ЛОГИКА ПОСТРОЕНИЯ РЕШЕНИЯ ПО ЗАЩИТЕ ОТ DDOS-АТАК

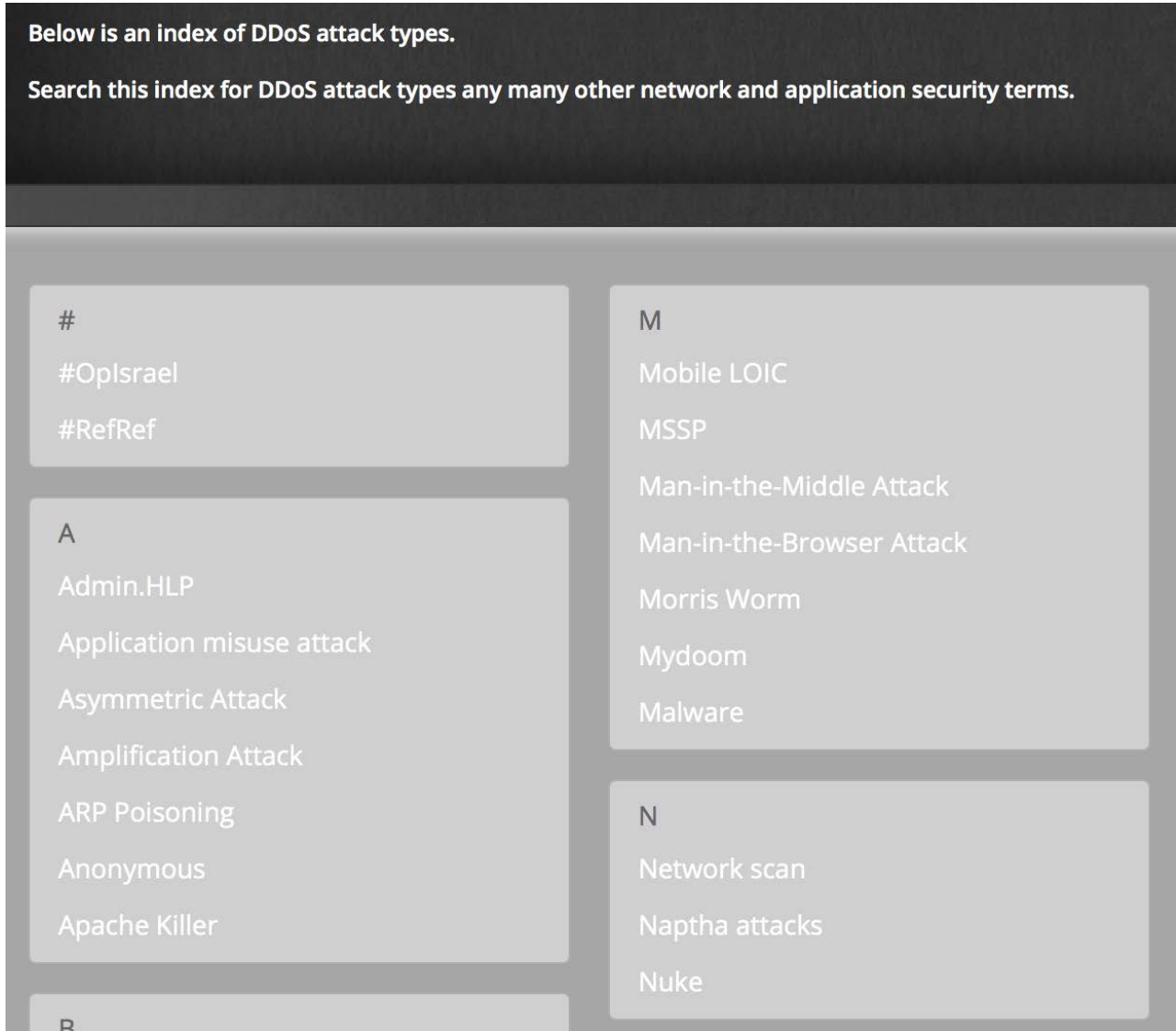
ВЗАИМОСВЯЗЬ С АКТУАЛЬНЫМИ УГРОЗАМИ

QRATOR

Классификация атак

Классификация списком?

- Но от каких из этих атак нужно защищаться?
- Что с теми атаками, которых нет в списке в документации на решение?
- Что, если появятся новые атаки – покупать новое оборудование?



