Beyond the botnet.

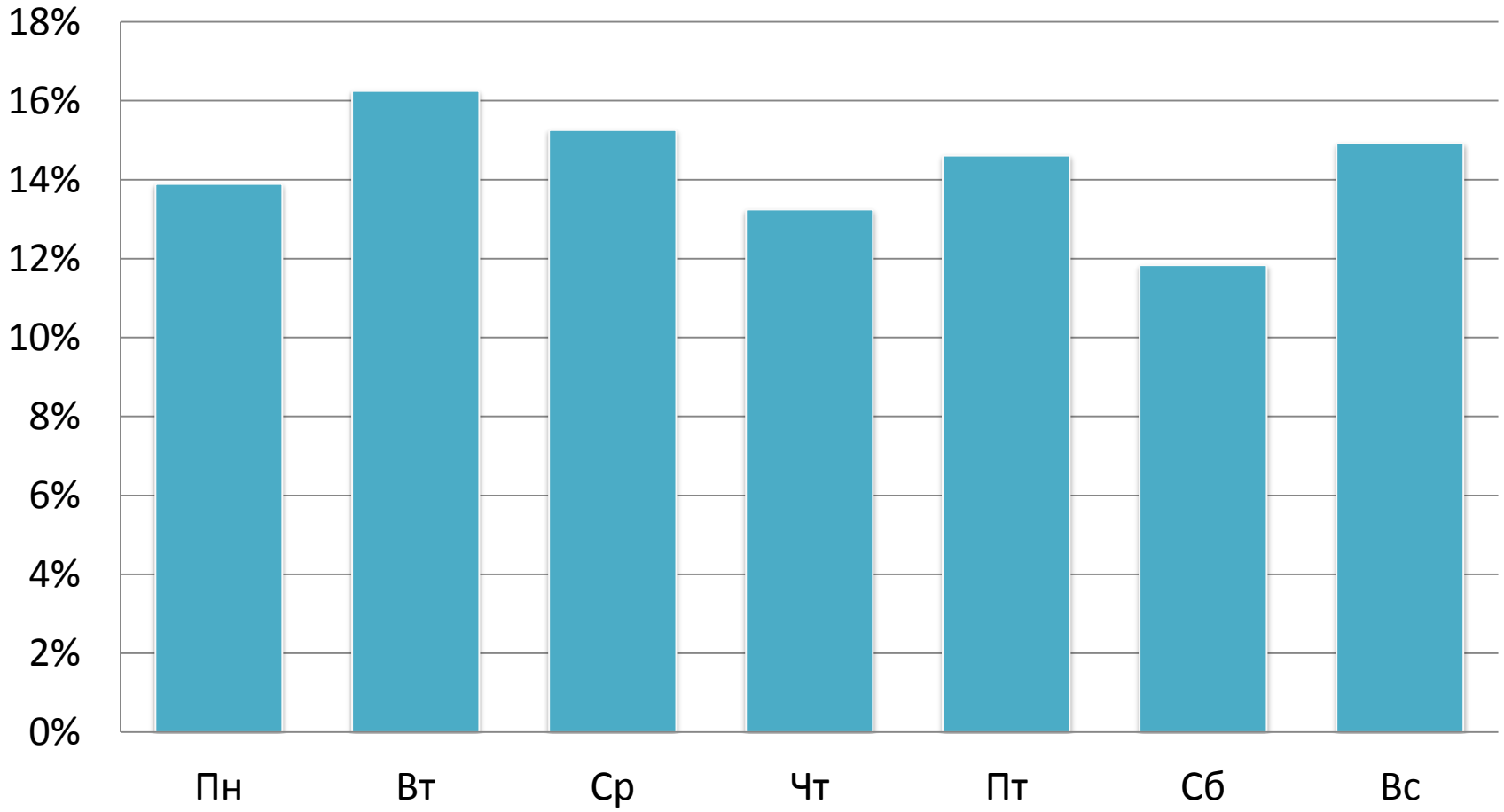
Александр Лямин
<la@highloadlab.com>

Qrator: 2012

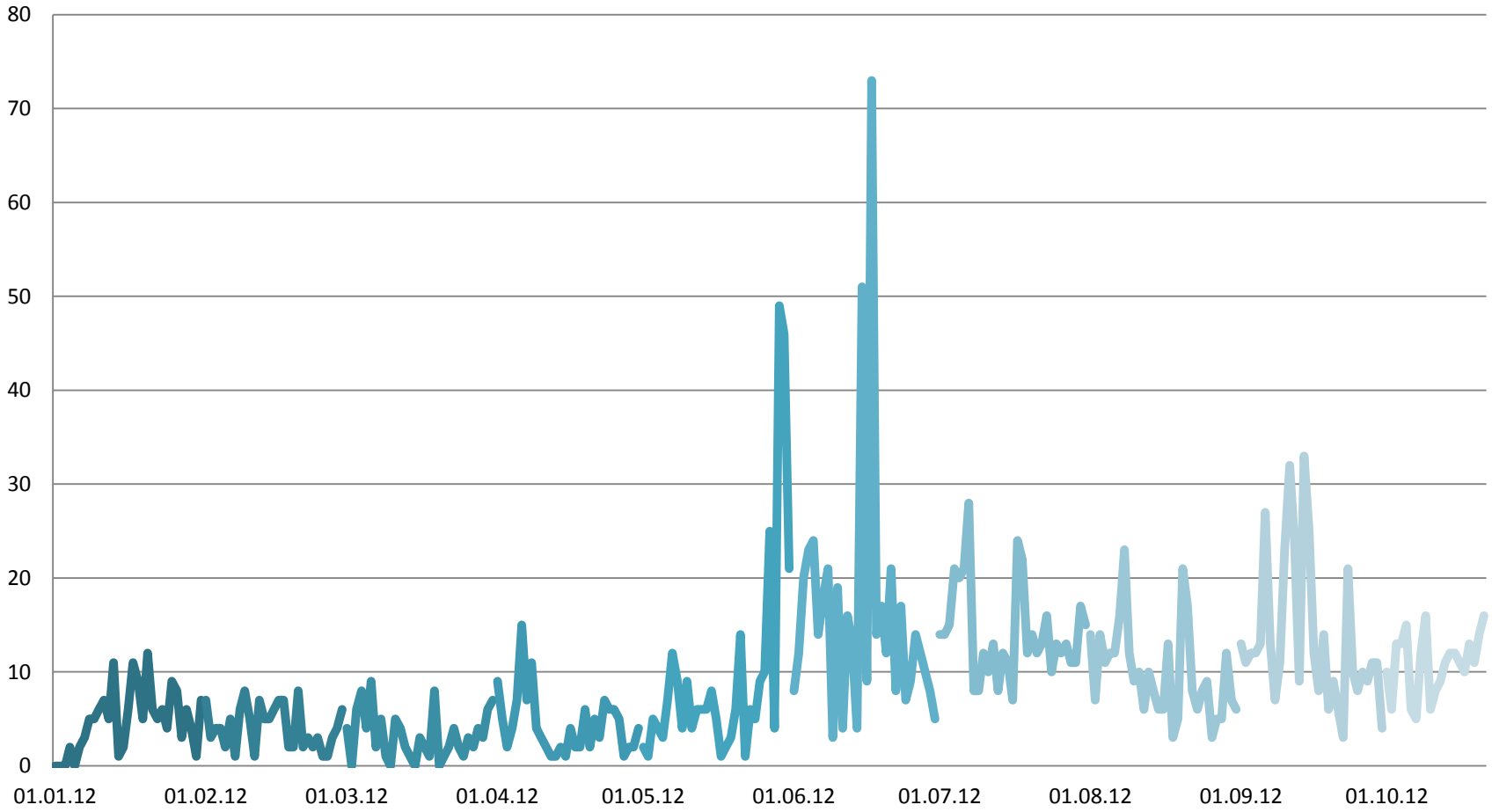
2012 2011

- Нейтрализовано атак: **2628**↑ (1972)
- Среднее атак в день: **9.18**↑ (6.16)
- Макс. в день: **73**↑ (32)
- Средний ботнет: **2070**↑ (1886)
- Макс. размер ботнета: **148563**↓ (239911)
- Макс. длительность: 83d↓ (253d)
- Средняя доступность:99.71%

