Coordinated Distributions Method for Tracking Botnets Sending out Spam

Andrey Bakhmutov

Kaspersky Lab

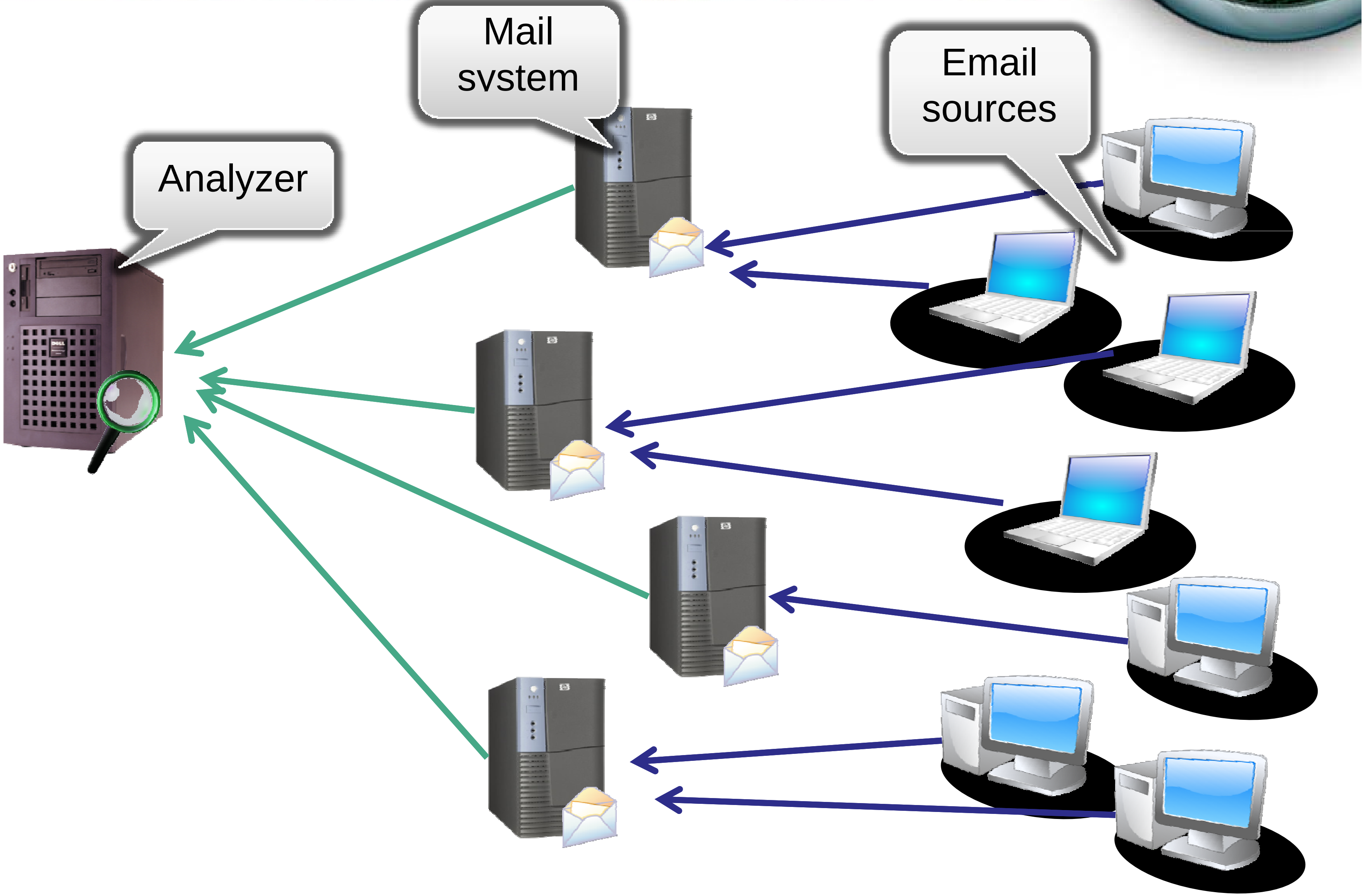
Andrey.Bakhmutov@kaspersky.com

Botnets and spam distributions

Botnets and spam distributions are closely tied together and benefit from each other

- Due to their immense size, combined with dynamically changeable IP addresses, botnets are a powerful tool for spam distribution.

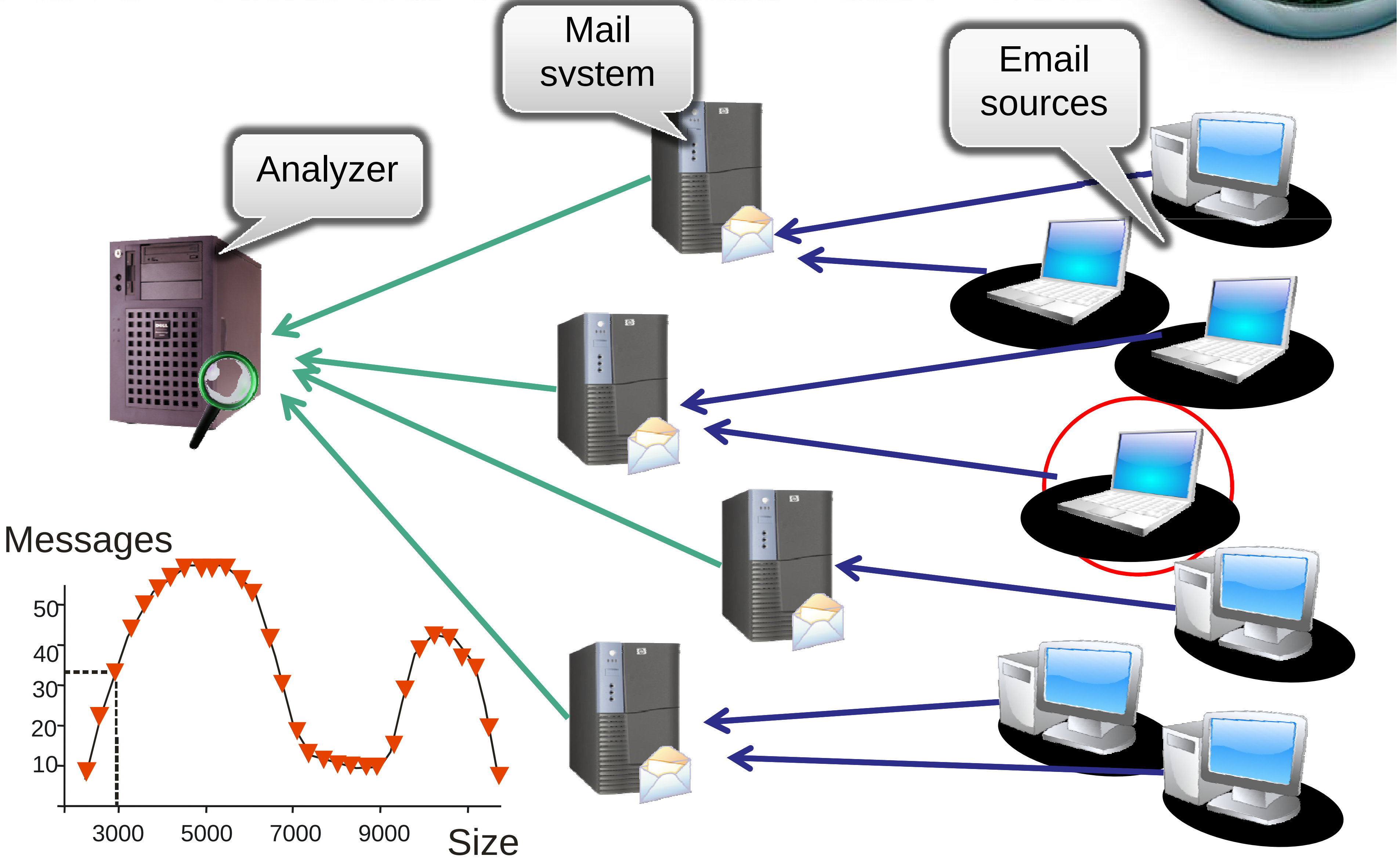
- Distributing spam messages with malicious content results in larger botnets.



