DDoS-атаки вчера, сегодня, завтра

Алексей Семеняка
Qrator Labs
as@qrator.net

Что такое DoS/DDoS-атака?

DoS = Denial of Service, отказ в обслуживании

DDoS = Distributed Denial of Service,
распределенный отказ в обслуживании

В обоих случаях речь идет про полную или частичную потерю доступности ресурса «извне» без нарушения его внутренней структуры («взлома»).

Обычно:

DoS – атака на отдельную уязвимость
(ping of death, INVITE of death, route leaks)

DDoS – атака на исчерпание каких-либо ресурсов
(SYN-flood, amp-атаки)

Классификация DDoS-атак

1. Канальная емкость
2. Инфраструктура
   - Сервисная инфраструктура (ex: DNS)
   - Сетевая инфраструктура (ex: BGP)
3. Операционная система (сетевой стек)
4. Приложение
5. Деньги жертвы

Инструменты DDoS

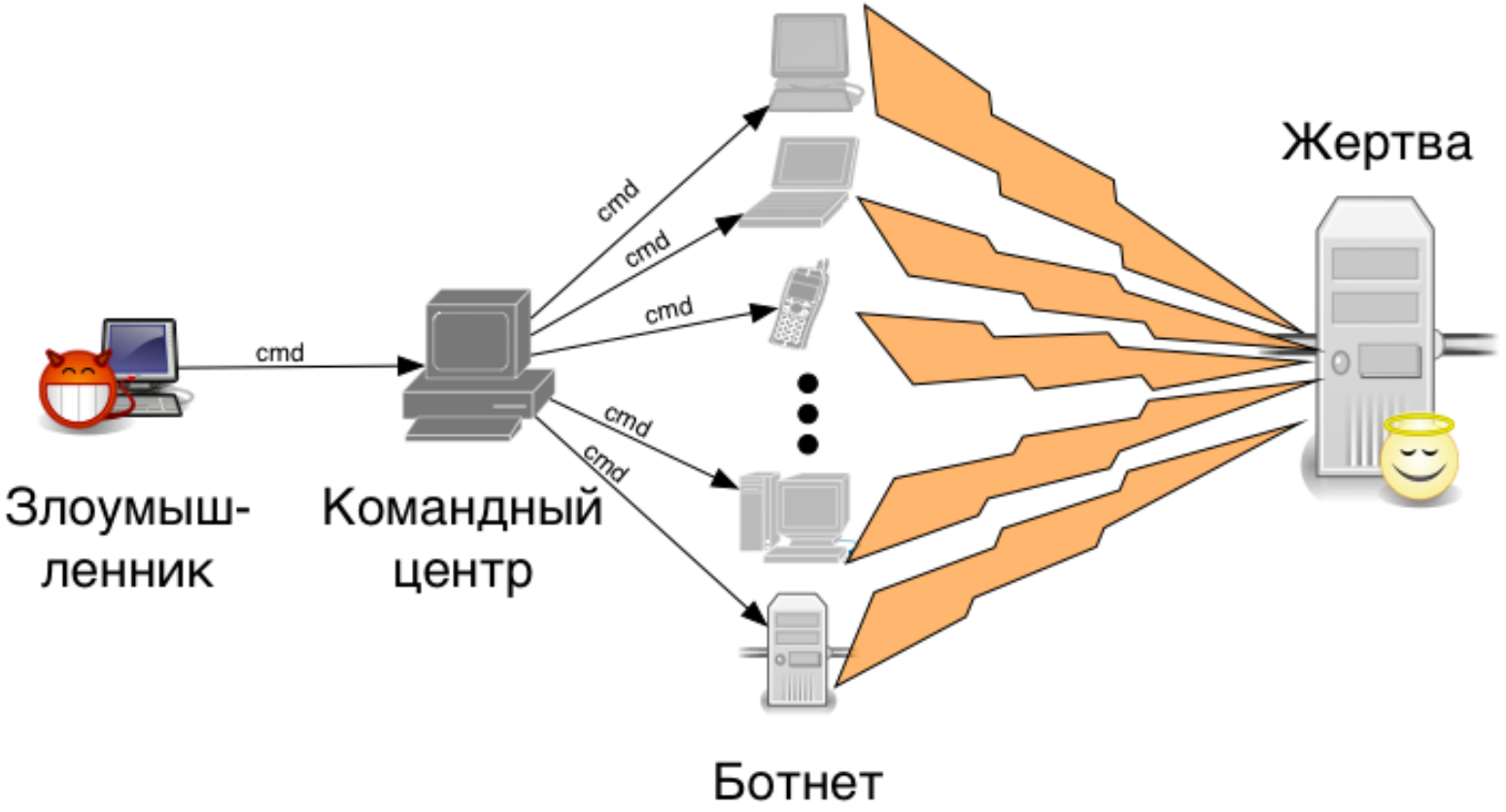
Два основных инструмента злоумышленника:

- Ботнеты
- Амплификаторы трафика

Что такое ботнет

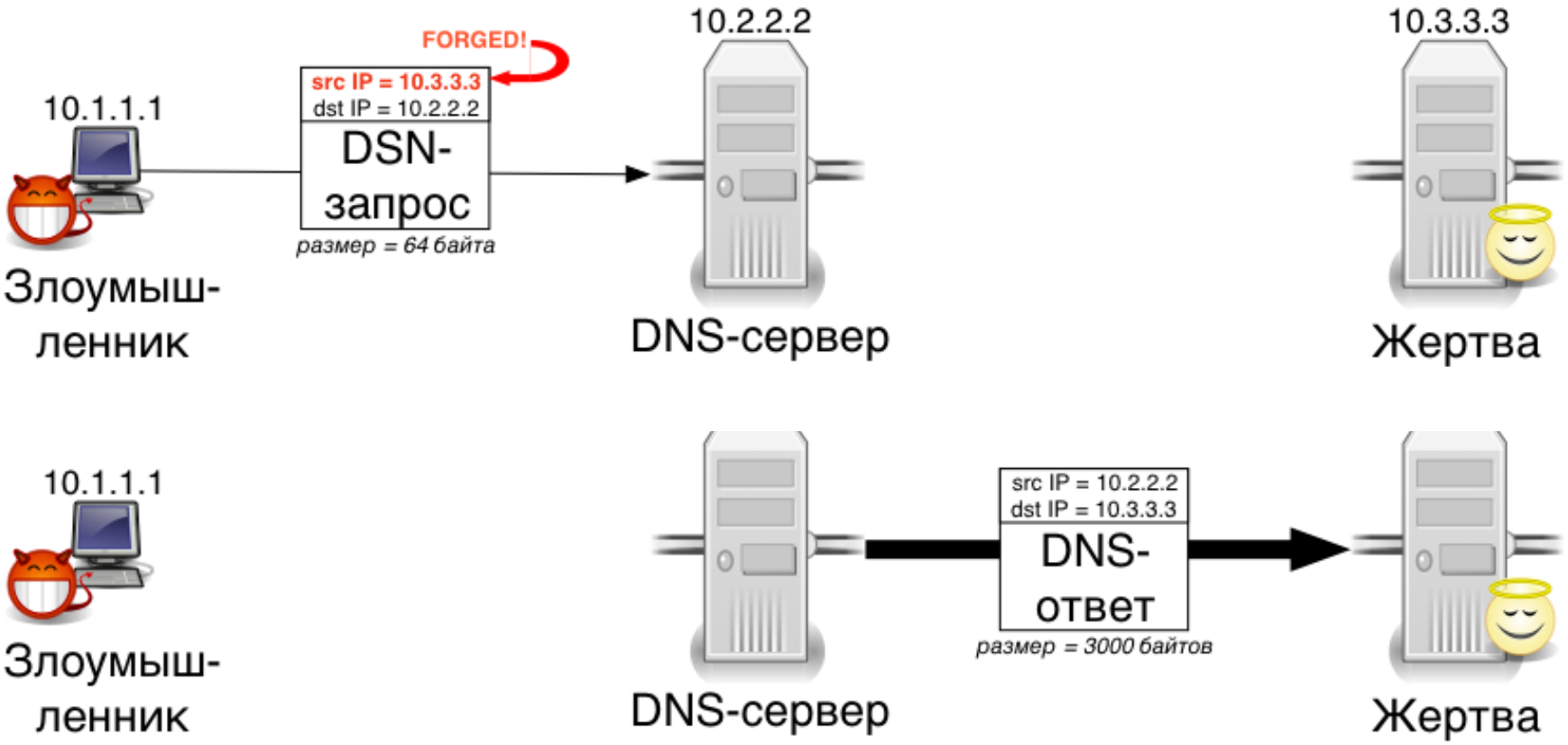
- Robot ➔ bot ➔ бот
- **Бот** – программный код, способный выполнять команды, поступающие из центра управления, работающий на
  - серверах,
  - пользовательских компьютерах,
  - мобильных устройствах
  - и любых других устройствах, подключенных к сети.
- Множество ботов под единым управлением называется **ботнетом**
- Ботнеты используются для атак разных видов, не только для атак на канальную емкость.
- Трафик, посылаемый ботнетами, может идти как с настоящих адресов ботов, так и с поддельных.
- Могут быть очень сильно распределенными

