

ZeuS v3 p2p network monitoring

Tomasz Bukowski
CERT Polska



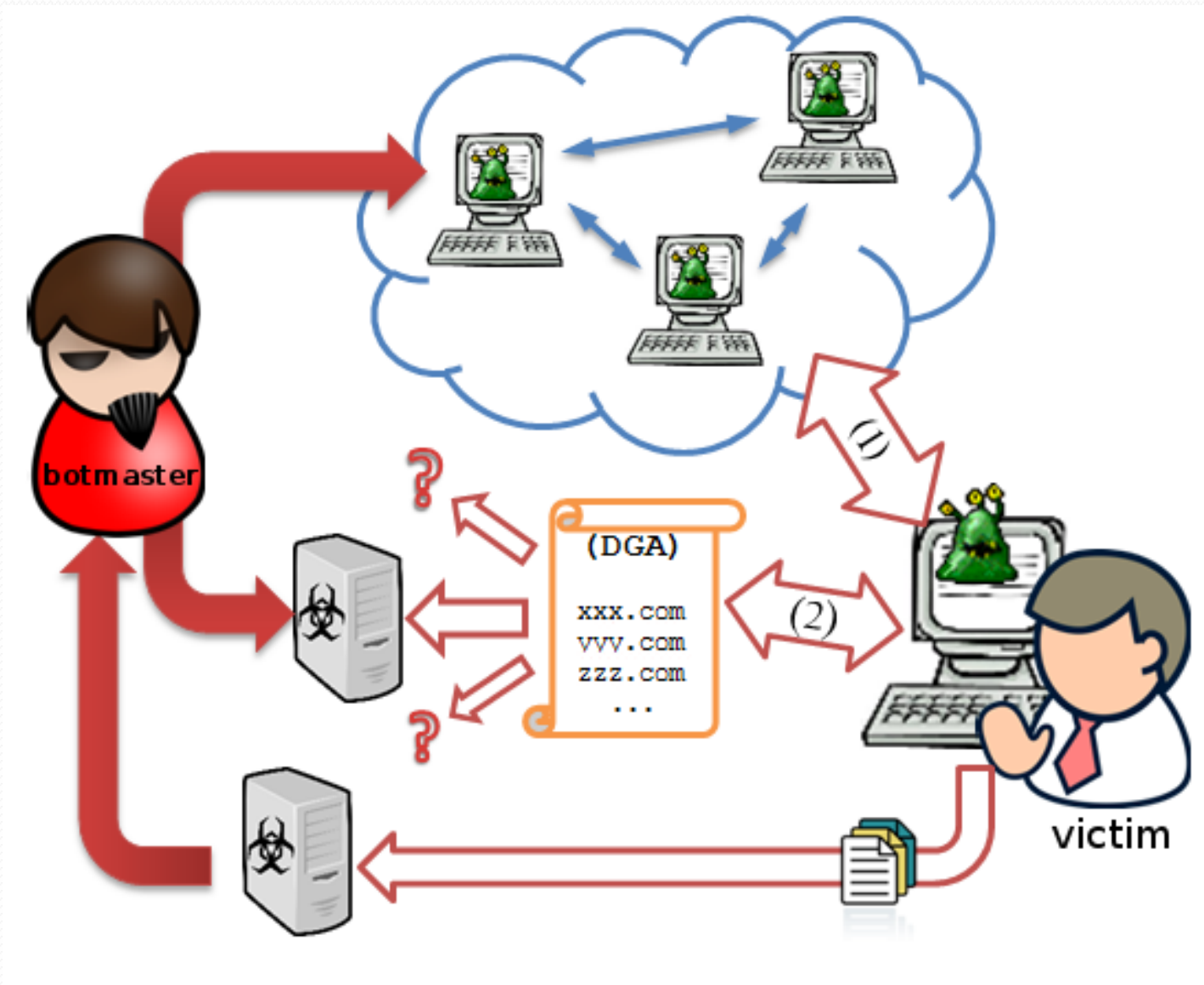
Agenda

- The history of this case
- Data distribution in new ZeuS [v3]
- ZeuS-p2p network
- p2p messages
- Our crawler
- p2p network structure
- Data propagation speed

The history ...

- September 2011
 - first news about zeus p2p/murofet
- October 2011
 - First articles on the web
- November 2011
 - We got the binary sample !
 - We suspected that the botnet will be inactive soon ...
- December 2011 - first results of analysis
 - Incubated sample is still active
 - Alpha version of crawler started - collected 10000 nodes
 - Beta version of crawler running till 20 Jan 2012
- January 2012
 - Crawler reports lower rate of valid answers
 - We suspected that the botnet will be inactive soon (again? :P)
 - After closer look -> there was bigger update at 15 Jan !
- February 2012
 - Still alive !

