

3rd NMRG Meeting

1st Large-scale network measurement



DDoS as a \$ervice

Jair Santanna
University of Twente



Flamingo
EU FP7

What?

SLOWLORIS



SSYN

(E,X,Z)



RUDY



SUDP



UDP-LAG



ARM

(ARME)



SMURF



DNS



GET



POST



CHARGEN



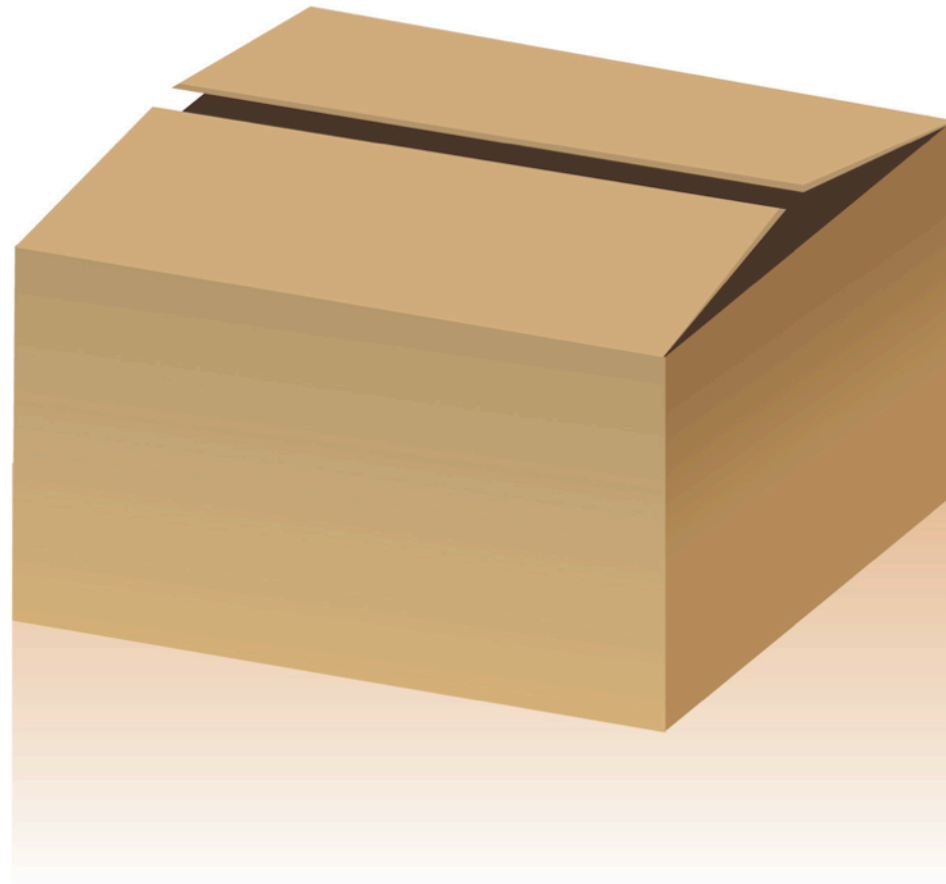
HEAD



What?



What?



What?

DDoS as a
\$ervice



Booter
DDoS
DDoS-to-hire
Stresser

What?

Why?



PayPal



Why?

A lot of traffic found by:



Hired by Gamers



Hired by Students

Why?

*Offer up to 25Gbps
for less than \$4*

Why?