Схема ботнета



Что такое амплификаторы

Маленький запрос «от имени жертвы» – и большой ответ в адрес жертвы:



Как работает атака с амплификацией

- Атака с амплификацией трафика становится возможна при выполнении нескольких условий:
  - Ни на прикладном уровне, ни на уровне приложения не устанавливается соединение,
  - Не производится авторизация запроса,
  - Размер ответа на запрос может существенно и воспроизводимо превышать размер запроса.
- Популярные протоколы, используемые для амплификации: DNS, NTP, SSDP, Chargen/UDP, ICMP.
- Общая полоса атаки свыше 100 Гбит/с с использованием набора амплификаторов – уже обыденное и рутинное явление.

Коэффициенты амплификации популярных протоколов

Протокол	Коэффициент
DNS	28-54
NTP	500-1300
SNMPv2	6
NetBIOS	4
SSDP	30
Chargen	350
QOTD	140
BitTorrent	4
Kad	16
Quake Network Protocol	64
RIPv1	130
Portmap (RPCbind)	7-28

Тенденции DDoS: эра динозавров

- Первые сообщения о DDoS-атаках относятся к 1996 году.
- Всерьез об этой проблеме заговорили в конце 1999 года, после атаки на Amazon, Yahoo, CNN, eBay, E-Trade и др.
- Ситуация до примерно 2002 года:
  - скорости в мегабитах или десятках мегабит
  - стандартные инструменты злоумышленников(Trinoo, TFN, Stacheldraht, TFN2K и т.д.)
  - Появляются **первые стартапы** для создания мер противодействия, в подавляющем большинстве случаев борьба осуществляется на уровне локальных конфигураций серверов и сетевого оборудования.

2003-2005 года

- 2003 год – **атака на DNS** (Chicago Webs), ботнет на 700 узлов.
- 2003 год – появление **ботнетов в современном понимании**. Максимальный зафиксированный размер ботнета в 2003 г. – **260000 машин**.
- 2003 год – Создана первая компания, специализирующаяся на борьбе с DDoS (Prolexic)
- 2003 год – Распространение технологии **амплификации** методом отправки ICMP-сообщений на броадкастовые адреса.
- 2004 год – **Появление гибридов «ботнет + амплификация»**
- Максимальные полосы атаки
  - 2003 год: 1Gbps
  - 2004 год: 3Gbps
- 2005 год – регулярные атаки на партнерские сети

2006-2009 года

- 2006 год – появление **технологии амплификации с использованием DNS** (пока без EDNS0, часто на специально создаваемых зонах)
- 2007 год – Появление атак планетарного масштаба. DDoS-атака вывела из строя два корневых DNS-сервера.
- 2007 год – атаки на игровые системы
- 2007 год – использование сети DC++ для DDoS
- 2009 год – регулярные **крупные атаки на DNS-сервера**