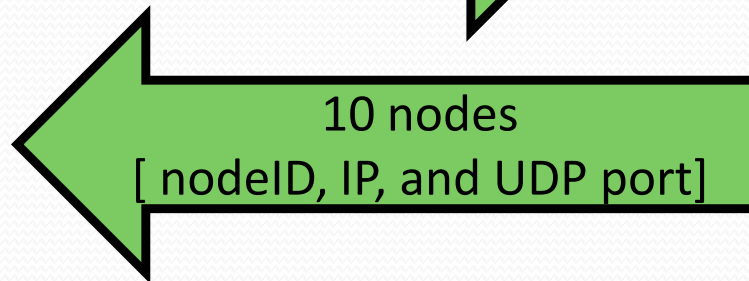
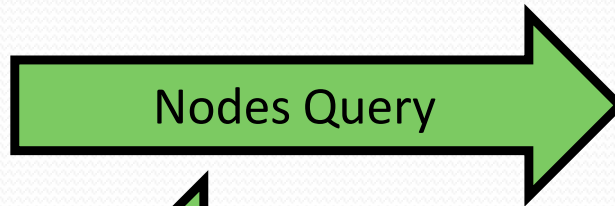
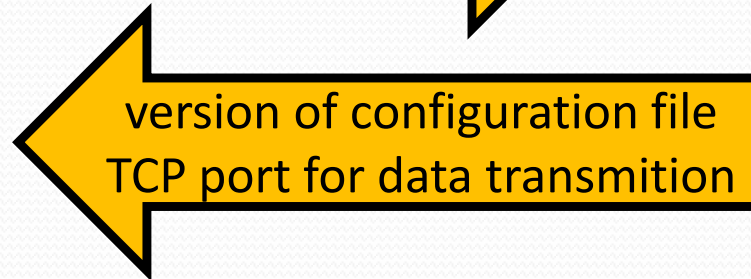
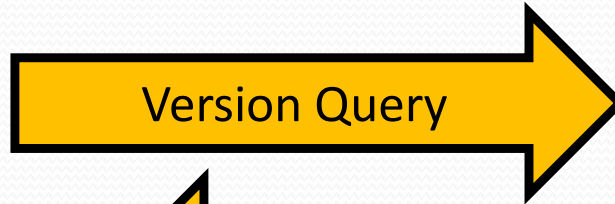
Zeus v3 - Data distribution



