DDoS Attacks, Russia, 2011-2012: Patterns and Trends

QRATOR

Artyom Gavrichenkov

ximaera@highloadlab.com

ЗАЩИТА ОТ DDOS АТАК

Statistics

- 2011-2012: > 2500 attacks
- 17% – ICMP/UDP/SYN/ACK flood
- 40 attacks > 1 Gbps

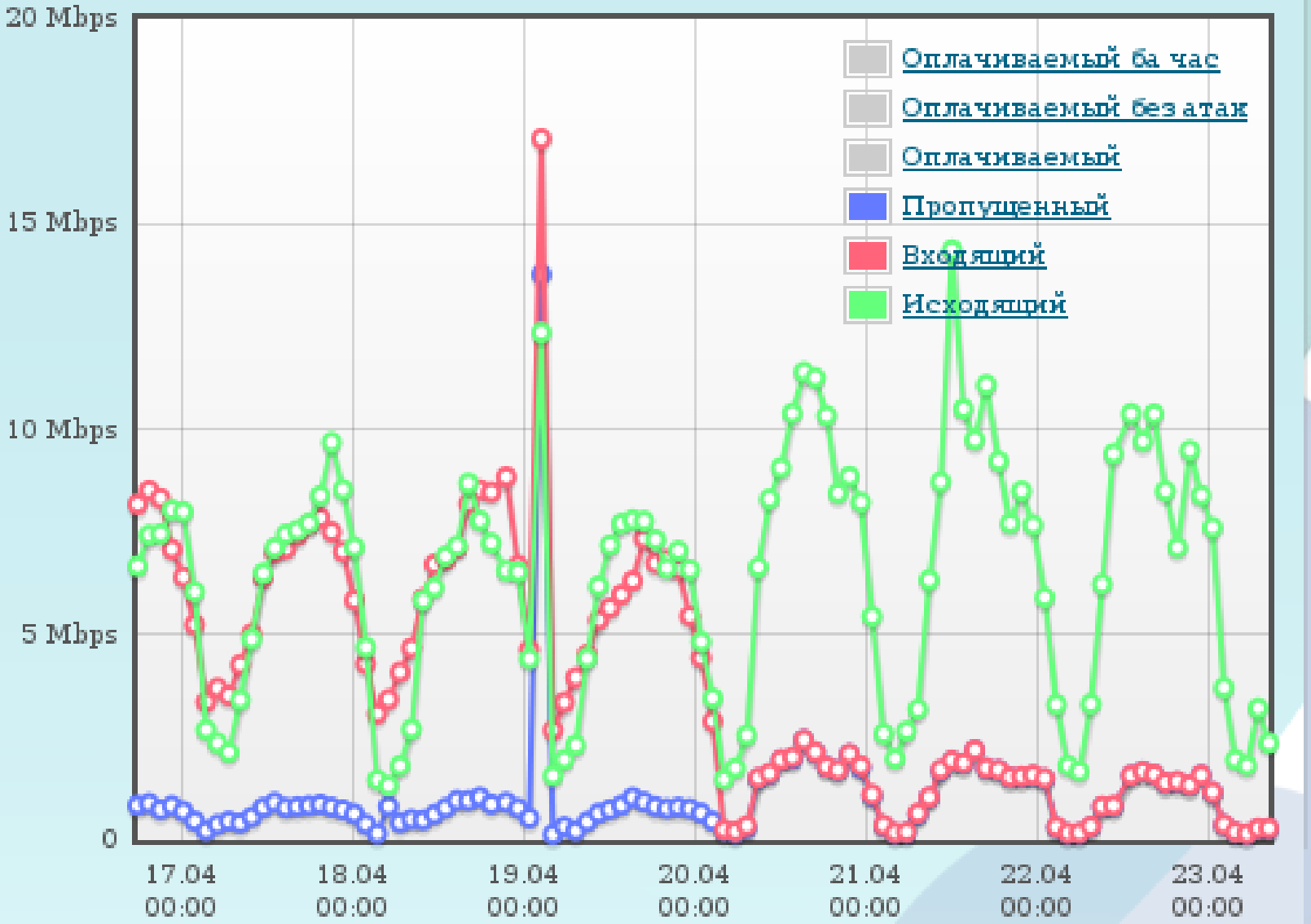
Statistics

- Max. attack duration before December, 2011: 486 hours

Трафик Пакеты Запросы Ответы Ошибки

Черный список

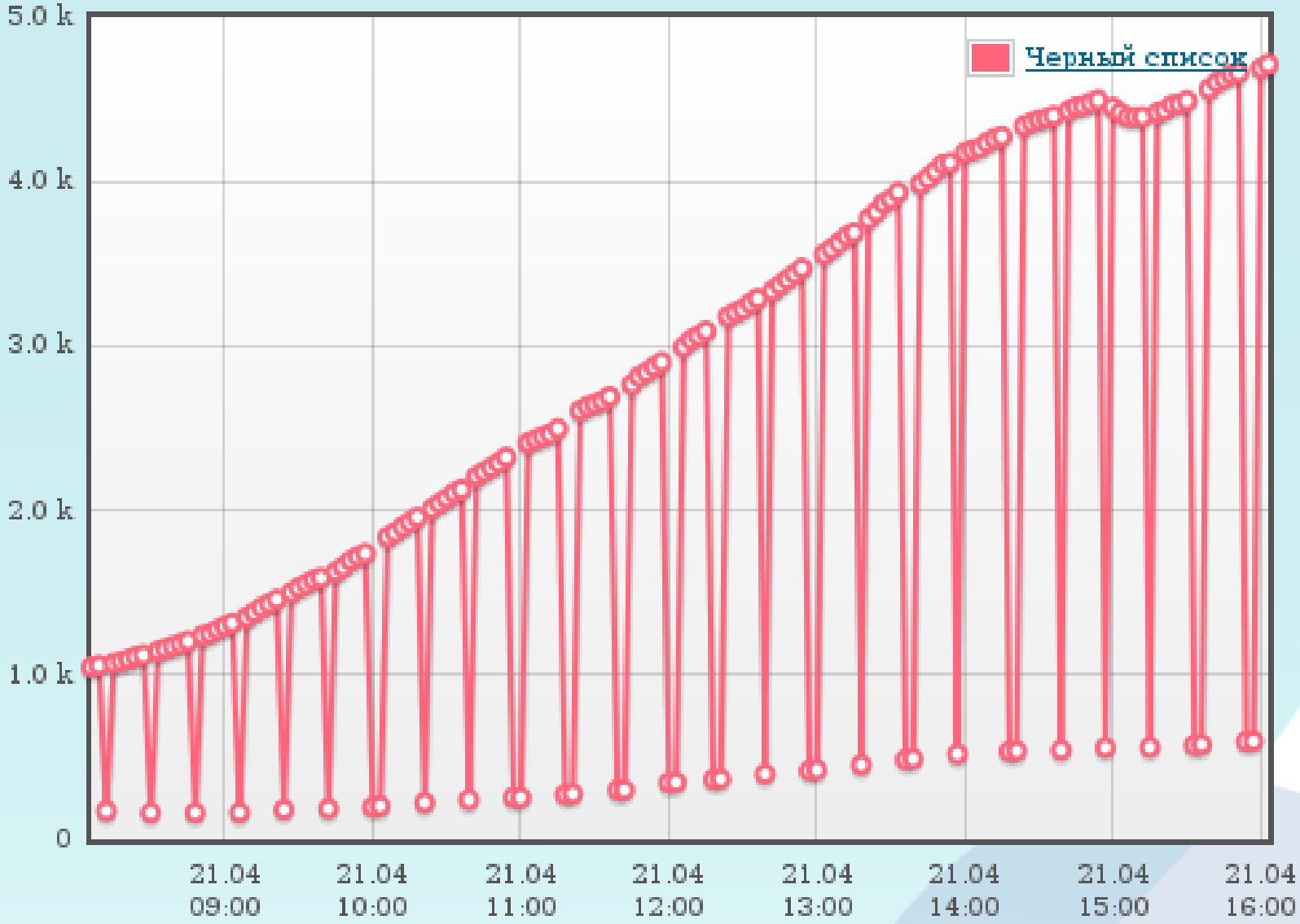
1 час 5 часов сутки неделя месяц полгода



