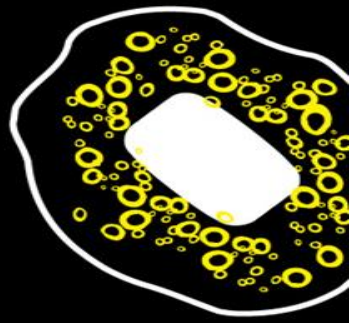
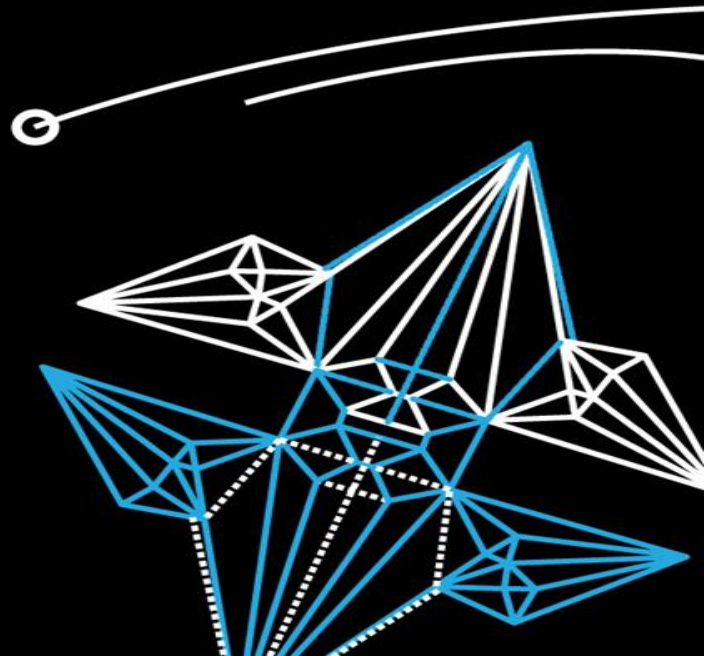
UNIVERSITEIT TWENTE.



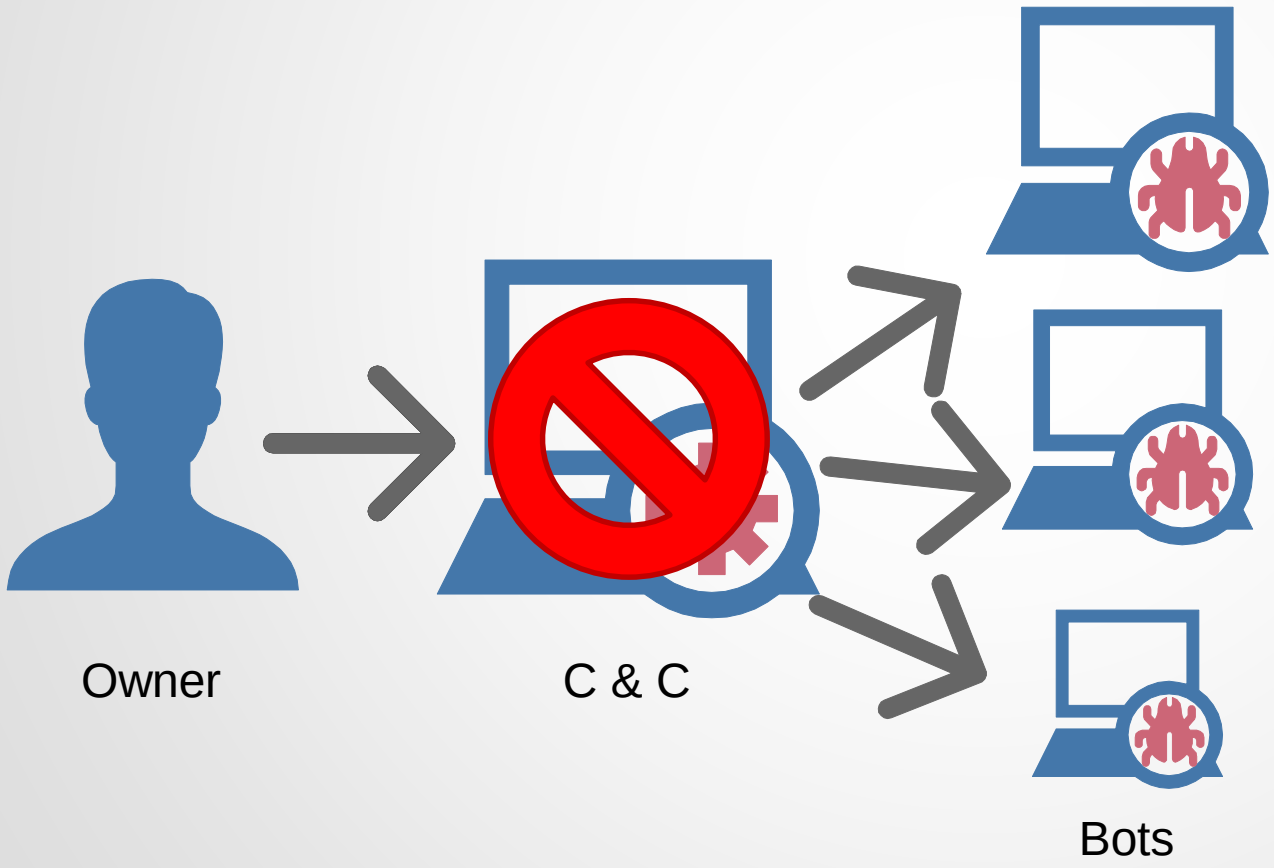
CHARACTERISATION OF THE KELIHOS.B BOTNET

MAX KERKERS, JOSÉ JAIR SANTANNA & ANNA SPEROTTO



WHAT IS A BOTNET?

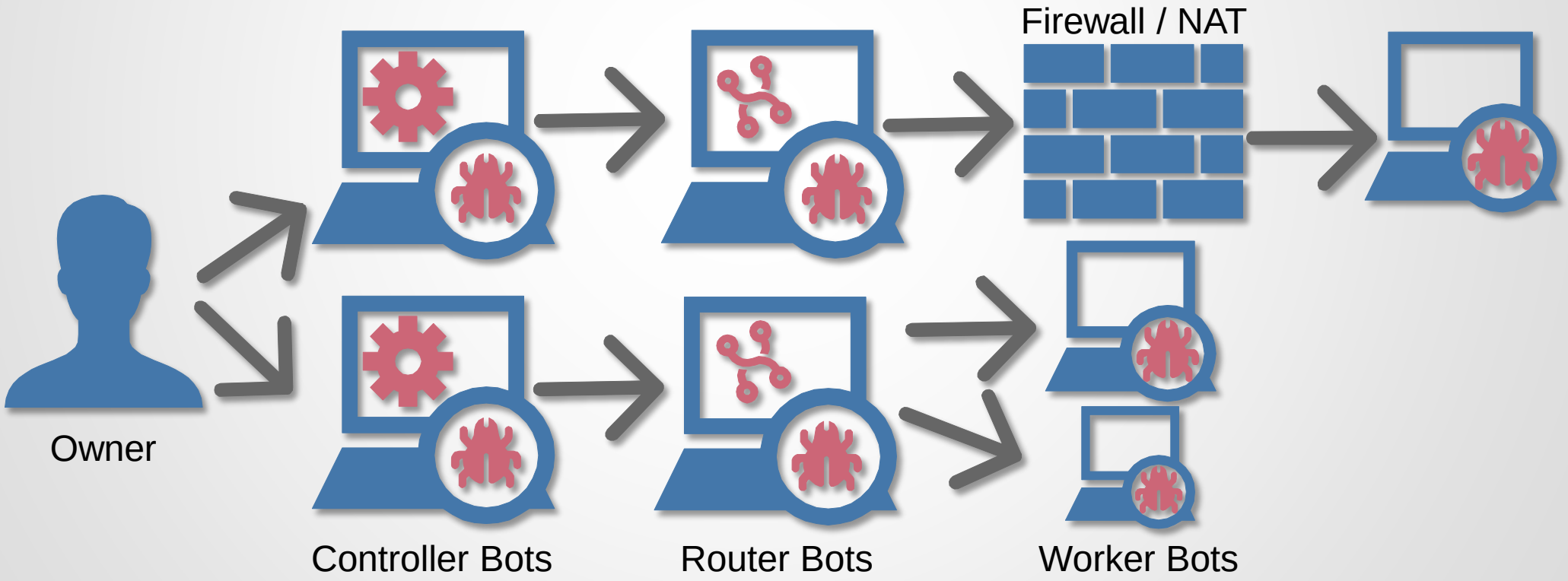
OVERVIEW OF A CLASSICAL BOTNET



WHAT IS A PEER-TO-PEER BOTNET?

