

# JET SECURITY CONFERENCE



## VIII ежегодная конференция Центра информационной безопасности

1-2 июня 2017 года

[WWW.JET.SU](http://WWW.JET.SU)



# Секция Защита web-приложений

01

**АЛЕКСАНДР ЛОПАТИН**

Как прокачать защиту web.  
Программы «минимум» и  
«максимум»

02

**АЛЕКСАНДР СЕРЕБРЯКОВ**

Подходы F5 к обеспечению вашей  
информационной безопасности

03

**АЛЕКСАНДР ШАХЛЕВИЧ**

Тренды безопасности web-  
приложений и основные  
компоненты надежного WAF

04

**ЕКАТЕРИНА СЮРТУКОВА**

Аутсорсинг эксплуатации WAF.  
Жизнь после внедрения

05

ВОПРОСЫ- ОТВЕТЫ



**JET** CONFERENCE

01/06/2017

# Как прокачать защиту web. Программы «минимум» и «максимум»

Александр Лопатин,  
менеджер по продвижению ЦИБ



## Событие года



- › Mirai (400 тыс.) – не самый большой, но самый известный ботнет
- › Количество IoT устройств 8,4 млрд., 5 млн новых устройств в день
- › Открытый, легко модифицируемый модульный код

## Смена парадигмы

- › Уязвимые протоколы (Dns, NTP, SSDP, Chargen, MSSQL и пр.)
- › Ботсеть сравнительно небольшого размера
- › Уязвимые хосты-отражатели
- › Спуфинг
- › Амплификация



- › Уязвимые IoT-устройства
- › Очень большие ботсети
- › Амплификация не требуется
- › Спуфинг не требуется
- › Любой тип атаки доступен
- › Боты сложно отличить от легальных пользователей

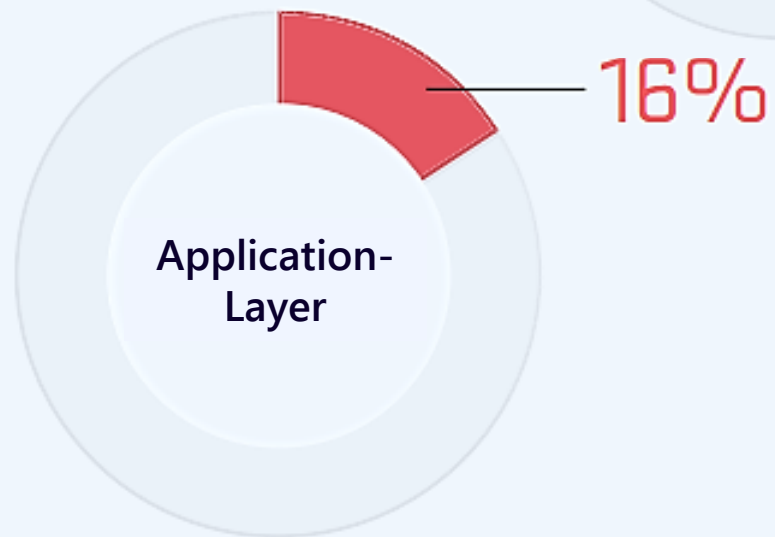
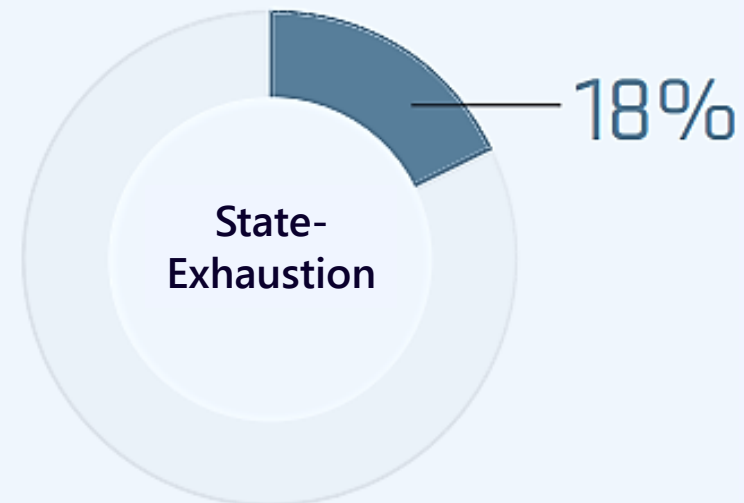
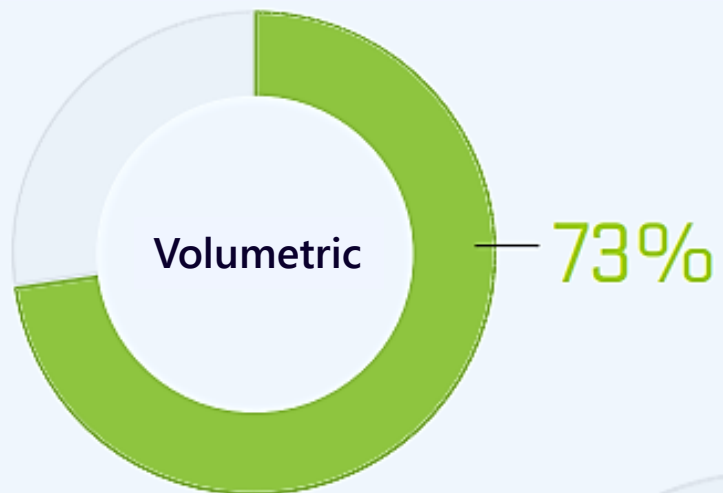
# JET