Mail svstem

Email sources

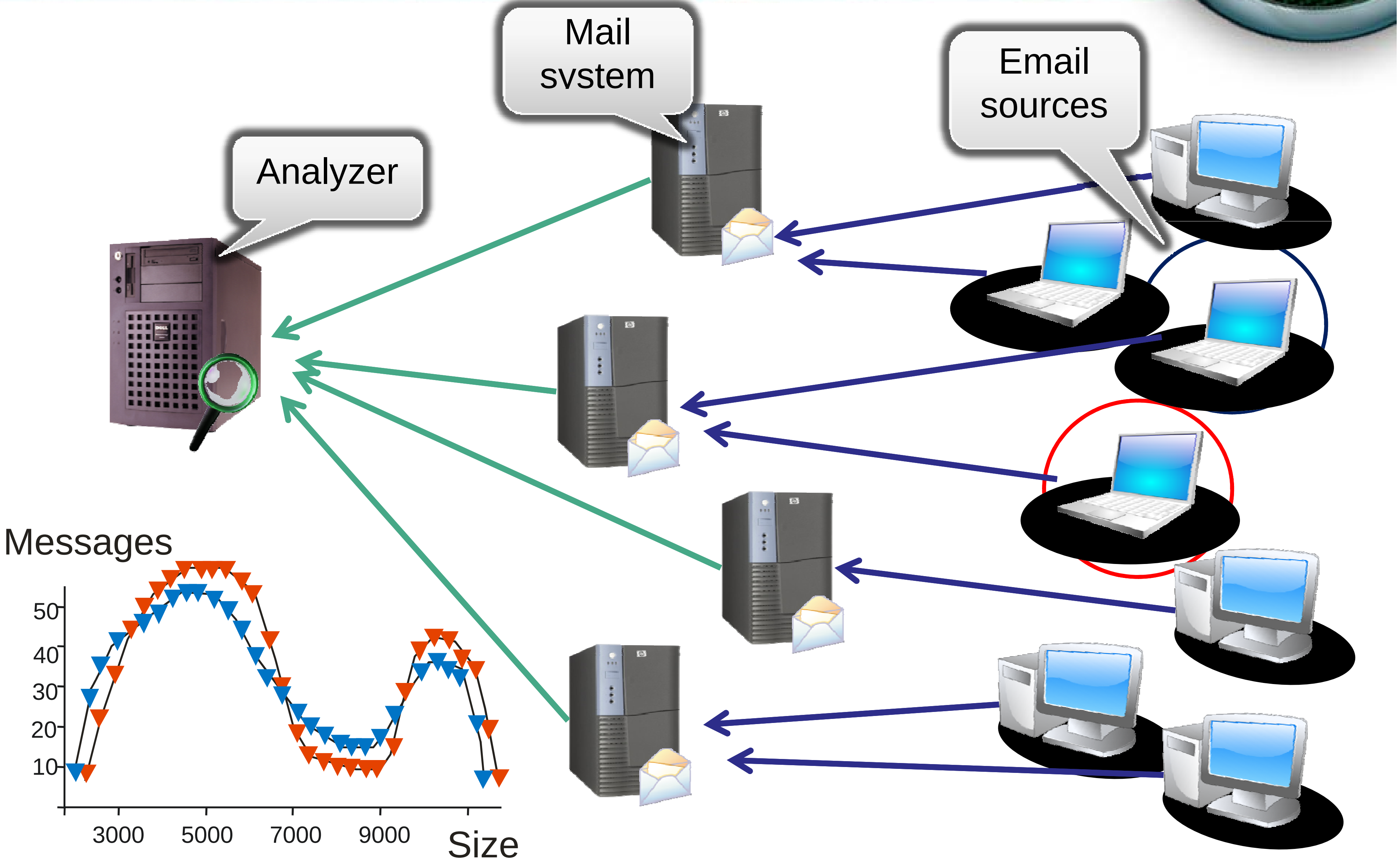
Analyzer



Mail svstem

Email sources

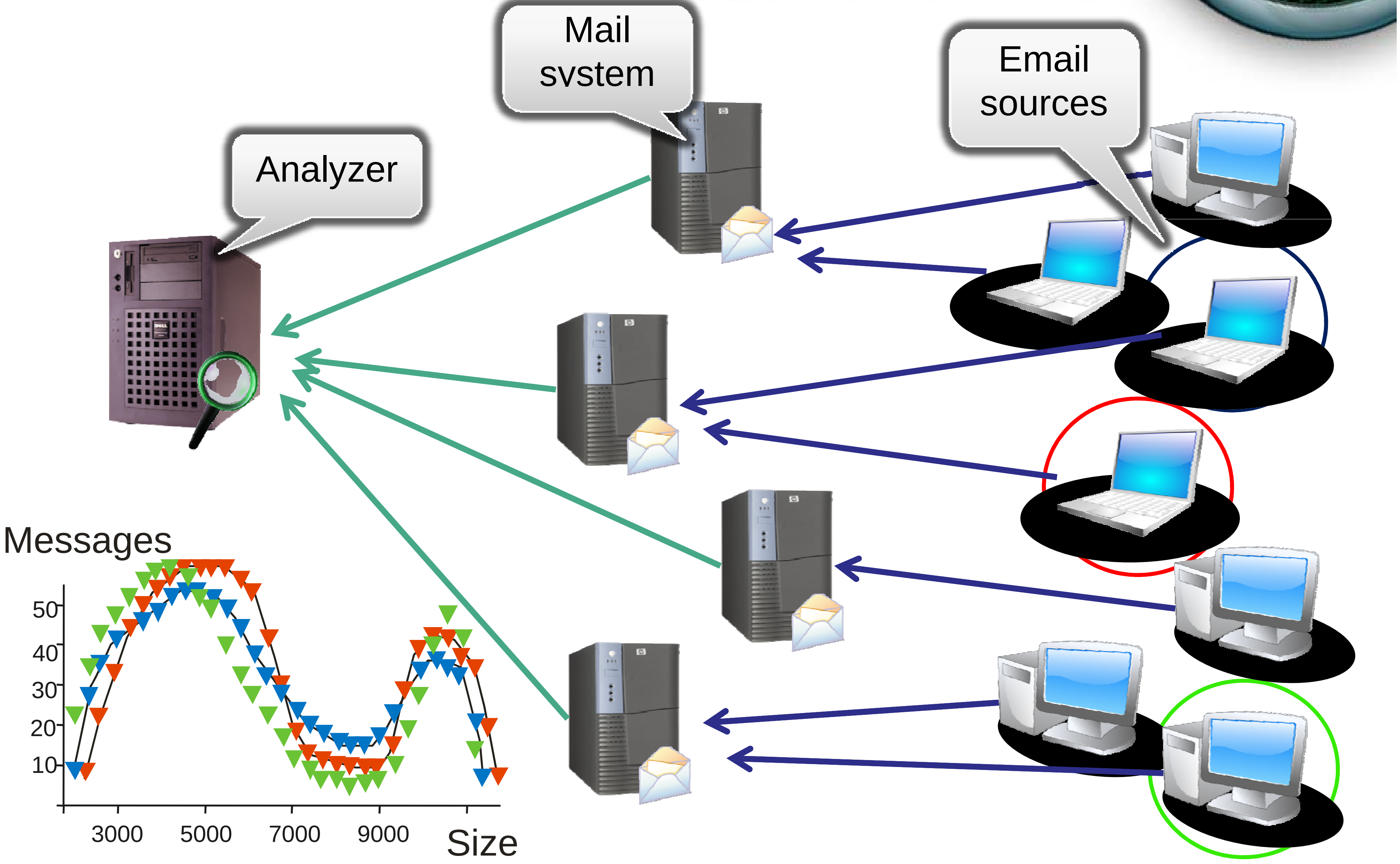
Analyzer