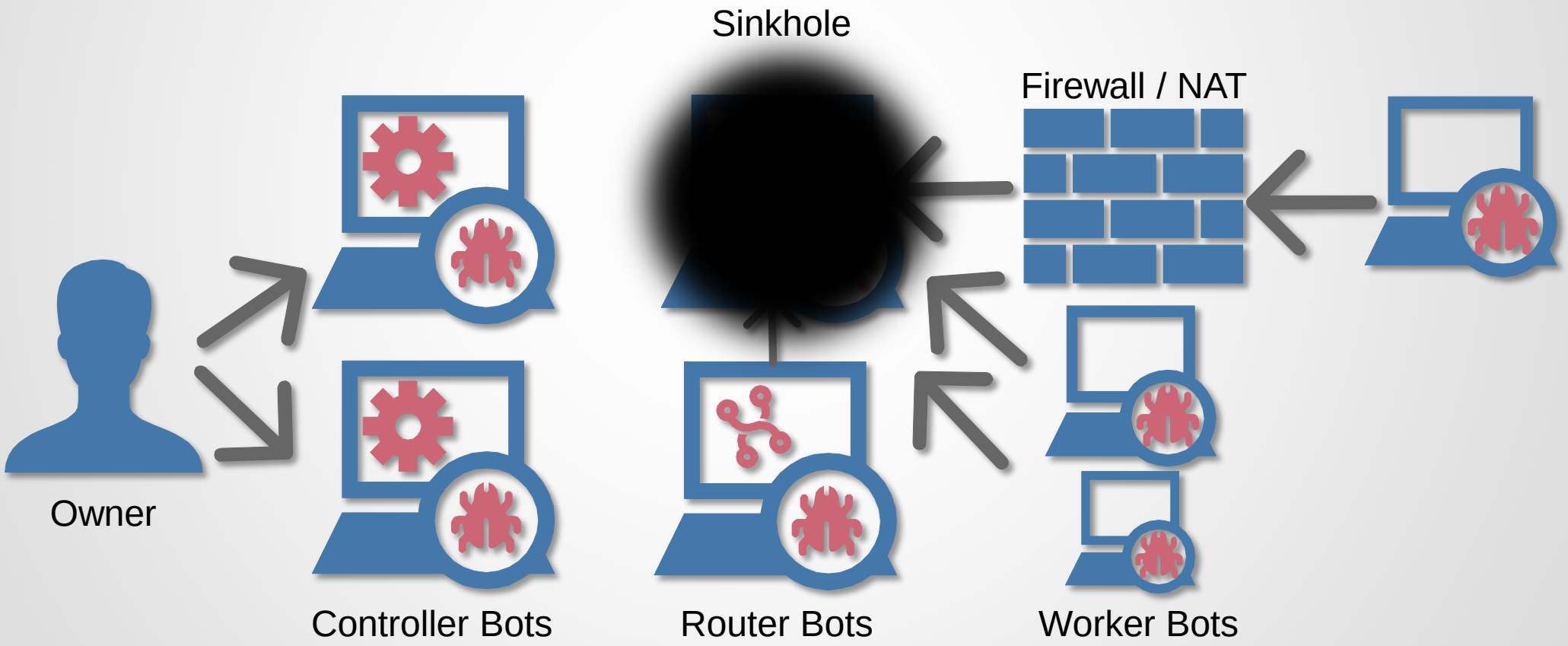
OVERVIEW OF A PEER-TO-PEER BOTNET

Kelihos.B



WHAT IS SINKHOLING?

HOW WAS KELIHOS.B SINKHOLED?



RESEARCH QUESTIONS

What are the characteristics of the sinkholed Kelihos.B botnet?

What is the overall behaviour of the Kelihos.B botnet?

What is the temporal behaviour of the Kelihos.B botnet?

WHAT DATA WAS USED?

21 March 2012 - 7 November 2013

593 401 638 requests

Unstructured

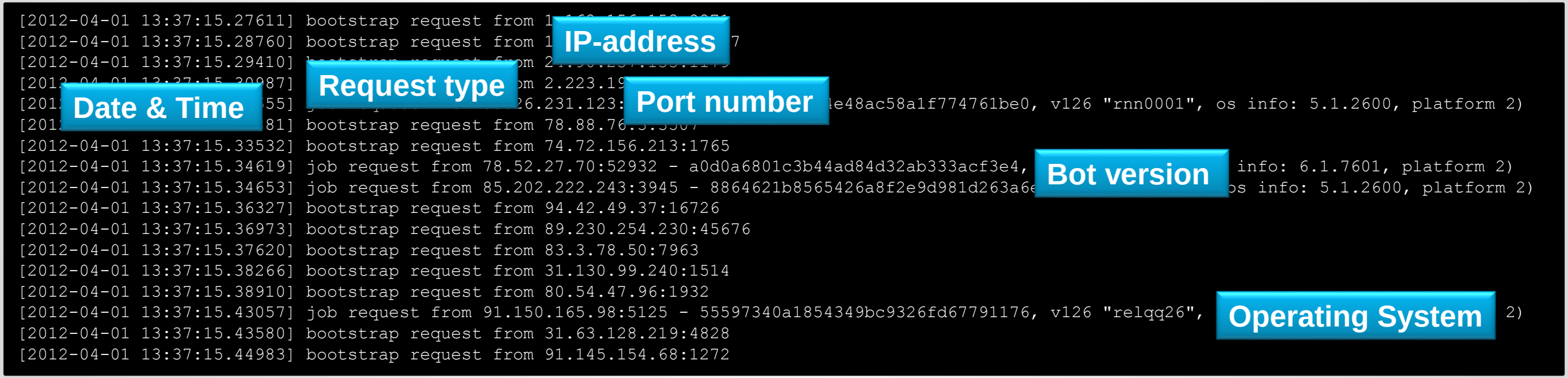

```
[2012-04-01 13:37:15.27611] bootstrap request from 1.162.156.153:2271
[2012-04-01 13:37:15.28760] bootstrap request from 188.230.107.39:2627
[2012-04-01 13:37:15.29410] bootstrap request from 24.90.237.133:1179
[2012-04-01 13:37:15.30987] bootstrap request from 2.223.191.163:51457
[2012-04-01 13:37:15.31655] job request from 83.26.231.123:3211 - 16dd9beba38d4e48ac58a1f774761be0, v126 "rnn0001", os info: 5.1.2600, platform 2)
[2012-04-01 13:37:15.32881] bootstrap request from 78.88.76.3:3507
[2012-04-01 13:37:15.33532] bootstrap request from 74.72.156.213:1765
[2012-04-01 13:37:15.34619] job request from 78.52.27.70:52932 - a0d0a6801c3b44ad84d32ab333acf3e4, v126 "relqq26", os info: 6.1.7601, platform 2)
[2012-04-01 13:37:15.34653] job request from 85.202.222.243:3945 - 8864621b8565426a8f2e9d981d263a6e, v126 "rtce003", os info: 5.1.2600, platform 2)
[2012-04-01 13:37:15.36327] bootstrap request from 94.42.49.37:16726
[2012-04-01 13:37:15.36973] bootstrap request from 89.230.254.230:45676
[2012-04-01 13:37:15.37620] bootstrap request from 83.3.78.50:7963
[2012-04-01 13:37:15.38266] bootstrap request from 31.130.99.240:1514
[2012-04-01 13:37:15.38910] bootstrap request from 80.54.47.96:1932
[2012-04-01 13:37:15.43057] job request from 91.150.165.98:5125 - 55597340a1854349bc9326fd67791176, v126 "relqq26", os info: 5.1.2600, platform 2)
[2012-04-01 13:37:15.43580] bootstrap request from 31.63.128.219:4828
[2012-04-01 13:37:15.44983] bootstrap request from 91.145.154.68:1272
```

WHAT DATA WAS USED?