Трафик Пакеты Запросы Ответы Ошибки

Черный список

1 час 5 часов сутки неделя месяц полгода



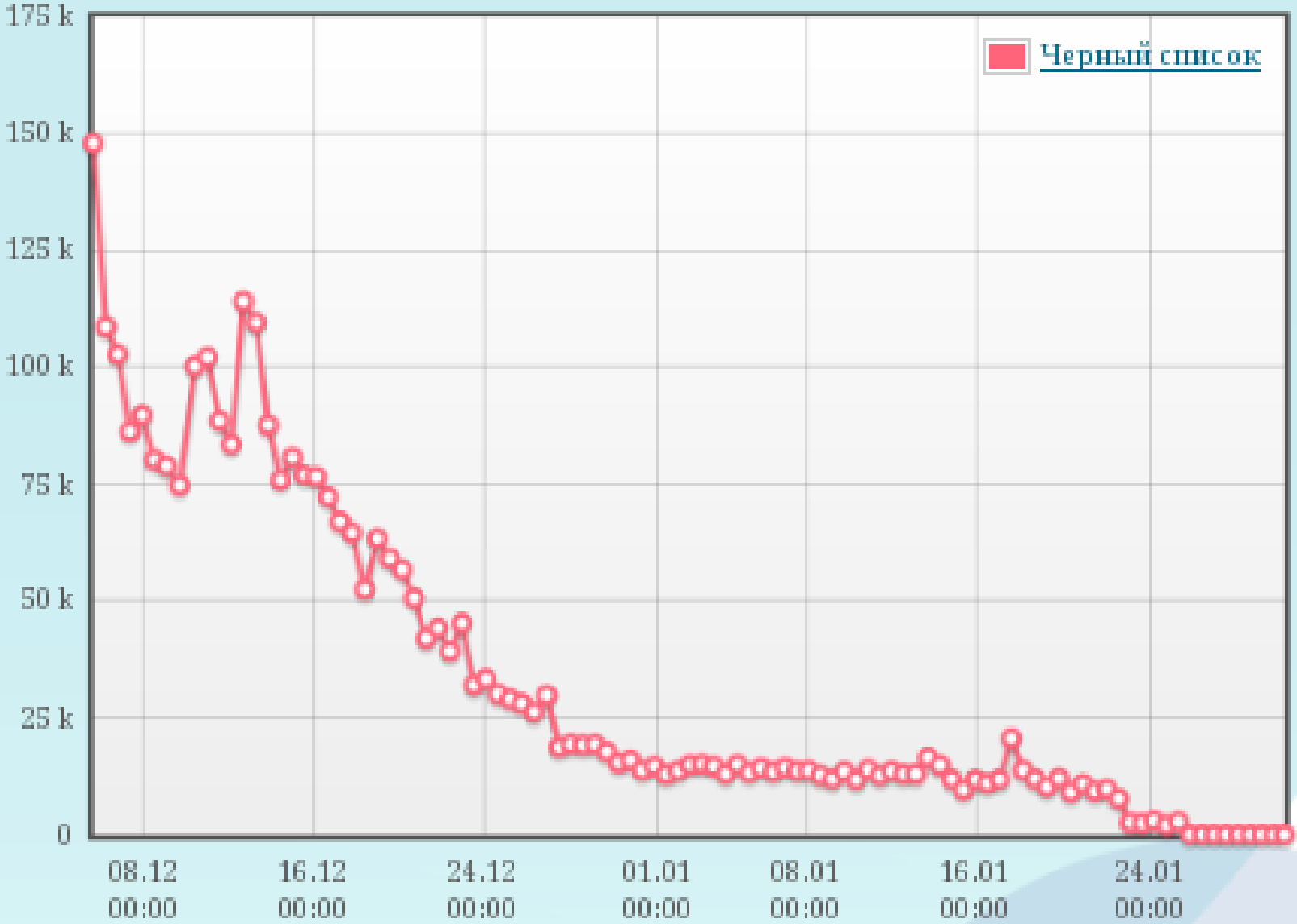
Statistics

- Max. attack duration, 2011-2012: 1228 hours

Трафик Пакеты Запросы Ответы Ошибки

Черный список SLA

1 час 5 часов сутки неделя месяц полгода



One botnet from Southern Asia

- 2011, December, http://slon.ru: ~200000 bots
- 2012, May, http://tvrain.ru: ~182000 bots
- ~500 IP addresses in common