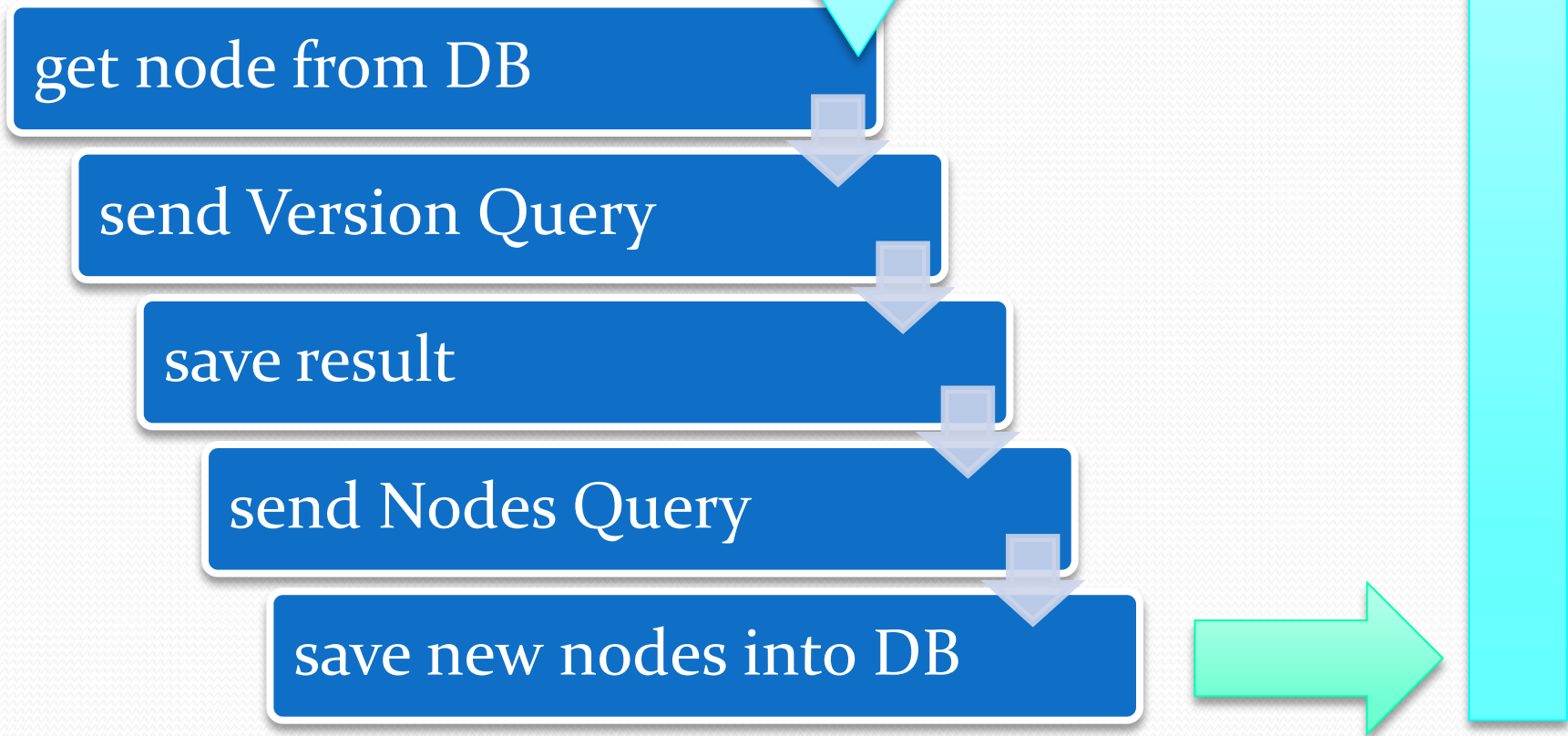
Zeus p2p network

- Based on kademlia
- Any ID = SHA1 hash [20 bytes]
- Communication on high TCP and UDP port
- Infected computer - node :
 - node-ID