21 March 2012 - 7 November 2013

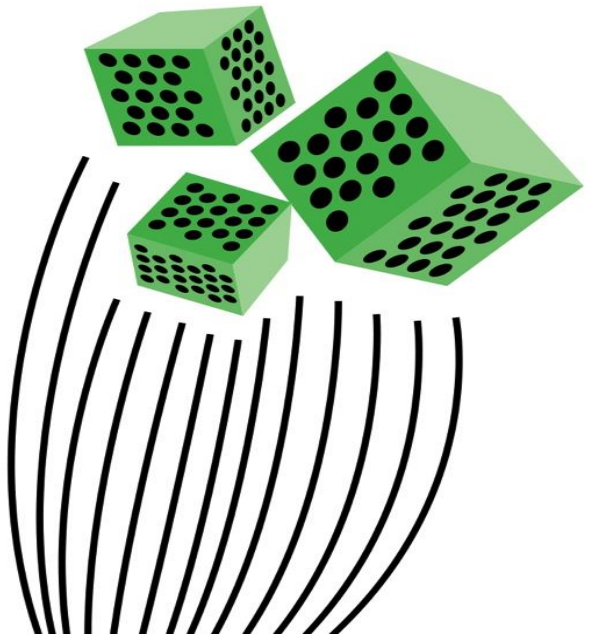
593 401 638 requests

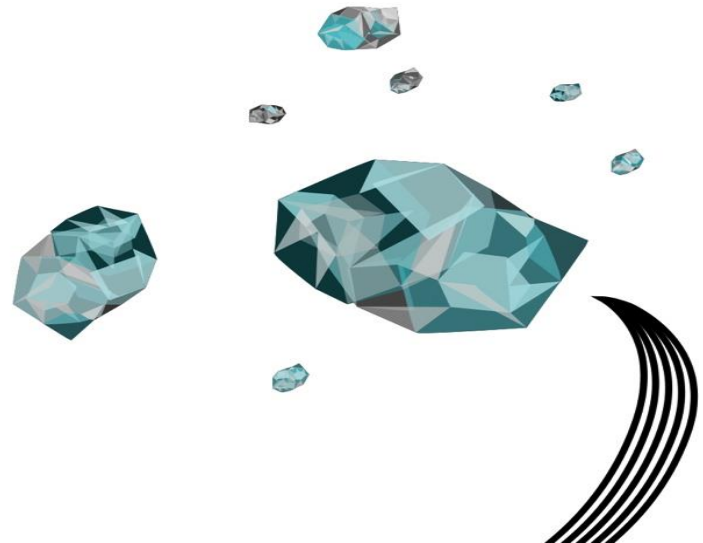
Unstructured



UNIVERSITEIT TWENTE.