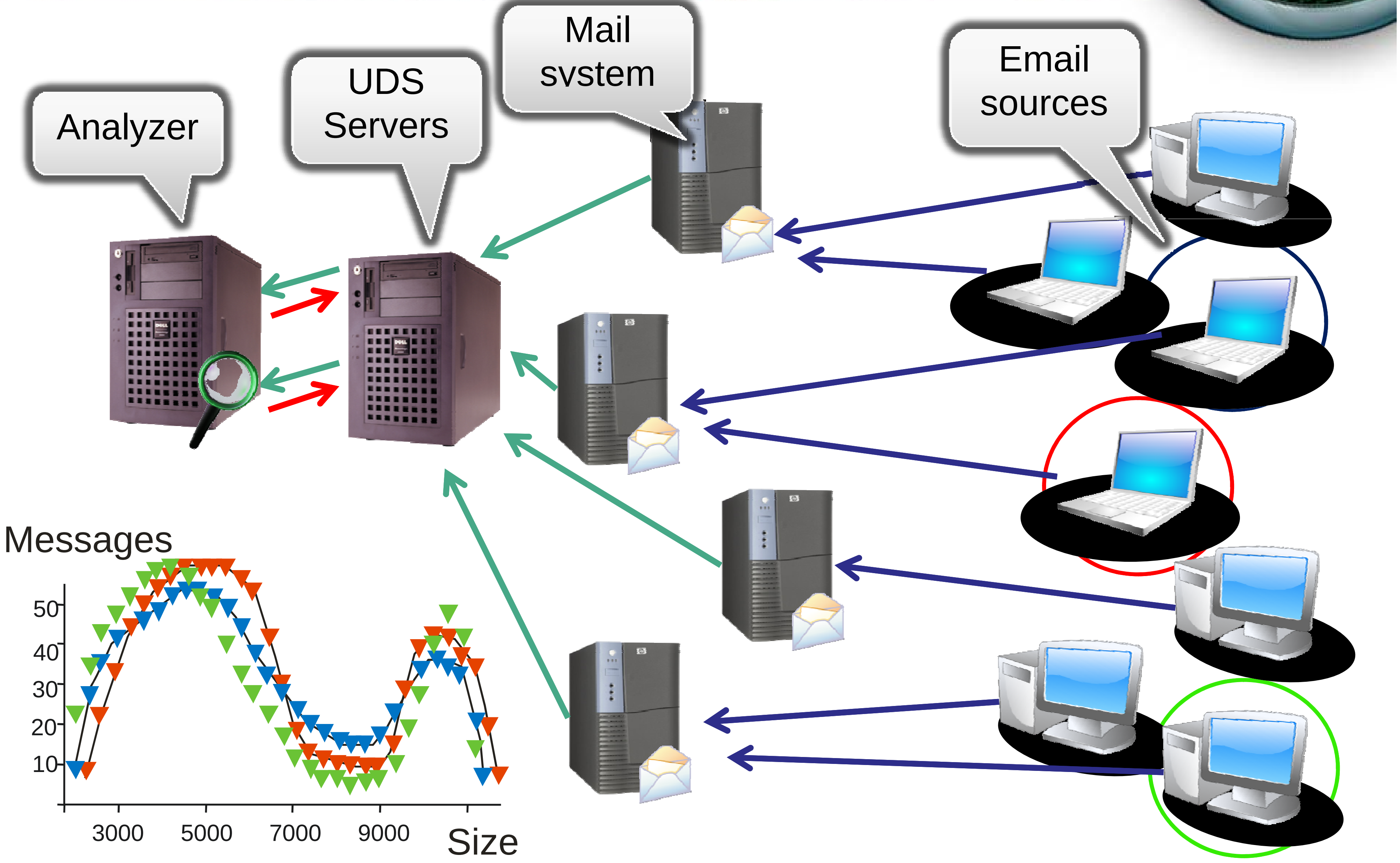


Mail svstem

Email sources

Analyzer


Mail
svstem
Email
sources
Analyzer
Messages
50
40
30
20
10
3000
5000
7000
9000
Size



