Сетевая гигиена и коллективная небезопаность

Алексей Семеняка
Highload Lab
ENOG 9

Чистота – залог здоровья

Сетевая гигиена

Контроль собственной инфраструктуры

- Корректные анонсы
- Контроль префиксов
- …

Мониторинг клиентов

- Ботнеты
- Амплификаторы
- …

Немного банальностей

Некорректные анонсы

- Неэффективное использование полосы
- Увеличение задержек
- Потеря видимости клиентов снаружи

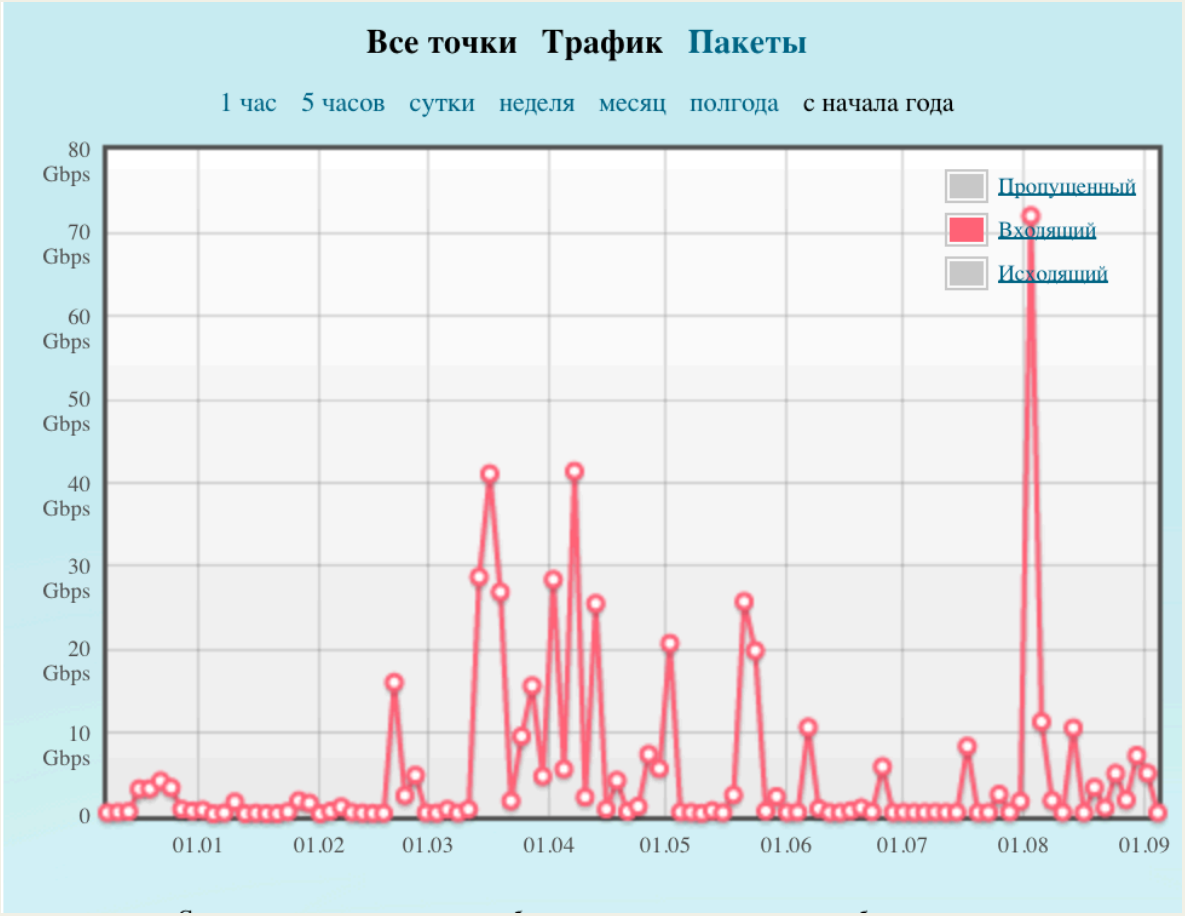
Не контролируются адреса источников

- Оборудование пропускает сетевой мусор, не препятствуя трафику DDoS-атак

Амплификаторы и боты в клиентских сетях

- Внутри есть источники паразитного трафика, используемого для организации DDoS-атак