OVERALL ANALYSIS

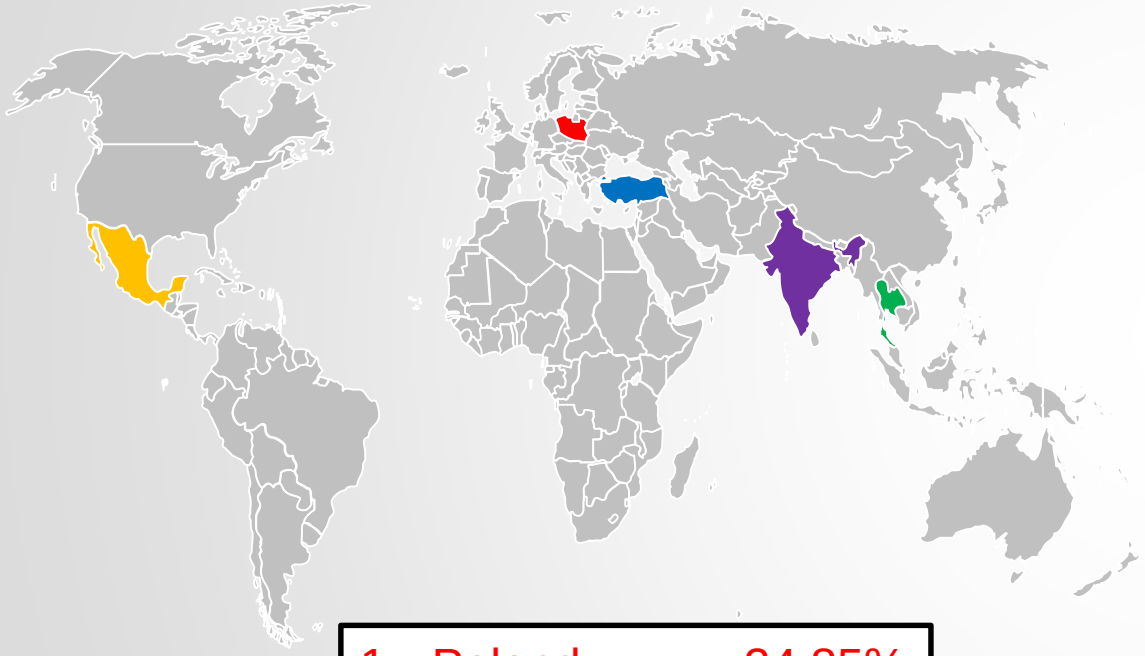




3.7 M unique IP-addresses sending 593.4 M requests

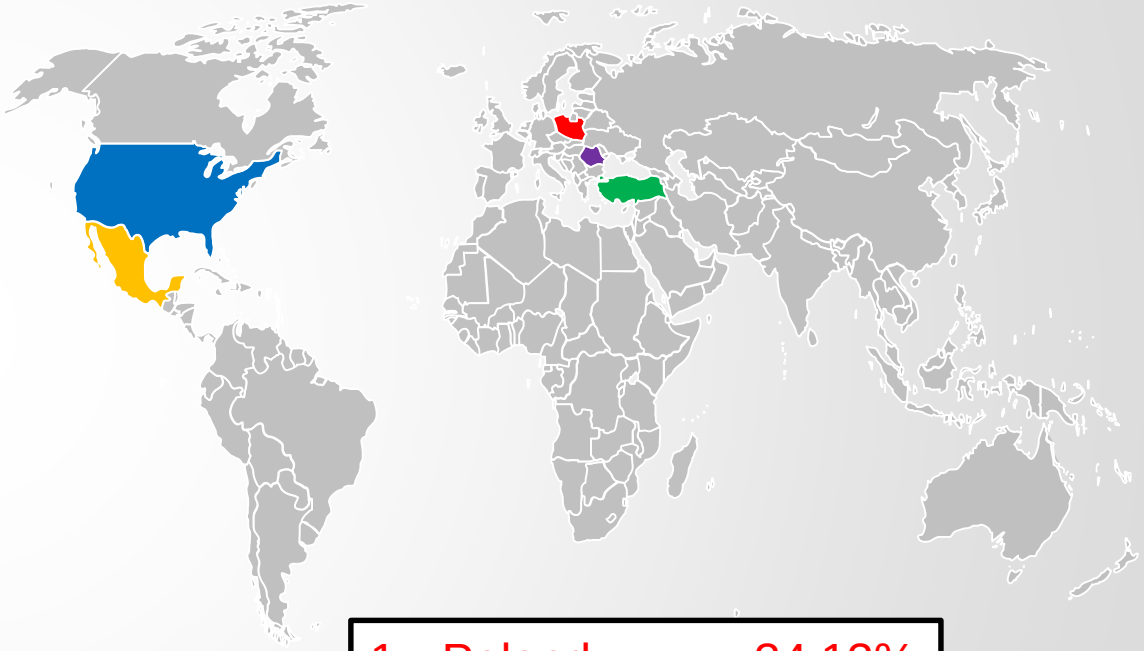
TOP 5'S OF COUNTRIES IN PERCENTAGE OF IP-ADDRESSES & REQUESTS

IP-ADDRESSES



1.	Poland	24.85%
2.	Turkey	11.08%
3.	Thailand	4.76%
4.	India	4.74%
5.	Mexico	4.50%

REQUESTS

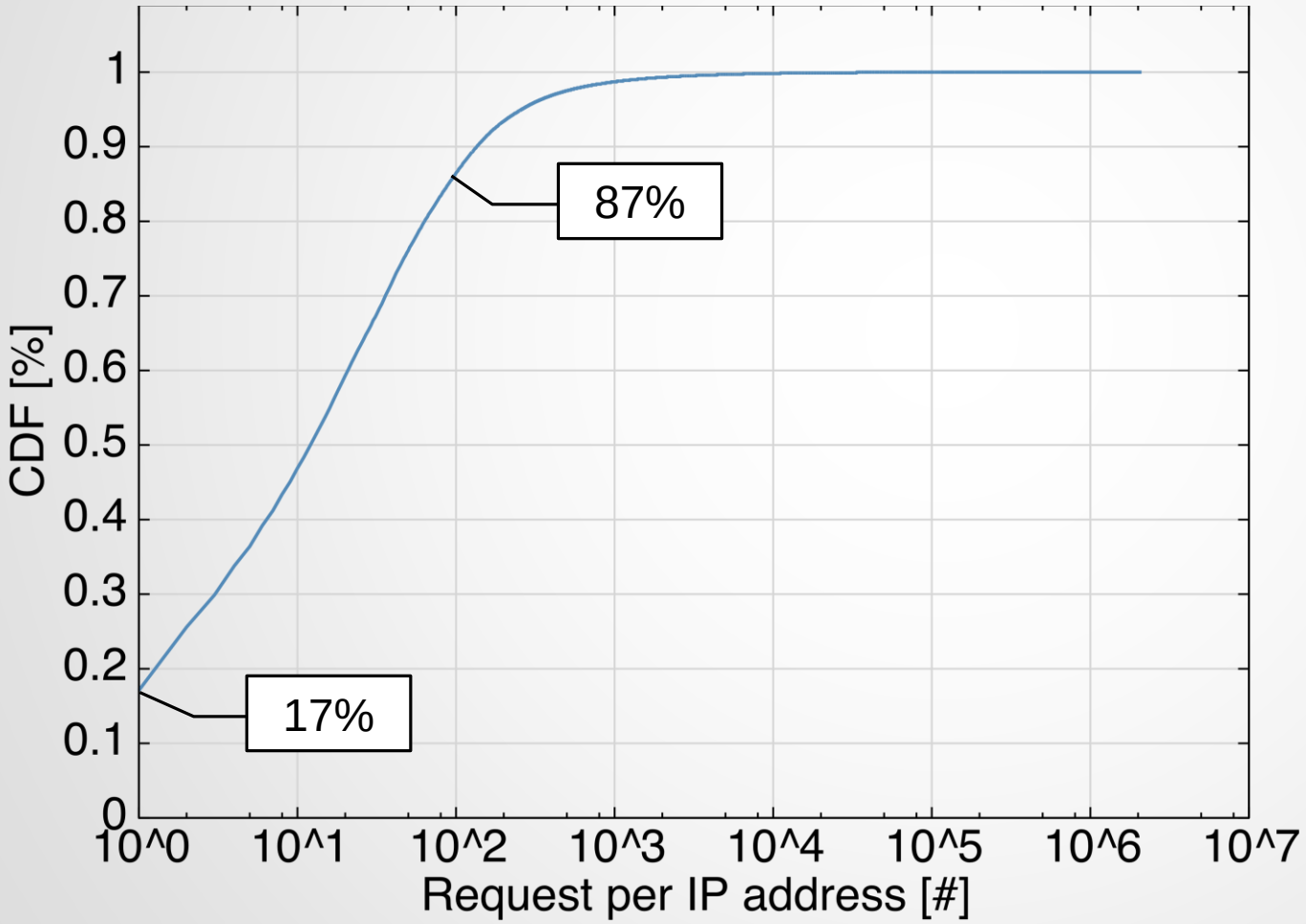


1.	Poland	34.13%
2.	United States	6.97%
3.	Turkey	6.85%
4.	Hungary	3.66%
5.	Mexico	3.38%

AUTONOMOUS SYSTEMS IN PERCENTAGE OF REQUESTS

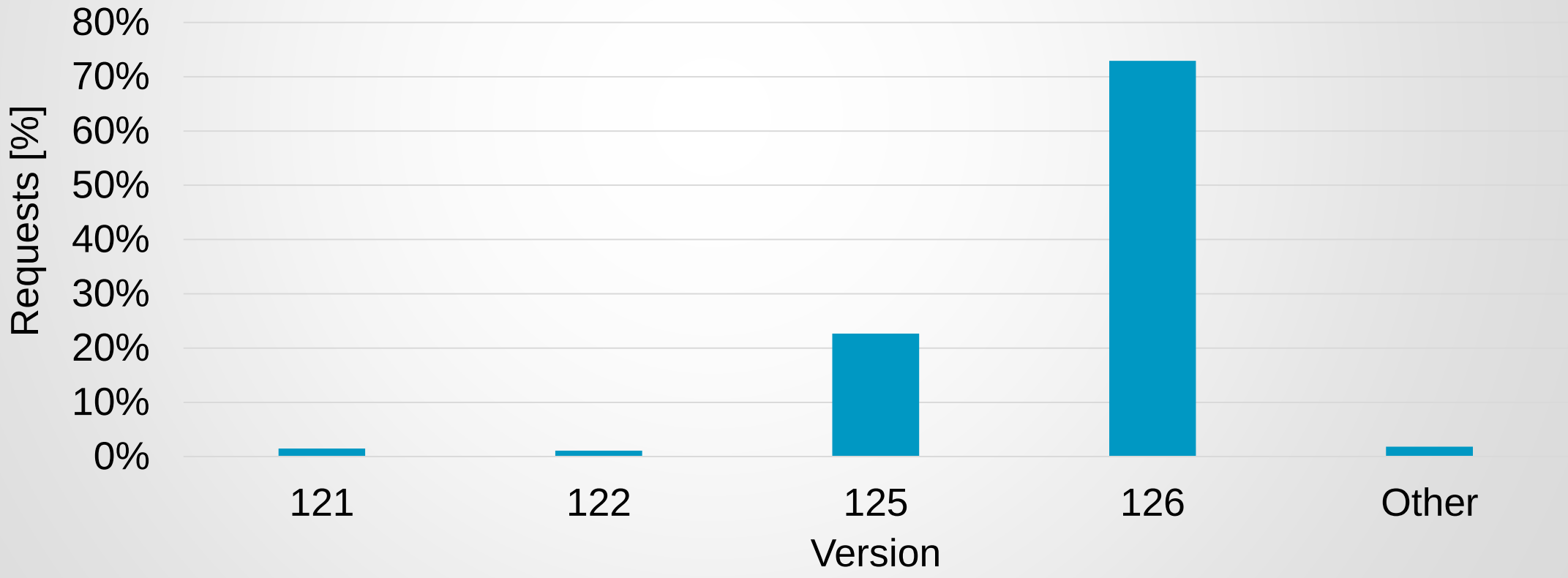
AS	Name	Requests (%)
5617	TPNET Telekomunikacja Polska S.A.	7.28%
9121	TTNET Turk Telekomunikasyon Anonim Sirketi	5.09%
6830	LGI-UPC Liberty Global Operations B.V.	3.78%
29314	VECTRANET-AS VECTRA S.A.	3.23%
21021	MULTIMEDIA-AS Multimedia Polska S.A.	3.20%
12741	INTERNETIA-AS Netia SA	2.50%
7922	COMCAST-7922 - Comcast Cable Communications, Inc.	2.00%
8151	Uninet S.A. de C.V.	1.91%
8048	CANTV Servicios, Venezuela	1.61%
10481	Prima S.A.	1.36%
Others		68.03%

