radware
Every second counts

Актуальные задачи отражения внешних атак. + Война IoT ботов

Михаил Суконник
michaels@radware.com

September 25, 2017

radware
Every second counts

About Radware

Our Mission

Обеспечить максимальный уровень сервиса
пользователям приложений
даже под атакой

Обеспечить максимальный уровень сервиса пользователям приложений даже под атакой

Application Delivery

Security

Оптимизация при нормальной работе

Минимизация деградации при росте нагрузок и атаках

Недопущение прерывания сервиса и обеспечение доступности

radware
Every second counts

Отражение атак – сегодняшние требования

Способы осуществления,
рекомендации
по противодействию

ОБЗОР ОСНОВНЫХ СПОСОБОВ ОСУЩЕСТВЛЕНИЯ DOS/DDOS-АТАК

1. Почему автоматизация?

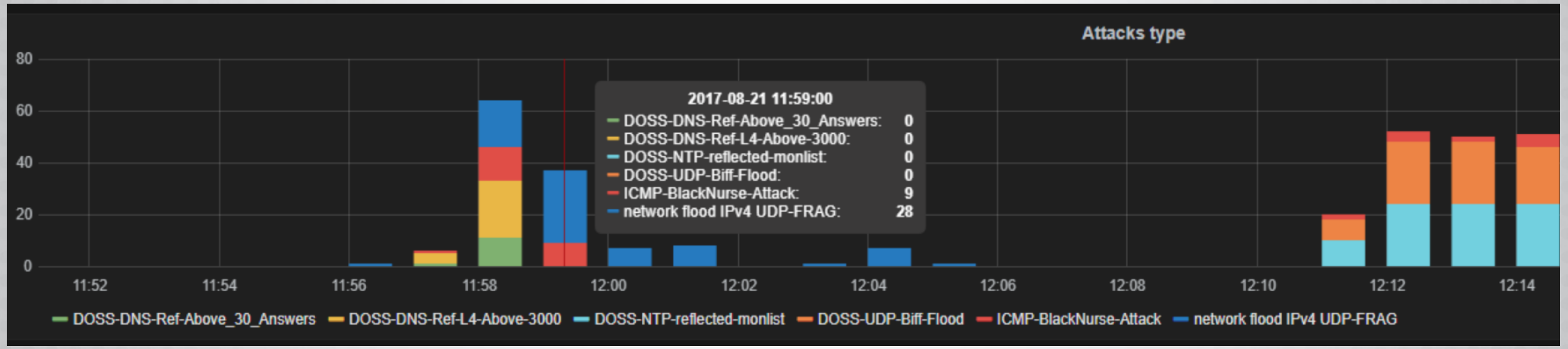
- Неавтоматизированные системы = требование к постоянному (24x7) наличию обученного персонала
- Атаки многовекторные с постоянно меняющимися векторами
- Практика атак за последние годы показывает (в т.ч. - в РФ), что атака может длиться несколько дней и недель. Даже крупнейшие организации не содержат достаточных людских ресурсов для атак такой продолжительной борьбы

Недавняя атака

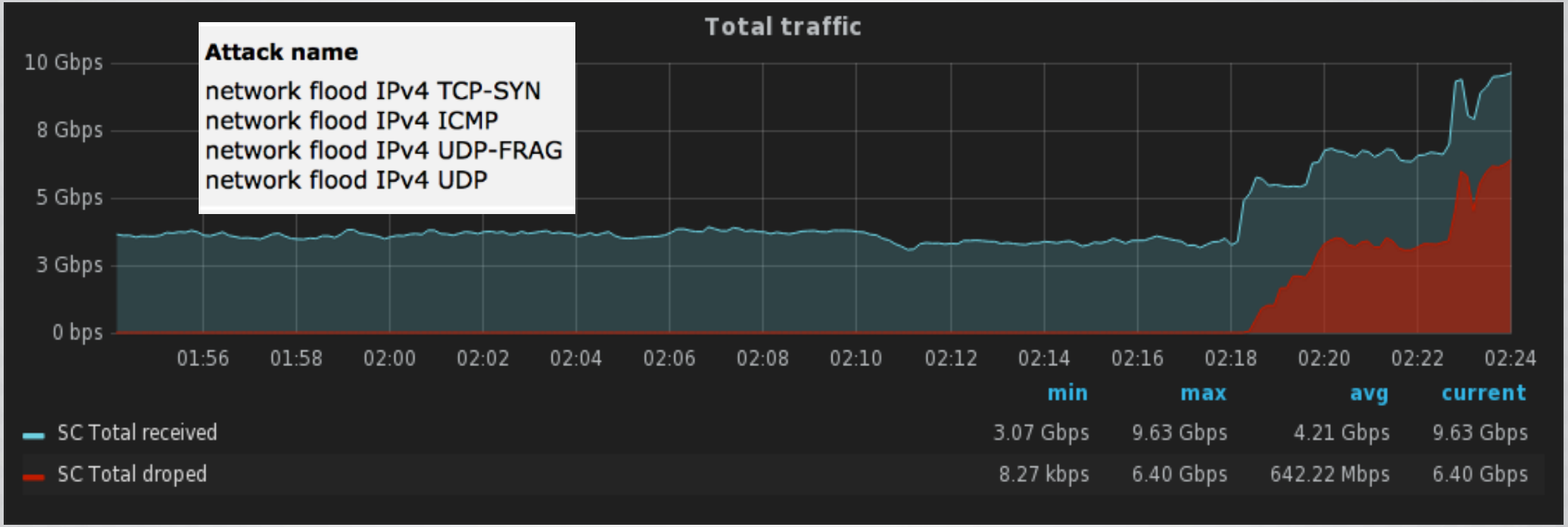
2. Почему реагирование за минуты?