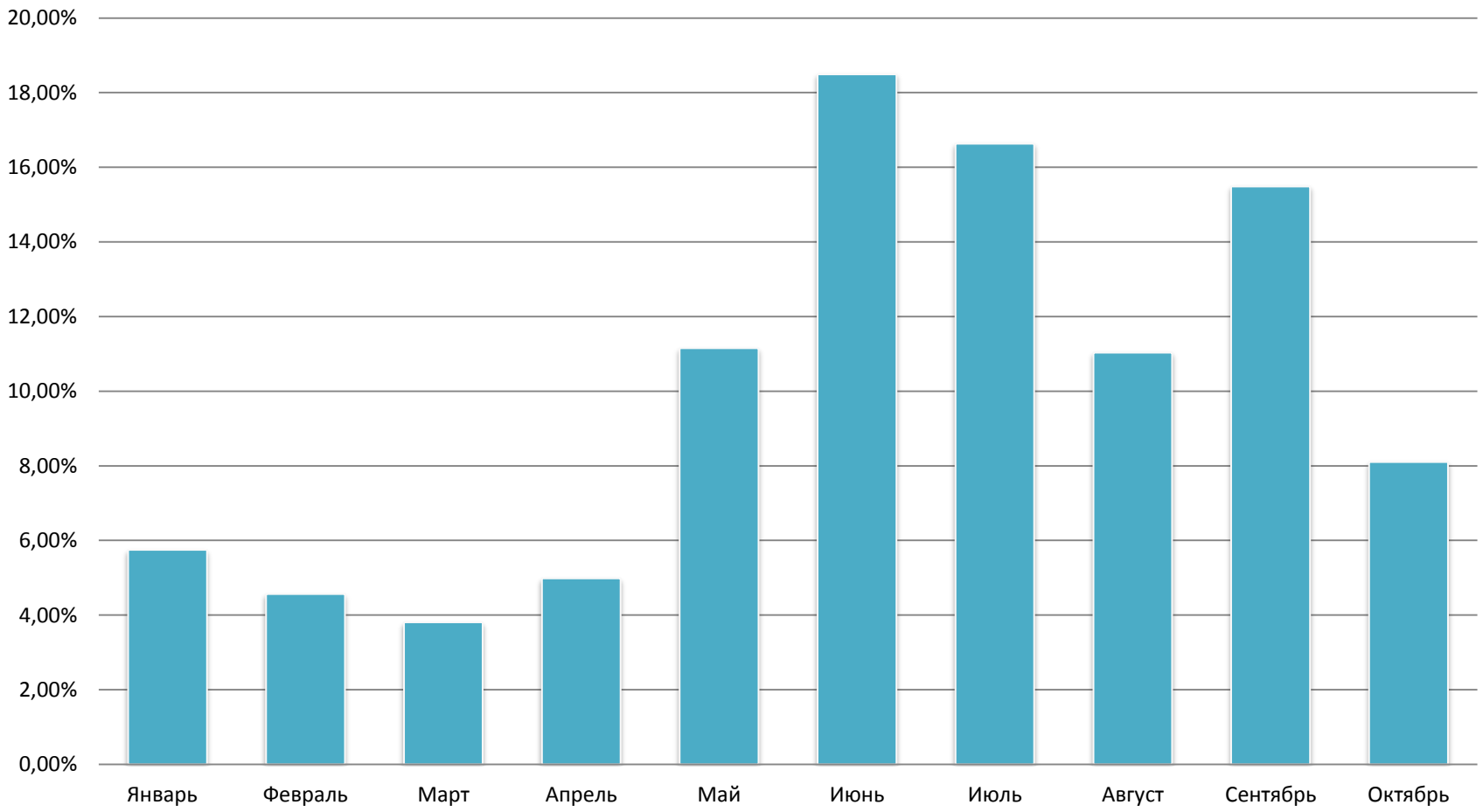
По дням недели.



По дням.

