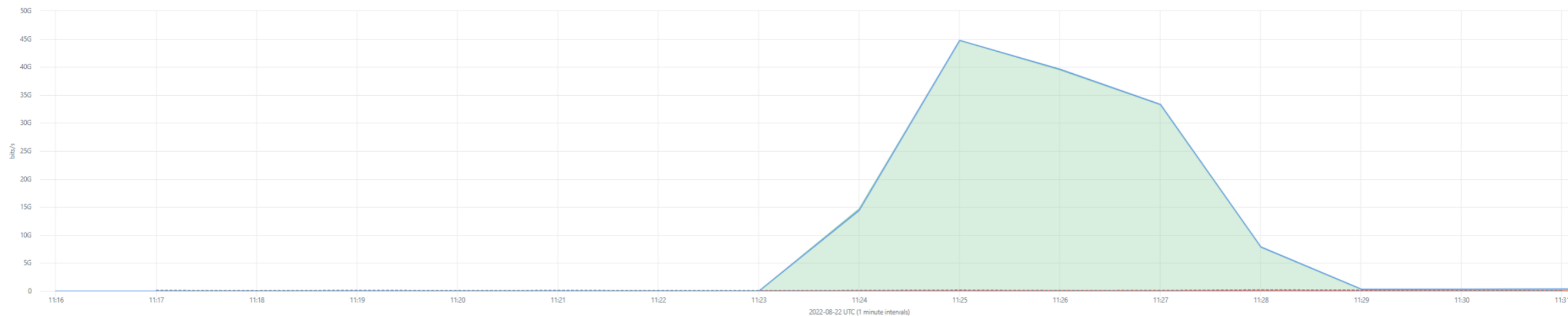


# Attack #3 – August 2022 (3)

- We hear rumors that **students may be involved**
- **We move services to a /24 for better control and analysis** and we make them “angry” as exams continue
- The attacker hits us hard (above 50 Gbit)

Top Dest IP/CIDR by Average bits/s

Last 15m 41 of 41 data sources 2 Filters





# Attack #3 – August 2022 (4)

- The cat/mouse game starts
- We create direct links for Netflow from Core routers for analysis
- We drop non needed traffic on the GEANT routers in SOF and VIE
- The Student enrollment system for UKIM gets attacked
- They start to “Carpet bomb” the whole IP range
- We see a large botnet in place (so students involvement is partially possible)