CUMMULATIVE DISTRIBUTION OF THE NUMBER OF REQUESTS PER IP

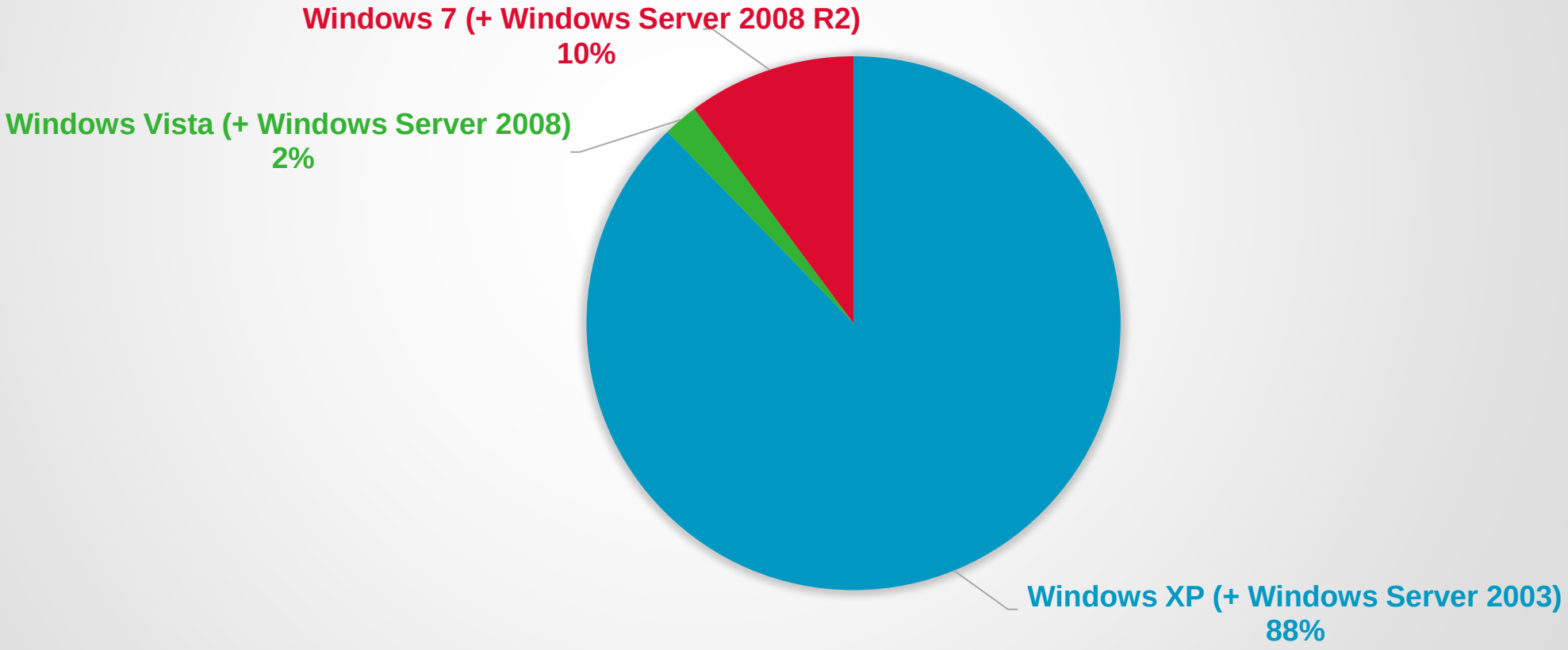


DISTRIBUTION OF REQUESTS PER BOT VERSION

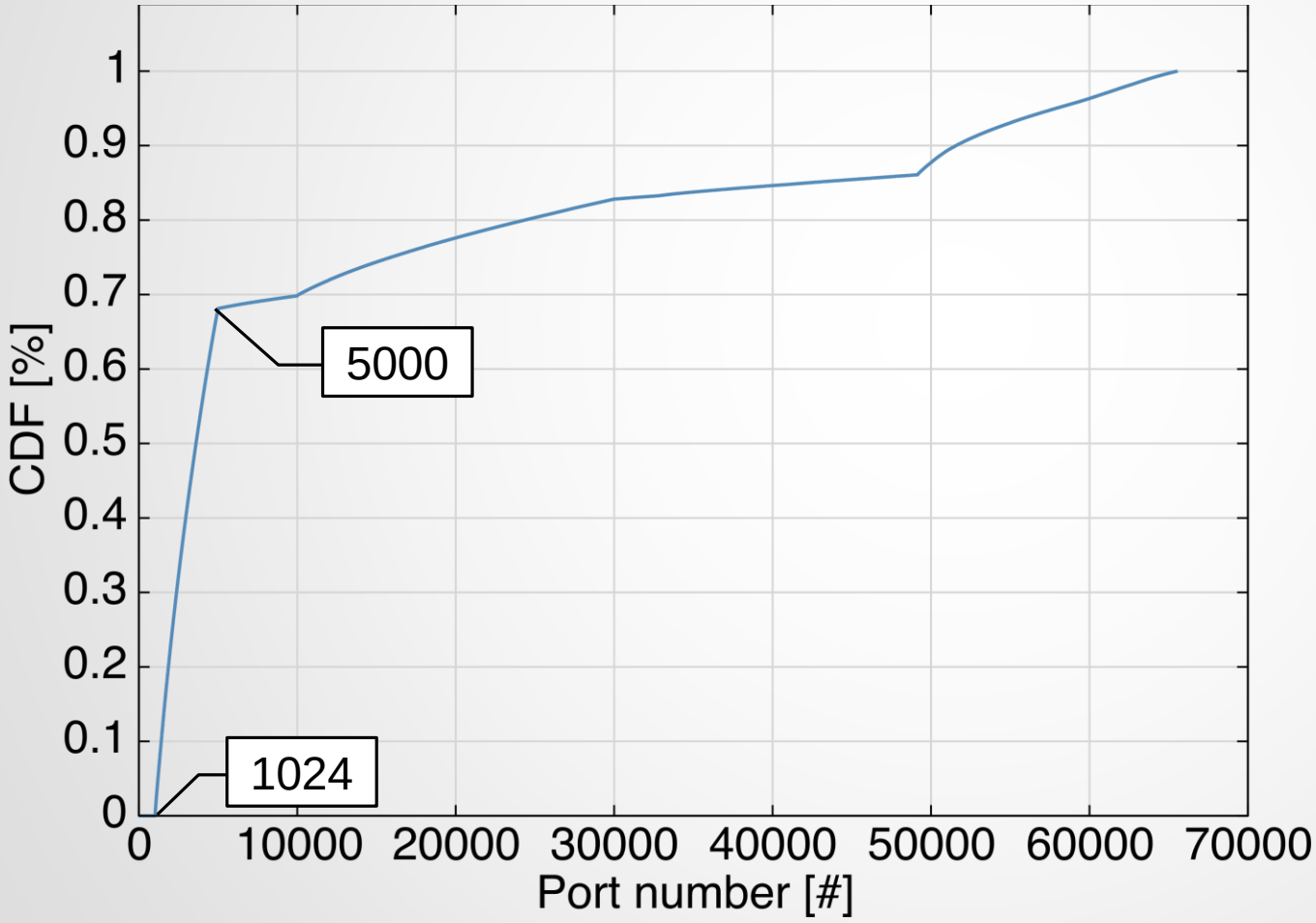
18 versions (111 – 128)