- Реагирование команды при ручных настройках/корректировках - десятки минут против единиц минут или секунд (!) автоматизированного C&C атаки
- Результат – противомеры борются с атакой, которая или уже закончилась, или – закончится через несколько минут

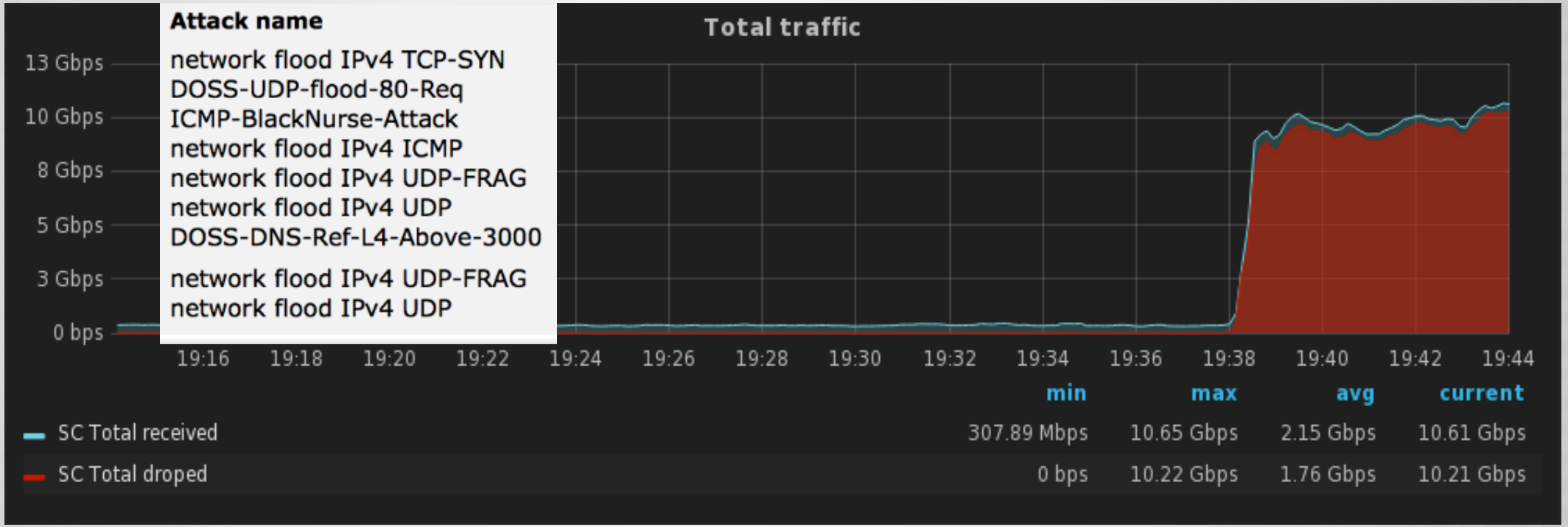
Пример атаки – смена векторов



Пример отражения - 1



Пример отражения- 2



3. Легитимные пользователи

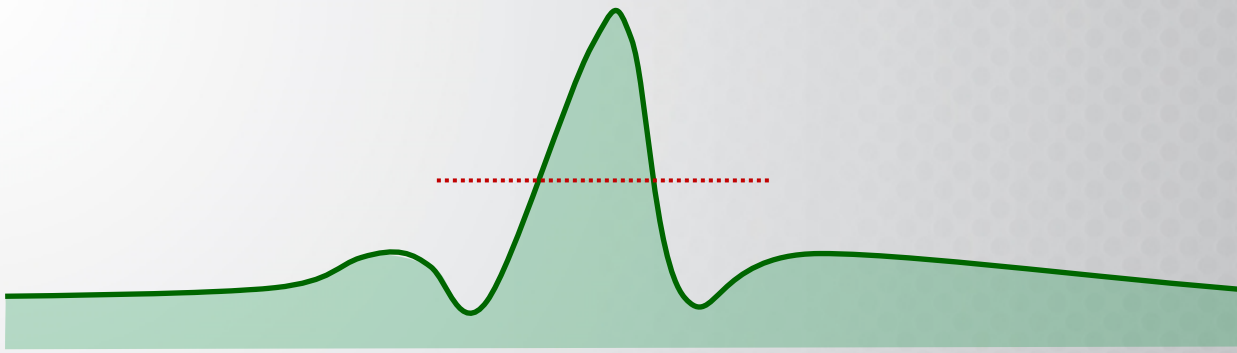
- Задачей противодействия атакам на самом деле является обеспечение доступа легитимным пользователям