 - node-IP
 - node-UDP-port

ZeusS p2p network - message types



Zeus p2p network crawler



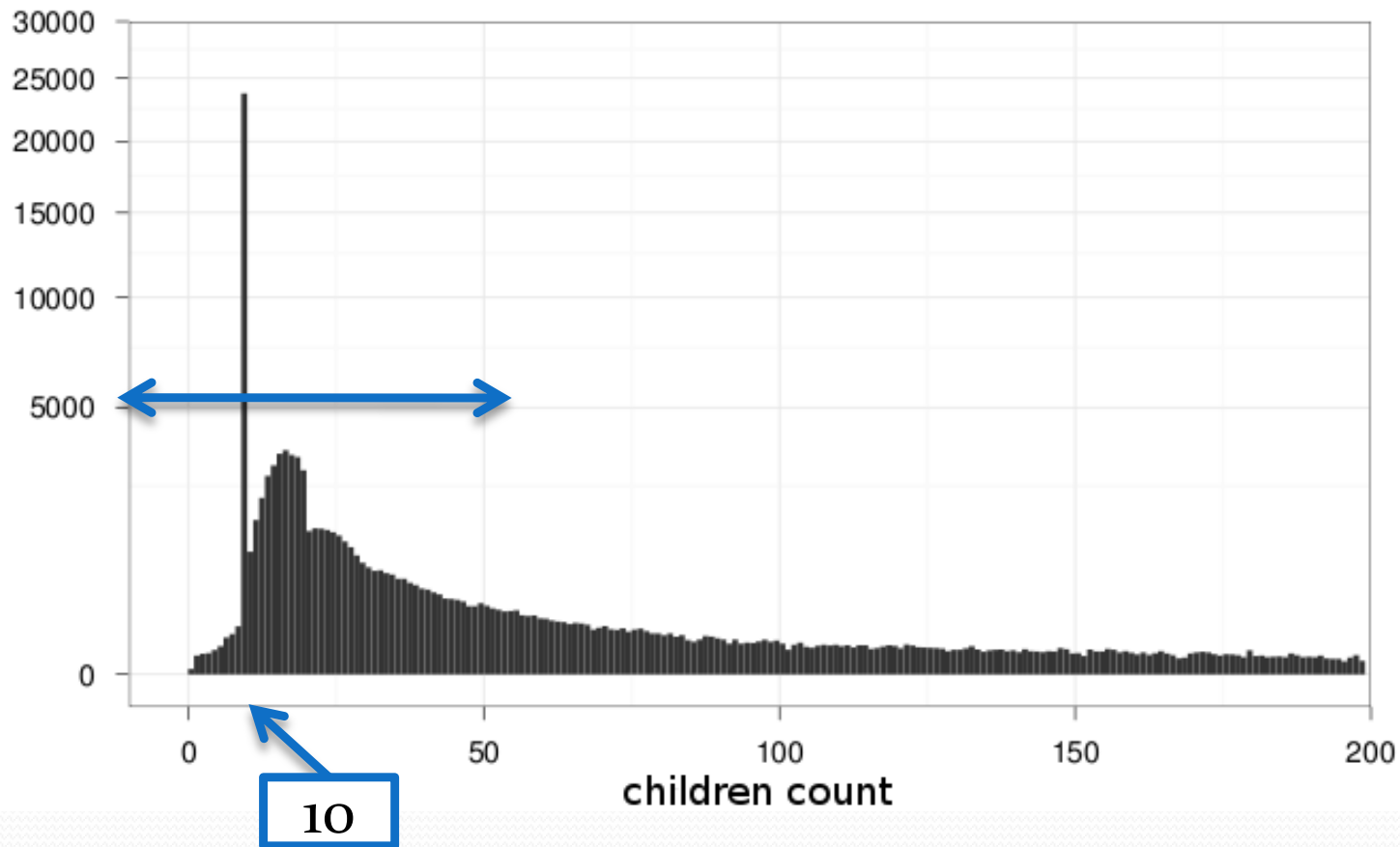
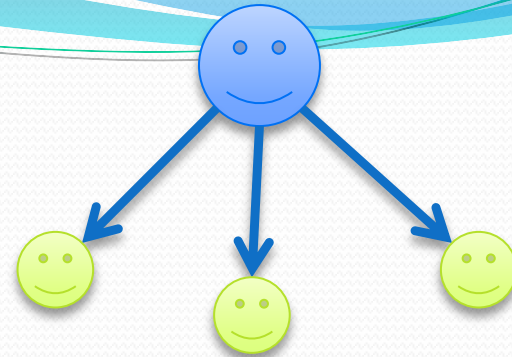
Crawling results

