Growing DDoS attacks – what have we learned

(29. June 2015)

Miloš Kukoleča

AMRES

milos.kukoleca@amres.ac.rs

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Network protection

- Strict network policy
  - Inbound traffic – limited set of allowed ports; everything else is discarded
  - Outbound traffic – antispoof rules; limited set of blocked ports; everything else is allowed
  - Router control plane is protected
  - Majority of users use proxy service; filtering the malware and phishing content
- In 2015 we started to liberalize this policy
  - Some customers have open network; they protect themselves

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Network monitoring

AMRES Serbian Academic Network

- Monitoring network using netflow and IPFIX
- Operators are monitoring traffic on backbone links
  - More links – difficult to monitor
- Alarm trigering mechanisms for links in down state
  - No alarm trigering mechanism for links that hit saturation point
- Occasional monitoring of netflow data
  - Response time for a particular network anomaly – within one working day

DANUBE REGION strategy START Danube Region Project Fund

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Previous DDoS attacks

- AMRES network was used as the source of attacks
  - Usualy DNS and NTP amplifications attacks
- Receiving external reports about our network involvement
- Detecting networks anomalies via netflow data
- AMRES network was the target of small scale DDoS attacks
  - NTP service on routers
  - Web service of particular customers
  - DNS service of particular customers
- Never a problem for the backbone in volume

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Detection of DDoS attacks

AMRES
Serbian Academic Network

- Small scale attacks were usualy detected by:
  - Report from our cutomers
  - Spotting network anomaly in SNMP data
  - Spotting network anomaly in netflow data
- Detection time is approx. one working day
- Services were partialy affected

DANUBE REGION strategy START Danube Region Project Fund

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Mittigating DDoS attacks

- Bandwidth used in these DDoS attacks was very limited
- Solutions applied:
  - Filtering the traffic in our core network
  - Route blackholing on our border routers
  - Parsing the netflow data, obtaining the source IP address used in the attack
  - Finding abuse contacts and sending reports
  - Everything is done manualy ☹
- Response time after DDoS detection: within 15 mins.

DANUBE REGION strategy START Danube Region Project Fund

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Roumors about DDoS attacks

- Many NRENs were targets of DDoS attacks in 2015.
- The volumes of attacks was huge
  - From several Gbps to couple of hundreds of Gbps !!!
- Volumes of attacks were bigger than the link capacities
- Reports about attacks reached the newspapers
  - Academic networks are very important for the educational system in many countries and the goverments were woried

DANUBE REGION strategy START Danube Region Project Fund

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Previous experience

- No experience with major DDoS attacks
- AMRES is not a user of GÉANT Firewall on Demand service
- No DDoS mitigation mechanisms in place

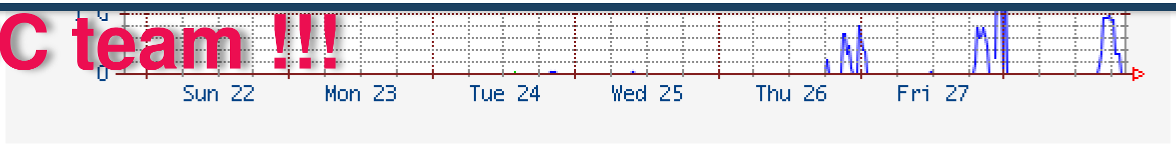
World according to AMRES

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

26th of November 2015

- NOC operators noticed larger traffice from one particular customer
  - Nothing to be worried about
- NOC notified customer and asked to investigate
- This was just one ticket among 10-20 other tickets

Lesson No. 1 : CSIRT engineer should be informed about all network anomalies noticed by NOC team !!!



CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Early stages of attack

- Several customers complained about slow network access in the evening
  - Low network activities on the links toward those customers
  - No syslog messages related to some errors on our devices
- However, AMRES core network links were saturated
  - Someone is overflowing our network, but who ?