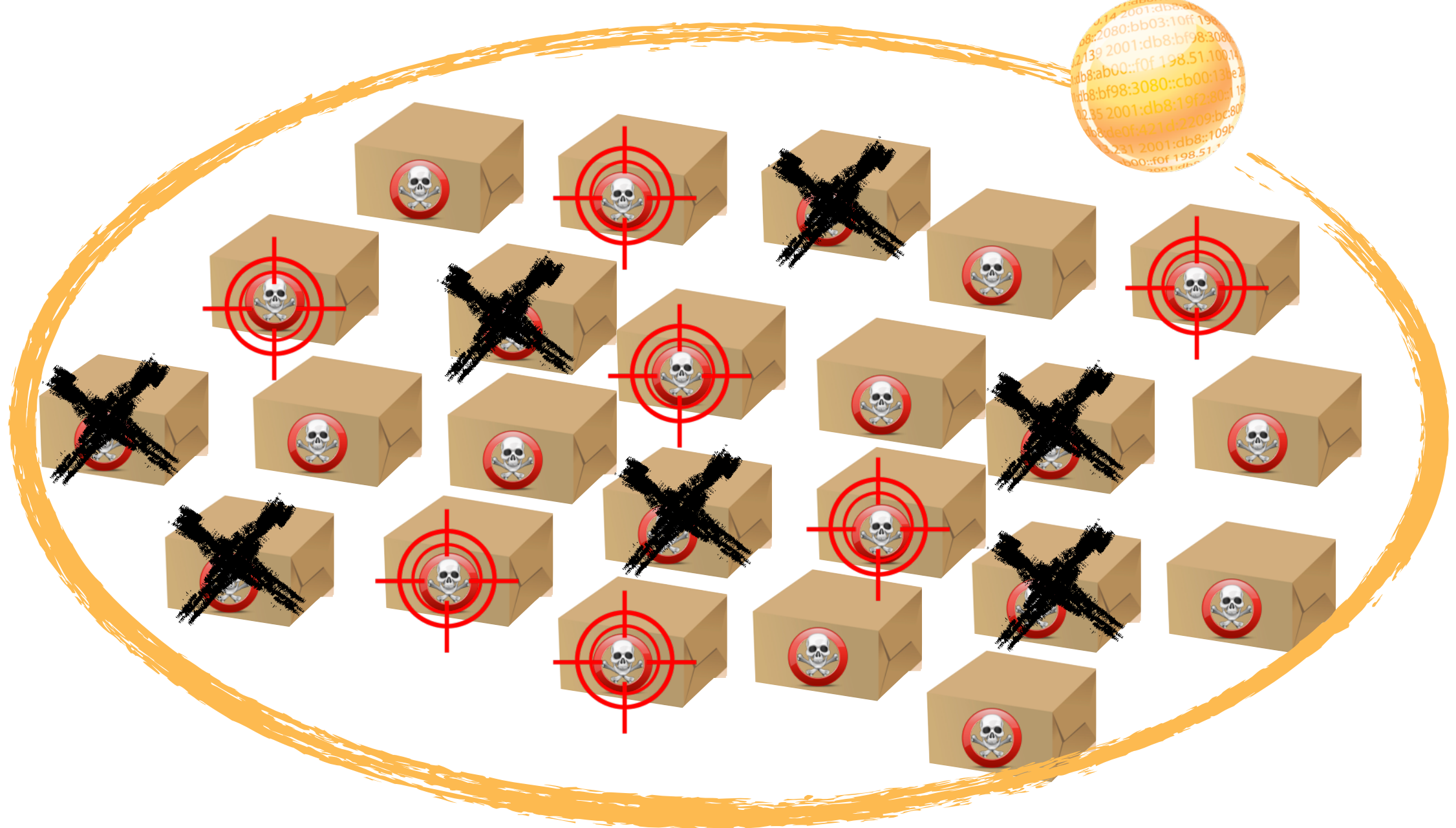
*Banks | UT
4Gb/s | 10Gb/s*

Goal

Understand
**Fingerprint and Mitigate*

Goal

How?



39 Mapped
14 Hired

23 Online
16 ~~Online~~

How?