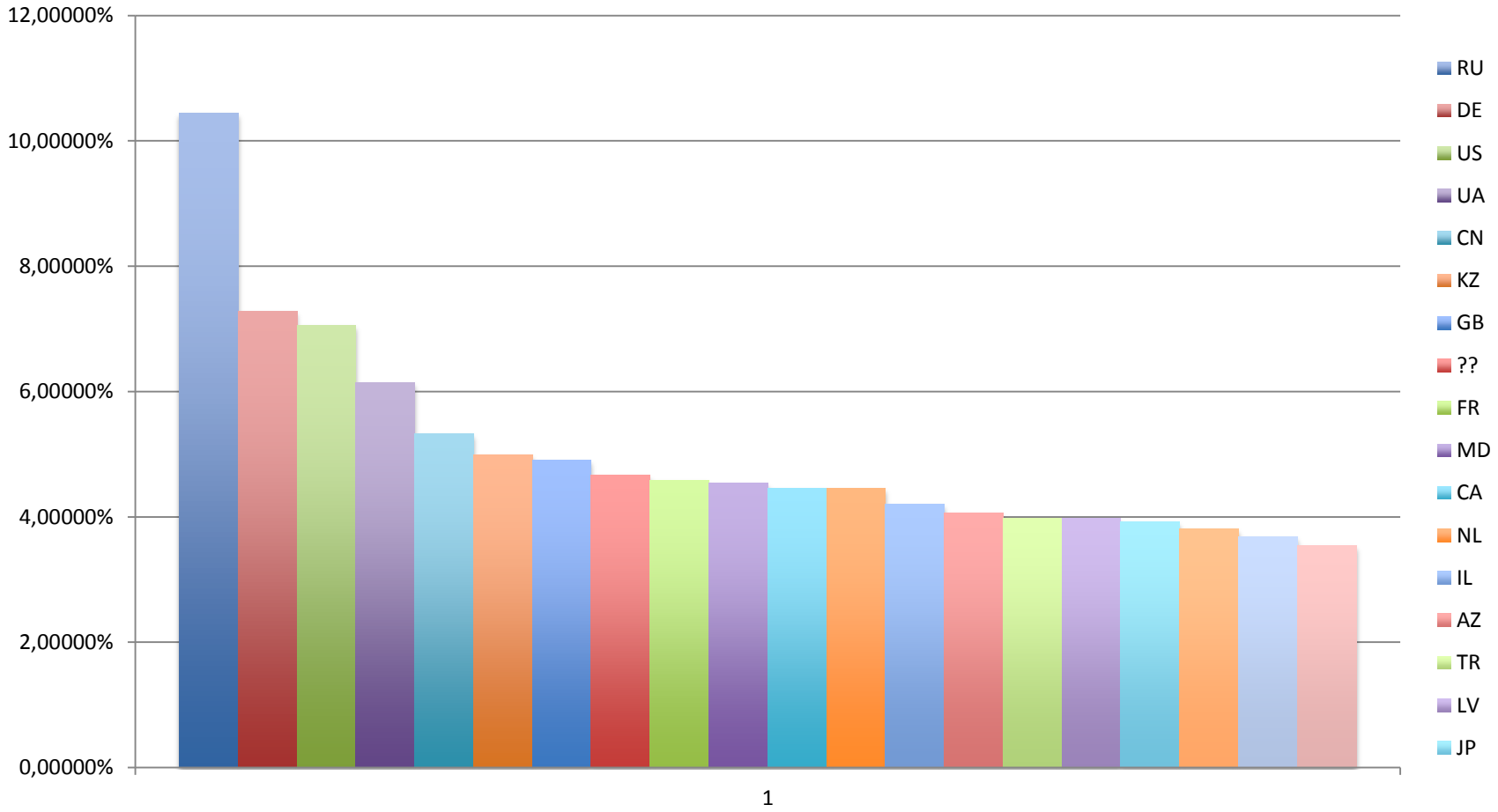

80
70
60
50
40
30
20
10
0
01.01.12
01.02.12
01.03.12
01.04.12
01.05.12
01.06.12
01.07.12
01.08.12
01.09.12
01.10.12

По месяцам.