Analyzer

UDS Servers

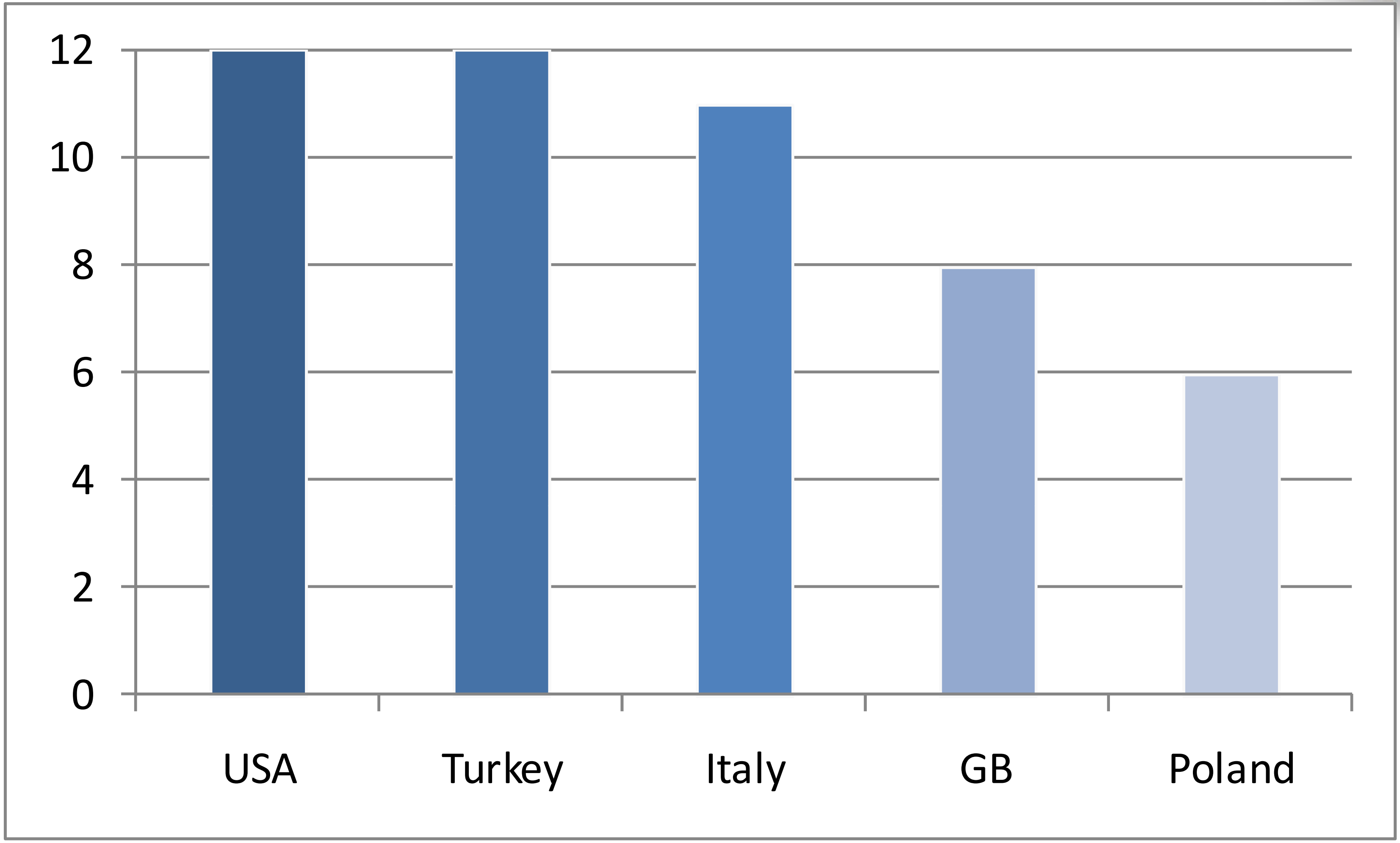
Mail svstem

Email sources

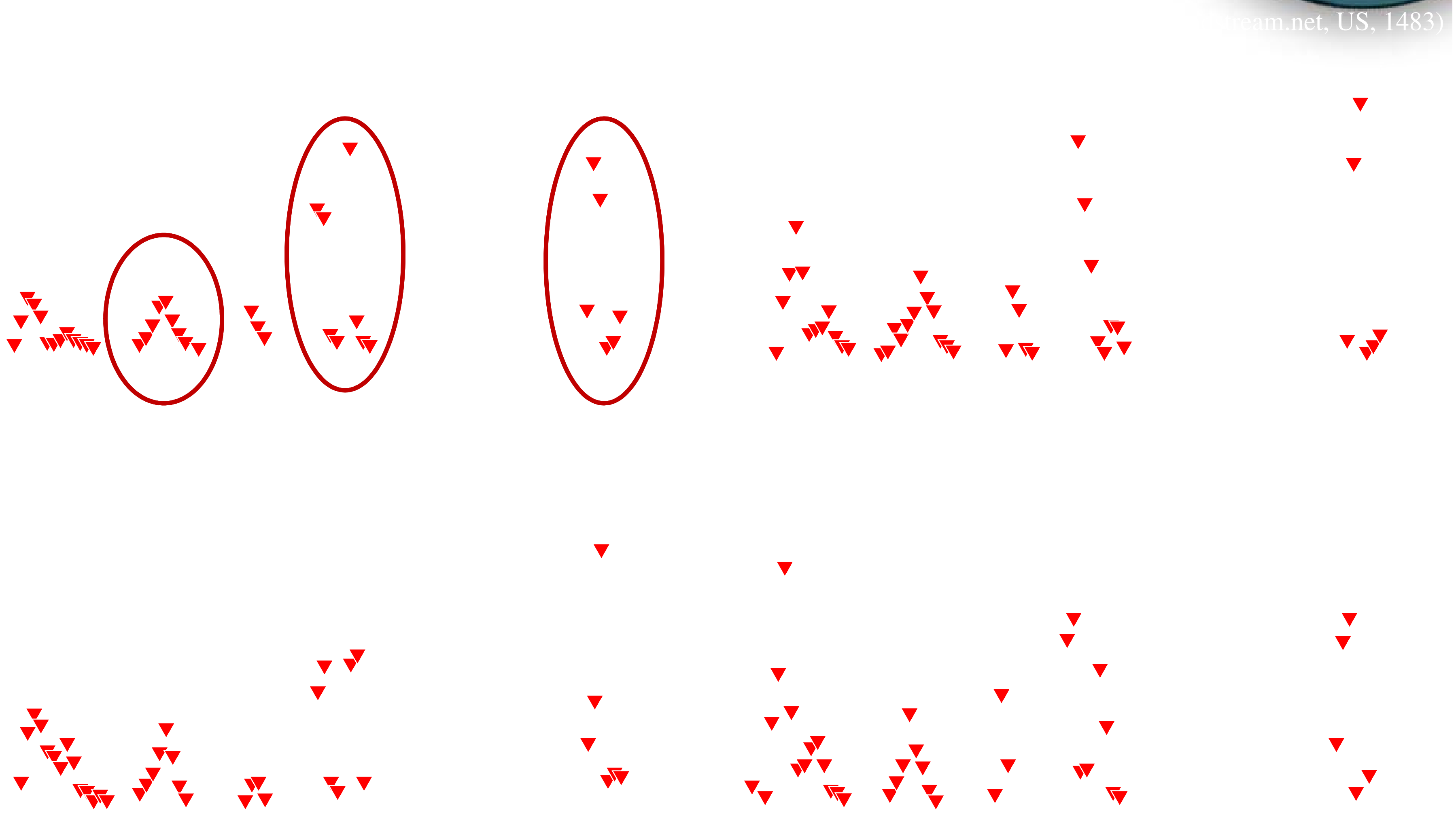
Statistical data and summary of results

- About 2000 active clients
- 1.5 million IP addresses per day
- 120,000 (8%) IP addresses suitable for analysis
- 40,000 IP addresses fall into botnet lists
- 4-5 botnets with 5,000-7,000 hosts and 10-15 botnets with fewer hosts
- Botnet regions: China, USA, Turkey, Russia

