

hl⁺⁺

HighLoad⁺⁺

Динамика DDoS-атак в России

Александр Лямин
<la@highloadlab.com>

hl⁺⁺

HighLoad⁺⁺

2010



hl⁺⁺

HighLoad⁺⁺

True story!



2010

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

Типы атак

Исчерпание канальной емкости

Инфраструктура сети

Сетевой стек системы

Приложение

100k+

10k+

1k+

100+



Типы атак

Исчерпание канальной емкости

Инфраструктура сети

Сетевой стек системы

Приложение

12.5Gbps

DNS

A.G.

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

hl⁺⁺

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

hl⁺⁺

HighLoad⁺⁺

Как сделать мир лучше?



WFO & THE ORACLE

RTFM!

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

hl⁺⁺

HighLoad⁺⁺

Расследования



hl⁺⁺

HighLoad⁺⁺

SLA

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

hl⁺⁺

HighLoad⁺⁺

Спасибо.

Александр Лямин

<la@highloadlab.com>