Политика

- 2007 год – появление LOIC, использование его движением **хактивизма**
- **Политические DDoS-атаки**:
  - 2007 год: против Эстонии (предположительно, со стороны России)
  - 2008 год: против Грузии (с текстом “win+love+in +Rusia”)
  - 2009 год: против Ирана (в поддержку иранской оппозиции на выборах)
  - 2009 год: на Google, Facebook, Twitter (по-видимому, против блоггера Cyxymu)
  - 2009 год: «июльские атаки» против правительственных ресурсов США и Южной Кории

2010-2012 года: Qrator

- 2010 – атаки на полосу >1Gbps становятся регулярными (Qrator: 15 за год)
- 2011 – максимальная полоса атаки – 15Gbps, **атак >1Gbps – 23 штуки**.
  - На это пока все же ботнеты.
- 2012 – атаки >**10Gbps** становятся регулярными (**28 таких атак за год**)

2013 год

- Атаки с использованием амплификаторов становятся обыденными
  - Первые амплификаторы – на базе DNS, благодаря распространению расширения EDNS0 (нужен для DNSSEC)
- Перебор технологий становится стандартным подходом осуществления атаки
  - атака на полосу – атака на стек – атака на приложение по очереди
- График полосы мусорного трафика дублирует СМИ
  - Атаки с максимальной полосой имеют политическую подоплеку
- «DDoS-атака затормозила интернет»: атака на Spamhaus, 300 Gbps