- Nodes count in DB on start : **1**
- After 4 weeks : over **925 000** nodes
 - **~870 000** with valid IP/PORT/ID [null values etc.]
- Uniq-IP : **~560 000**
- Uniq-ID : **~230 000**

- **20 000** ID have mor than **10** IP addresses

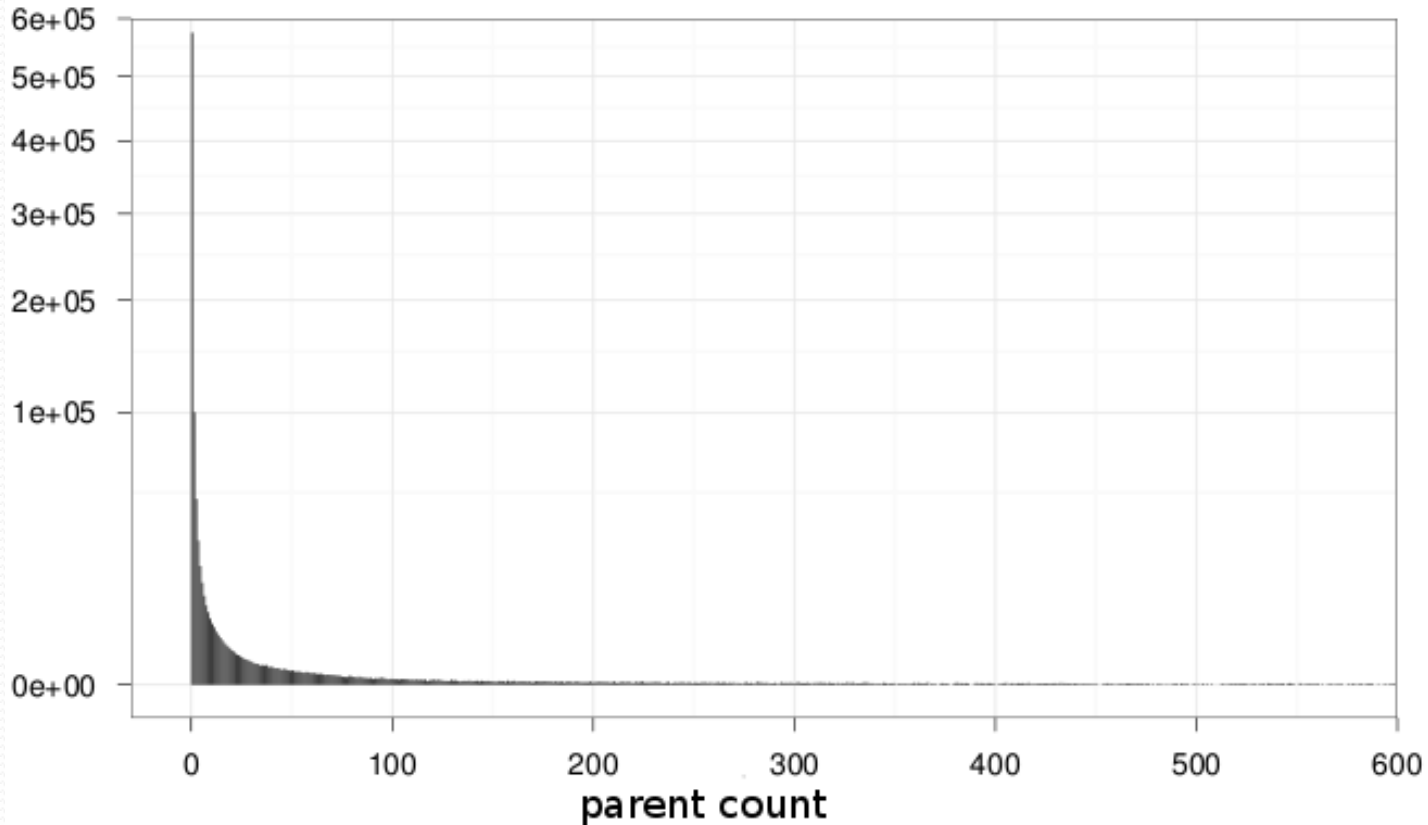
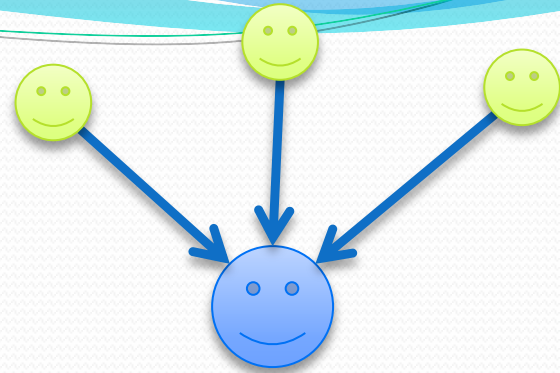
Crawling results