Классификация атак

ISO/OSI:

- L2
- L3
- L4
- L5-L7

- Каждый из уровней сети выполняет свою функцию, предоставляет сервис вышестоящему и зависит от нижележащего
- Если сетевой сервис не работает, значит, один из уровней сети не функционирует

Классификация атак

ISO/OSI:

- L2
- L3
- L4
- L5-L7

- Корректная классификация атак вводится, исходя из производимого эффекта с точки зрения архитектуры сети: какой именно уровень сети выводится из строя
- Такая классификация по построению состоит из взаимоисключающих и совместно исчерпывающих элементов
- Декомпозиция проблемы позволяет для каждой составляющей в отдельности построить исчерпывающее решение

Классификация атак

- L2
  ICMP Flood, UDP Flood, * Amplification, …
- L3
  Атаки на сетевую инфраструктуру
- L4
  Атаки на TCP: SYN Flood, TCP connection flood, …
- L5-L7
  Атаки прикладного уровня, имитирующие поведение пользователя

Классификация атак

- L2
  ICMP Flood, UDP Flood, * Amplification, … **1 терабит/с**
- L3
  Атаки на сетевую инфраструктуру
- L4
  Атаки на TCP: SYN Flood, TCP connection flood, …
- L5-L7
  Атаки прикладного уровня, имитирующие поведение пользователя

Атаки с амплификацией

- NTP
- DNS
- SNMP
- SSDP
- ICMP
- NetBIOS
- LDAP
- RIPv1
- PORTMAP
- CHARGEN
- QOTD
- **Quake**
- **Steam**
- …

Спад в низкоуровневых атаках

Новые угрозы

- Интернет Вещей

Интернет Вещей

- IP-камеры, роутеры, смартфоны, кофеварки…
- Дешёвое ПО без обновлений безопасности
- Число подключенных устройство растёт, а безопасность падает

Интернет Вещей

- **Множество** ботнетов

Интернет Вещей

- **Множество** ботнетов
  - Mirai

Internet

Major cyber attack disrupts internet service across Europe and US

Denial of service attack from unknown culprits on domain name system company Dyn caused access to be severely restricted for users on Friday

Интернет Вещей

- **Множество** ботнетов
  - Mirai: сложные атаки, причём не только пакетные

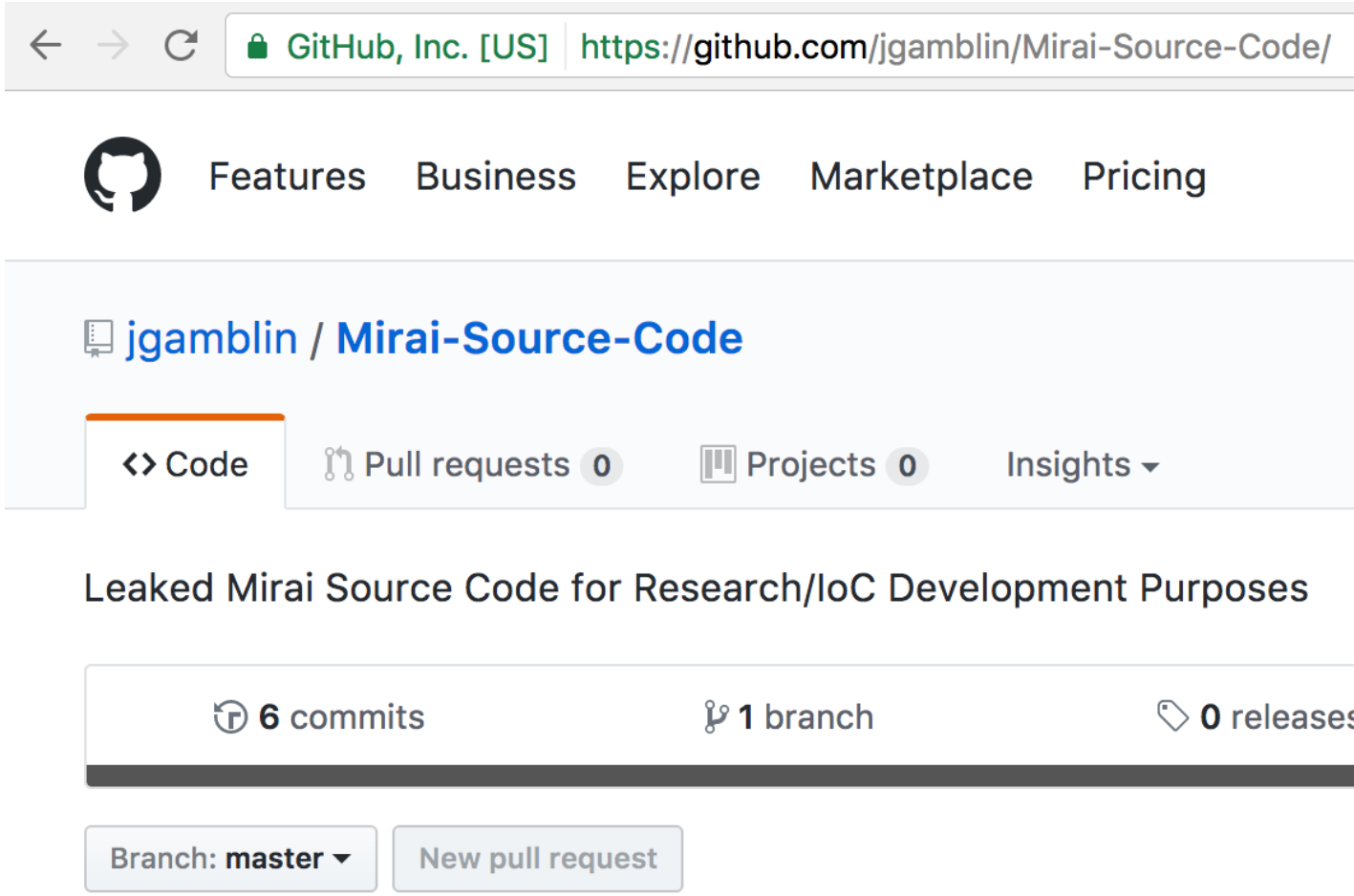
```
21:30:01.226868 IP 94.251.116.51 > 178.248.233.141:
  GREv0, length 544:
  IP 184.224.242.144.65323 > 167.42.221.164.80:
  UDP, length 512

21:30:01.226873 IP 46.227.212.111 > 178.248.233.141:
  GREv0, length 544:
  IP 90.185.119.106.50021 > 179.57.238.88.80:
  UDP, length 512

21:30:01.226881 IP 46.39.29.150 > 178.248.233.141:
  GREv0, length 544:
  IP 31.173.79.118.42580 > 115.108.7.79.80:
  UDP, length 512
```