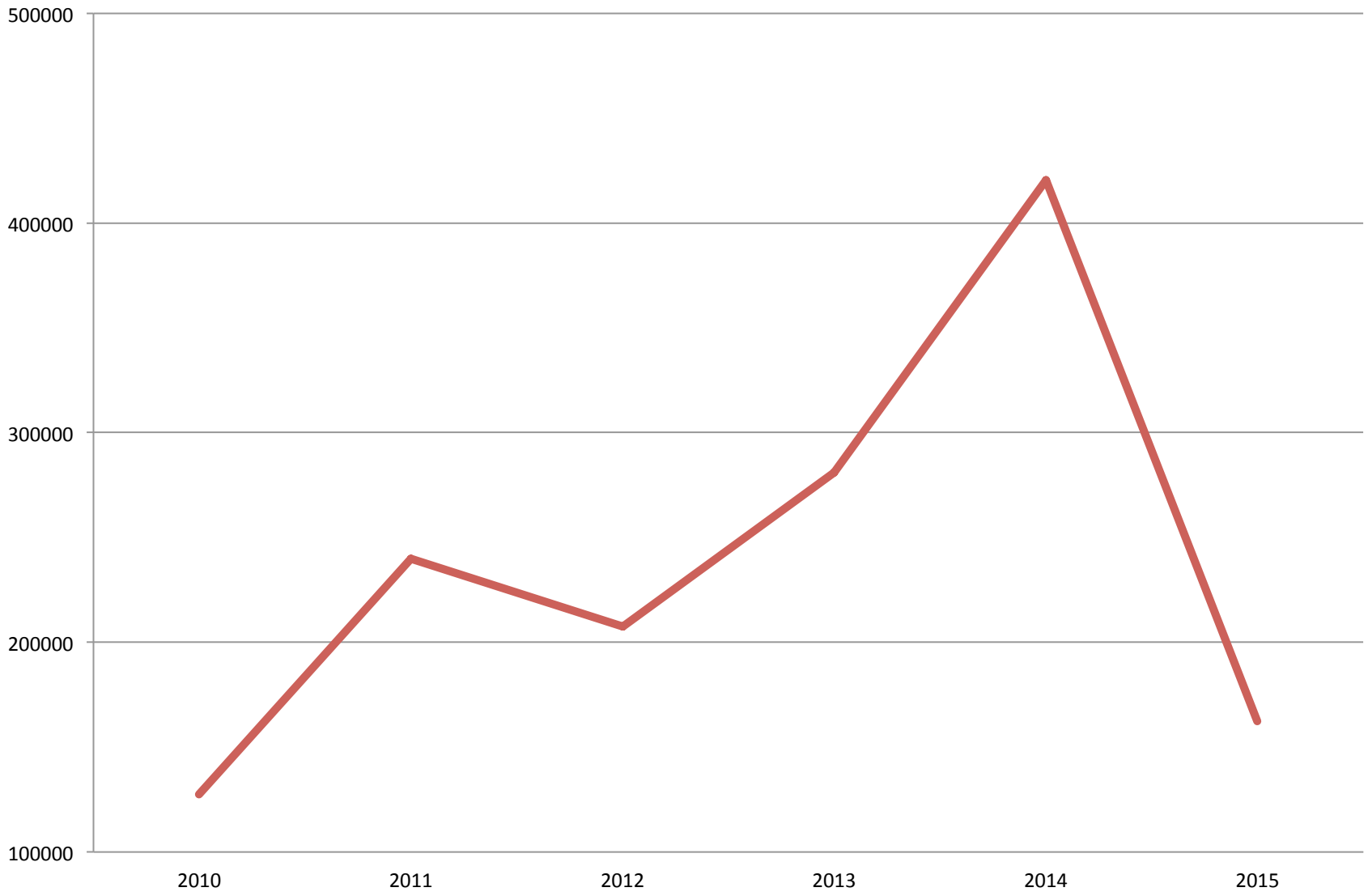
2014 год

- Переход с DNS-амплификации на NTP-амплификацию
  - Коэффициент около 1000 (!)
- Рекордная полоса атаки: 400Gbps в мире.
- Конец 2014 года: потеря политического фокуса
  - Политически мотивированные атаки и хактивизм не исчезли, но перестали выделяться на фоне экономически обусловленных
- Крупные атаки на игровые системы и **команды игроков**
- На черном рынке появляются готовые сложные ботнеты на продажу
  - CapEx против OpEx