- Метод – выявление моделей поведения легитимных пользователей с конкретными приложениями и борьба за живучесть пользователей, ведущих себя в соответствии с этими моделями
- Метод – динамическое создание описания моделей поведения атакующих
- Широко применяются атаки со скрытым IP, что не дает возможности блокировать атакующих по адресу

Поведенческий анализ

Обеспечение SLA легитимным клиентам под атакой

Поведенческий анализ распознает легитимных клиентов по статистическим моделям 4-7 уровня

По сравнению с грубым анализом на базе общего (атака+легитимные клиенты) трафика



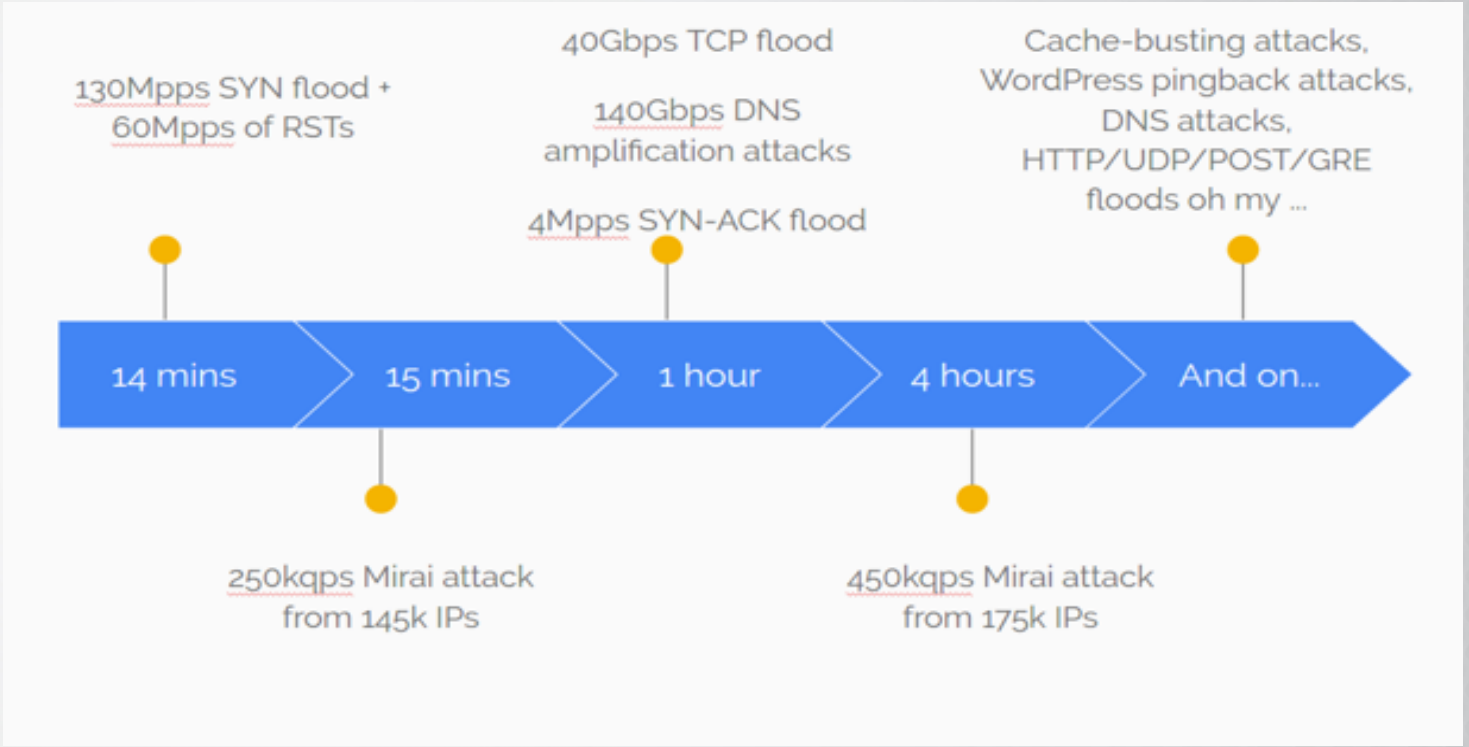
4. Почему – весь спектр атак?