DISTRIBUTION OF OPERATING SYSTEMS

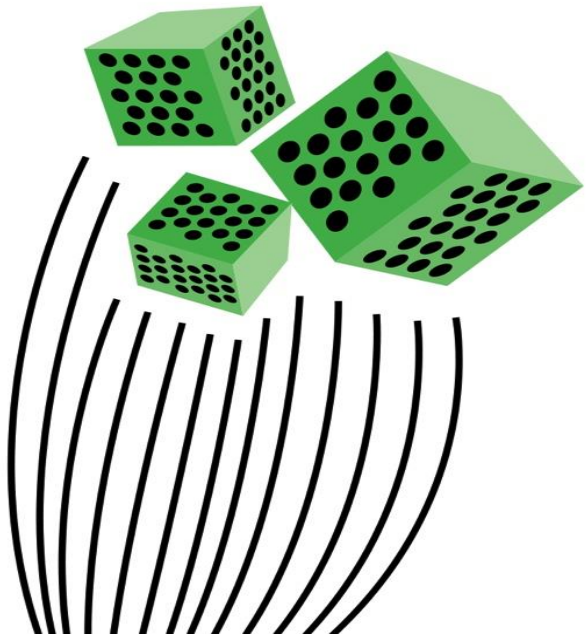


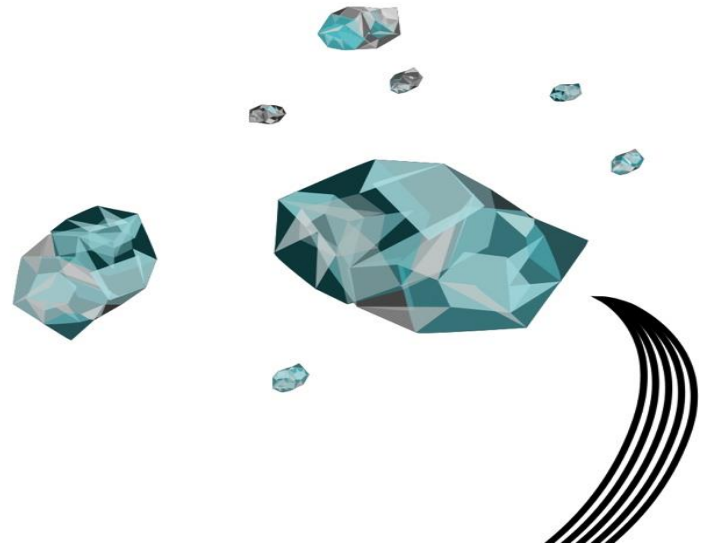
CUMULATIVE DISTRIBUTION OF ORIGINATING PORTS OF REQUESTS



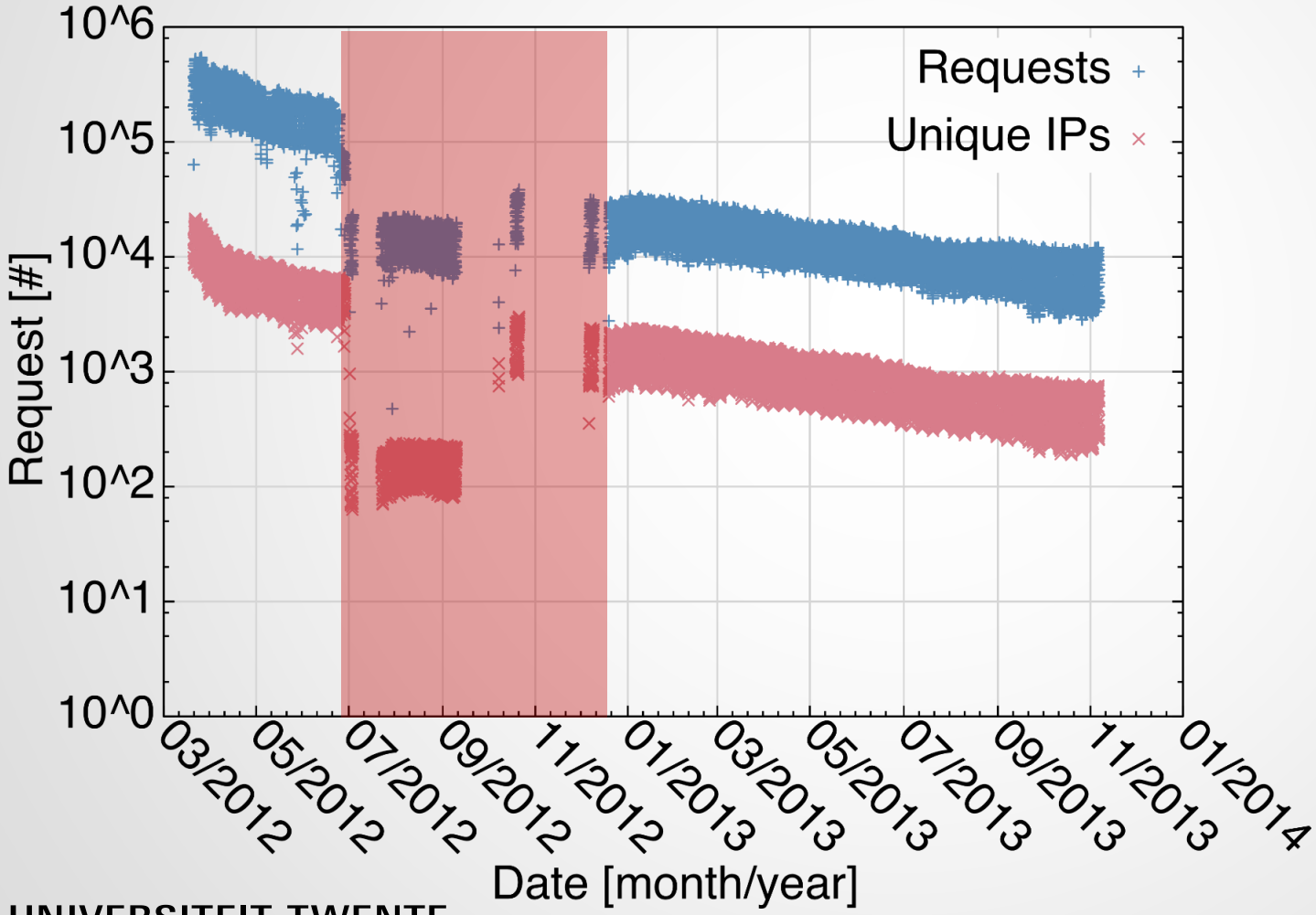
UNIVERSITEIT TWENTE.