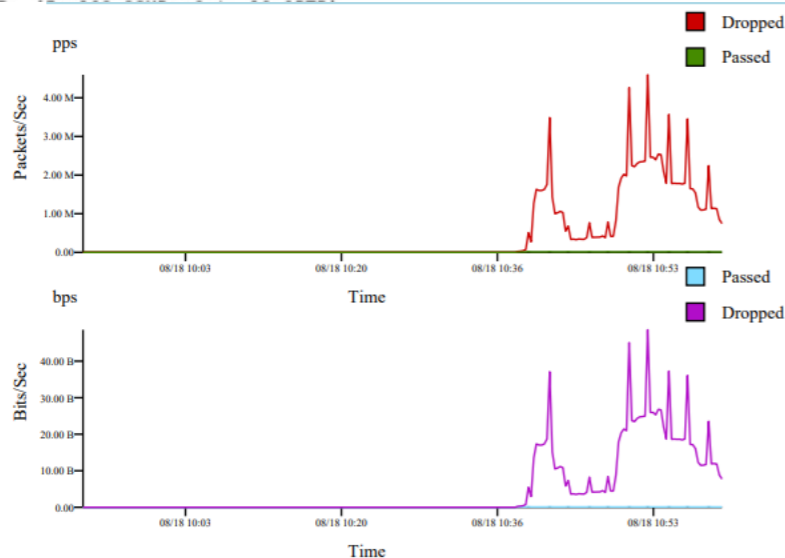
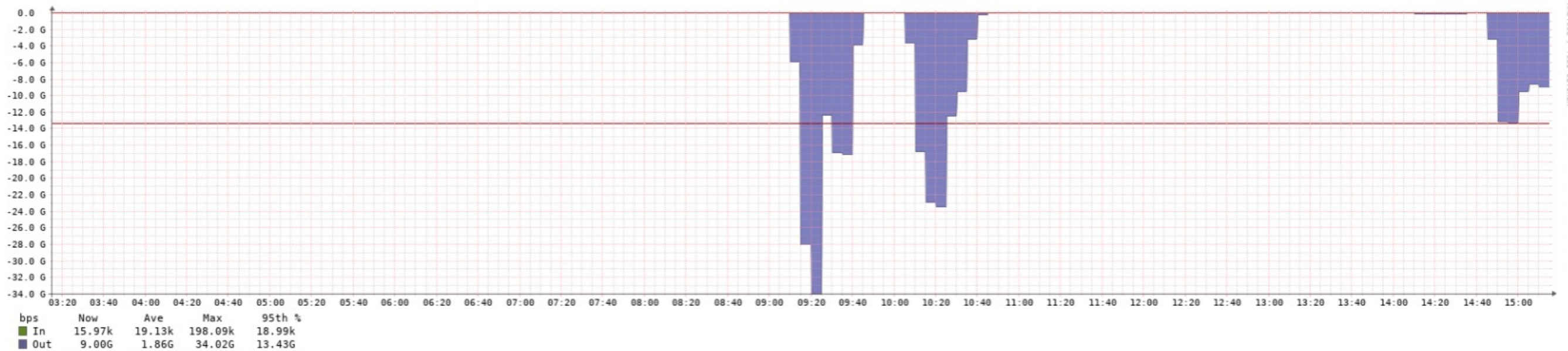
```
=====
Segment: DST MARnet (subnets: )
Time: 2022-08-18 07:27:48 - 2022-08-18 10:31:43 UTC
Event type: Ended
Triggered detection methods: UDP, TCP (flag SYN, ACK), All, ICMP
Attack ID: 6591
Attack signature: (protocol 1 AND source 112.0.0.0/4 AND destination 194.149.137.130/32) OR (protocol 17 AND source 101.51.224.0/20 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 6 AND source 185.8.0.0/14 AND destination 194.149.135.130/32) OR (protocol 17 AND source 204.0.0.0/6 AND destination 185.153.48.10/32) OR (protocol 17 AND source 189.203.192.0/21 AND destination 194.149.137.199/32 AND destination-port =80) OR (protocol 17 AND source 173.208.192.0/18 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 1 AND source 101.0.0.0/9 AND destination 194.149.137.160/32) OR (protocol 17 AND source 51.128.0.0/9 AND destination 194.149.137.199/32 AND destination-port =80) OR (protocol 17 AND source 217.160.0.0/11 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 17 AND source 167.114.4.72/32 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 1 AND source 1.20.0.0/16 AND destination 194.149.137.130/32) OR (protocol 17 AND source 203.192.0.0/11 AND destination 185.153.48.10/32) OR (protocol 17 AND source 64.0.0.0/3 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 17 AND source 196.250.0.0/15 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 1 AND source 10.0.0.0/7 AND destination 194.149.137.130/32) OR (protocol 1 AND source 36.0.0.0/6 AND destination 194.149.137.160/32) OR (protocol 17 AND source 202.0.0.0/8 AND destination 185.153.48.10/32) OR (protocol 6 AND source 0.0.0.0/4 AND destination 194.149.137.160/32) OR (protocol 1 AND source 104.0.0.0/5 AND destination 194.149.135.130/32) OR (protocol 1 AND source 10.0.0.0/7 AND destination 194.149.137.160/32) OR (protocol 17 AND source 128.0.0.0/2 AND destination 185.153.48.10/32) OR (protocol 17 AND source 208.0.0.0/4 AND destination 185.153.48.10/32) OR (protocol 6 AND source 24.0.0.0/5 AND destination 194.149.137.160/32) OR (protocol 17 AND source 137.74.95.61/32 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 17 AND source 103.151.64.0/18 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 1 AND source 128.0.0.0/2 AND destination 194.149.135.130/32) OR (protocol 6 AND source 64.0.0.0/2 AND destination 194.149.137.160/32) OR (protocol 6 AND source 16.0.0.0/6 AND destination 194.149.137.160/32) OR (protocol 17 AND source 144.0.0.0/4 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 1 AND source 5.0.0.0/8 AND destination 194.149.137.130/32) OR (protocol 17 AND source 202.64.0.0/10 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 1 AND source 192.0.0.0/3 AND destination 194.149.137.160/32) OR (protocol 1 AND source 1.10.128.0/17 AND destination 194.149.137.160/32) OR (protocol 1 AND source 64.0.0.0/3 AND destination 194.149.137.130/32) OR (protocol 17 AND source 199.0.0.0/8 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 17 AND source 207.128.0.0/10 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 6 AND source 20.0.0.0/8 AND destination 194.149.135.130/32) OR (protocol 1 AND source 101.108.0.0/15 AND destination 194.149.137.130/32) OR (protocol 6 AND source 128.0.0.0/2 AND destination 194.149.137.160/32) OR (protocol 17 AND source 194.0.0.0/8 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 6 AND source 128.0.0.0/3 AND destination 194.149.135.130/32) OR (protocol 17 AND source 0.0.0.0/1 AND destination 194.149.137.199/32) OR (protocol 17 AND source 144.0.0.0/8 AND destination 194.149.137.199/32 AND destination-port =80) OR (protocol 6 AND source 160.0.0.0/4 AND destination 194.149.135.130/32) OR (protocol 1 AND source 64.0.0.0/3 AND destination 194.149.135.130/32) OR (protocol 17 AND source 184.128.0.0/10 AND destination 194.149.135.130/32) OR (protocol 1 AND source 101.0.0.0/10 AND destination 194.149.137.130/32) OR (protocol 17 AND source 103.227.144.97/32 AND destination 194.149.137.199/32 AND destination-port =80) OR (protocol 17 AND source 192.192.0.0/10 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 17 AND source 129.0.0.0/8 