Children count distribution

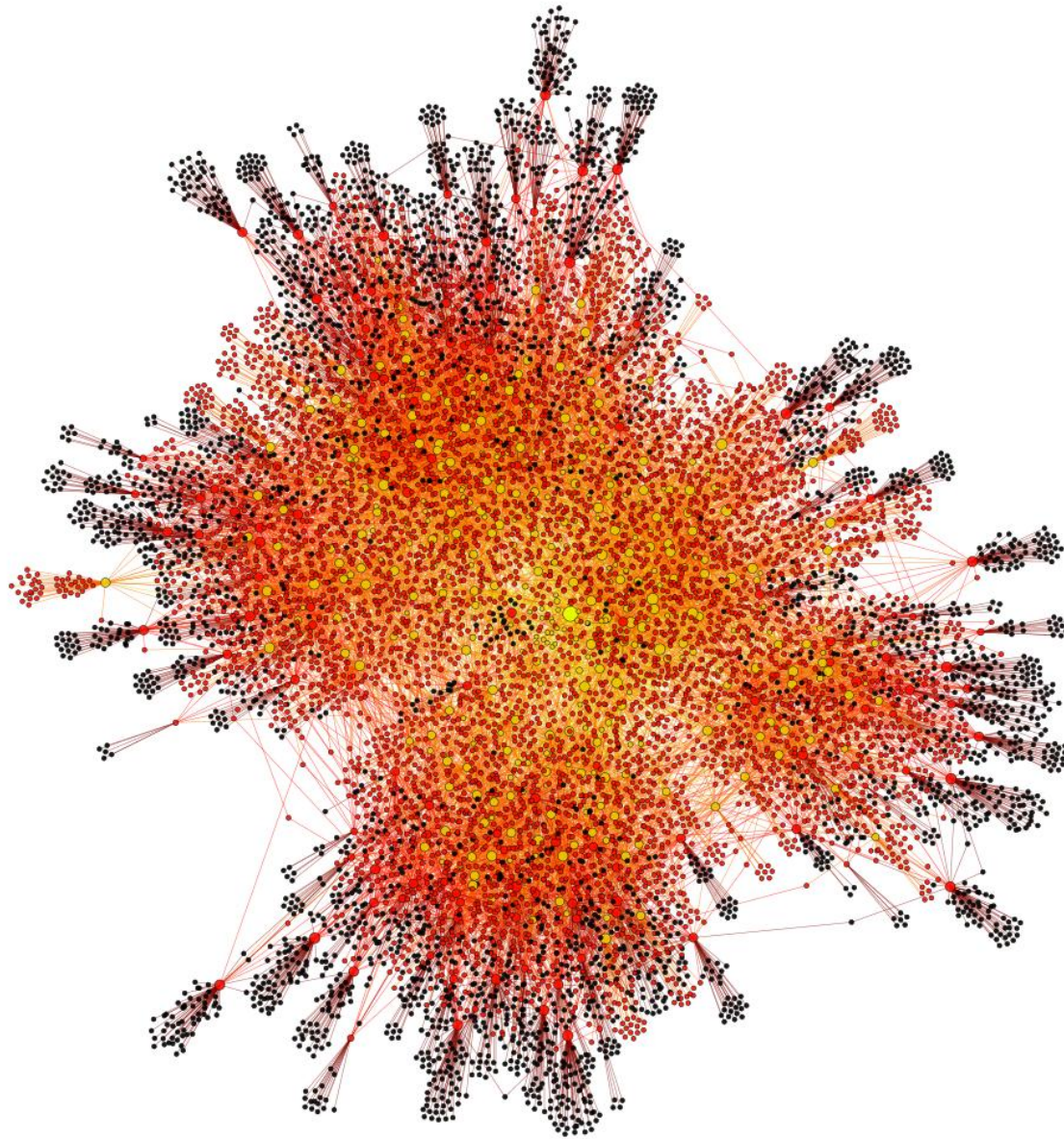


Crawling results

Parent count distribution



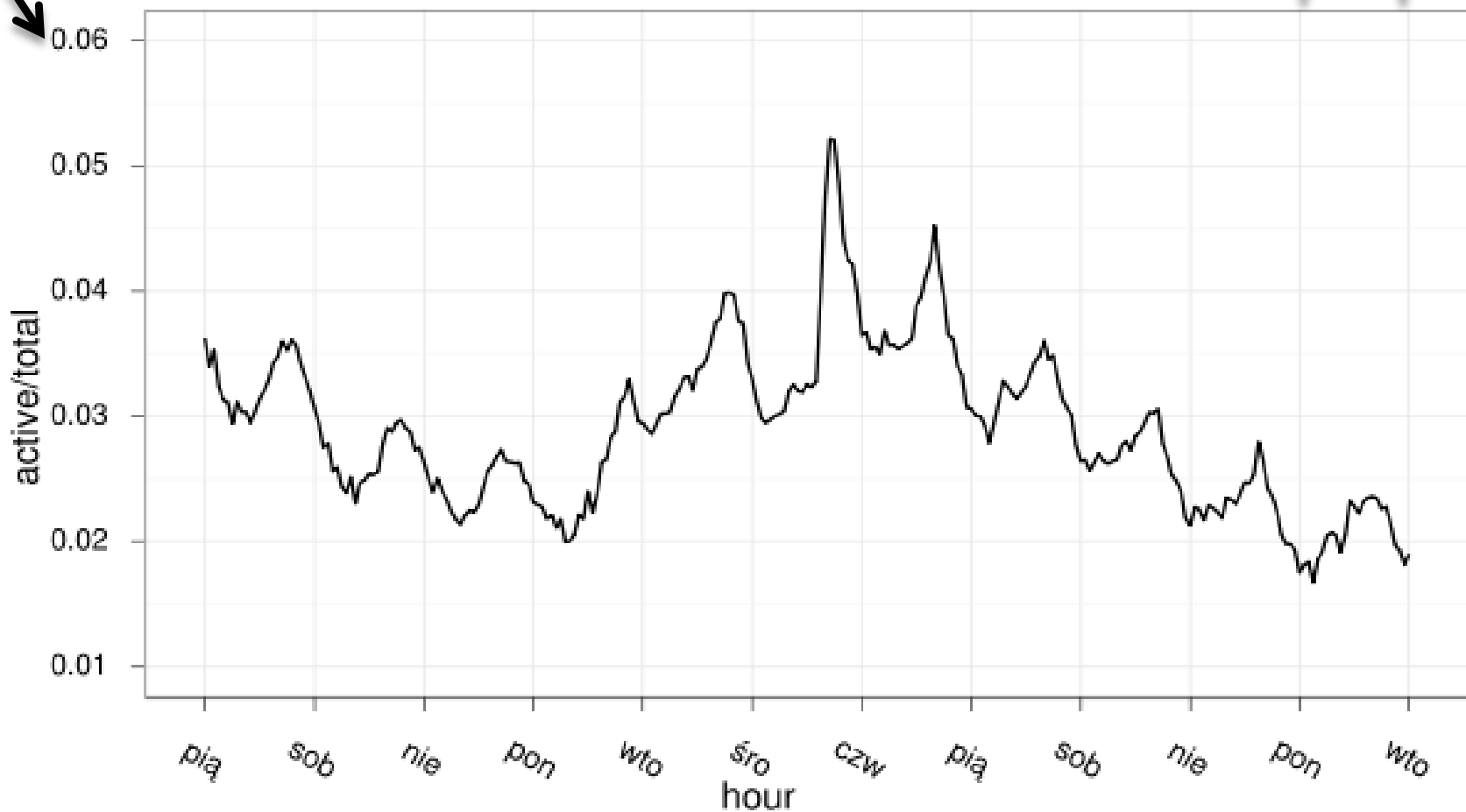