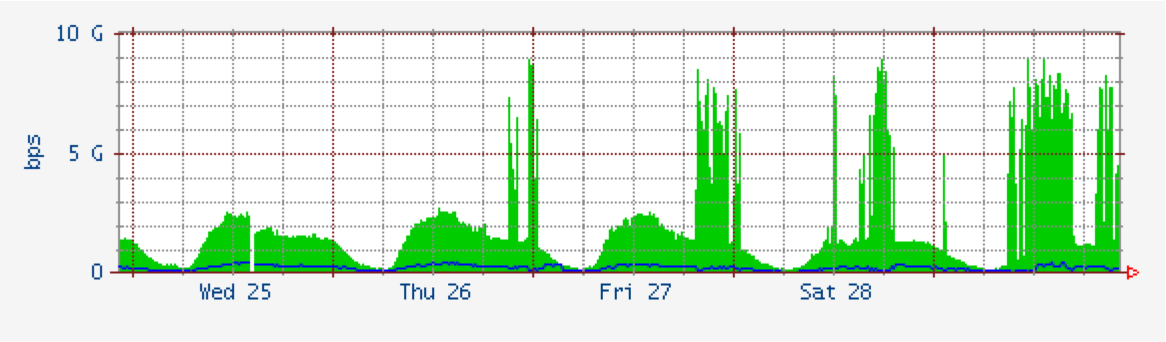
Lesson No. 2 : Set up alarm triggering mechanism on all major links !!!

- After some time, we finaly found the troubling host/customer

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Link saturation

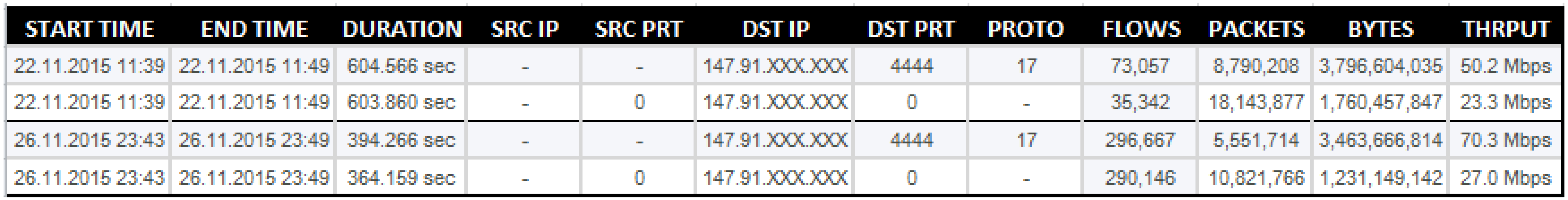
- Our external network links are 10G capacity



CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Attack analysis

- Huge amount of traffic was entering our network
  - Link toward GÉANT was saturated
  - Links toward domestic ISPs were saturated
- Web server was the target of DDoS attack
- Attackers used UDP traffic, random source port, destination port 4444
- Sample of aggregated netflow logs



START TIME	END TIME	DURATION	SRC IP	SRC PRT	DST IP	DST PRT	PROTO	FLOWS	PACKETS	BYTES	THRPUT
22.11.2015 11:39	22.11.2015 11:49	604.566 sec	-	-	147.91.XXX.XXX	4444	17	73,057	8,790,208	3,796,604,035	50.2 Mbps
22.11.2015 11:39	22.11.2015 11:49	603.860 sec	-	0	147.91.XXX.XXX	0	-	35,342	18,143,877	1,760,457,847	23.3 Mbps
26.11.2015 23:43	26.11.2015 23:49	394.266 sec	-	-	147.91.XXX.XXX	4444	17	296,667	5,551,714	3,463,666,814	70.3 Mbps
26.11.2015 23:43	26.11.2015 23:49	364.159 sec	-	0	147.91.XXX.XXX	0	-	290,146	10,821,766	1,231,149,142	27.0 Mbps

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Solution ?

- No point in blocking the traffic on our end since the volume of incoming traffic exceeds the bandwidht on external links
- Traffic should be blocked in the neighbouring networks with higher capacities