Интернет Вещей

- **Множество** ботнетов
  - Mirai: исходный код открыт.



Интернет Вещей

- **Множество** ботнетов
  - Mirai: исходный код открыт, и только на Github 2415 fork’ов!

Mirai фактически представляет собой фреймворк для новых ботнетов, как Drupal, Joomla или ASP.NET являются фреймворками для сайтов

Couldn’t load network graph.

Too many forks to display.

Интернет Вещей

- **Множество** ботнетов
  - Mirai
  - Hajime
  - Persirai
  - …

Новые угрозы

- Интернет Вещей
- ShadowBrokers

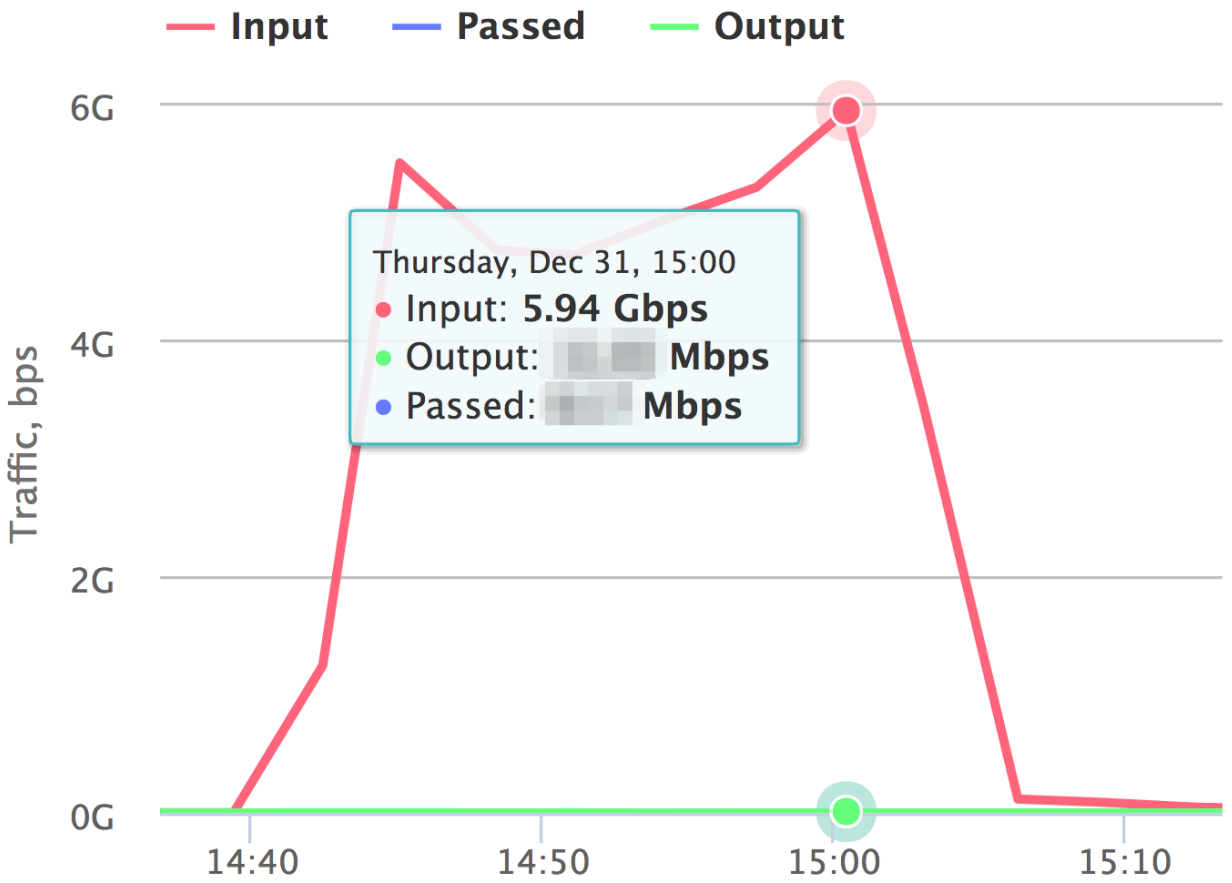
Новые угрозы

- Интернет Вещей
- ShadowBrokers