Abuse from Indonesia

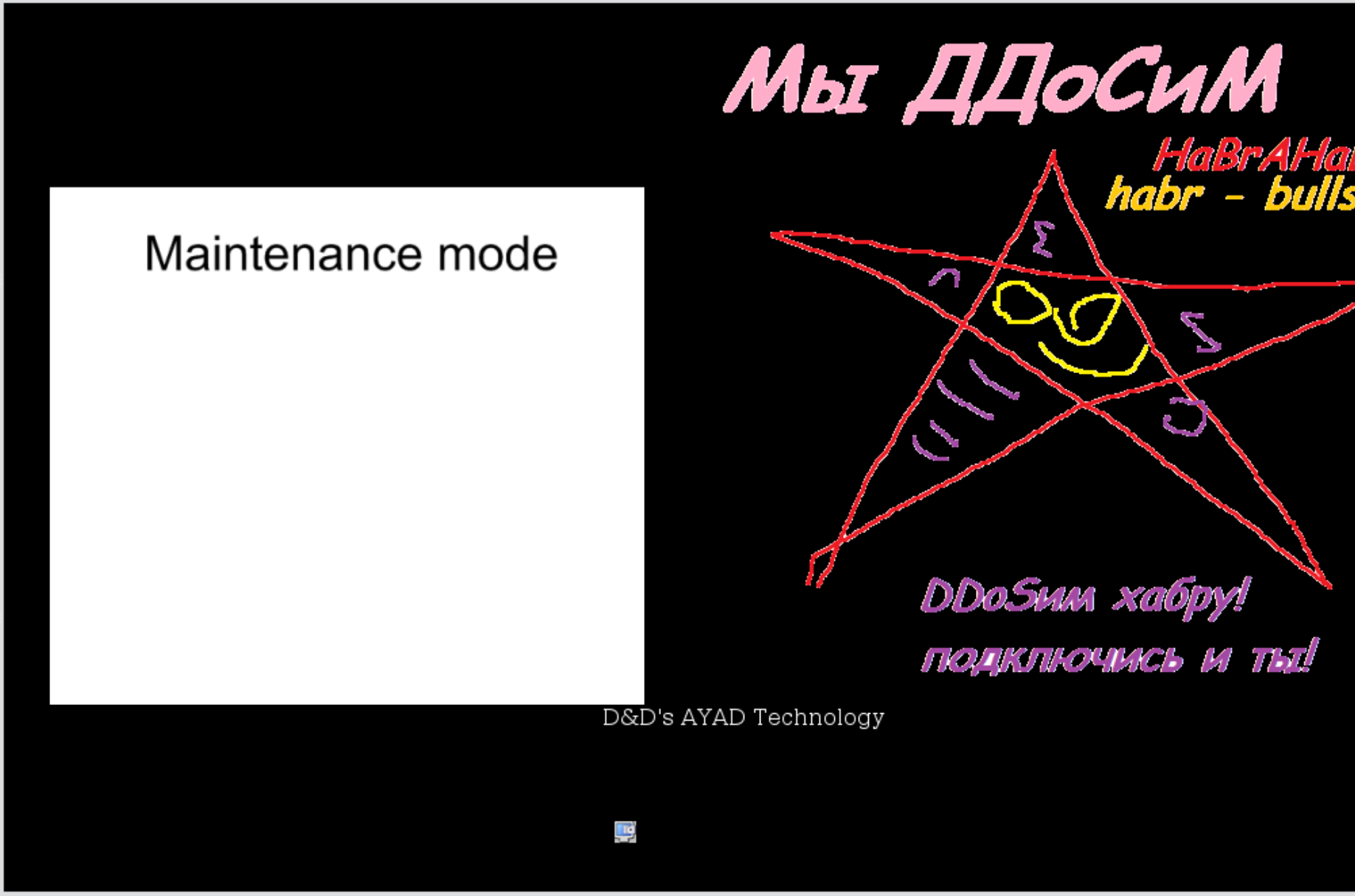
"*what is your ip address 178.248.233.23. you've done ip flooding / ddos to my server. please stop to all conveniently. thx*

```
178.248.233.23.80 > x.x.x.x.56834: S ack
178.248.233.23.80 > x.x.x.x.3821: S ack
178.248.233.23.80 > x.x.x.x.4947: S ack
178.248.233.23.80 > x.x.x.x.4948: S ack
178.248.233.23.80 > x.x.x.x.32935: S ack
```