Regional distribution of the botnet

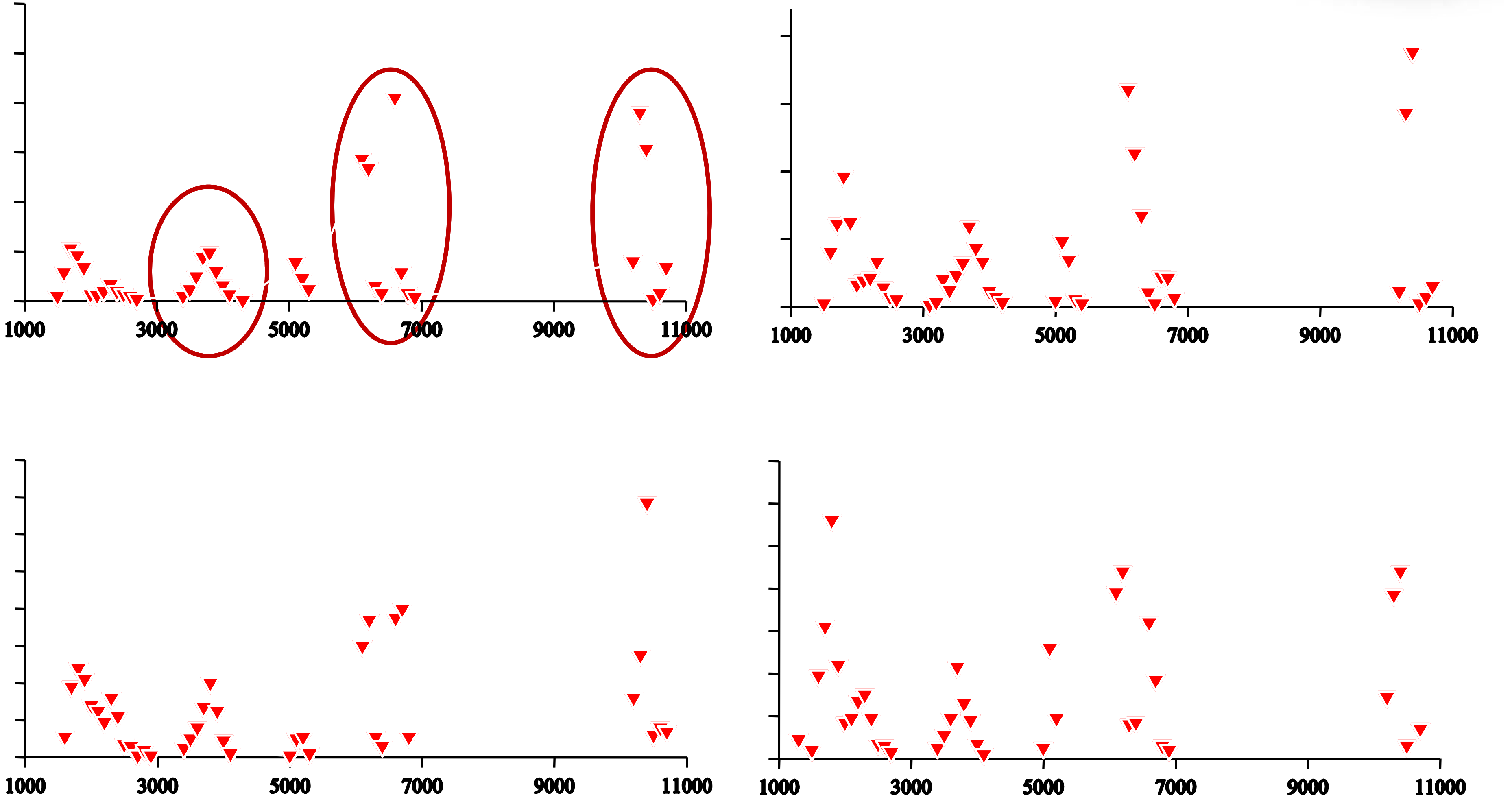


Distributions of the number of messages by size

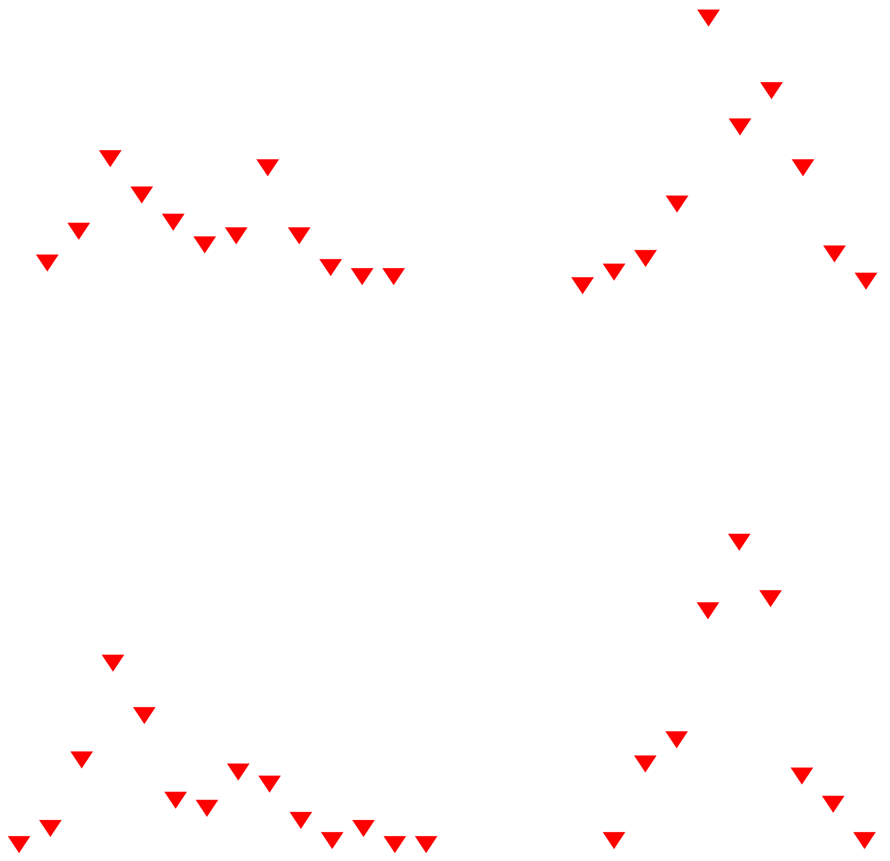


Distributions of the number of messages by size

stream.net, US, 1483)