Results

 Mapped  Hired

20 Probes
*since April

#	Description	%	
0	Online	~59% (23/39)	~64%(25/39)
1	Change the IP address once or more	~82% (32/39)	
2	Protected by the same DDoS Protection Service (offered by CloudFlare)	~74% (29/39)	
3	**CDN-like	~0,05 (2/39)	

Results


Mapped

#	DDoS as a Service	Offer [Gbps]	price [€]	Attacks based on	Peak Delivered [Gb]	Average Traffic Delivered [Gbps]	IPs involved *
1	http://booter.tw	?	10,90	*DNS	0,07	0,05	8.280
2	http://restricted-stresser.info	5	1,95	*DNS	1,22	0,54	7.369
3	http://anonymous-stresser.net	5	3,12	*DNS	0,38	0,26	6.075
4	http://destressbooter.com	25	3,89	*DNS	0,72	0,32	4.486
5	http://flashstresser.net	?	3,89	?	3,0	0,83	3.779
6	http://dejabooter.com	10	3,89	*DNS	1,1	0,65	2.970
7	http://rebel-security.com	up to 3	3,00	*Chargen	1,0	0,32	281
8	http://grimboot.com	6	3,90	*DNS	0,37	0,22	78
9	http://quantumbooter.net	1,5	8,00	*DNS	0,37	0,34	54
10	http://olympusstresser.org		4,90				33.372 *27.289
11	http://ebooter.5gbfree.com		free				
12	http://vdoss.net		3,11				
13	http://respawn.ca		3,90				
14	http://onionstresser.com		3,90				
			€58,35				