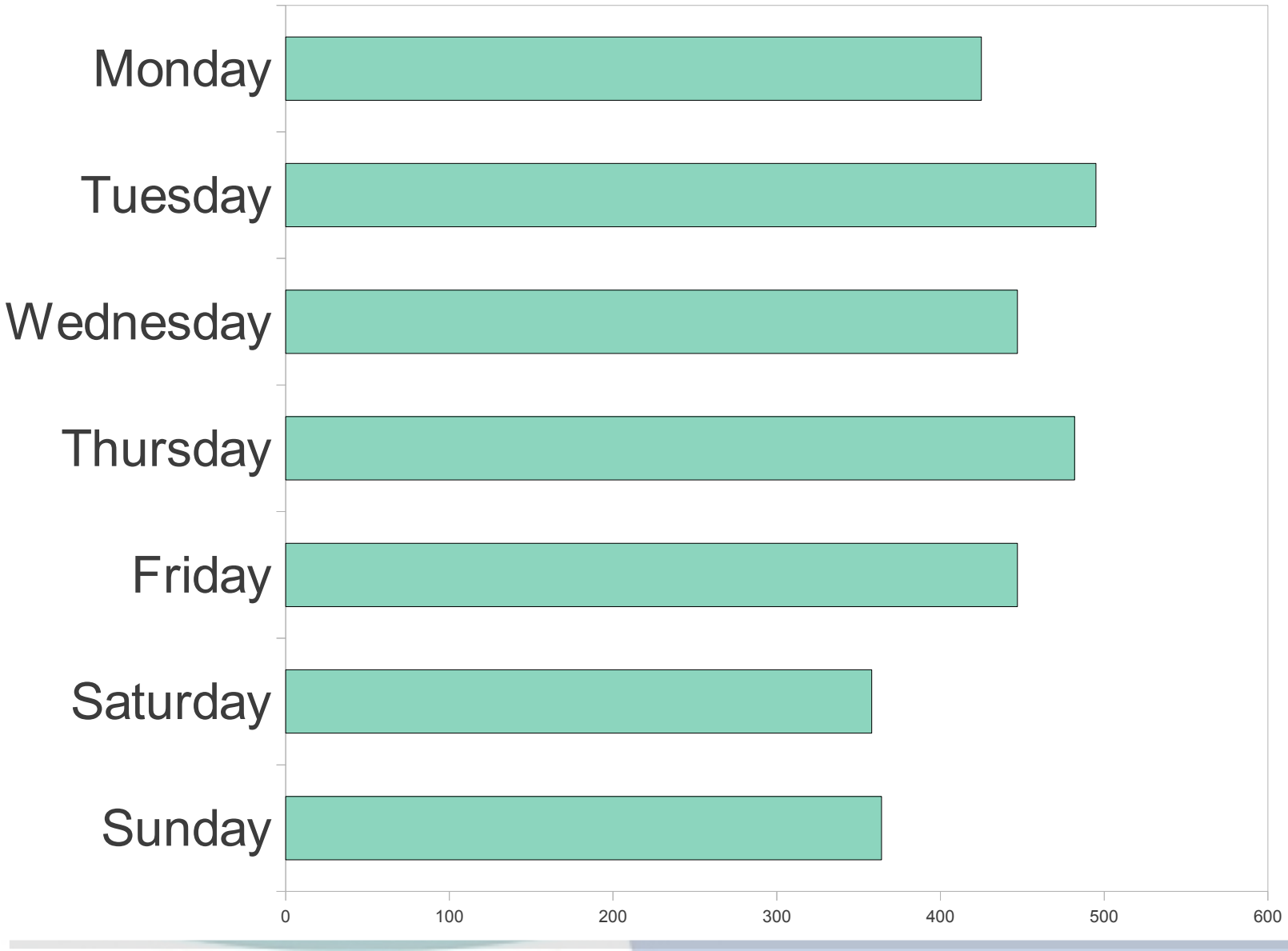
Statistics

- Max. registered bandwidth:
  56 Gbps (July, 2011)
- Max. botnet size:
  200000 bots (December, 2011)
- 4 attacks from multiple botnets simultaneously
- Attacks often utilize the newest vulnerabilities