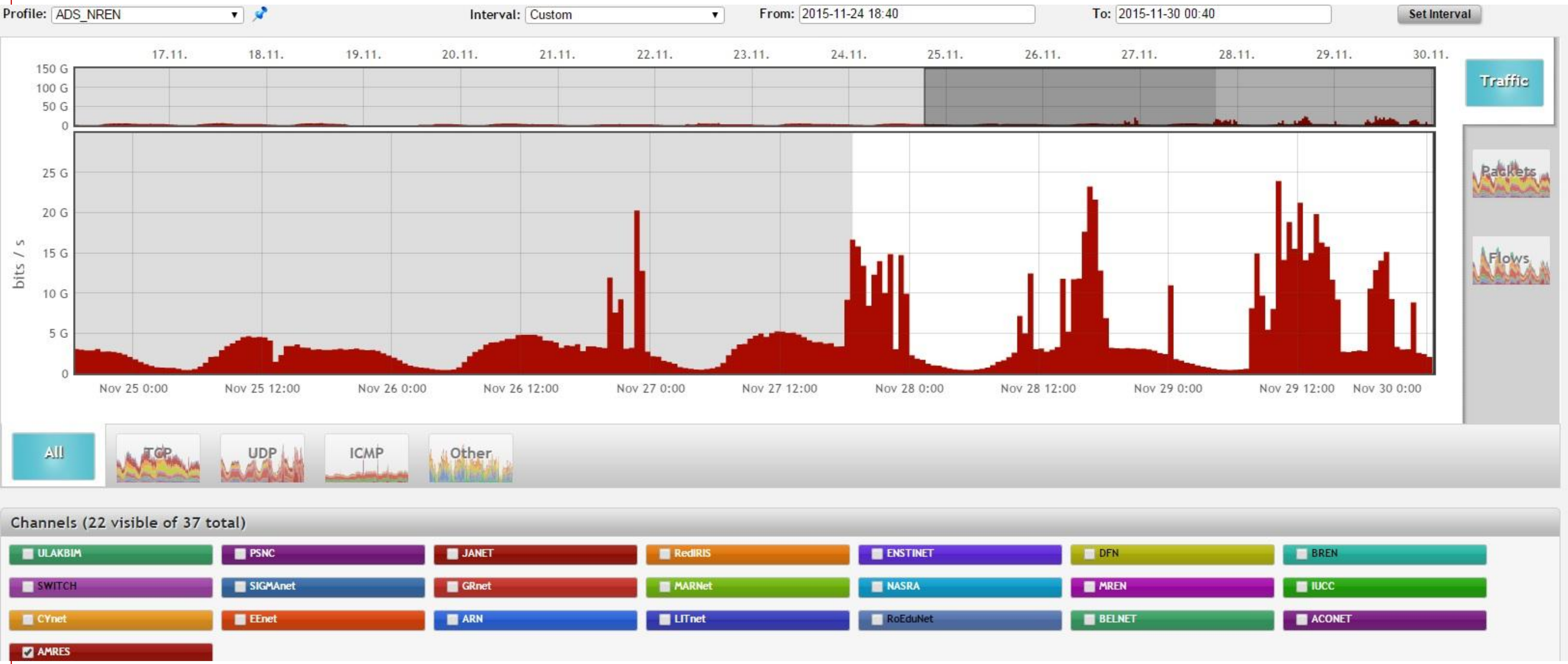
Lesson No. 3 : Keep the good relationship with your neighbouring ISPs !!!

DANUBE REGION strategy START Danube Region Project Fund

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

DDoS attack volume

- Graphs provided by GEANT – neighbouring ISP



Profile: ADS_NREN

Interval: Custom

From: 2015-11-24 18:40

To: 2015-11-30 00:40

Set Interval

Channels (22 visible of 37 total)

□ ULAKBIM □ PSNC □ JANET □ RedIRIS □ ENSTINET □ DFN □ BREN

□ SWITCH □ SIGMAnet □ GRnet □ MARNet □ NASRA □ MREN □ IUCC

□ CYnet □ EEnet □ ARN □ LITnet □ RoEduNet □ BELNET □ ACONET

☑ AMRES

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Coordination

AMRES
Serbian Academic Network

- GÉANT reacted quickly and blackholed traffic destined to the targeted web server
  - Firewall on Demand is a great service in these situations
  - Domestic ISPs were little bit slower
- Our network became operational once again…
  - Until the customer decided to change the IP address of a web server
  - The attackers targeted the DNS name of the web server
  - Let’s dance again…

Lesson No. 4 : Maintain the good communication channel with the customer and coordinate actions !!!

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Final Solution

- Simply blackholing the traffic isn’t the final solution
- The attack needs to be stopped at the source
- It is important to notify the networks which are the source of the attack
- Around 55,000 different IP addresses were involved in this attack
  - Find the abuse contact
  - Find the log lines which prove the attack
  - Send the generic e-mail with the log lines attached

Lesson No. 5 : Deploy the solution which will automatically send reports on DDoS attack !!!

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Reports about DDoS attack

- We managed to generate reports manualy for all domestic IPs used in this attack
- Arround 5,000 domestic Ips were involved
- 10 domestic ISPs were source of attack
- Each report had: IP adresses involved, matching log lines and request to block this traffic
- Network admins didn’t know what actions to take
- Eventualy majority patched and cleaned their systems (PCs, NAT routers etc.)