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 1 AND source 102.0.0.0/7 AND destination 194.149.135.130/32) OR (protocol 17 AND source 192.0.0.0/3 AND destination 194.149.137.199/32) OR (protocol 17 AND source 101.96.120.0/22 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 1 AND source 135.125.233.240/32 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 17 AND source 192.185.178.103/32 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 1 AND source 1.0.0.0/13 AND destination 194.149.135.130/32) OR (protocol 17 AND source 135.181.132.177/32 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 1 AND source 45.7.135.174/32 AND destination 194.149.137.160/32) OR (protocol 6 AND source 32.0.0.0/3 AND destination 194.149.137.160/32) OR (protocol 17 AND source 192.99.55.22/32 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 17 AND source 176.0.0.0/4 AND destination 194.149.135.130/32) OR (protocol 17 AND source 48.0.0.0/4 AND destination 194.149.135.130/32) OR (protocol 17 AND source 139.0.0.0/8 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 17 AND source 103.131.104.0/23 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 6 AND source 216.0.0.0/5 AND destination 194.149.135.130/32) OR (protocol 6 AND source 184.0.0.0/9 AND destination 194.149.135.130/32) OR (protocol 1 AND source 48.0.0.0/4 AND destination 194.149.135.130/32) OR (protocol 6 AND source 24.0.0.0/5 AND destination 194.149.135.130/32) OR (protocol 17 AND source 196.202.128.0/17 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 17 AND source 203.128.0.0/10 AND destination 185.153.48.10/32) OR (protocol 6 AND source 36.0.0.0/6 AND destination 194.149.137.130/32) OR (protocol 17 AND source 104.0.0.0/5 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 17 AND source 192.0.0.0/5 AND destination 185.153.48.10/32) OR (protocol 6 AND source 192.0.0.0/3 AND destination 194.149.137.160/32) OR (protocol 17 AND source 207.192.0.0/12 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 1 AND source 104.0.0.0/5 AND destination 194.149.137.130/32) OR (protocol 1 AND source 112.0.0.0/6 AND destination 194.149.137.160/32) OR (protocol 17 AND source 135.181.134.56/32 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 17 AND source 195.201.9.76/32 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 1 AND source 5.0.0.0/8 AND destination 194.149.135.130/32) OR (protocol 6 AND source 23.0.0.0/8 AND destination 194.149.137.160/32) OR (protocol 1 AND source 128.0.0.0/2 AND destination 194.149.137.130/32) OR (protocol 1 AND source 1.20.0.0/16 AND destination 194.149.135.130/32) OR (protocol 17 AND source 101.96.120.0/22 AND destination 194.149.137.199/32 AND destination-port =80) OR (protocol 17 AND source 38.43.77.12/32 AND destination 194.149.137.199/32 AND destination-port =80) OR (protocol 17 AND source 49.0.80.0/20 AND destination 194.149.137.199/32 AND destination-port =80) OR (protocol 1 AND source 10.0.0.0/7 AND destination 194.149.135.130/32) OR (protocol 1 AND source 1.20.0.0/16 AND destination 194.149.137.160/32) OR (protocol 17 AND source 15.192.0.0/10 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 17 AND source 193.0.0.0/8 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 17 AND source 180.26.80.55/32 AND destination 194.149.137.199/32 AND destination-port =80) OR (protocol 1 AND source 1.10.128.0/17 AND destination 194.149.135.130/32) OR (protocol 1 AND source 40.0.0.0/5 AND destination 194.149.135.130/32) OR (protocol 17 AND source 210.87.250.107/32 AND destination 194.149.137.199/32 AND destination-port =80) OR (protocol 6 AND source 0.0.0.0/4 AND destination 194.149.135.130/32) OR (protocol 17 AND source 192.208.0.0/12 AND destination 194.149.137.199/32 AND destination-port =80) OR (protocol 17 AND source 192.99.1.6/32 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 17 AND source 101.200.0.0/15 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 1 AND source 16.0.0.0/4 AND destination 194.149.135.130/32) OR (protocol 17 AND source 93.126.64.0/19 AND destination 194.149.137.199/32 AND destination-port =80) OR (protocol 1 AND source 192.0.0.0/3 AND destination 194.149.137.130/32) OR (protocol 1 AND source 40.0.0.0/6 AND destination 