CONFERENCE

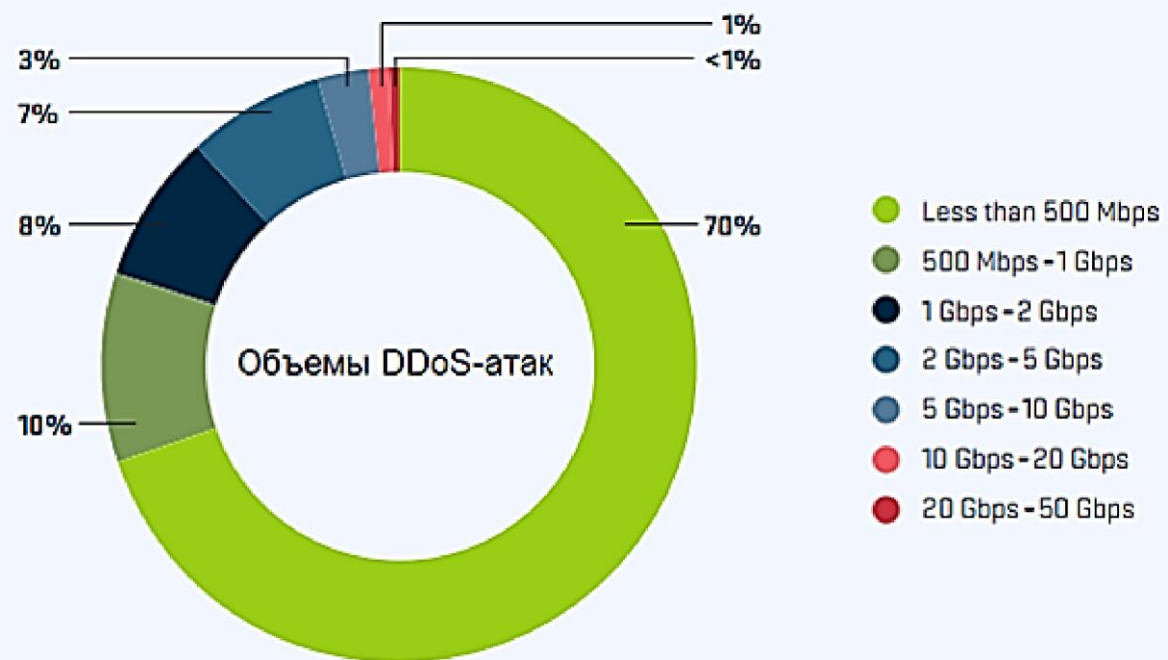
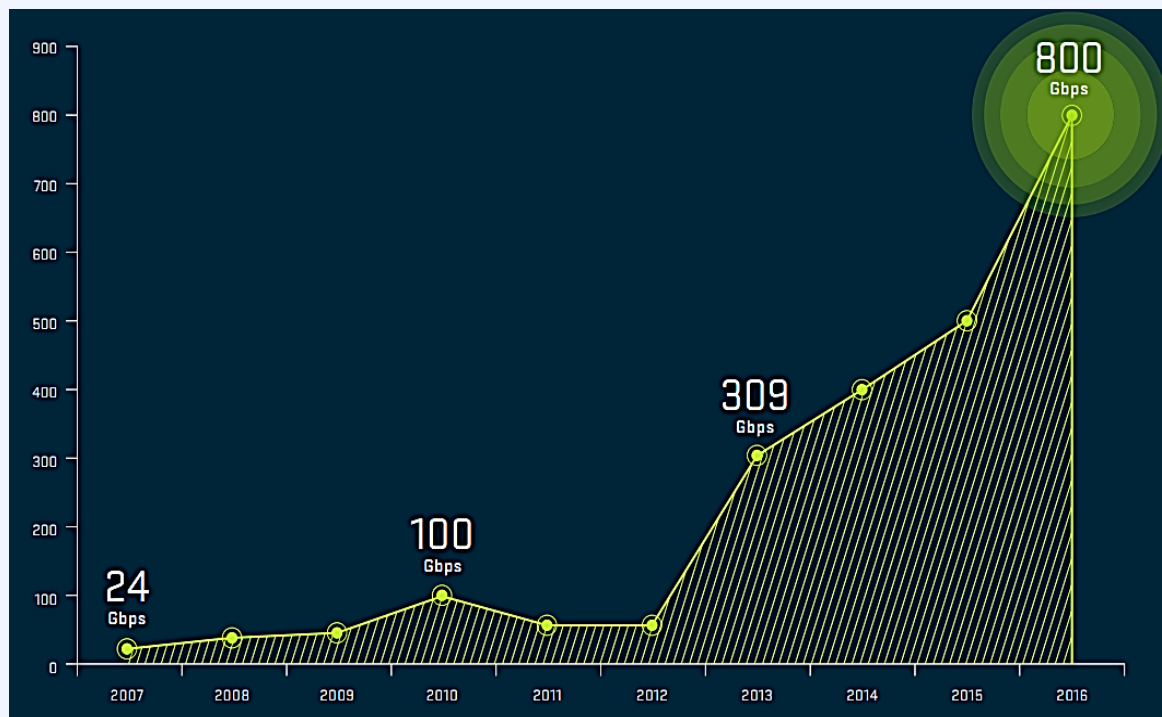
## «Стрессерный» бум