Crawling results - zp2p network



Crawling statistics

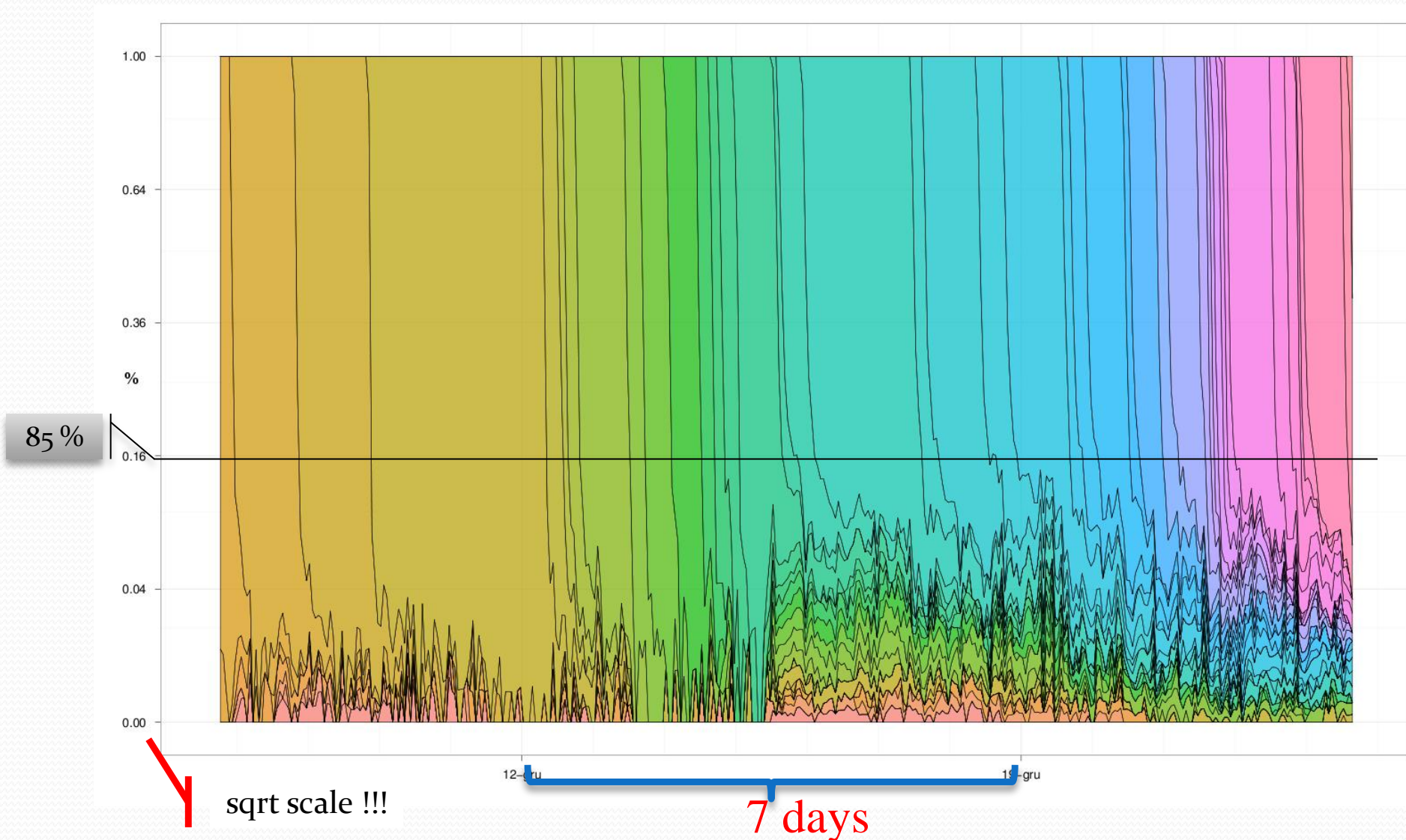
$\frac{\text{number of answers}}{\text{number of queries}}$