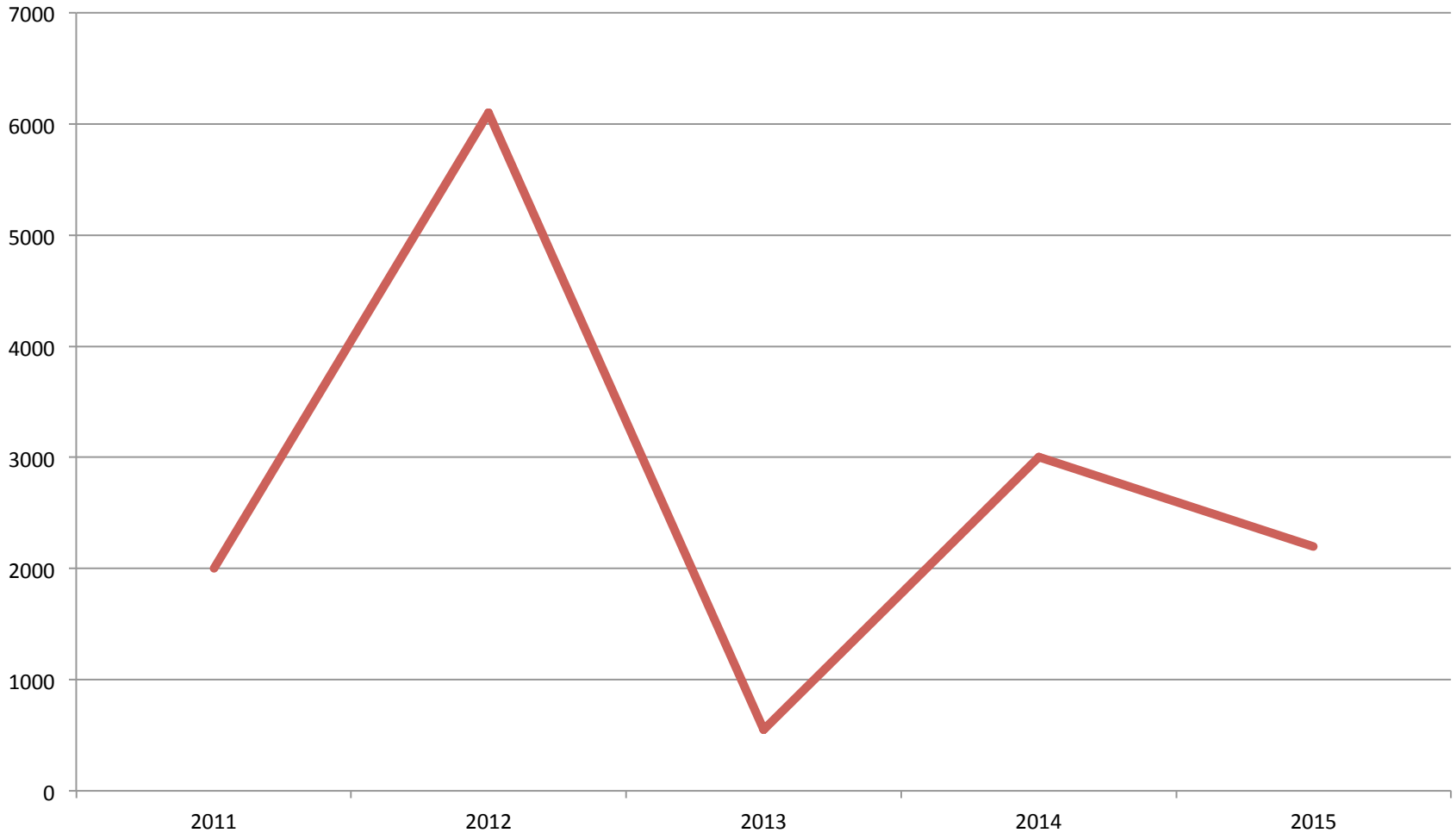
2015 год

- NTP-амплификация уступает место SSDP-амплификации
  - С NTP-амплификаторами успешно боролись
  - SSDP-устройств **очень** много
- Резкий рост числа атак (Qrator: в 2015Q1 – в 2.5 раза больше, чем в 2014Q1).
- Атаки на конечных пользователей стали обыденностью (игры!)
  - Новые жертвы: операторы (особенно операторы ШПД) оказались в зоне риска.
- Выросла популярность атак на инфраструктуру DNS
  - Которая часто беззащитна
- Массовые случаи шантажа DDoSом (DD4BC, Armada Cooperative).

Размер максимального ботнета



Максимальная продолжительность атаки, ч



О чем нам говорят эти цифры?

Тенденций нет. Почему?