- Pingback

Wordpress **Pingback**

```
GET /whatever
User-Agent: WordPress/3.9.2;
 http://example.com/;
 verifying pingback
 from 192.0.2.150
```

- 150 000 – 170 000
  уязвимых серверов
  в одной атаке



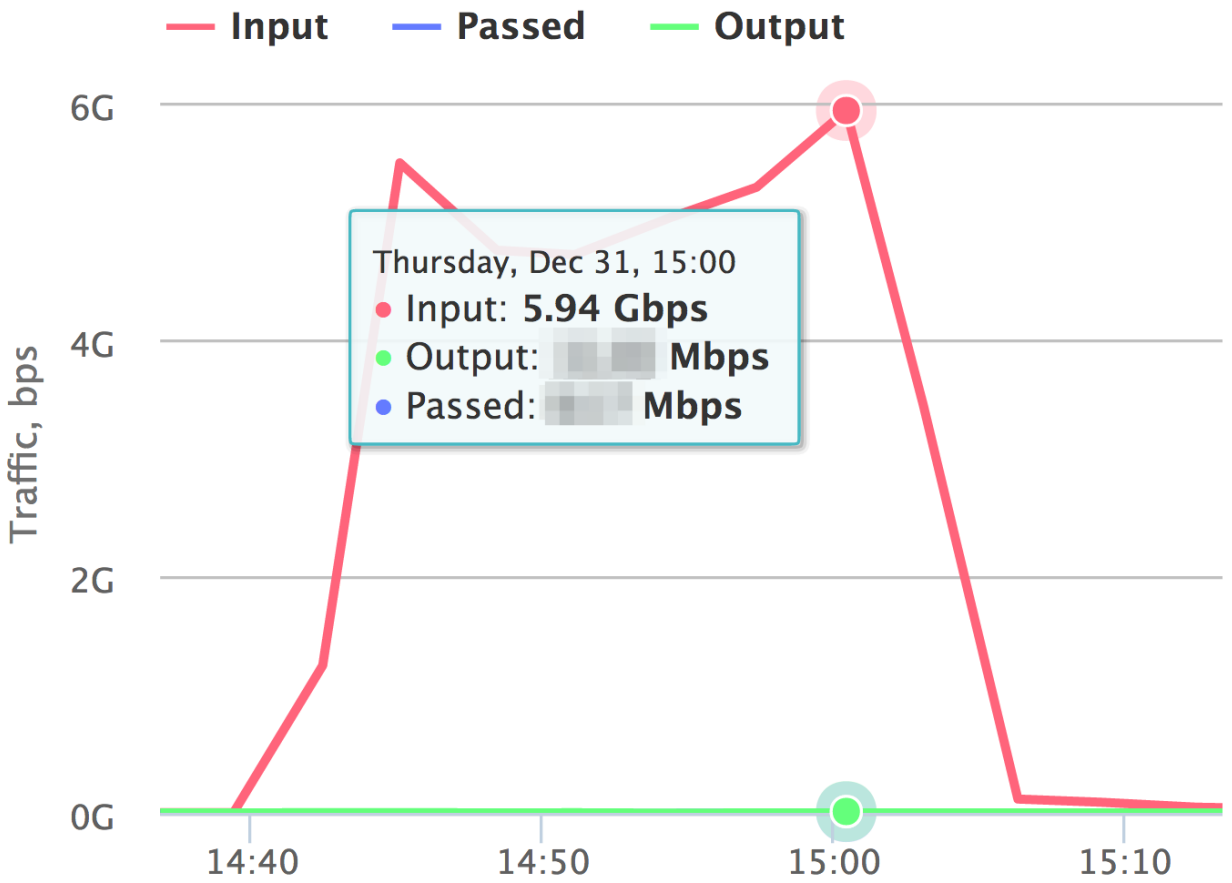
Pingback: HTTP/HTTPS

```
<methodCall>
  <methodName>pingback.ping</methodName>
  <params>
    <param>
      <value><string>https://victim.com/</string></value>
    </param>
    <param>
      <value>
        <string>
          http://reflector.blog/2016/12/01/blog_post
        </string>
      </value>
    </param>
  </params>
</methodCall>
```