194.149.137.160/32) OR (protocol 17 AND source 195.90.1.153/32 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 17 AND source 128.0.0.0/2 AND destination 194.149.137.199/32) OR (protocol 1 AND source 104.0.0.0/5 AND destination 194.149.137.160/32) OR (protocol 17 AND source 191.192.0.0/11 AND destination 194.149.137.199/32 AND destination-port =80) OR (protocol 6 AND source 34.0.0.0/8 AND destination 194.149.135.130/32) OR (protocol 17 AND source 200.0.0.0/7 AND destination 185.153.48.10/32) OR (protocol 1 AND source 2.188.192.0/18 AND destination 194.149.135.130/32) OR (protocol 17 AND source 112.0.0.0/4 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 6 AND source 23.0.0.0/8 AND destination 194.149.135.130/32) OR (protocol 17 AND source 208.0.0.0/5 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 17 AND source 0.0.0.0/1 AND destination 194.149.137.130/32) OR (protocol 17 AND source 16.0.0.0/4 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 6 AND source 64.0.0.0/2 AND destination 194.149.135.130/32) OR (protocol 17 AND source 160.0.0.0/6 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 17 AND source 135.181.0.0/17 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 6 AND source 176.0.0.0/5 AND destination 194.149.135.130/32) OR (protocol 1 AND source 112.0.0.0/4 AND destination 194.149.135.130/32) OR (protocol 17 AND source 43.224.0.0/14 AND destination 194.149.137.199/32 AND destination-port =80) OR (protocol 1 AND source 101.0.0.0/8 AND destination 194.149.135.130/32) OR (protocol 17 AND source 204.12.252.122/32 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 17 AND source 196.207.28.146/32 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 17 AND source 103.0.0.0/9 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 1 AND source 120.0.0.0/5 AND destination 194.149.137.160/32) OR (protocol 6 AND source 35.128.0.0/9 AND destination 194.149.135.130/32) OR (protocol 17 AND source 192.0.0.0/3 AND destination 194.149.137.130/32) OR (protocol 17 AND source 169.62.81.64/29 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 6 AND source 20.0.0.0/8 AND destination 194.149.137.160/32) OR (protocol 17 AND source 51.210.0.0/16 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 1 AND source 48.0.0.0/4 AND destination 194.149.137.160/32) OR (protocol 1 AND source 192.0.0.0/3 AND destination 194.149.135.130/32) OR (protocol 1 AND source 64.0.0.0/3 AND destination 194.149.137.160/32) OR (protocol 1 AND source 1.4.128.0/17 AND destination 194.149.137.130/32) OR (protocol 6 AND source 17.0.0.0/8 AND destination 194.149.135.130/32) OR (protocol 17 AND source 54.36.19.34/32 AND destination 194.149.137.199/32 AND destination-port =80) OR (protocol 17 AND source 203.0.0.0/9 AND destination 185.153.48.10/32) OR (protocol 17 AND source 100.42.80.0/20 AND destination 194.149.137.199/32 AND destination-port =80) OR (protocol 1 AND source 16.0.0.0/4 AND destination 194.149.137.130/32) OR (protocol 17 AND source 93.122.168.0/22 AND destination 194.149.137.199/32 AND destination-port =80) OR (protocol 1 AND source 46.0.0.0/7 AND destination 194.149.137.160/32) OR (protocol 17 AND source 210.0.0.0/10 AND destination 194.149.137.199/32 AND destination-port =80) OR (protocol 17 AND source 197.254.0.0/17 AND destination 194.149.137.199/32 AND destination-port =80) OR (protocol 17 AND source 192.99.11.195/32 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 1 AND source 128.0.0.0/2 AND destination 194.149.137.160/32) OR (protocol 17 AND source 216.0.0.0/8 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 17 AND source 218.0.0.0/7 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 1 AND source 32.0.0.0/3 AND destination 194.149.137.130/32) OR (protocol 17 AND source 211.20.0.0/15 AND destination 194.149.137.199/32 AND destination-port =80) OR (protocol 17 AND source 110.49.144.0/25 AND destination 185.153.48.10/32 AND destination-port =80) OR (protocol 17 AND source 211.36.193.253/32 AND destination 194.149.137.199/32 AND destination-port =80) OR (protocol 17 AND source 0.0.0.0/5 AND destination 194.149.137.130/32 AND destination-port =80) OR (protocol 1 AND source 1.0.0.0/14 AND destination 194.149.137.130/32)
```