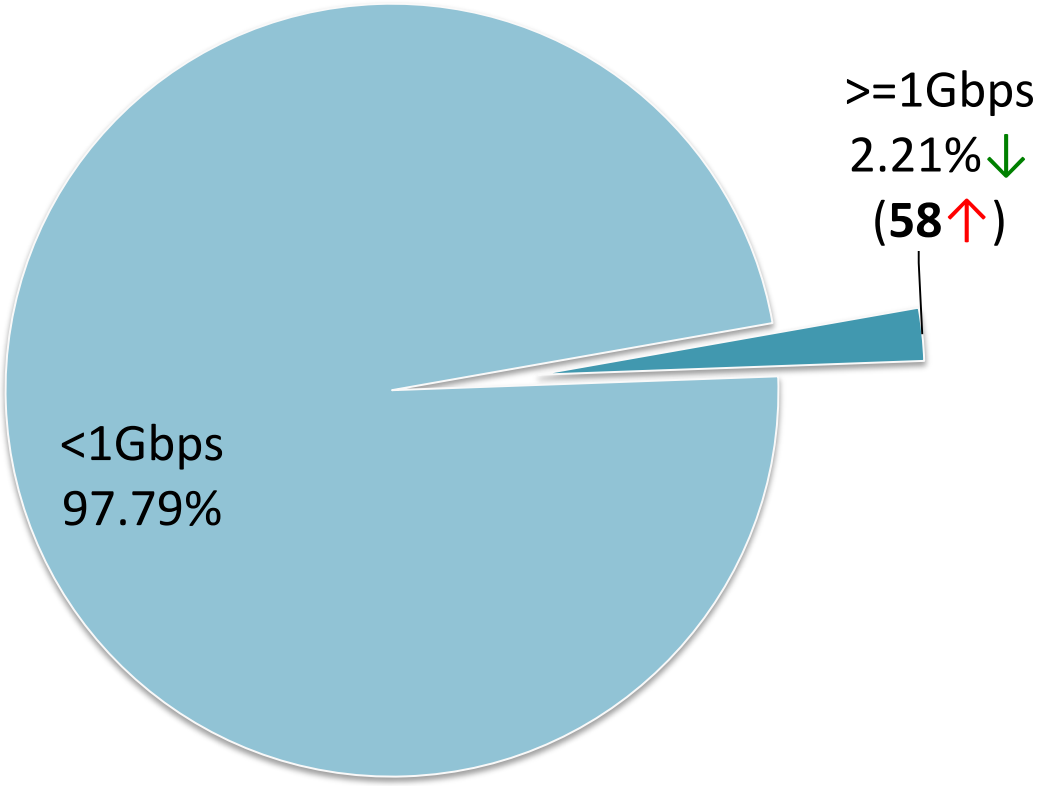

20,00%
18,00%
16,00%
14,00%
12,00%
10,00%
8,00%
6,00%
4,00%
2,00%
0,00%
Январь
Февраль
Март
Апрель
Май
Июнь
Июль
Август
Сентябрь
Октябрь

Где живут ботнеты.

(геопривязка)

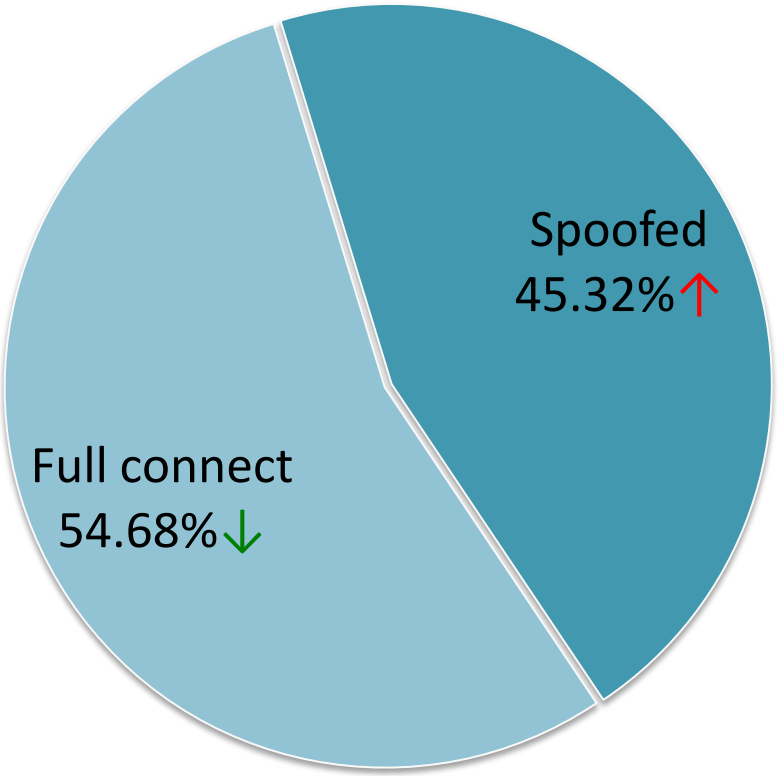


Скоростные атаки.