Wordpress **Pingback**

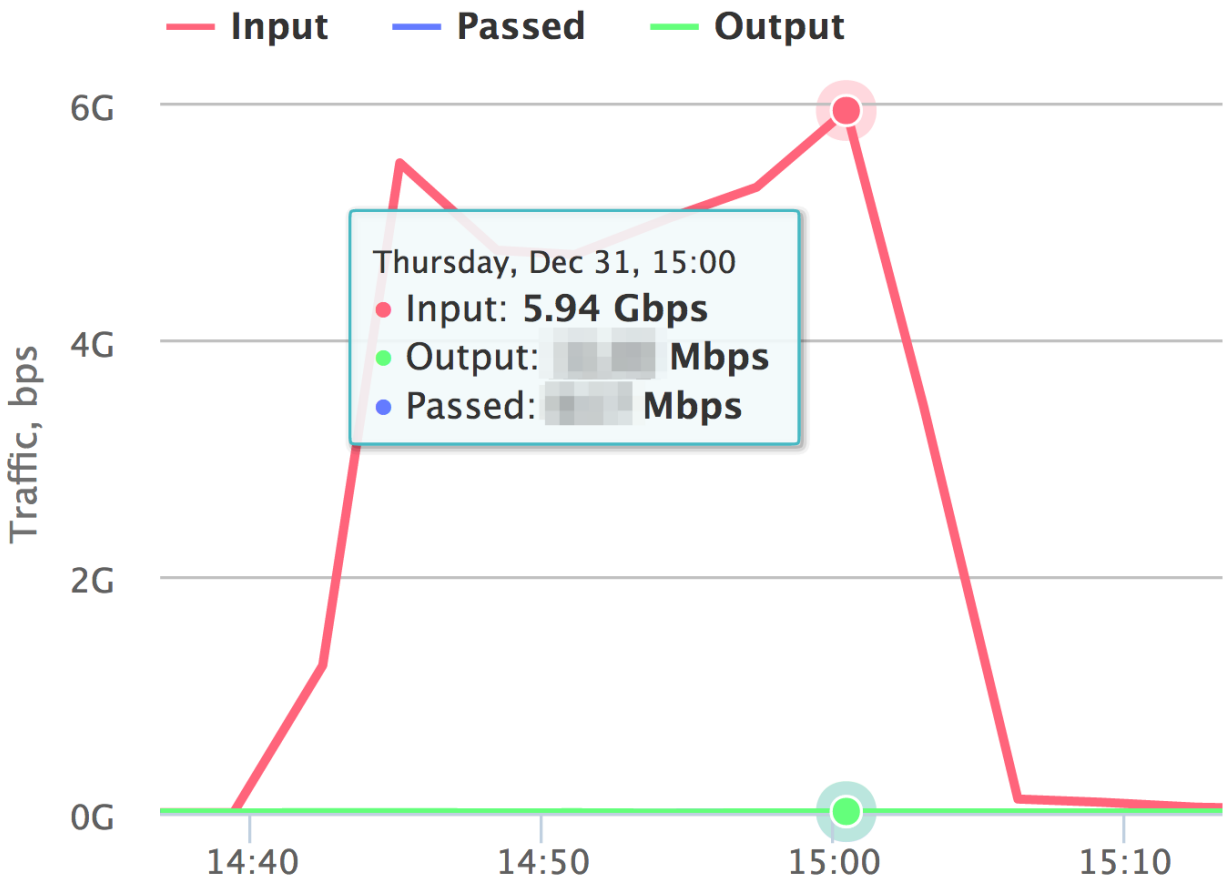
```
GET /whatever
User-Agent: WordPress/3.9.2;
 http://example.com/;
 verifying pingback
 from 192.0.2.150
```