Mitigation status: Auto-mitigation selected by the customer



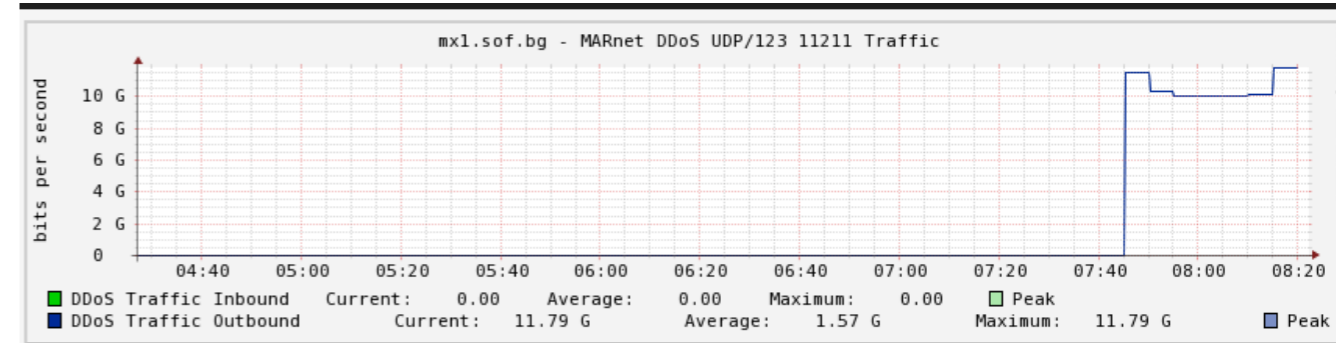
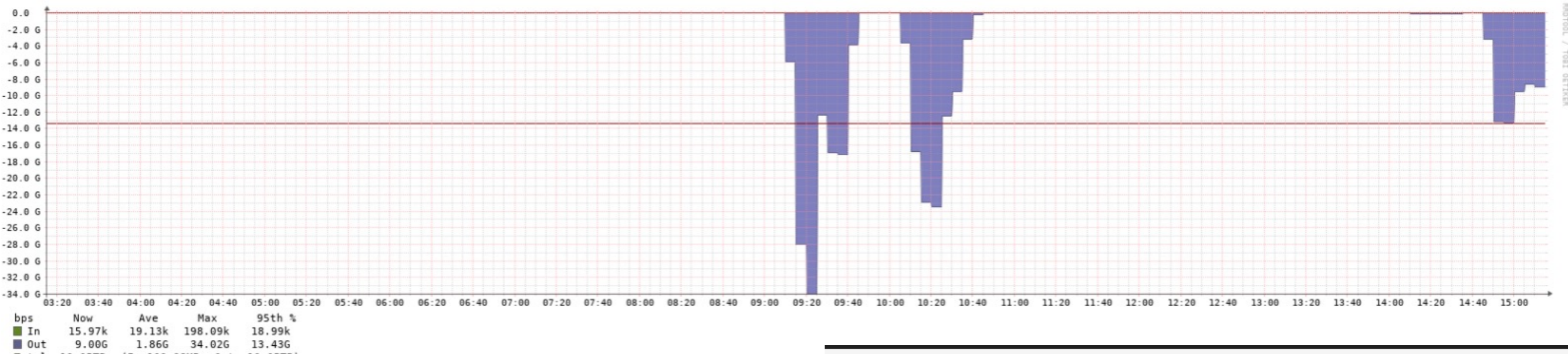
# Attack #3 – August 2022 (5)

- Lets collect data about machines attacking us, but make services available
- We move important services to new /24 which is IXP.mk only, our users are in .mk and all operators in MK have peering with us
- We drop volumetric (UDP: 53, 80, 123) at GEANT but still monitor all else
- We see more TCP advanced flooding

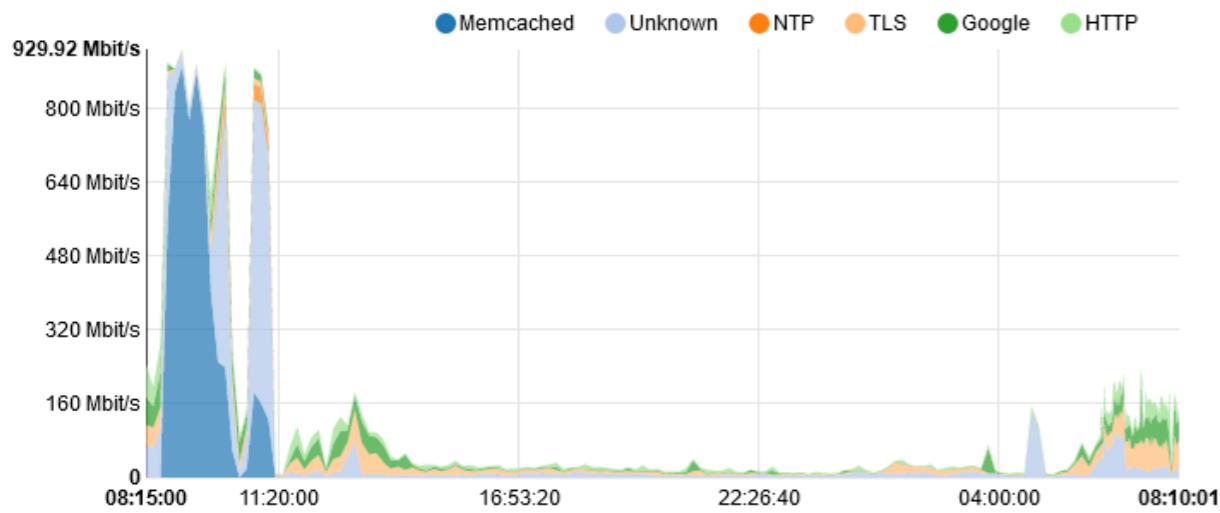


# Attack #3 – August 2022 (6)

- Lets collect data about machines attacking us, but make services available
- MEMCACHE enters the arena