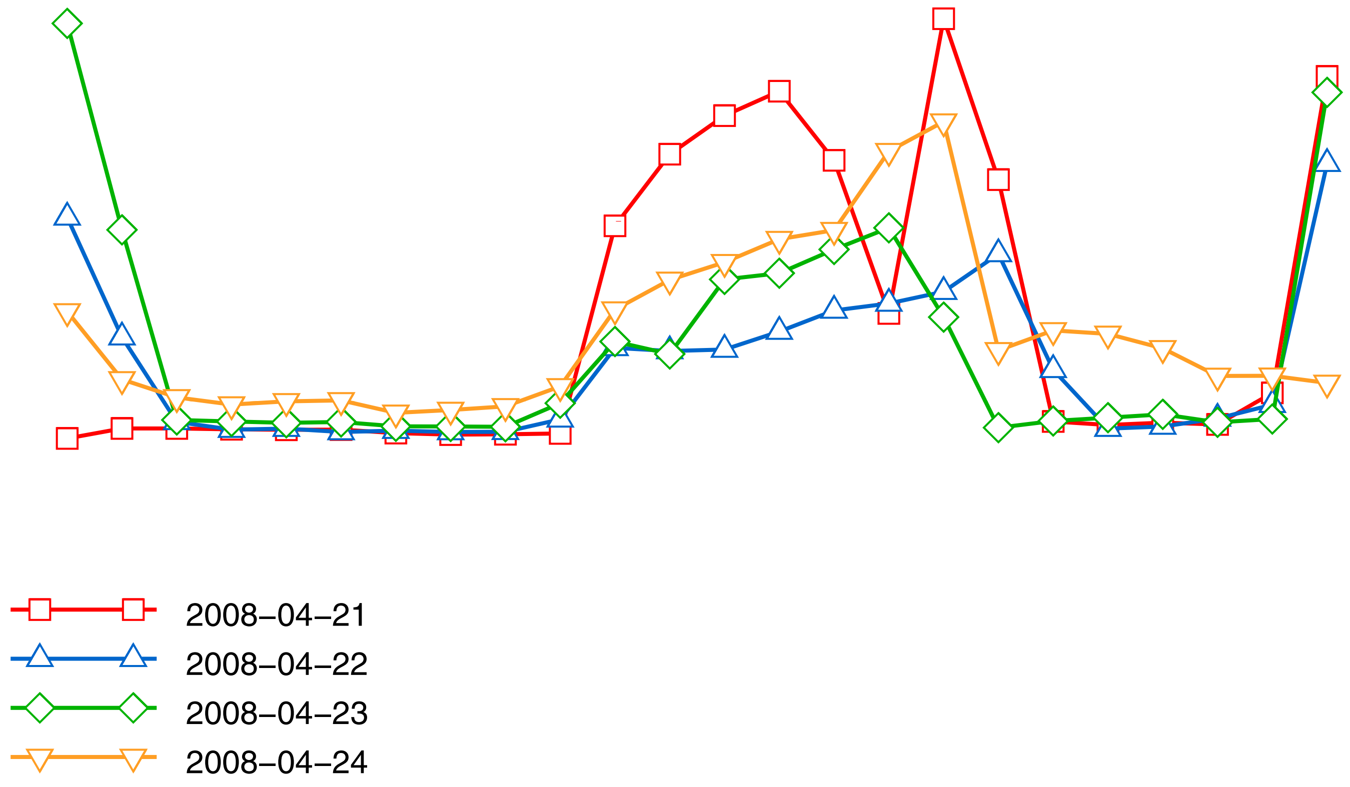


Distributions of the number of messages by size



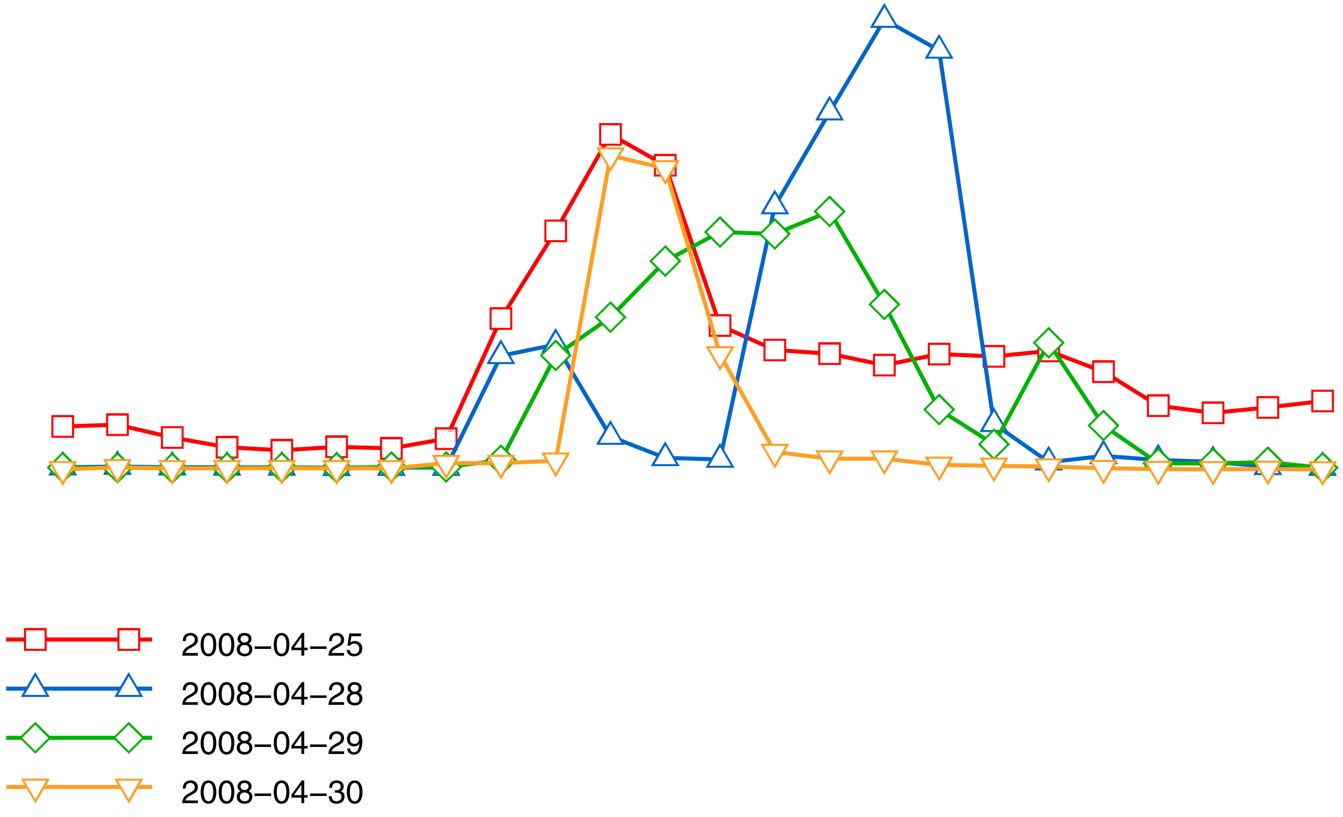
Jun 12 and Jun 15

Hourly botnet activity



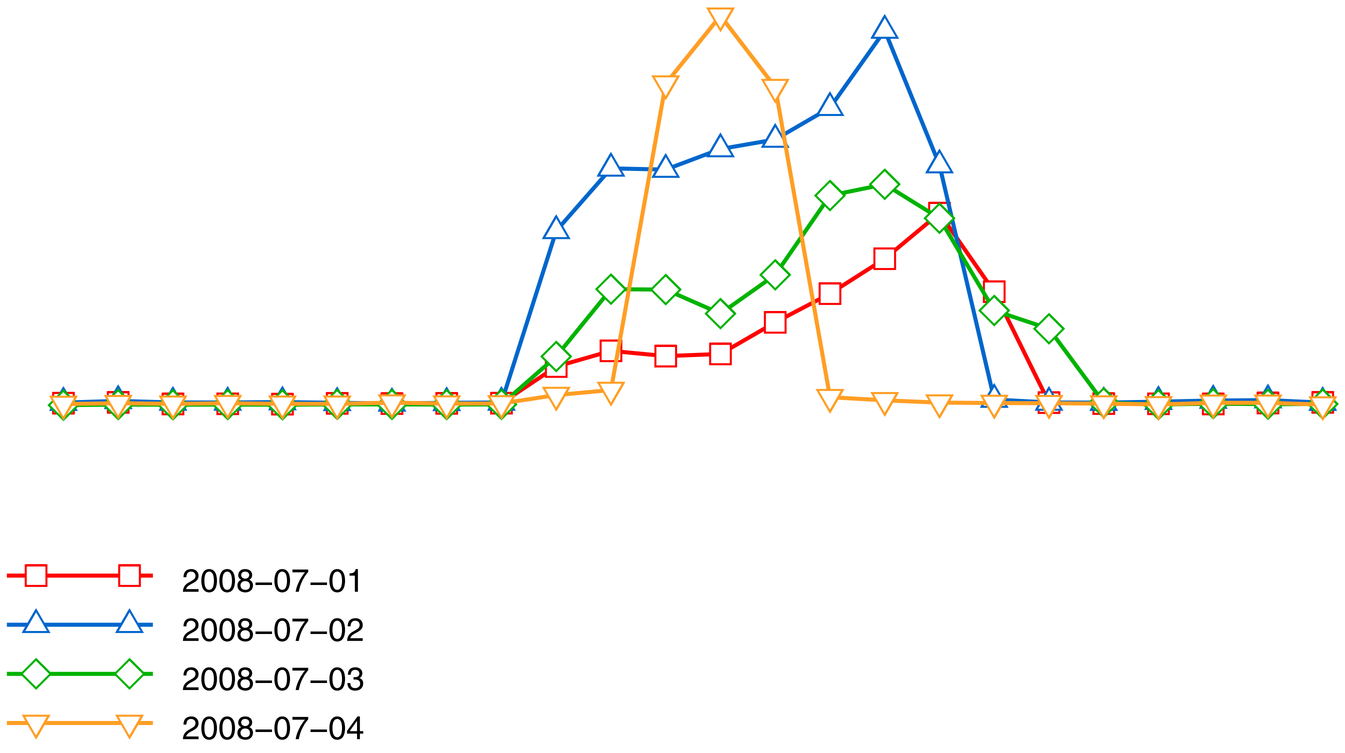
Apr 21-24

Hourly botnet activity



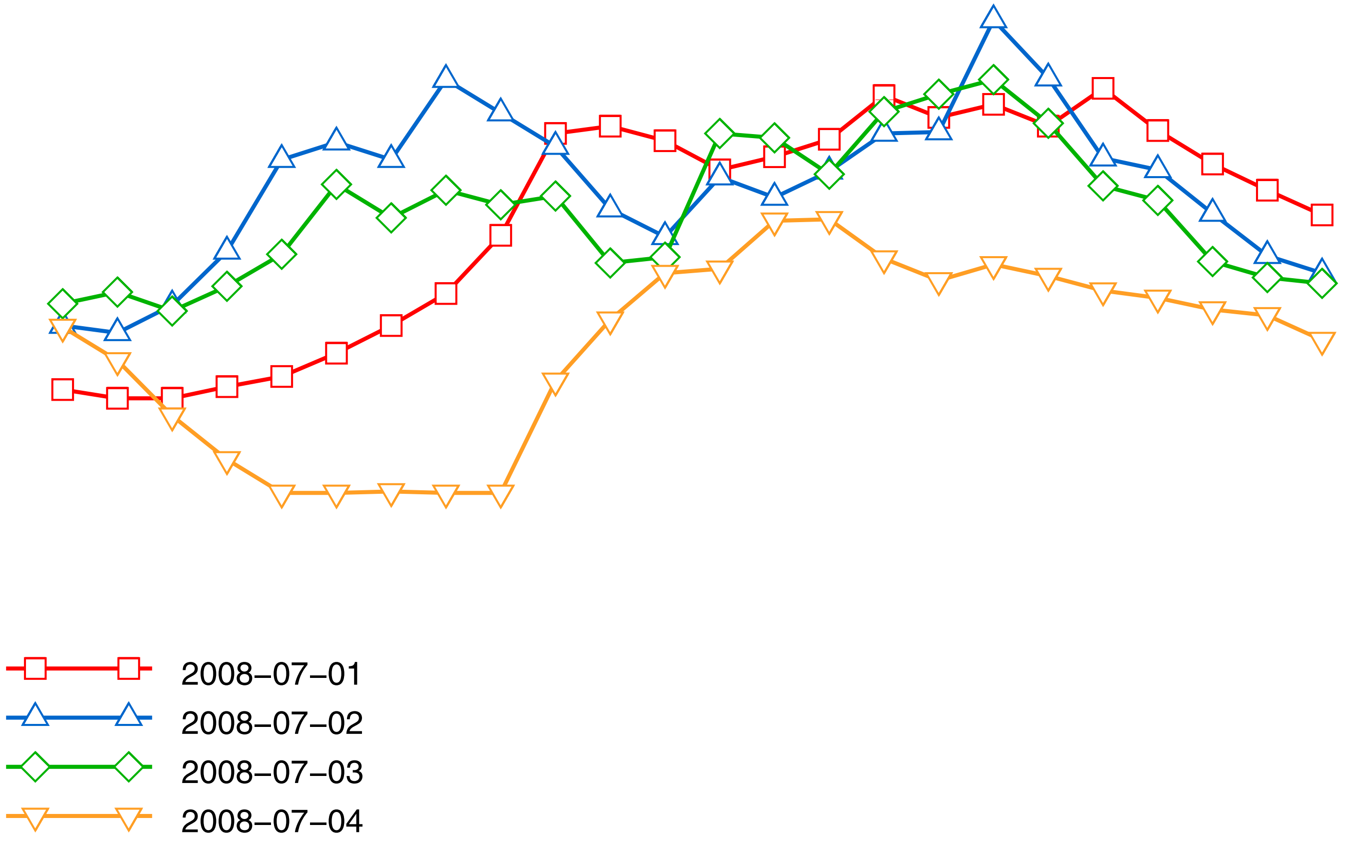
Apr 25-30

Hourly botnet activity



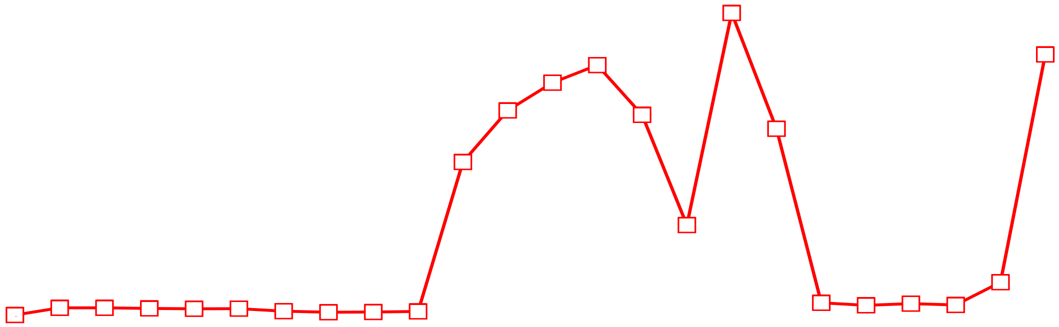
Jul 1-4

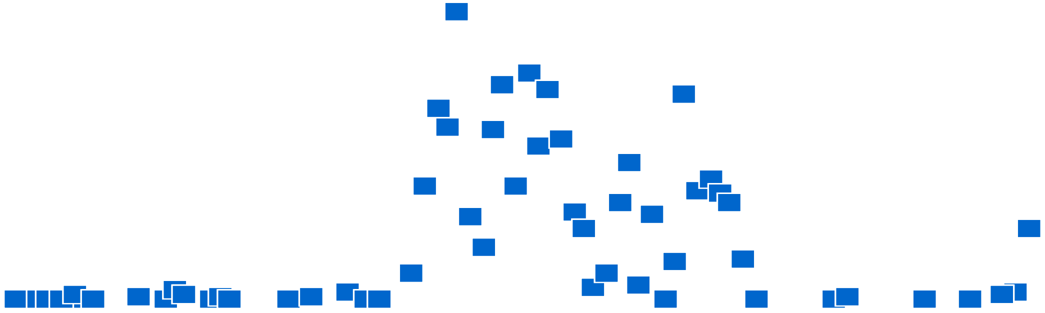