- 150 000 – 170 000 уязвимых серверов в одной атаке
- Умеют SSL/TLS



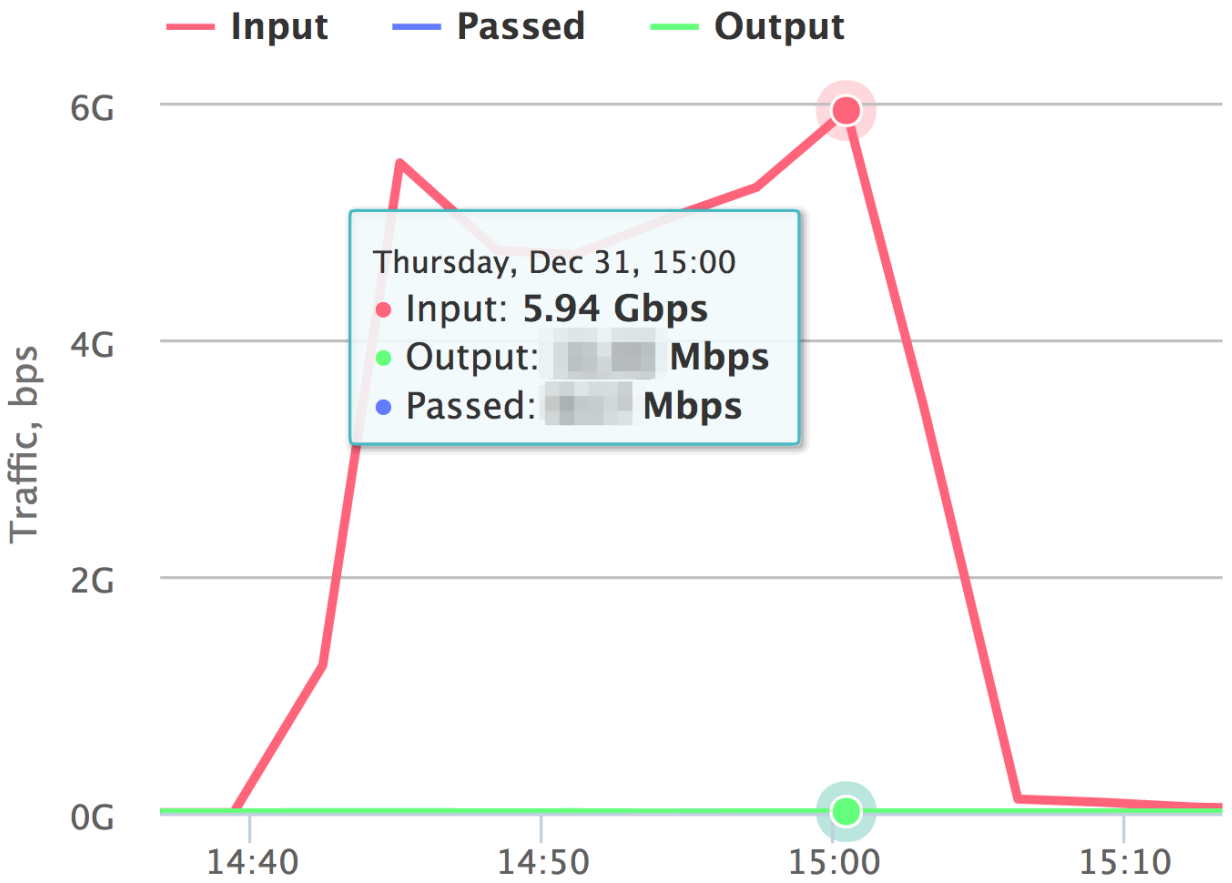
Wordpress **Pingback**

- В 2016 году 29,98 % от числа атак Pingback были выполнены с помощью протокола HTTPS.
- Для борьбы с такими атаками требуется ключ шифрования, пересборка и анализ сессии.