## UKIM: Top Applications (Last Day)



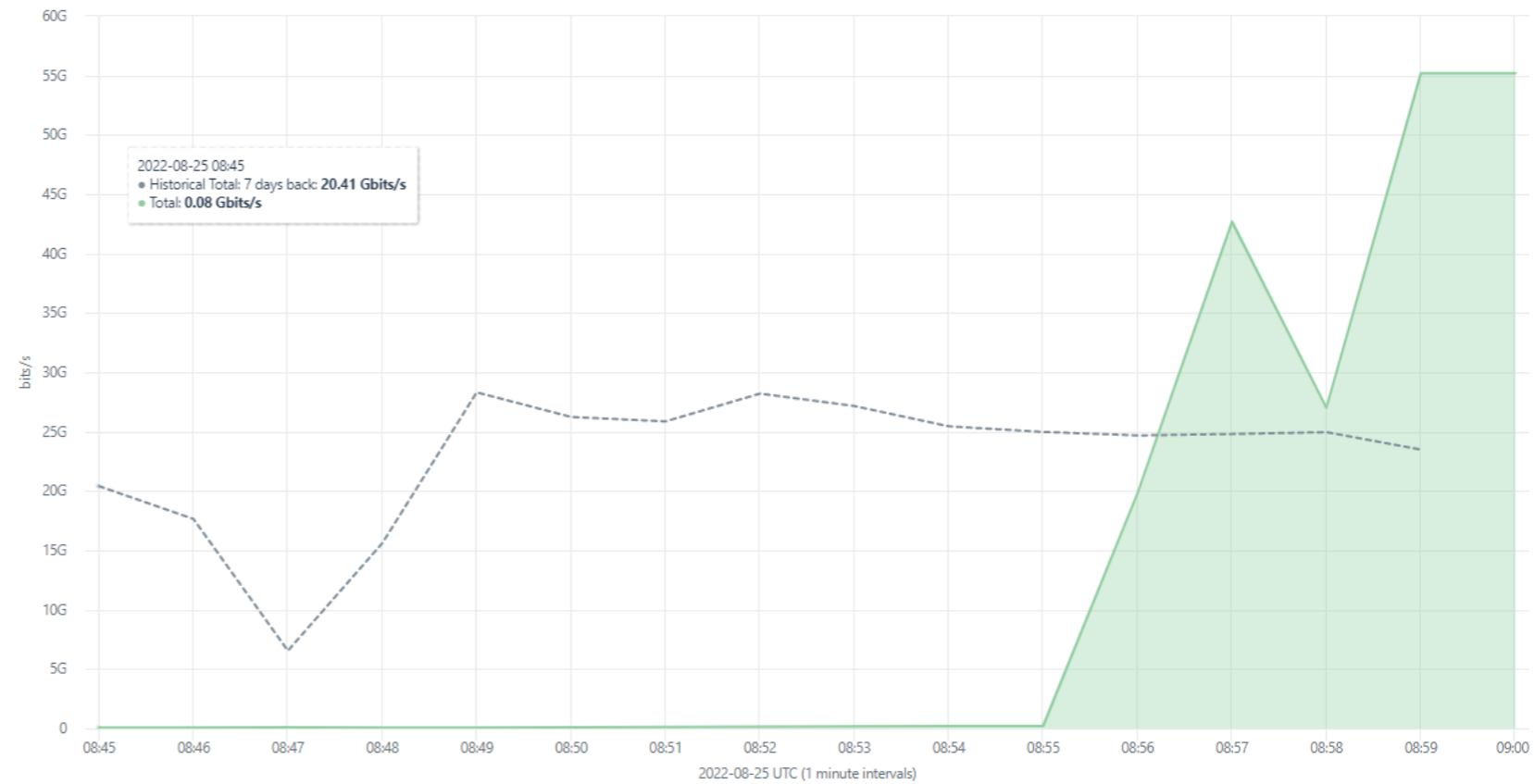


# Attack #3 – August 2022 (7)

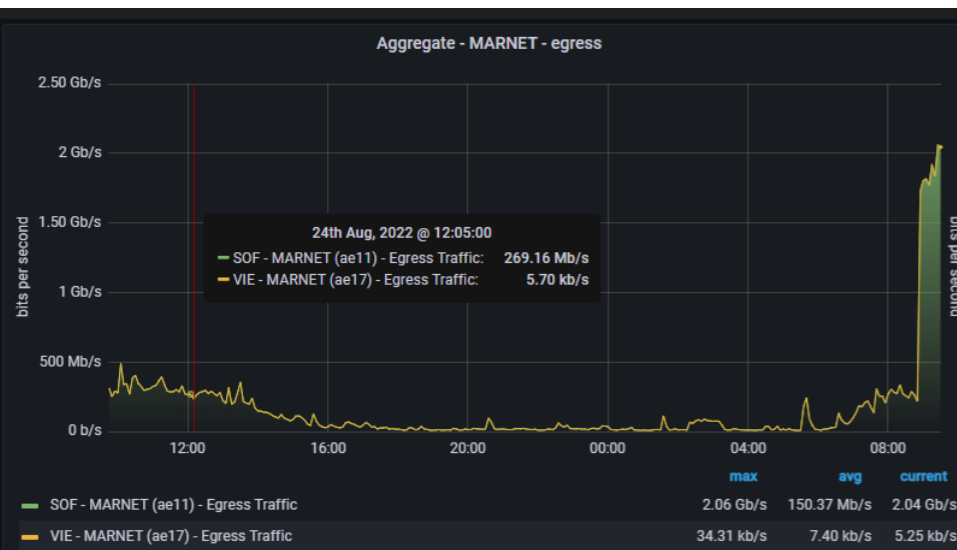
- Volumes are over the top...
- Routers start to go 100% CPU