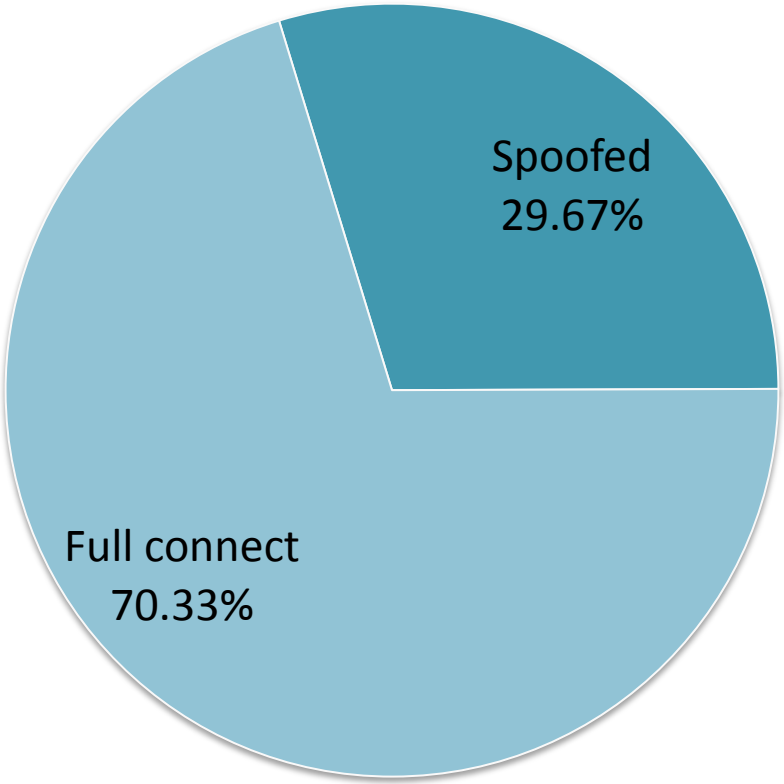


>=10Gbps 28

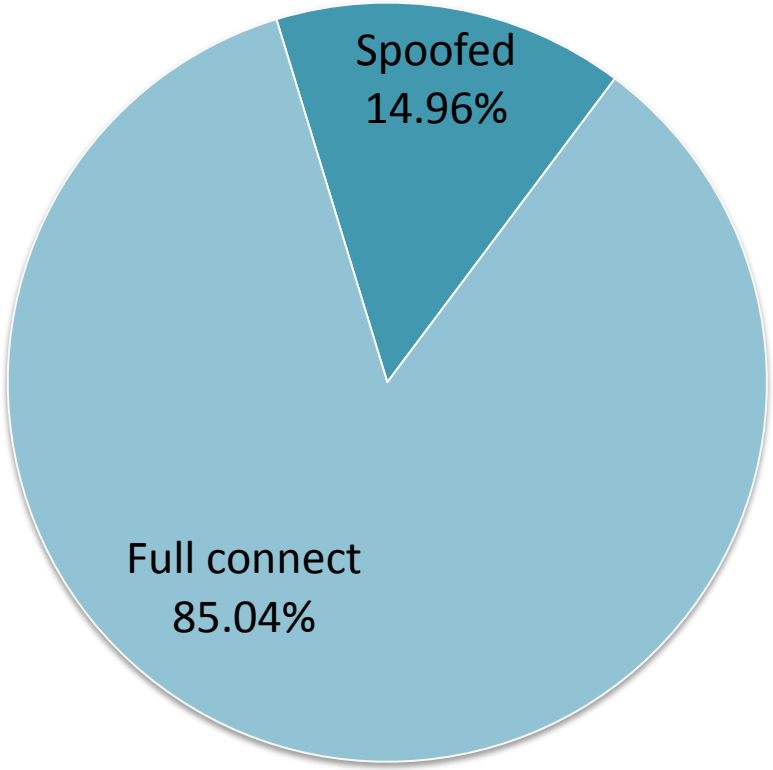
Типы атак.



Типы атак Q1 2012



Типы атак 2011.



И снова о скоростях.

PPS

Защищающаяся сторона.

- Доступные L7 контр-меры

VS

- Настроенный сервер – 600kpps
- Спец.конфигурация и настройки - 1Mpps

Нападение.

- Конкуренция за ботнет.
- Эффективные L7 контрмеры.