Results


Hired

<http://booter.tw>



<http://restricted-stresser.info>



<http://anonymous-stresser.net>



Cheaper and more Powerful

<http://destressbooter.com>



<http://flashstresser.net>



<http://dejabooter.com>



<http://rebel-security.com>



<http://grimboot.com>



<http://quantumbooter.net>

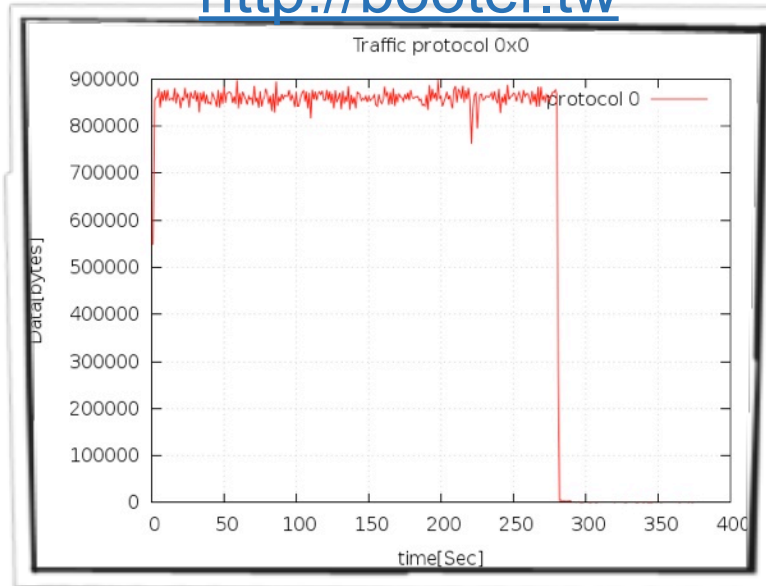


Results

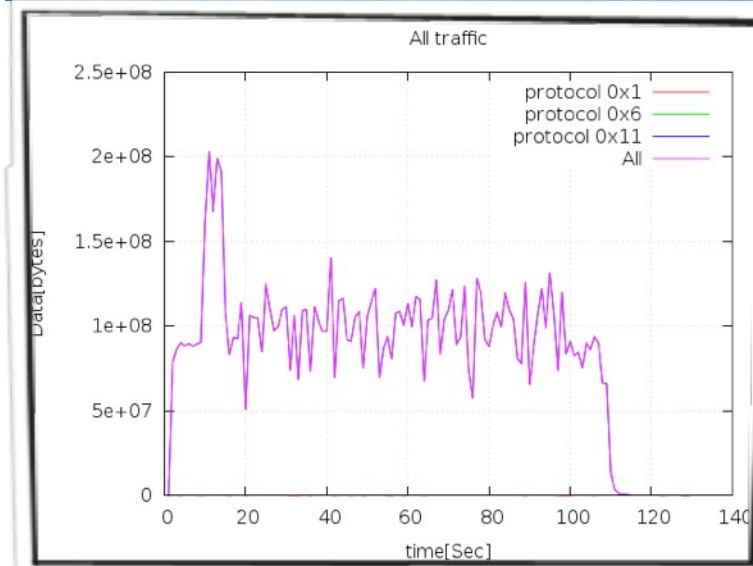
Hilbert Curve
representation


Hired

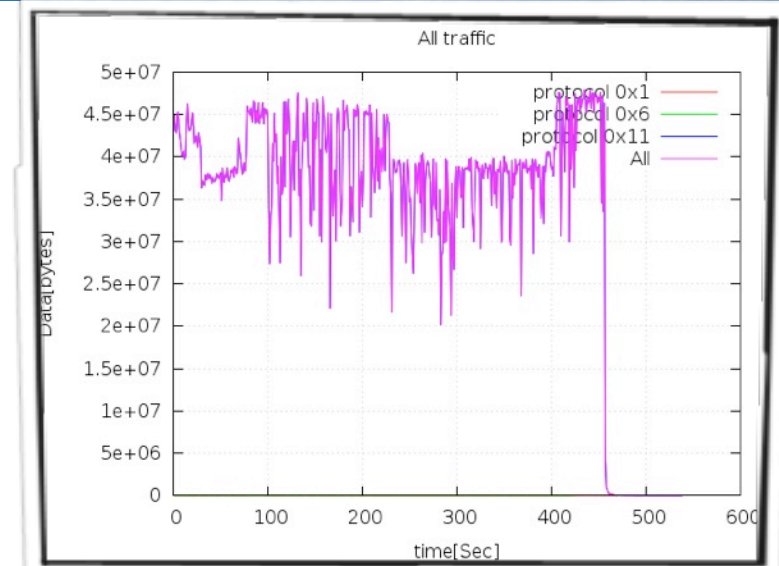
<http://booter.tw>



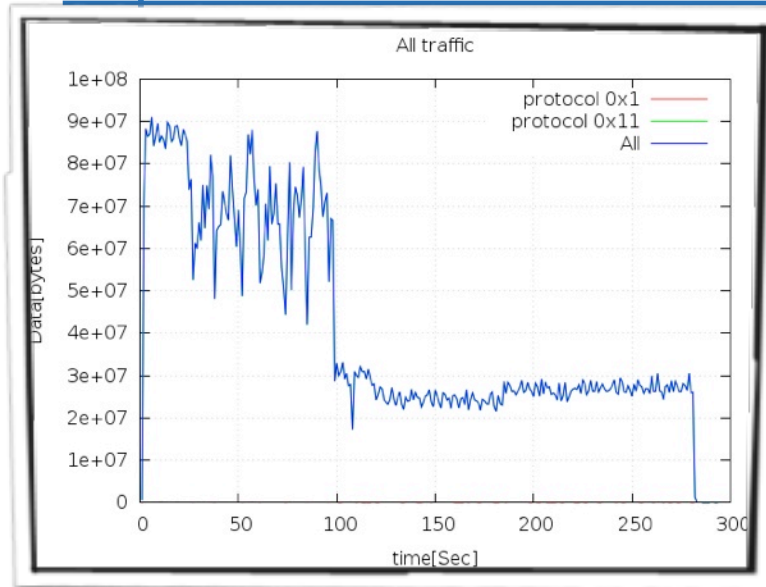
<http://restricted-stresser.info>



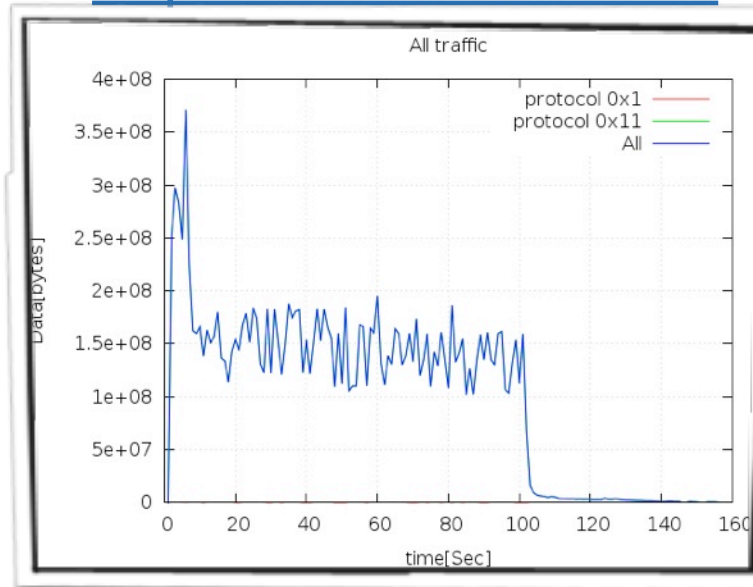