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

End of Attack

- Attack was active for more than 45 days
- This happens when CSIRT is unable to send generlic e-mail reports to the networks which are source of attack
- Buying specialized equipment for dealing with this type od DDoS is not effective
- Subscription for DDoS protection service might be the good solution

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

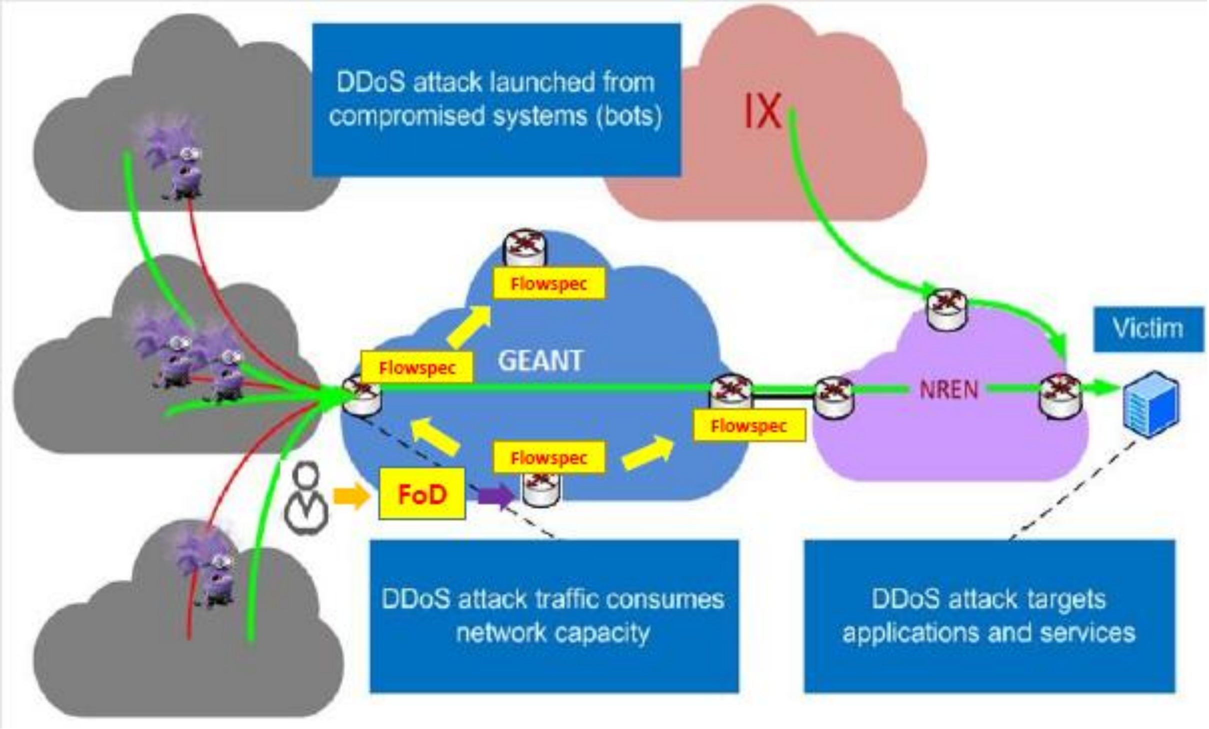
Firewall on Demand

- Service offered by GEANT
- NRENs have access to a specialized portal
    - Route blackholing can be implemented
    - Firewall filters for particular source and destination addresse can be made
- Use of BGP flowspec capability on Juniper routers
- Rules defined on portal are pushed to the GEANT backbone network effectively blocking the unwanted traffic

DANUBE REGION strategy START Danube Region Project Fund

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Firewall on Demand


DDoS attack launched from compromised systems (bots)
IX
Flowspec
Flowspec
GEANT
Flowspec
Flowspec
FoD
NREN
Victim
DDoS attack traffic consumes network capacity
DDoS attack targets applications and services

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Conclusions

- Have the alarm trigering mechanisms in network monitoring system
- Keep the good relationships with the neighbouring ISPs
- Keep the good communication channel with the customers and always coordinate actions
- Deploy the solution that will automatically generate reports on DDoS attack and send it to respecive abuse contacts
- Think about DDoS protection services offered by commercial or academic sector

DANUBE REGION strategy START Danube Region Project Fund

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Questions & Answers?

CS Danube (Cyber Security in Danube Region) project is supported by START Programme within the EU strategy for Danube Region.