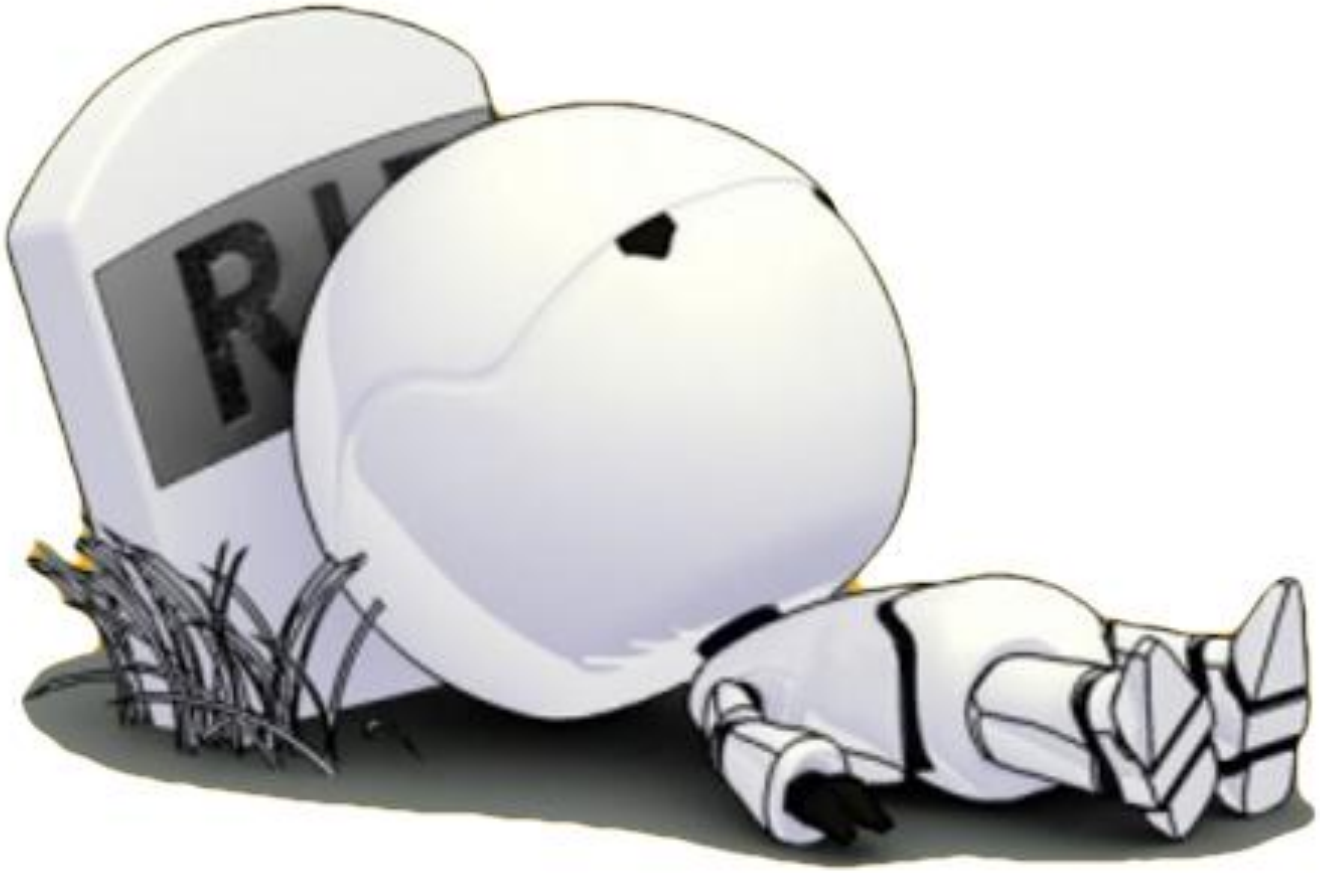
VS

- Доступный инструментарий (i.e. netmap)
- Опорные сети, хостинги и IX пропускающие spoofed flood.

Специфика ботнетов.

- Посредственная связность.
- Ограниченность ресурсов.
- Ограниченность возможностей.

Old and busted.



Сетевая топология.

- Протоколы маршрутизации.
- Проколы маршрутизации ;)
- Индуцируемые проколы маршрутизации.

TCP стэк.

- Состояния.
- Таймауты.
- (Неспецифицированные) переходы.

Helping hand – IPV6

IPV6

- Размеры структур данных.
- Плотность адресации.

Что еще интересного?

- BGP Flowspec* enabled networks (радуемся**)
- Google’s TFO (выдыхаем)
- DNS/DNSSEC – void (медитируем)
- RPKI – все так-же обсуждается (молимся)
- IPV6 – будет много «приключений»
- Обновили мировой рекорд:268Gbps/32Mpps

* RFC-5575

** Не все и не всегда.

Вопросы?