<http://anonymous-stresser.net>



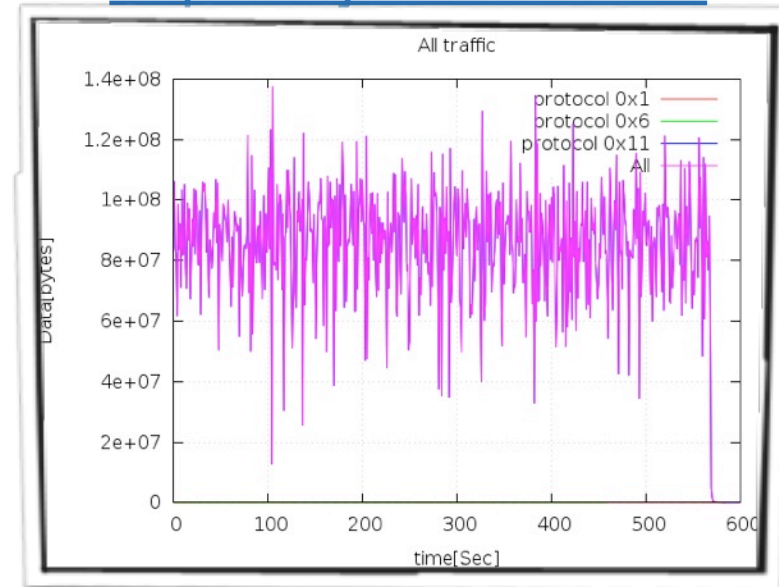
<http://destressbooter.com>



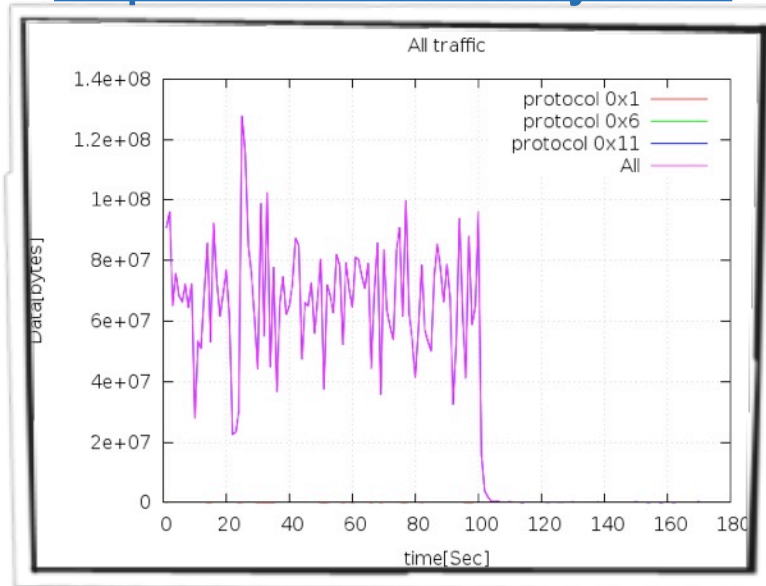
<http://flashstresser.net>



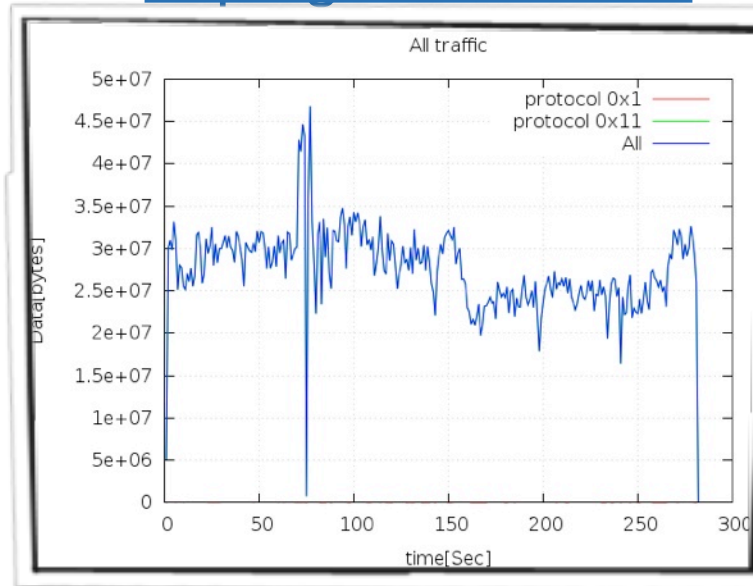
<http://dejabooter.com>



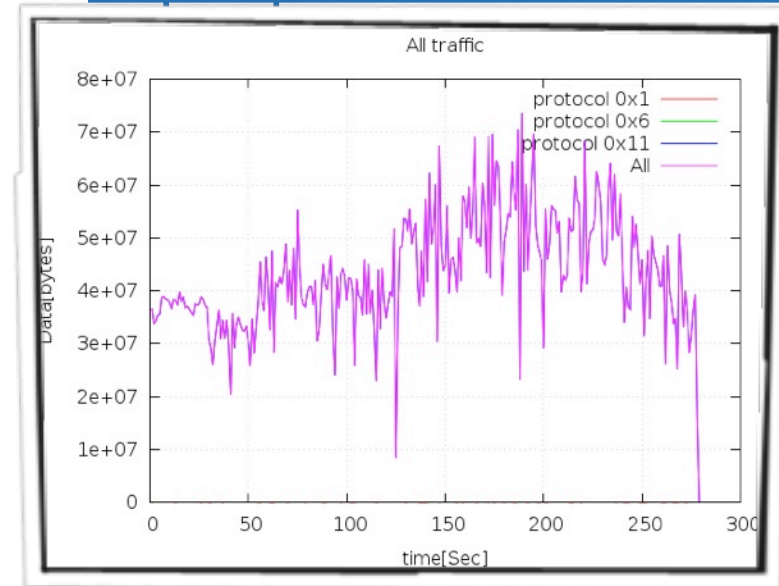
<http://rebel-security.com>