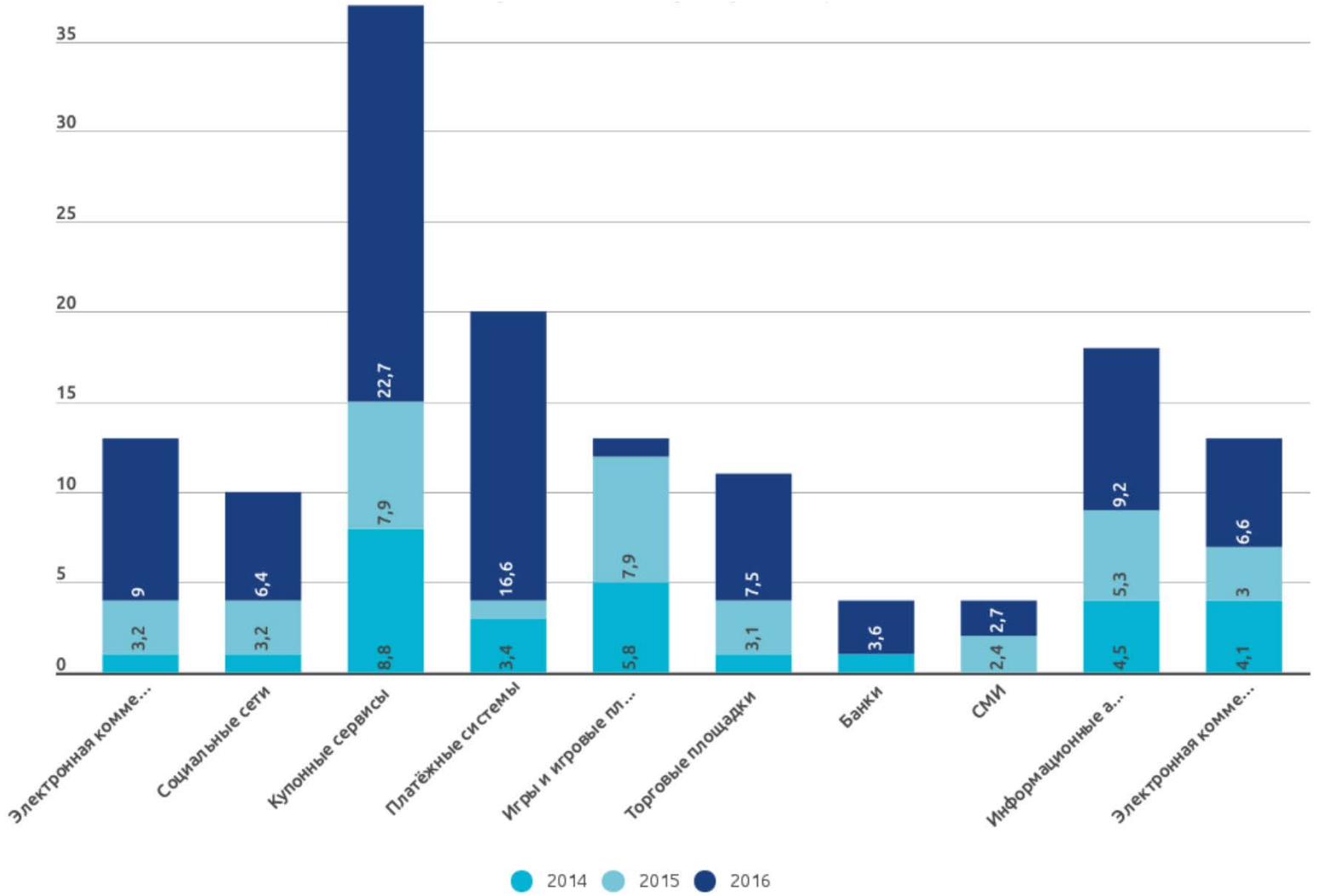


Wordpress **Pingback**

- **Миллионы** уязвимых серверов в Интернете
- Атака подробно разбирается в «Обзоре основных способов осуществления DDoS-атак» Банка России



Активность DDoS-атак по отрасли, 2014-2016 гг.