- Профессиональные атаки включают одновременно 5-10 вектором (от сетевого до аппликационного уровня)
- Этот факт не изменился с началом использования IoT ботов
- Для нанесения ущерба достаточно не отразить 1 вектор атаки
- Защищаться должны все элементы сети – FW, серверы, приложения, балансировщики, сетевое оборудование, а не только каналы

Пример – атаки Mirai 9’16-2’17

Attack Type	Attacks	Targets	Class
HTTP flood	2,736	1,035	A
UDP-PLAIN flood	2,542	1,278	V
UDP flood	2,440	1,479	V
ACK flood	2,173	875	S
SYN flood	1,935	764	S
GRE-IP flood	994	587	A
ACK-STOMP flood	830	359	S
VSE flood	809	550	A
DNS flood	417	173	A
GRE-ETH flood	318	210	A

Источник – Usenix association



Источник – Google Shield

Network vs Application

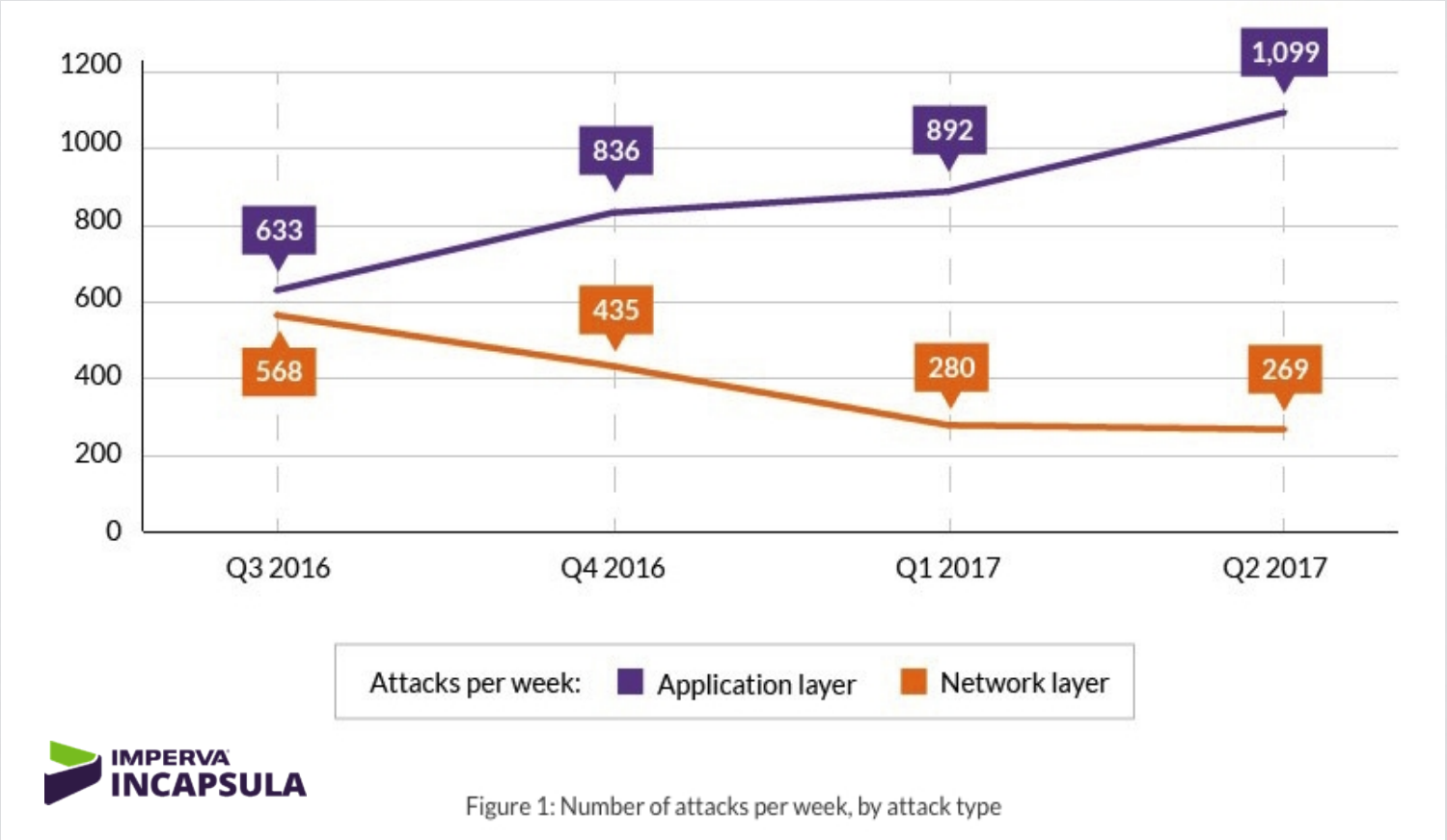
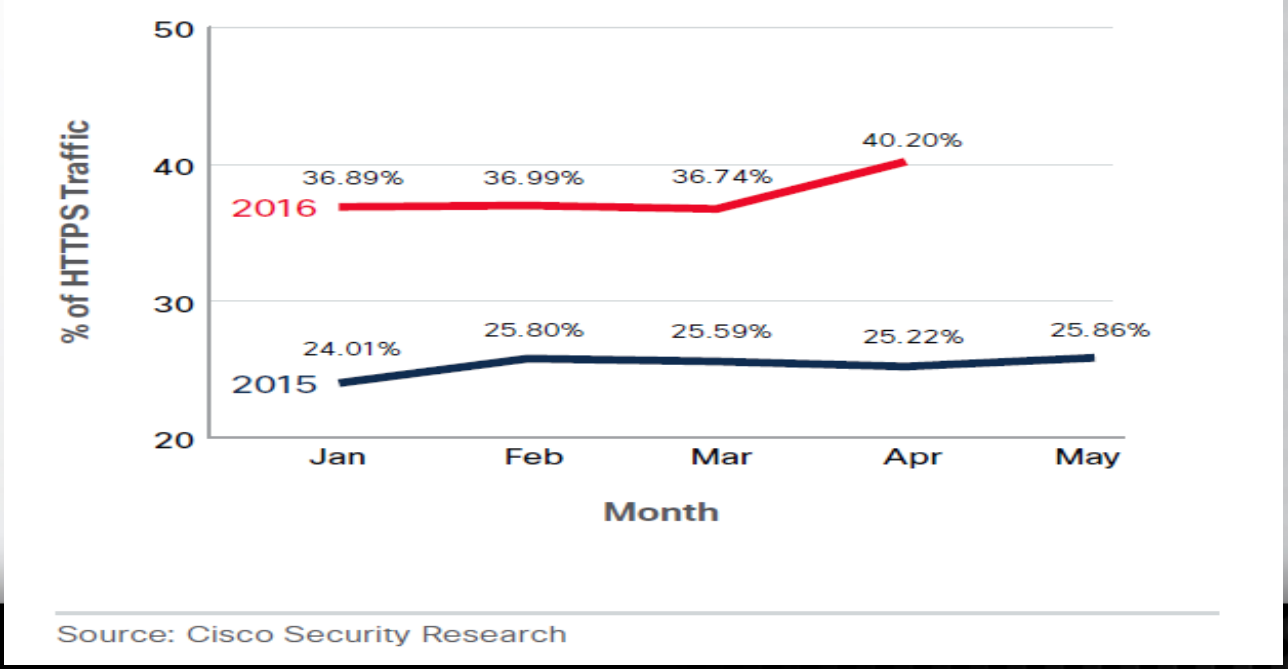


Figure 1: Number of attacks per week, by attack type

7. Шифрованные атаки

- Более 50% траффика – под SSL
- Новые протоколы шифрования усложняют работу по анализу
- Отражение со вскрытием трафика вне «доверенной сети» – нарушение PCI DSS
- Отражение в 2 этапа – на периметре (без вскрытия сессий пользователей) и – внутри сети (со вскрытием SSL) с возможностью блокировать атаку, обнаруженную на 2ом этапе, на периметре



6. Оборудование или - услуга?