TEMPORAL ANALYSIS

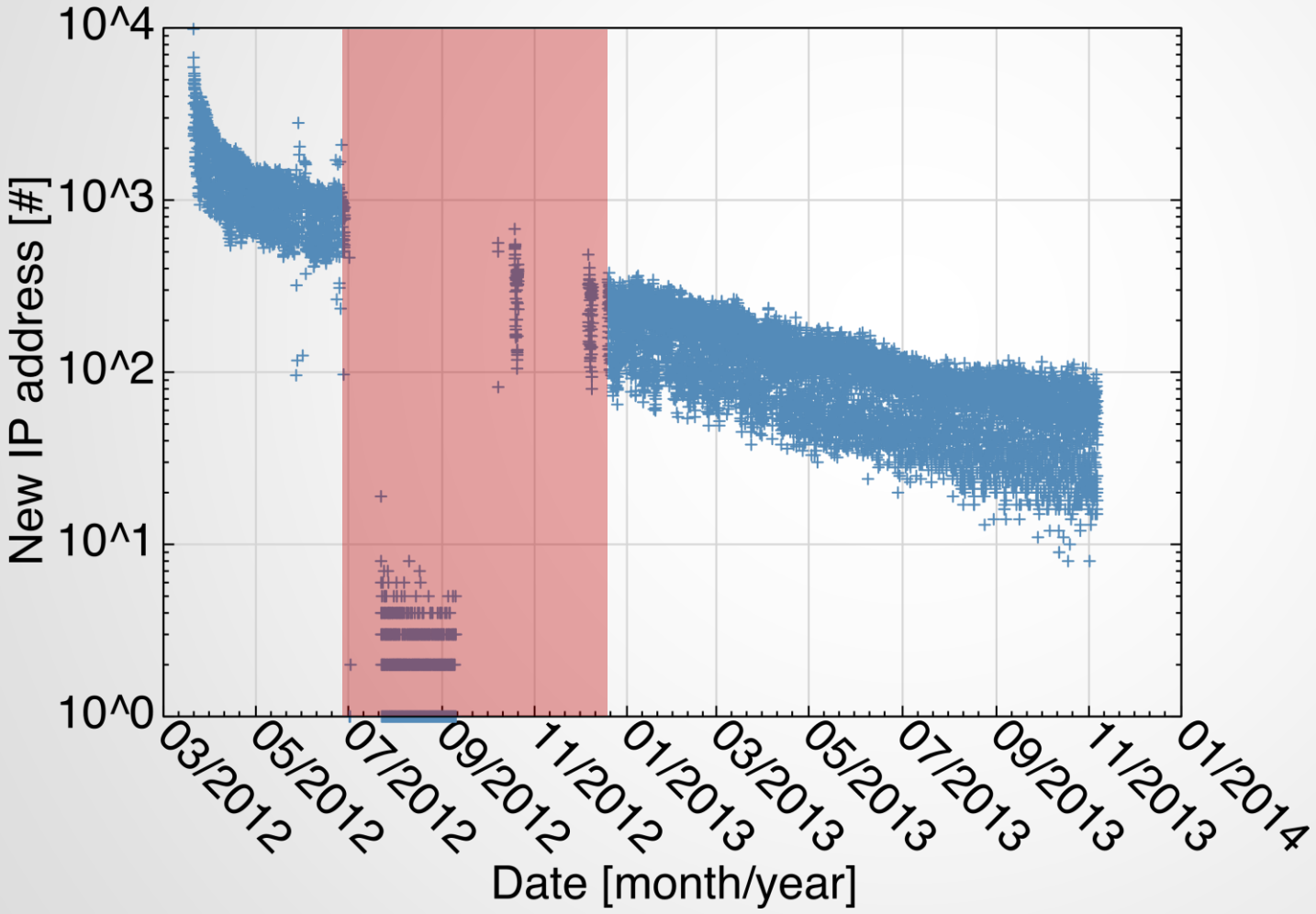




TOTAL NUMBER OF REQUESTS & IP-ADDRESSES PER HOUR



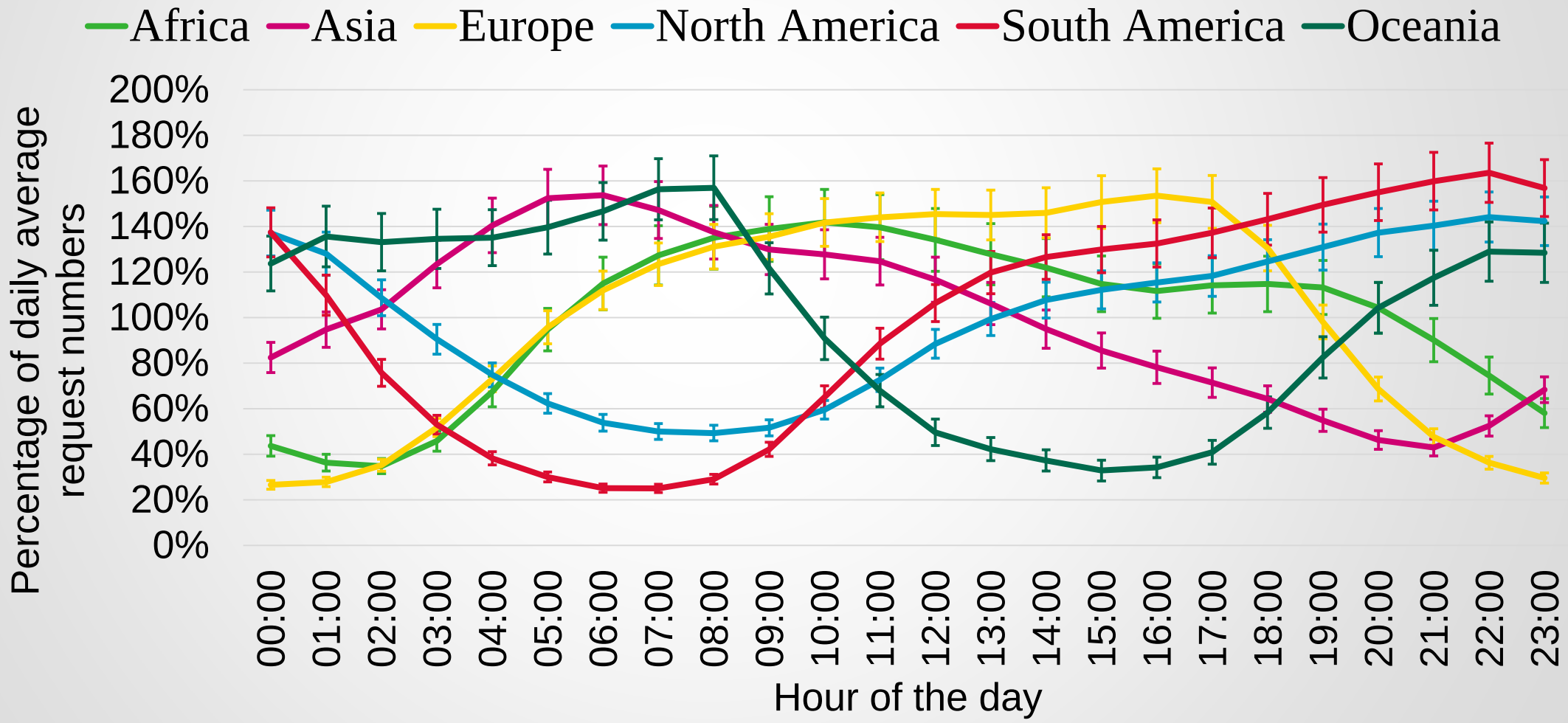
NUMBER OF NEW IP-ADDRESSES PER HOUR & NEW AS'ES PER Q OVER TIME



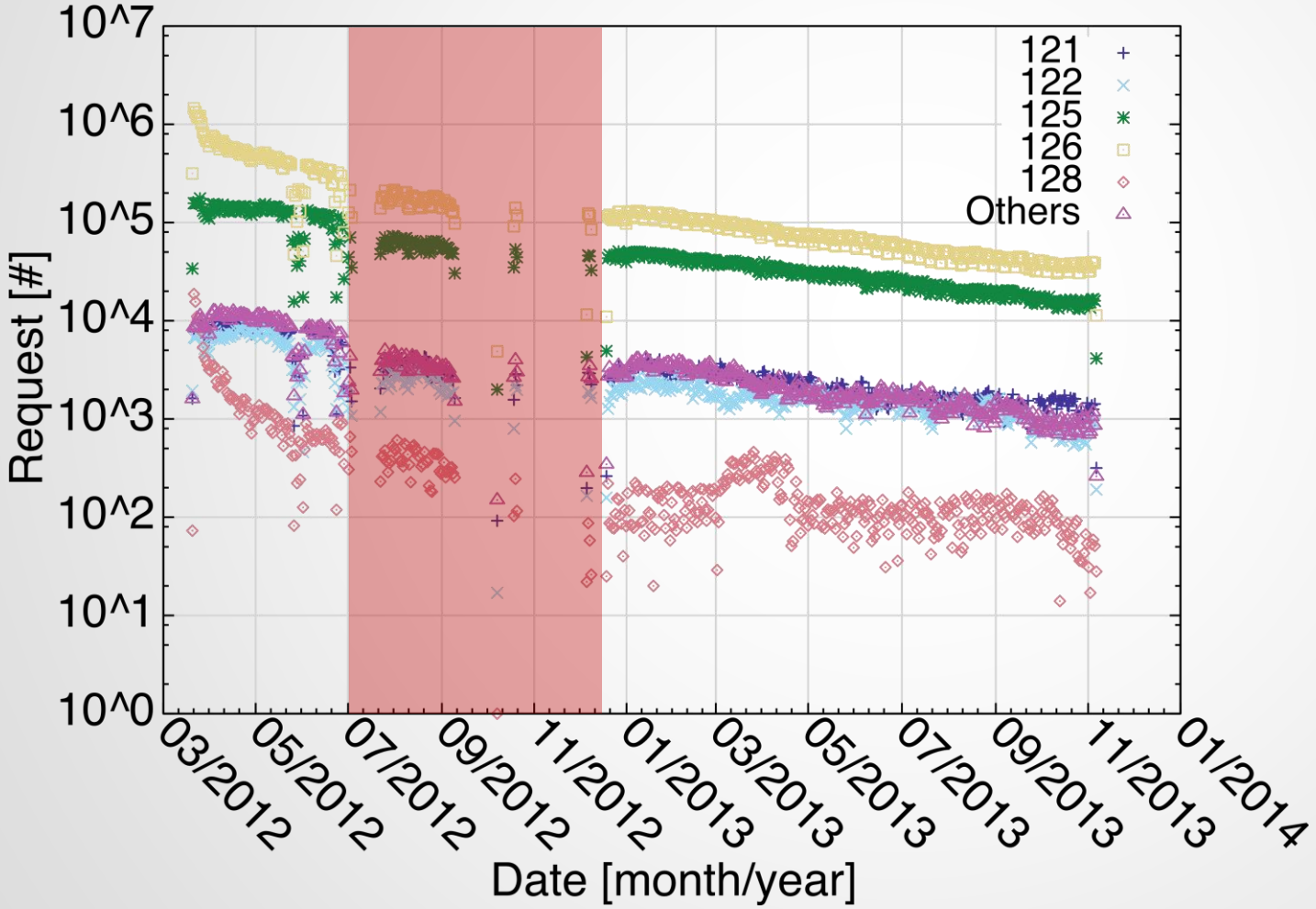
Quarter	Number of new ASes
2012 Q1	4628
2012 Q2	2805
2012 Q3	5
2012 Q4	62
2013 Q1	69
2013 Q2	33