ид Журнал Закладки Инструменты Справка

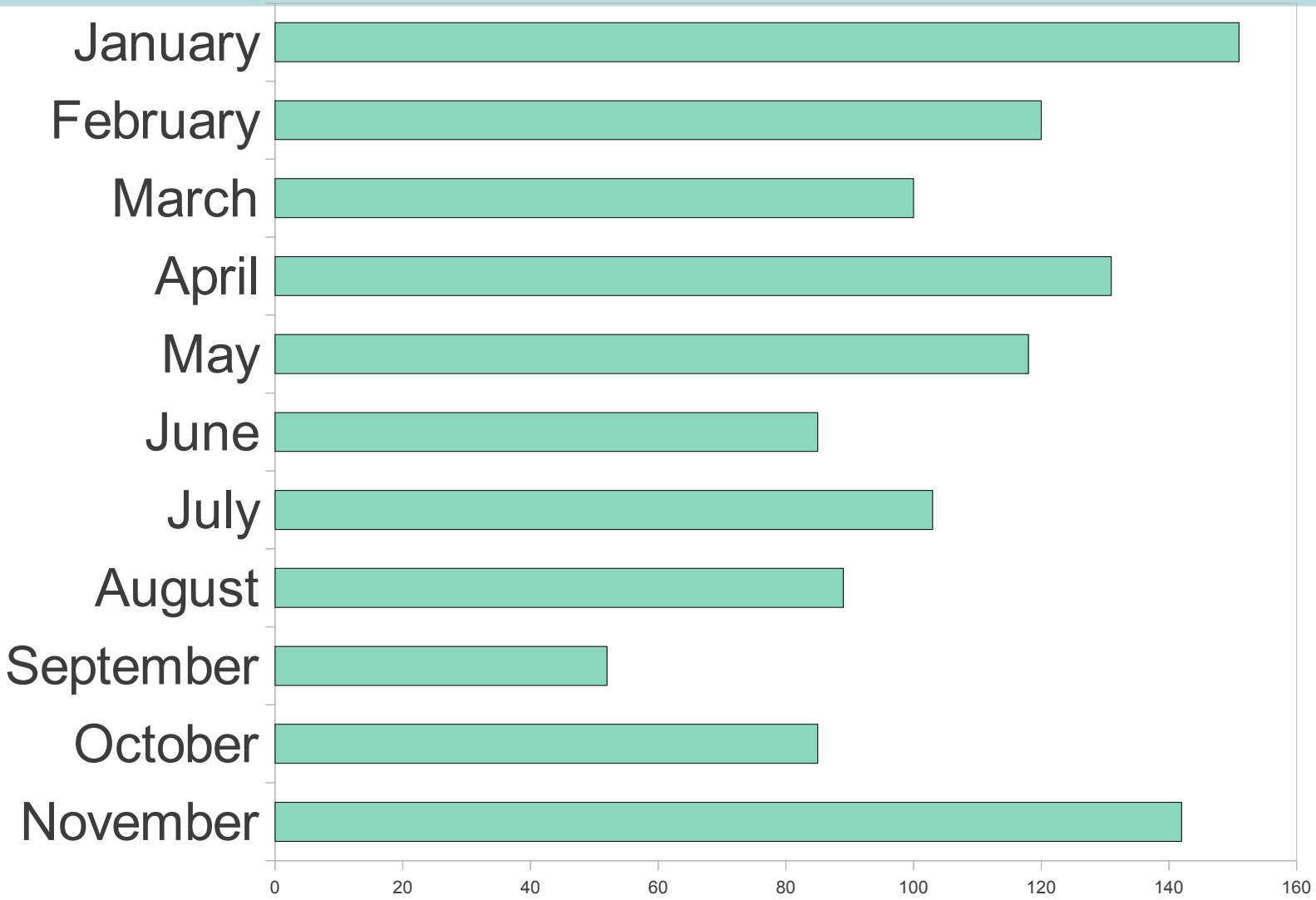


http://www.nic.ly/


Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday
0
100
200
300
400
500
600

ISPs

- Weekends often see larger attacks
- ISP tech. support in Russia works better on workdays
- ISPs and IXPs often totally ignore abuses



December excluded as untypical (legislative election)

Attack Goals

- Money
- Politics
- Botnet promotion
- Protest

+ B1TCo1N$: BKDR_BTMINE.DDOS