- Атаки на приложения, медленные атаки, шифрованные атаки и т.д. – собственное оборудование, постоянно отражающее атаки
- Мощные сетевые флуды, «забивающие» последнюю милю – услуга провайдера (лучше – интегрированная с вашим оборудованием)

Война 3 ботнетов за IoT

radware
Every second counts

Mirai Milestones

Sept 20, 2016

620Gbps attack GRE in payload, No amplification, No reflection

Sept 21, 2016

~ 1 Tbps in volume SYN and ACK floods Over 140,000 unique IPs

Sept 30, 2016

Mirai Source Code Released Hackforums.com Anna-Senpai

Oct 21, 2016

DNS Water Torture attack with other vectors. Some comprised of Mirai 100k end-points reported

Nov 27, 2016

DT Router Takeover Attempt Mirai w/ TR-064 Exploit 900,000 consumer's internet connection affected

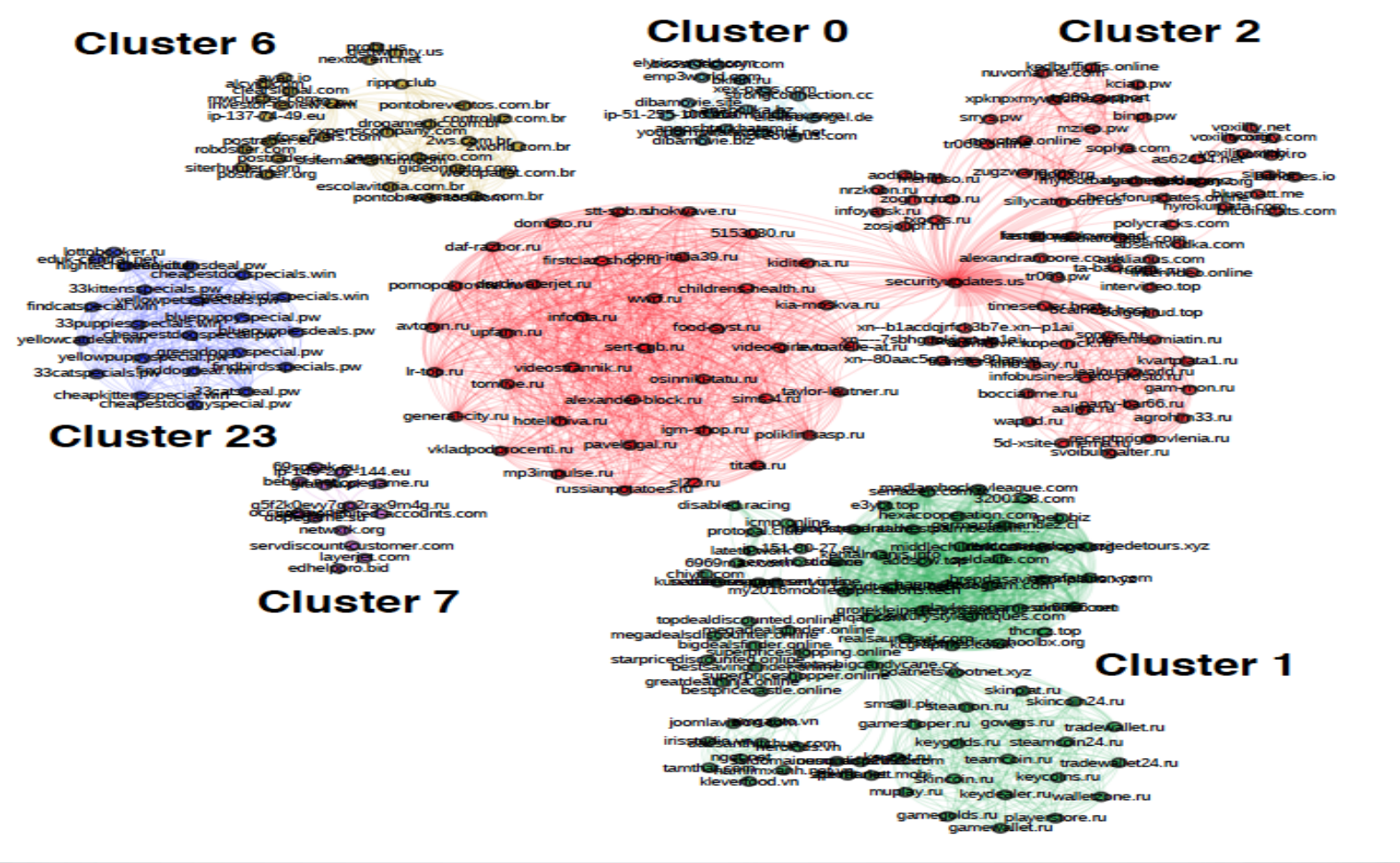
Feb 8, 2017

Mirai Gets a Windows Trojan to Boost Harvesting

Original Mirai Attack Vectors

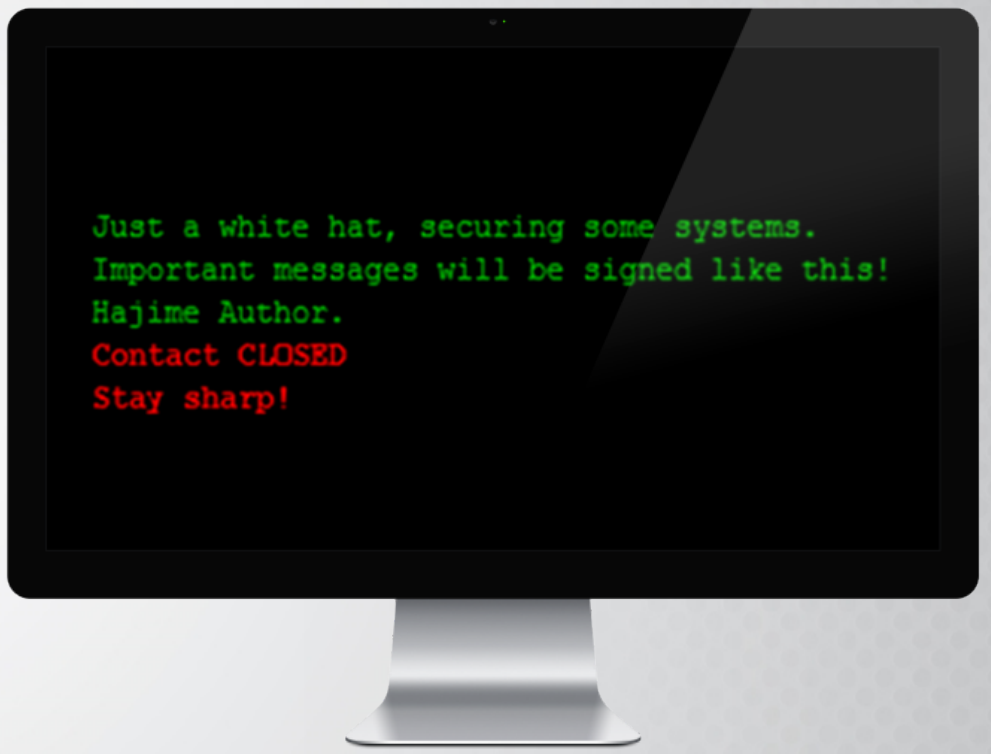
```
mirai-user@botnet# ?
Available attack list
udp: UDP flood
syn: SYN flood
ack: ACK flood
stomp: TCP stomp flood
udpplain: UDP flood with less options. optimized for higher PPS
vse: Valve source engine specific flood
dns: DNS resolver flood using the targets domain, input IP is ignored
greip: GRE IP flood
greeth: GRE Ethernet flood
http: HTTP flood

mirai-user@botnet#
 0 mirai-util   1 mirai-ns1   2 mirai-cnc   3 mirai-scan   4 sniffer   5 cr1
```