2013 Q3	21
2013 Q4	6

AVERAGE NUMBER OF REQUESTS PER HOUR OF THE DAY PER CONTINENT

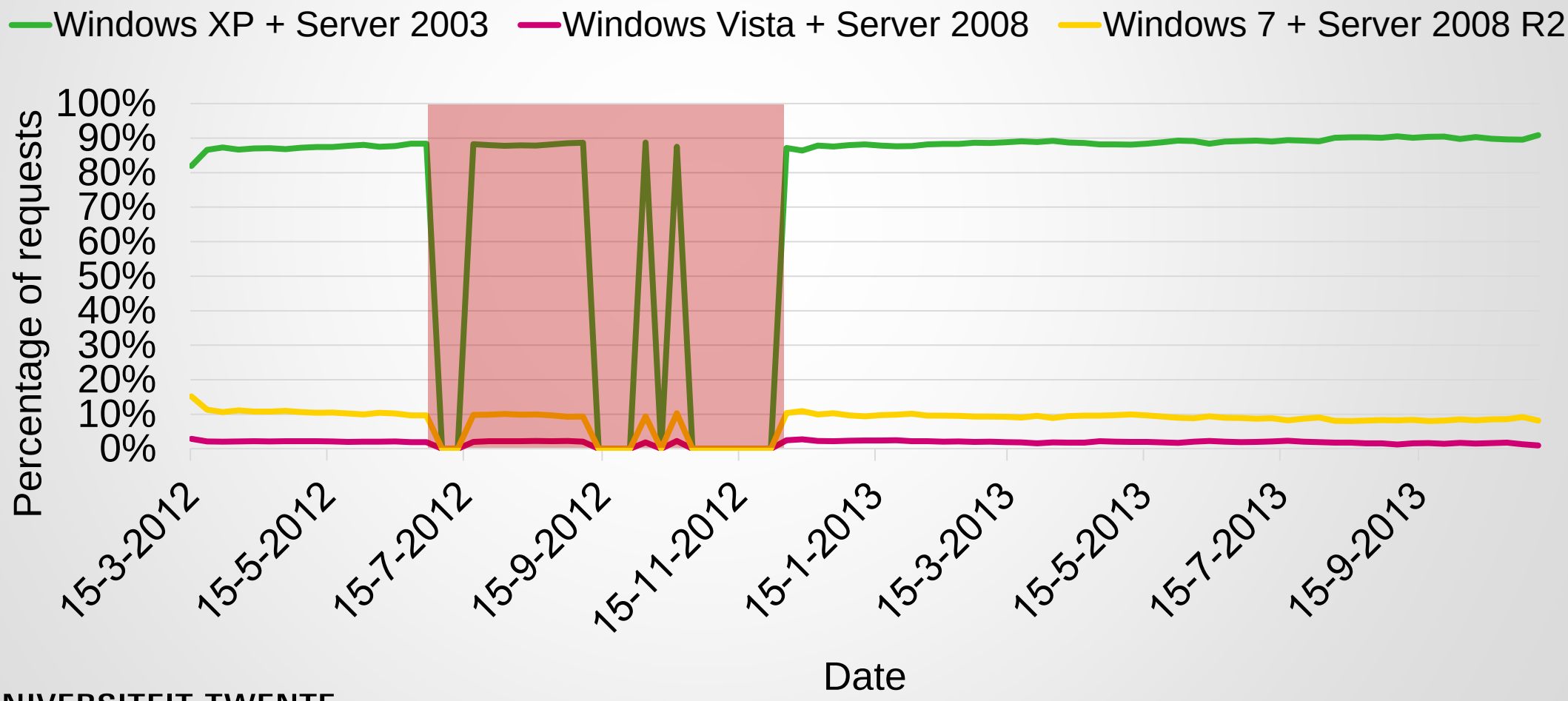
NORMALISED BY THE AVERAGE NUMBER OF REQUESTS PER CONTINENT



NUMBER OF REQUESTS FROM VERSION NUMBER OF BOTS PER DAY



PERCENTAGE OF USED OPERATING SYSTEMS FOR REQUESTS PER WEEK



CONCLUSION

Thank you for your attention!

QUESTIONS?