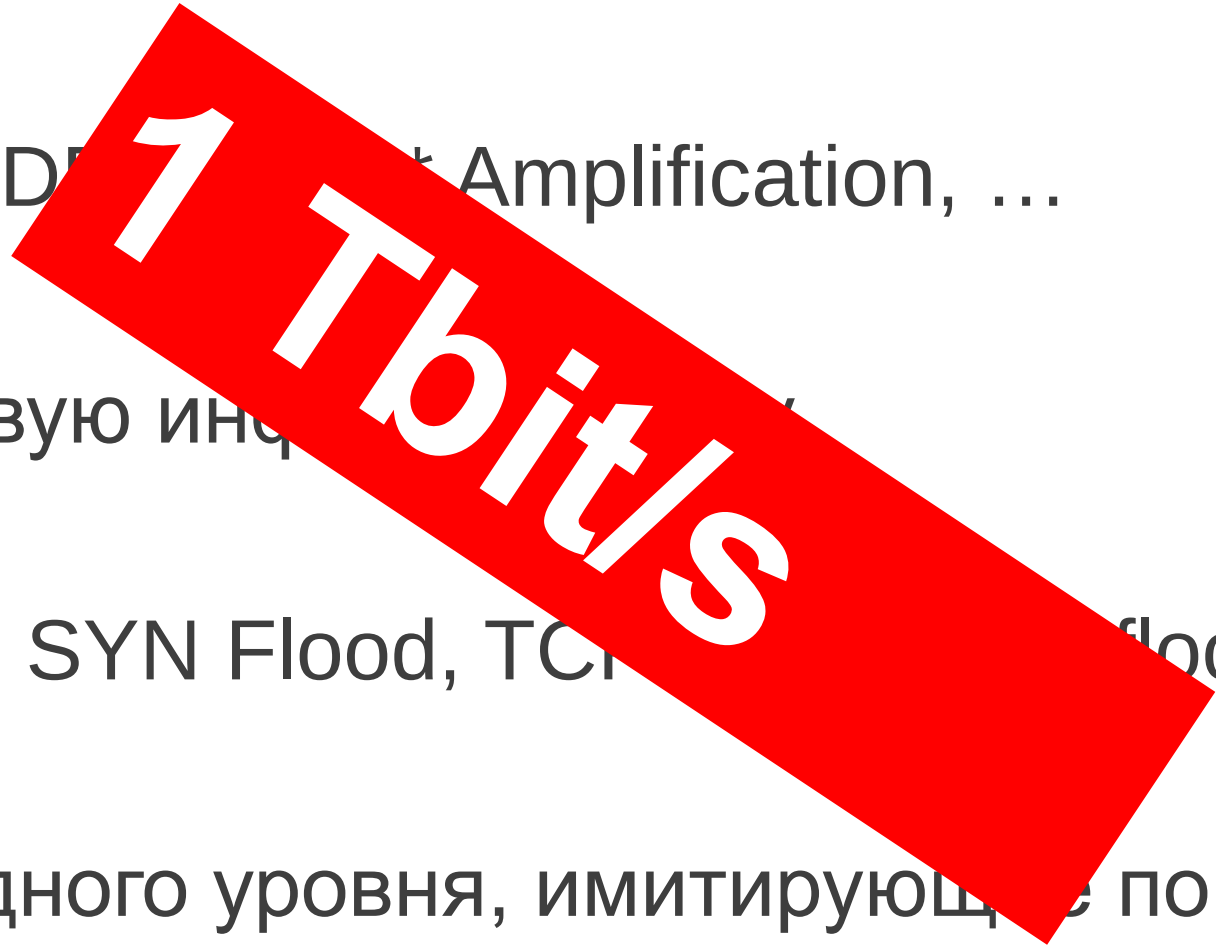


Классификация атак

- L2
  ICMP Flood, UDP Flood, * Amplification, …
- L3
  Атаки на сетевую инфраструктуру
- L4
  Атаки на TCP: SYN Flood, TCP connection flood, …
- L5-L7
  Атаки прикладного уровня, имитирующие поведение пользователя

Классификация атак

- L2
  ICMP Flood, UDP [illegible] Amplification, …
- L3
  Атаки на сетевую инф[illegible]
- L4
  Атаки на TCP: SYN Flood, TCP [illegible] flood, …
- L5-L7
  Атаки прикладного уровня, имитирующие поведение пользователя



Проблематика DDoS у оператора связи

- Проблема 1
  - Старые простые пакетные и/или CPE-решения, которые мог бы легко внедрить оператор связи, перестают работать
  - Требуются средства фильтрации, поддерживающие анализ сессий, работу с шифрованным трафиком на большой скорости

Проблематика DDoS у оператора связи

- Проблема 2
  - С технической точки зрения, построение анти-DDoS-решения очень похоже на те процессы, которые происходят у оператора связи:
    - проектирование сетевой связности
    - расчёт пропускной способности каналов связи
    - тестирование показателей производительности и надёжности оборудования

– во всех выполняемых функциях нет ничего нового по сравнению с сетевым администрированием обычного оператора связи.

Есть только одна разница, но она существенна.

Логика построения сети

- Рост сети оператора обусловлен **внутренними** факторами (за исключением форс-мажора в виде требований регулятора):
  - рост пользовательской базы
  - планы по продвижению на новые рынки
  - запросы от клиентов-юридических лиц
- Анти-DDoS-решение проектируется, исходя из факторов **внешних**
  - А именно – из *оценки рисков*, которая должна учитывать текущий уровень угроз, то есть – текущие и потенциальные возможности атакующих
  - Те самые сотни гигабит в секунду шифрованного трафика на прикладном уровне сети

Логика построения сети

- Основная задача анти-DDoS-решения: **аутсорсинг управления рисками**
- Главный фокус оператора связи – **связность и задержки**
- Модель угроз, модель нарушителя, управление рисками – **не входят в типичные компетенции оператора связи**
- В ряде случаев оператор защиты вписывает предельную пропускную способность атаки в договор. Это – **перекладывание своей ответственности на клиента**

Логика построения решения

- Поставщик анти-DDoS-решения должен оперативно масштабировать свою сеть и своё оборудование, чтобы адекватно отвечать текущим угрозам
- Для этого он должен исследовать предметную область и заниматься прогнозированием угроз, относящихся к сфере как раз исследований ИБ
- Вопросы количественного роста угрозы, IoT и прочая – находятся полностью в зоне компетенции провайдера защиты.
- Управление рисками для клиента должно эффективно сводиться к выбору подходящего тарифа у провайдера защиты.

Вопросы, замечания, предложения?

Артём Гавриченков <ag@qrator.net>

Цели

- Забава
- Самореклама, демонстрация возможностей
- Ограничение доступа к информации
- Месть
- Шантаж
- Конкуренция на рынке

Цели

- Забава
- Самореклама, демонстрация возможностей
- Ограничение доступа к информации
- Месть
- Шантаж
- Конкуренция на рынке

Цели

- Забава
- Самореклама, демонстрация возможностей
- Ограничение доступа к информации
- Месть
- Шантаж
- Конкуренция на рынке

Цели

- Забава
- Самореклама, демонстрация возможностей
- Ограничение доступа к информации
- Месть
- **Шантаж**
- Конкуренция на рынке