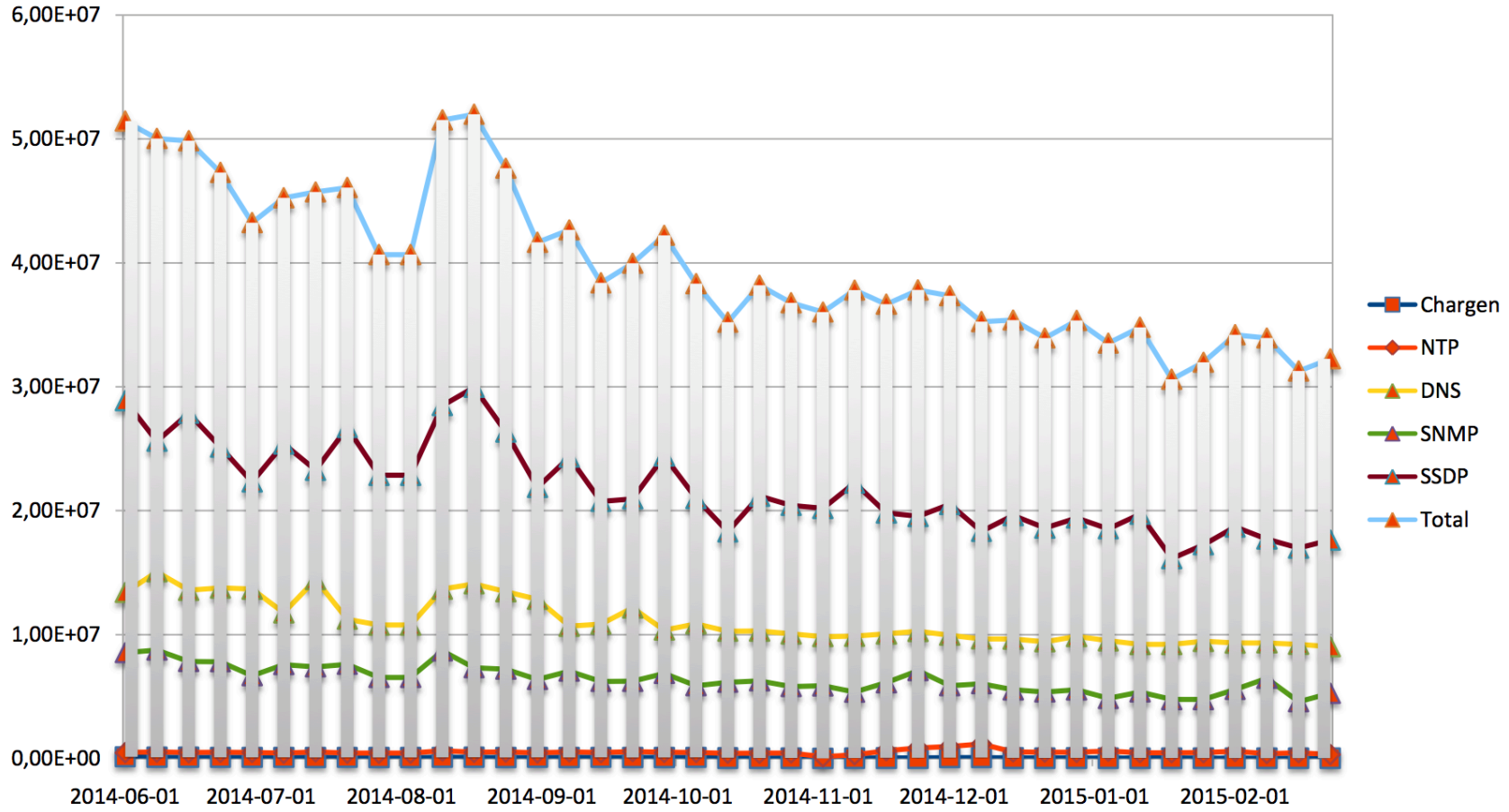
- Война «щита и меча» не прекращается.
- Используемые средства крайне адаптивны, их подстраивают под ситуацию в индустрии.
- Забытые технологии легко оживают, если для них появляются use cases
  - Комплекс ботнет+амплификаторы?

И еще немного статистики…

DDoS сегодня

- DDoS-атаки – это **взрослый бизнес**, а не игра хакерских амбиций.
  - Нет задачи создать рекордный ботнет или провести особо сложную атаку.
  - Есть задача сделать «заказанный» ресурс недоступным и получить за это деньги, чем проще – тем лучше.
- DDoS-атаки не бесплатны и поэтому практически всегда являются производными от денег.
- Основная проблема – широкое распространение инструментария для осуществления атак
  - DDoS-атака – больше не прерогатива «элиты».

Количество амплификаторов в интернете



Прогнозы

- Лучше не будет
  - В частности: количество амплификаторов снижается, но их все равно еще очень много
  - Системный подход к борьбе пока всё еще отсутствует
- Будет разнообразнее
  - Атаки становятся изощрённее.
  - Следует ожидать увеличение доли атак на инфраструктуру (не только инфраструктуру DNS, но и сетевую инфраструктуру – утечка префиксов).
  - Цели диверсифицируются. Теперь это не только веб-сайты, но и голосовые шлюзы, игровые системы и конечные пользователи.
  - Атаки «на исчерпание кошелька» будут развиваться по мере развития эластичных облачных сервисов.

Некоторые жертвы DDoS-атак:

Важные инициативы индустрии

- MANRS = Mutually Agreed Norms for Routing Security
  - Цель: противодействие искажению маршрутной информации и спуфингу IP-адресов
  - Инициатива ISOC, описывающая предметный набор действий для достижения цели
  - Операторам можно (и нужно) присоединиться уже сейчас
- DOTS = DDoS Open Threat Signalling
  - Цель: создание инфраструктуры для сквозной сигнализации об аномалиях трафика начиная с CPE и кончая облачным сервисом.
  - Рабочая группа в IETF
  - Приглашаются сетевые вендоры и разработчики

Спасибо!