Total by Average bits/s

Last 15m | 41 of 41 data sources | 2 Filters



Aggregate - MARNET - egress

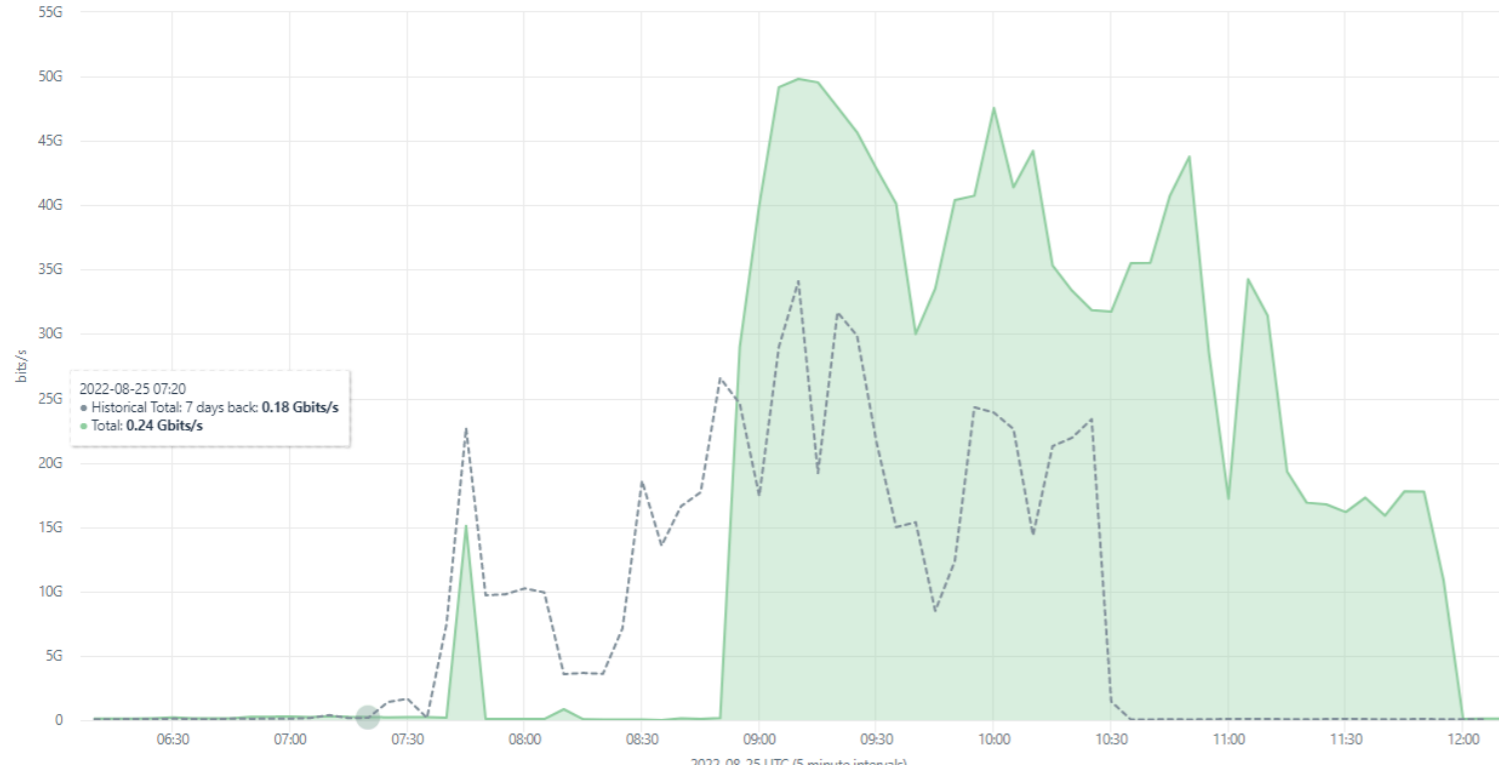


# Attack #3 – August 2022 (8)

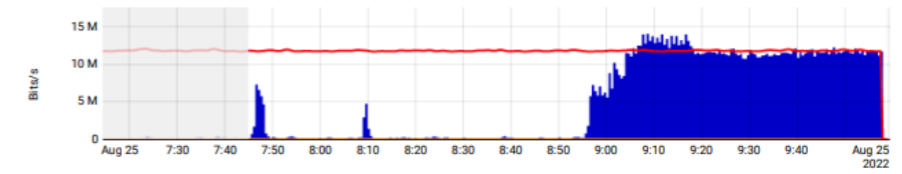
- Battle stations!!!