Hourly botnet activity, (another botnet)



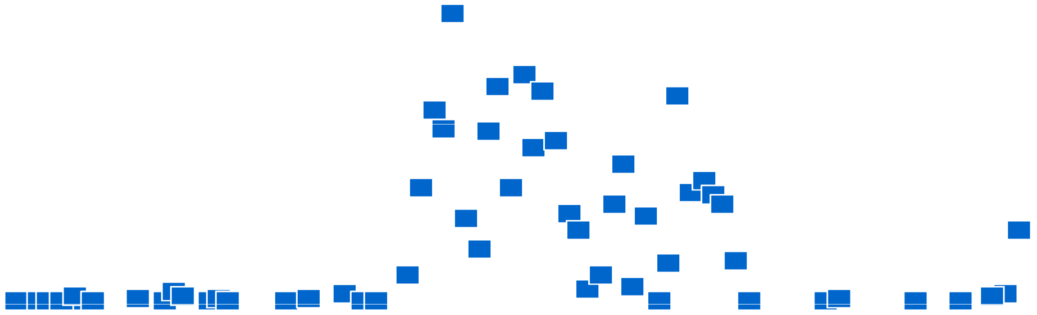
Jul 1-4

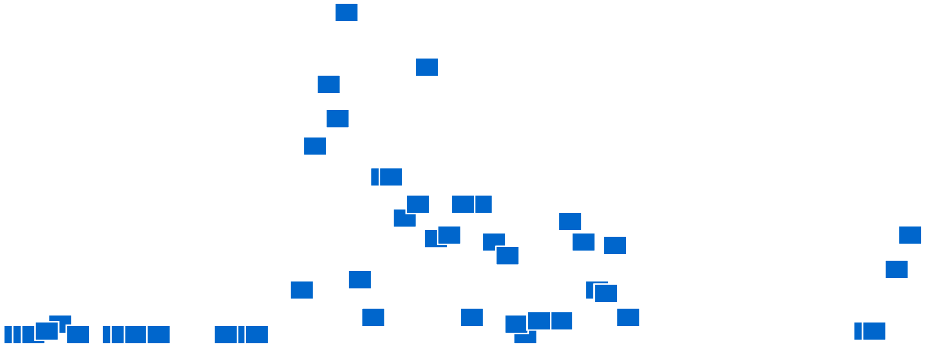
Hourly botnet activity vs. individual host activity



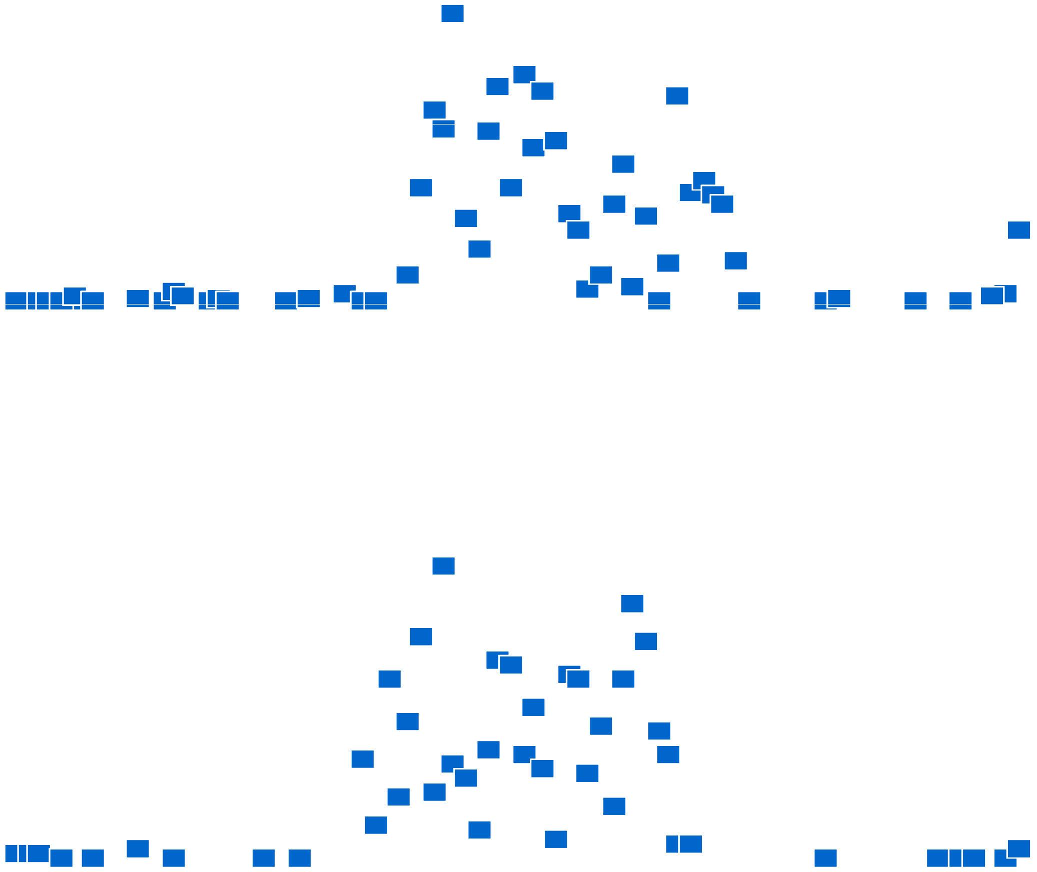


Distributions of the number of messages by time





Distributions of the number of messages by time



Apr 21 and Jul 2

Pros and Cons

Pros

- Independence from bot implementations and botnet control infrastructure protocols
- Simple implementation, especially on the client side
- Low maintenance cost: once implemented, the system does not require much human intervention

Cons

- The need to gather a large quantity of statistical information from many sources
- Inability to block a botnet until enough statistical information is gathered

THANK YOU

Andrey Bakhmutov

Kaspersky Lab

Andrey.Bakhmutov@kaspersky.com