1 day

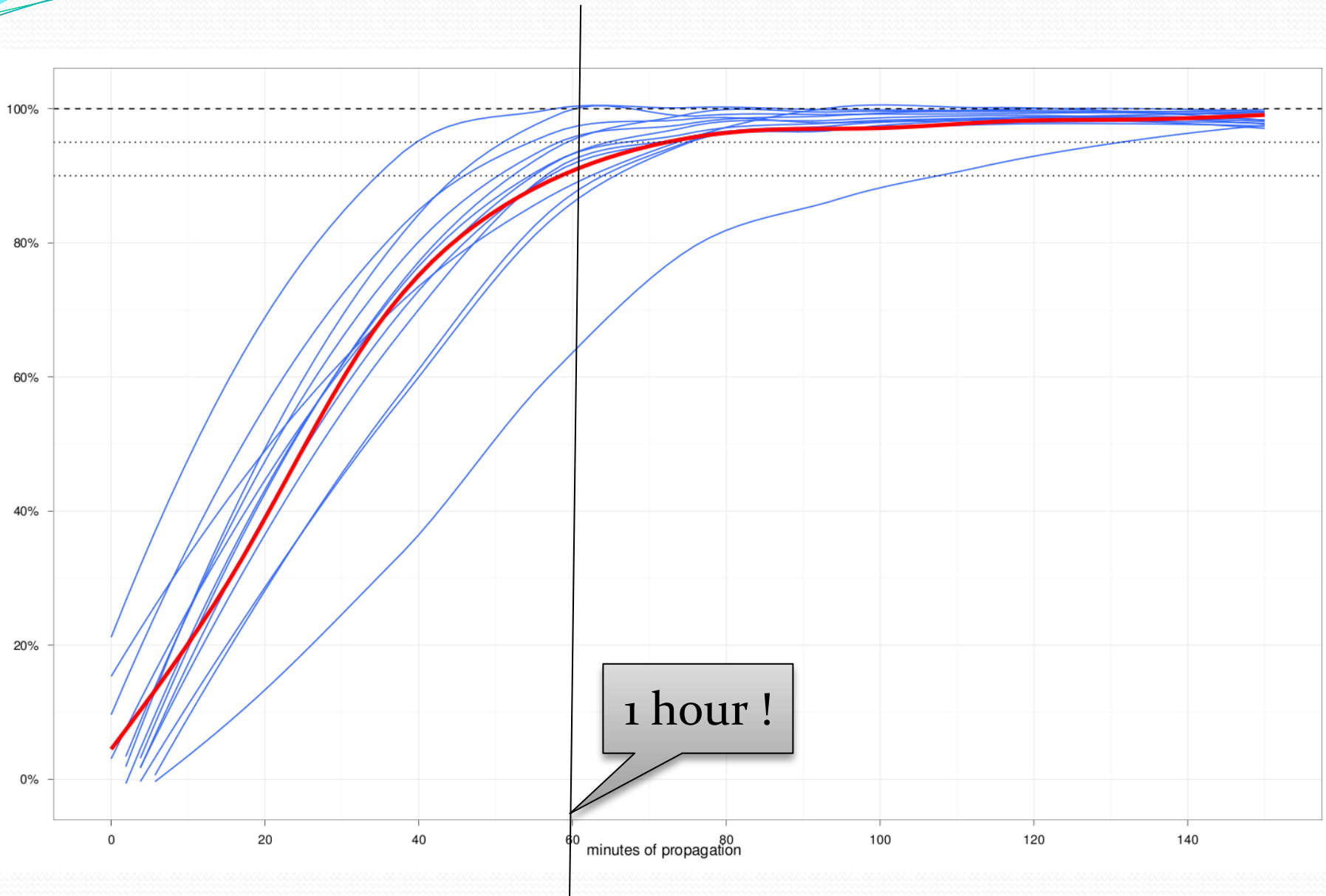


Zeus p2p network - information propagation

Results of analysis of collected 'version responses' over time :



Zeus p2p network - information propagation





**List of IP + ASN + CC
collected by crawler !**

Questions ?

Contact:

www.cert.pl

[info\[at\]cert.pl](mailto:info[at]cert.pl)

[tomasz.bukowski\[at\]cert.pl](mailto:tomasz.bukowski[at]cert.pl)

CERT
POLSKA

 **NASK**