MONTHLY BRONZE	MONTHLY SILVER	MONTHLY DIAMOND
19.99\$	24.99\$	29.99\$
☉ XyZ Public Network	☉ XyZ Public Network	☉ XyZ Public Network
☉ 150-200Gbps Network Capacity	☉ 150-200Gbps Network Capacity	☉ 150-200Gbps Network Capacity
☉ 26 Attack Methods	☉ 26 Attack Methods	☉ 26 Attack Methods
☉ 1800(s) Stress Time	☉ 2400(s) Stress Time	☉ 3600(s) Stress Time
☉ 1 Months Membership	☉ 1 Months Membership	☉ 1 Months Membership
☉ 1 Parallel attacks	☉ 1 Parallel attacks	☉ 1 Parallel attacks

## Распределение атак

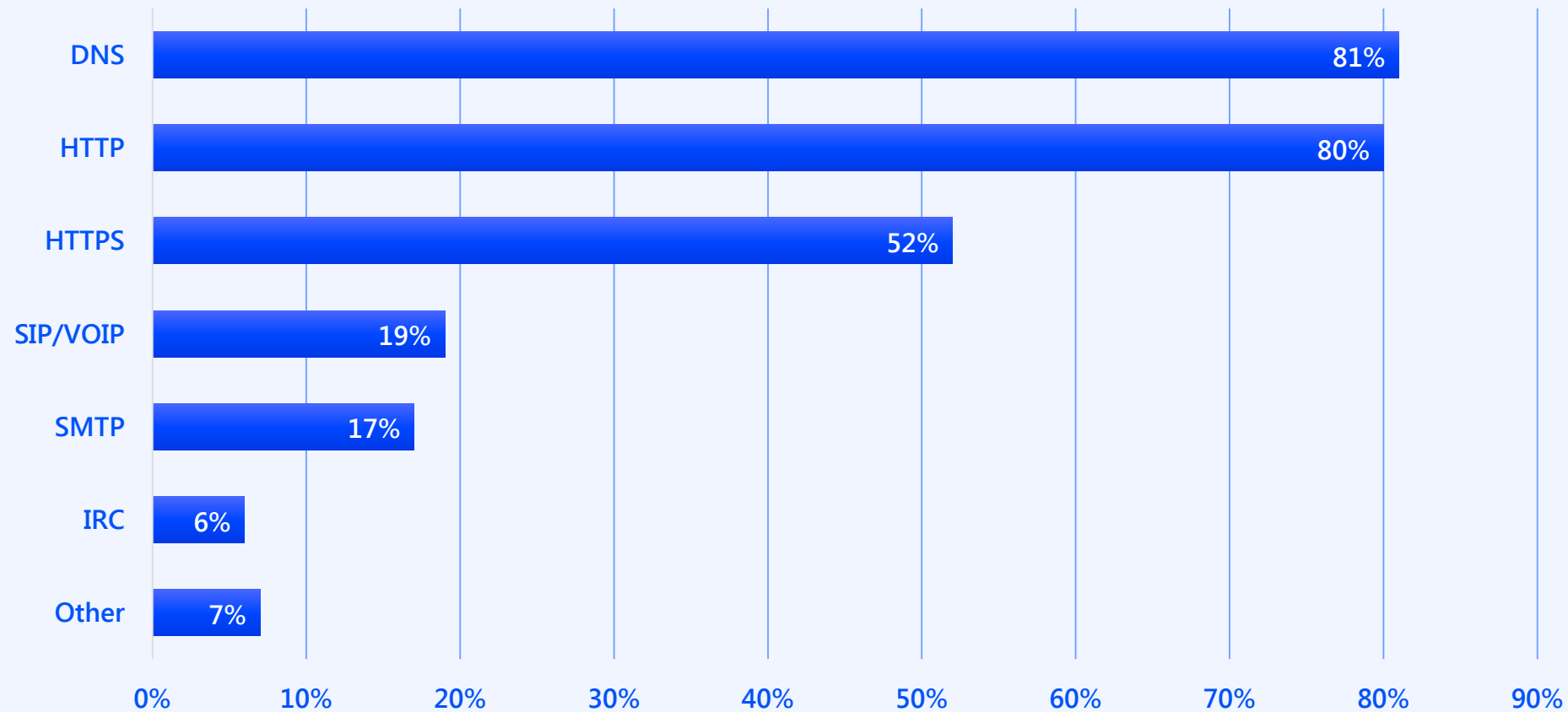


## Новый рекорд volumetric-атаки





## Application Layer



## Программы защиты

### Вчерашний день



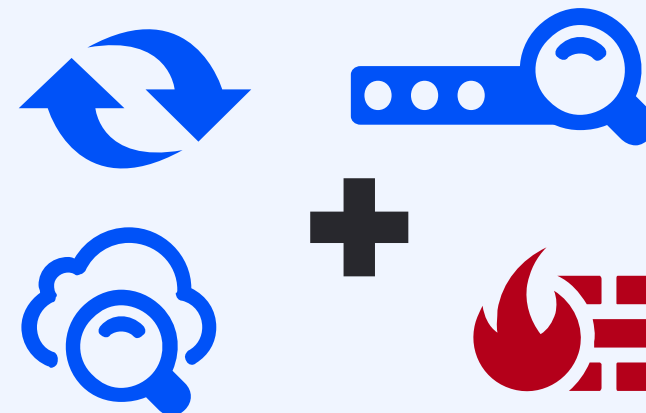
Фильтрация DDoS  
on-demand в облаке

### Econom



Фильтрация DDoS  
always-on в облаке  
