HighLoad++

Динамика DDoS-атак в России

Александр Лямин

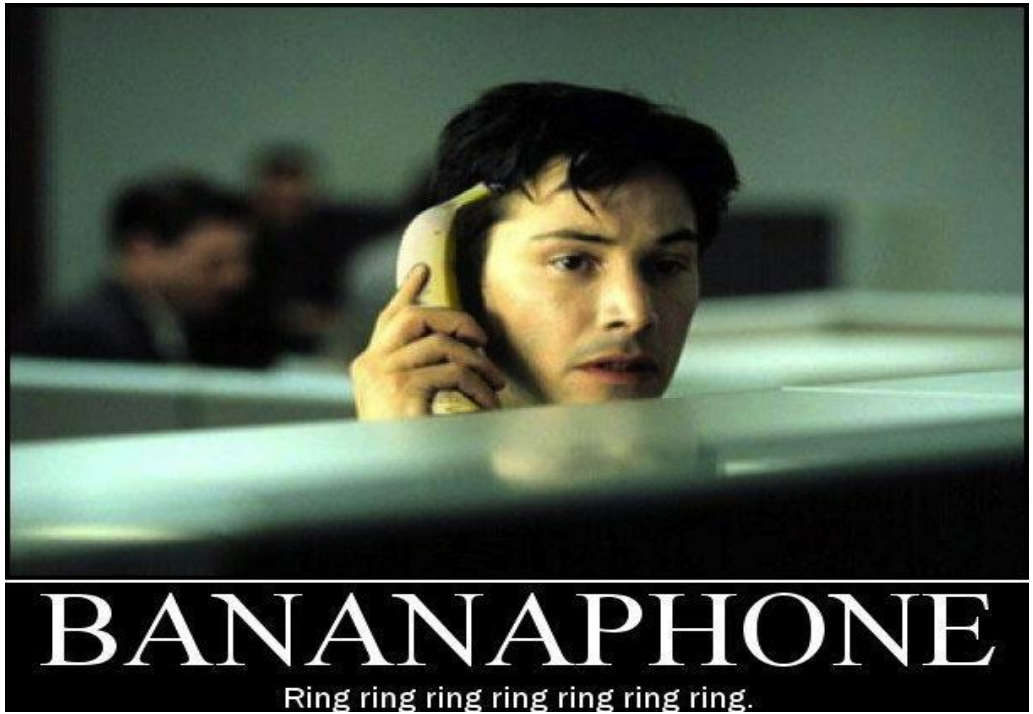
<la@highloadlab.com>

HighLoad++

2010

HighLoad++

True story!

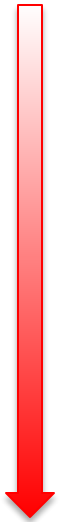


2010

- 600+ обратившихся за помощью
- 15+ атак > 1Gbps
- 4 атаки > 3Gbps
- 2 > 5Gbps
- 1 > 10Gbps

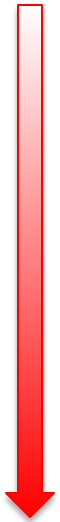
Типы атак

Исчерпание канальной емкости	100k+
Инфраструктура сети	10k+
Сетевой стек системы	1k+
Приложение	100+



Типы атак

Исчерпание канальной емкости	12.5Gbps
Инфраструктура сети	DNS
Сетевой стек системы	A.G.
Приложение	Slow Smart Bots



Свойства ботнета

- Транснациональность
- Инертность
- Ущербность
- Жадность
- Конечность

Свойства ботнета

- ~~Транснациональность~~
- Инертность
- Ущербность
- Жадность
- Конечность

Свойства ботнета

- ~~Транснациональность~~
- ~~Инертность~~
- Ущербность
- Жадность
- Конечность

Свойства ботнета

- ~~Транснациональность~~
- ~~Инертность~~
- ~~Ущербность~~
- Жадность
- Конечность

Свойства ботнета

- ~~Транснациональность~~
- ~~Инертность~~
- ~~Ущербность~~
- Жадность?
- Конечность

Свойства ботнета

- ~~Транснациональность~~
- ~~Инертность~~
- ~~Ущербность~~
- Жадность! Но иначе…
- Конечность

HighLoad++

DDoS без ботнета

DDoS без ботнета

- DNS Amplification
- И без DNS Amplification
- И Amplification без DNS (NTP)
- … и еще, но об этом завтра.

Особый случай

DDoS пришел на ваше приложение,

но цель

не

ВЫ

HighLoad++

Как сделать мир лучше?

RTFM!

- Network Ingress Filtering (IETF BCP-38)
- UDP Services (RIPE-52 DNSAMP)

HighLoad++

Расследования

SLA

- Bandwidth (Active/Passive)
- Uptime
- Problem Escalation

HighLoad++

Спасибо.

Александр Лямин

<la@highloadlab.com>