<http://grimboot.com>



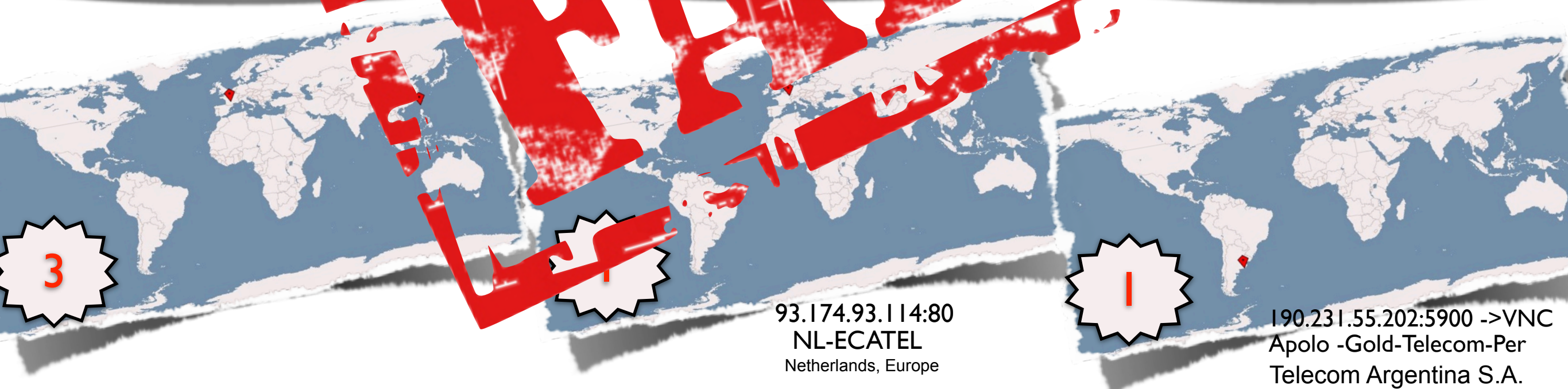
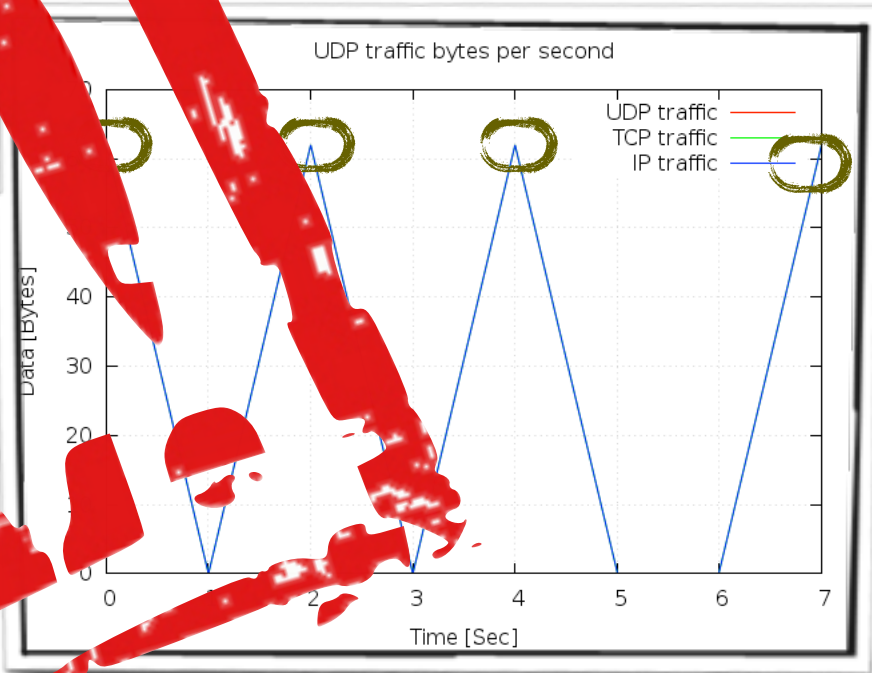
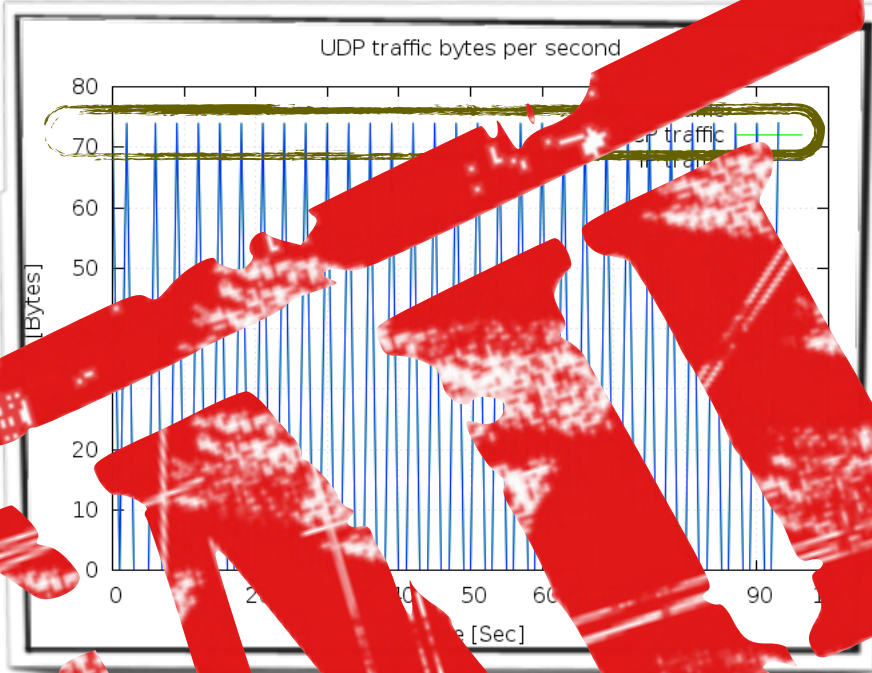
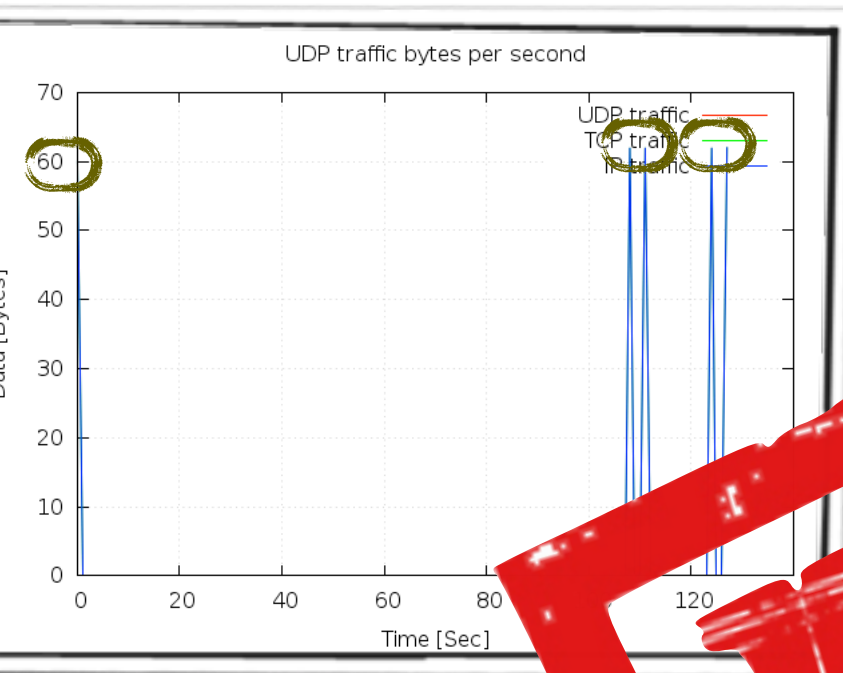
<http://quantumbooter.net>



<http://olympusstresser.org>

<http://vdoss.net>

<http://ebooter.5gbfree.com>



93.174.93.114:80
NL-ECATEL
Netherlands, Europe

190.231.55.202:5900 ->VNC
Apolo -Gold-Telecom-Per
Telecom Argentina S.A.

Results



<http://respawn.ca>



<http://unionsboss.com>



Results


Hired

31st NMRG Meeting

1st NMRG workshop on large scale network measurements

DDoS as a \$ervice

Jair Santanna
University of Twente



Flamingo
EU FP7