## Total by Average bits/s

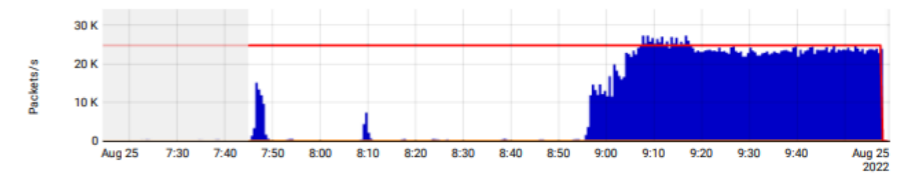
Last 6h 41 of 41 data sources 2 Filters



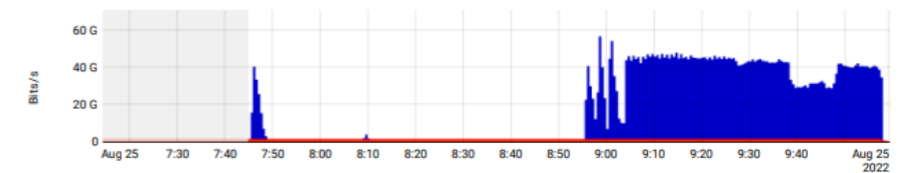
## ICMP (Values in relation to the same day in the last week)



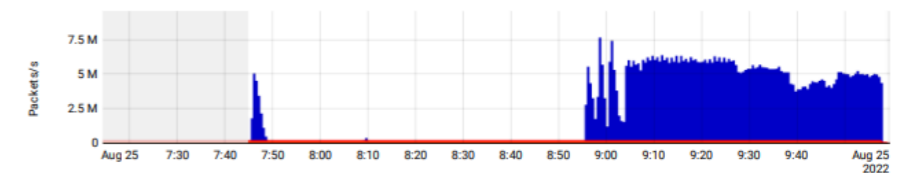
## ICMP



## UDP



## UDP



## Aggregate - MARNET - egress





# Attack #3 – August 2022 (8)

- We decide and announce to move exams back in the classrooms/labs
- We create some volumetric rules

Name	Match	Then	Status	Expires	Actions
MARNET_ATTACK_5MPFL0	Dst Addr 185.153.48.10/32 Src Addr 0.0.0.0/0	discard	ACTIVE	2022-09-18	<a href="#">Edit</a> <a href="#">Deactivate</a>
MARNET2_VCL002	Dst Addr 194.149.137.199/32 Src Addr 0.0.0.0/0	discard	ACTIVE	2022-09-18	<a href="#">Edit</a> <a href="#">Deactivate</a>
MARNET_6_8I5UQE	Dst Addr 194.149.137.138/32 Src Addr 0.0.0.0/0 Protocols udp DstPorts 80	discard	ACTIVE	2022-09-19	<a href="#">Edit</a> <a href="#">Deactivate</a>
MARNET_9_U04ITS	Dst Addr 194.149.137.231/32 Src Addr 0.0.0.0/0 Protocols udp DstPorts 80	discard	ACTIVE	2022-09-19	<a href="#">Edit</a> <a href="#">Deactivate</a>
MARnet_194-149-137-131_NJTKI4	Dst Addr 194.149.137.131/32 Src Addr 0.0.0.0/0 Protocols udp SrcPorts 11211	discard	ACTIVE	2022-09-20	<a href="#">Edit</a> <a href="#">Deactivate</a>

# Post analysis

---

- We survived 😊
- We collected botnet data and shared with all important parties
- We are (re)building our network

How did we survive – we used a **magical recipe called IXP**

- We announced one /24 only to IXP.mk and moved all services
- Local operators had unlimited access to services – this means students and professors can use all services. For outside world services where not accessible.
- Latency was “super low”, traffic volume was realistic.

# Network upgrades

---

- More powerful routers for FCSE
- GEANT Network upgrade – 2 x 100Gb
- Total visibility (we will monitor Netflow with several options and try to correlate)
- BGP black hole (looking into options)
- Onsite DDOS filter/scrubber for “high profile targets”
- More upstream capacity and diversity
- We have a big list of tools/products we are analyzing one by one and see which has best value for money (budget is almost always “zero”)
- **Need some fast network transport system (we have some fiber, we do not have the right technology like CDWM/DWDM for speeds faster than 10G**
- **Make IXP.mk even more useful for local ISP in case of big DDOS like this...**

Connect with us – [www.ixp.mk](http://www.ixp.mk)

# Questions?



[vladislav.bidikov@finki.ukim.mk](mailto:vladislav.bidikov@finki.ukim.mk)  
[@bidikov](https://www.instagram.com/bidikov)