+  
WAF в облаке

### Standard



Фильтрация DDoS в облаке +  
фильтрация DDoS on-premise +  
облачная сигнализация +  
WAF on-premise

## SSL требует отдельного внимания

Сервер в 15 раз больше  
клиента тратит ресурсов на SSL  
соединение

Для облачной фильтрации  
SSL требуется передача  
закрытых ключей



Традиционные средства  
защиты «не смотрят»  
внутри SSL

IoT-ботнеты научатся  
проводить SSL-атаки в 2017

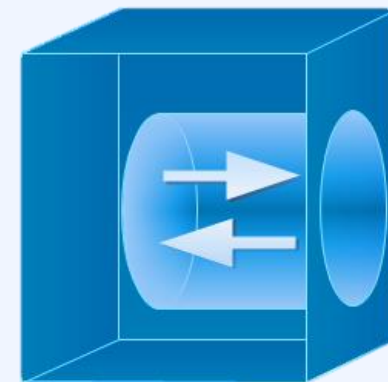
## Защита SSL



Увеличение количества  
application-серверов



Передача ключей  
в облако anti-DDoS и  
WAF сервис-провайдера



SSL terminator

Вынос задачи терминации  
SSL на выделенные  
устройства защиты  
с аппаратной акселерацией





**JET** CONFERENCE

01/06/2017

**ИНФОСИСТЕМЫ ДЖЕТ**

Спасибо за внимание!