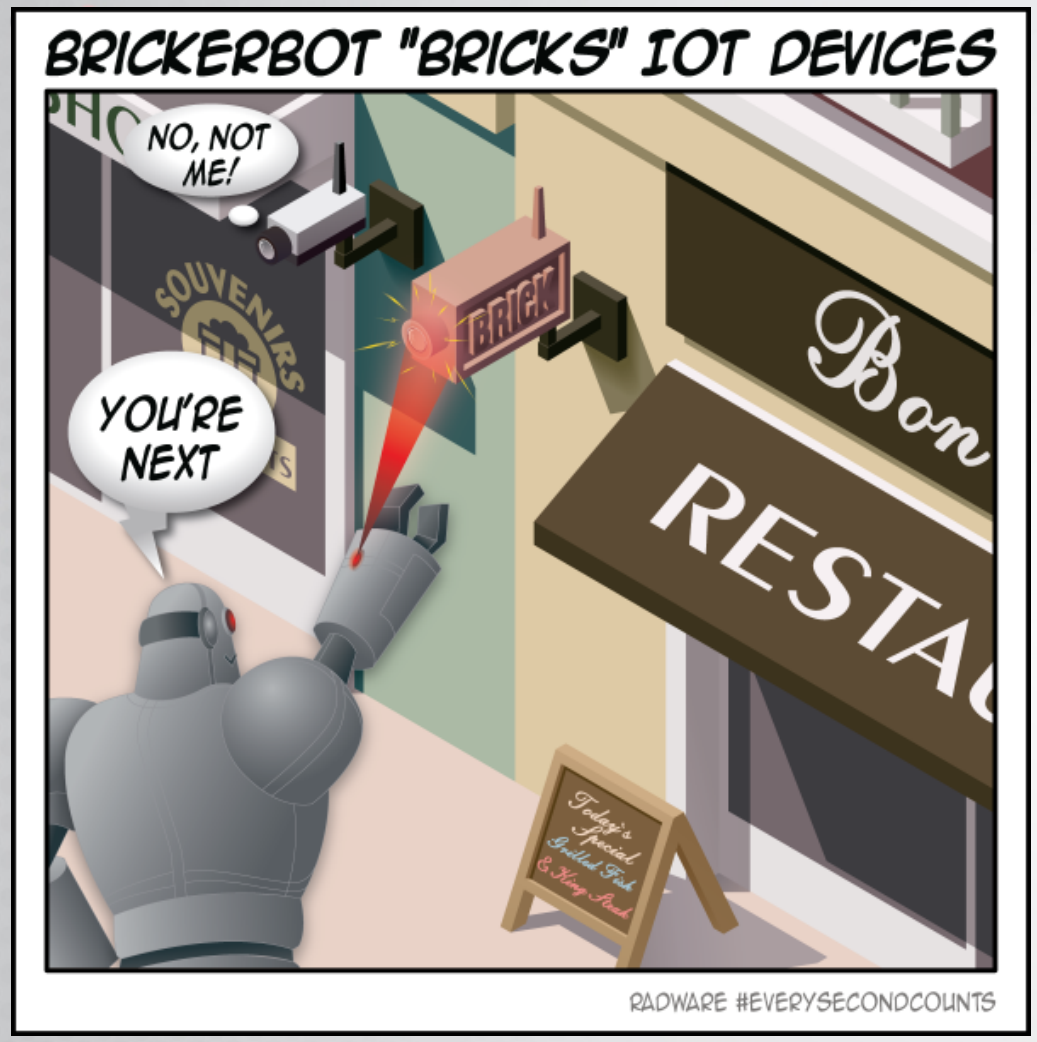
Mirai C2 Domain Relationships—



Hajime: Друг или враг?

- Обнаружен Oct 16, 2016 by Rapidity Networks
  - 5 дней до атаки на Dyn
  - 2 недели после обнародования кода Mirai
- Утверждается, что создавался с благими намерениями
- Гибкий, самораспространяющийся
- Блокирует незащищенные порты
- Реальная цель создания непонятна





Introducing BrickerBot

Первый PermanentDOS (PDoS) Botnet для IoT

Обнаружен Radware в Марте 2017

Блокирует участие устройств в атаках

Уничтожает только зараженные IoT устройства

No malware binary downloaded or executed on the victim

BrickerBot Characteristics

- SSH and Telnet are brute forced using factory default credentials
- Runs from the Deep Web, concealed by TOR exit nodes
- Only attacks devices infected with IoT bots
- Requires full TCP connect on port 23, 7547, others
- Attacks the source IP of the poking device

Summary - Battle of the IoT Bots

Mirai – the Bad

- Создает армию атакующих ботов
- Много векторов с потенциалом X ТБс
- Простой, легко распространяющийся

Hajime – the Good (at least for now)

- Вытесняет другие боты и перекрывает незащищенные порты
- Агрессивно сканирует и заражает
- Конечная цель непонятна

BrickerBot – the Vigilante

- Атакует только зараженные устройства, ожидая попыток заражения
- Уничтожает их PDoS

radware

Every second counts