С высоты птичьего полета…



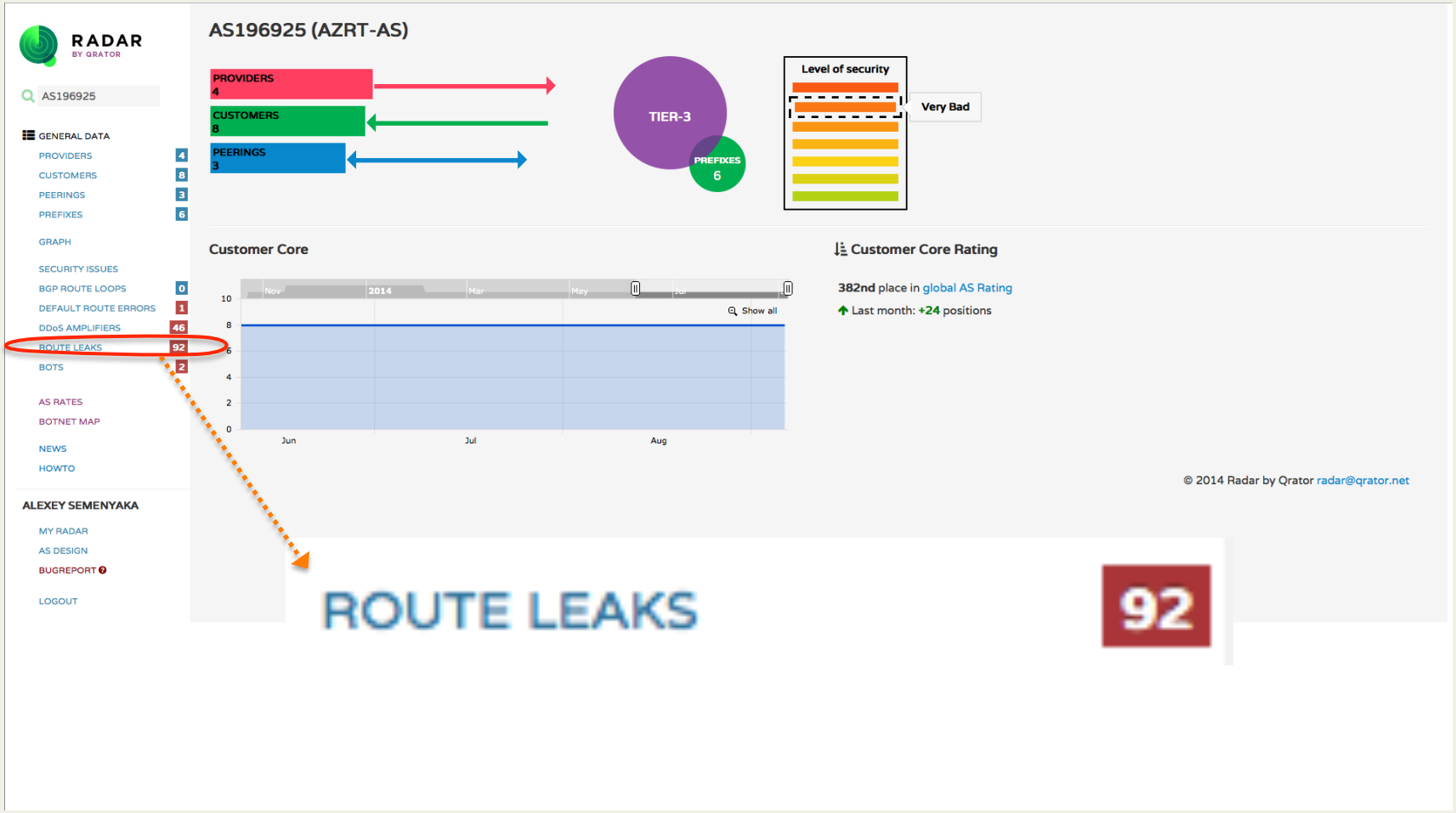
Среднесуточная полоса DDoS-атак в 2014 году по данным сервиса Qrator.

Домашнее задание.
Расставьте на графике слова:

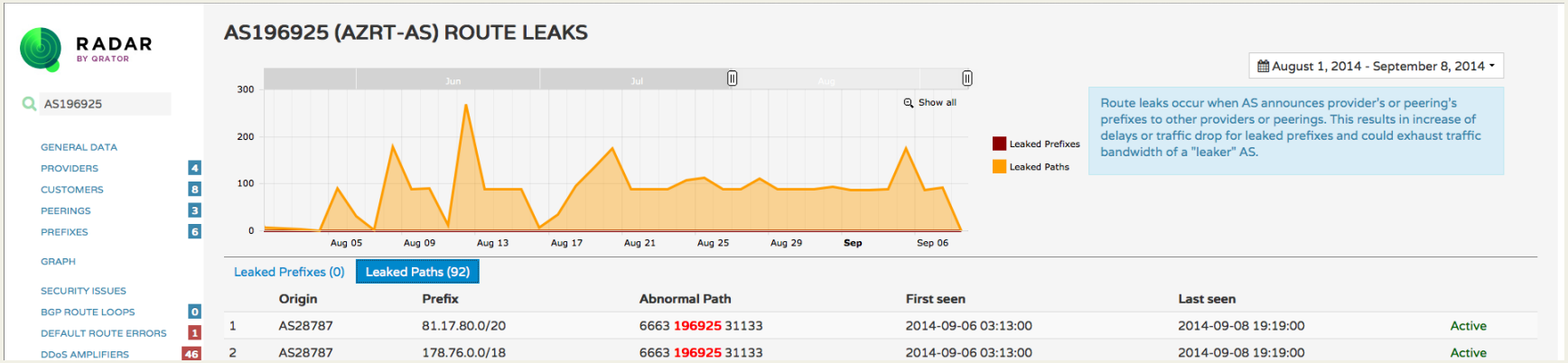
- *Олимпиада*
- *Крым*
- *MH17*
- *АТО*

Иллюстрация

Radar: Azertelekom, AS196925

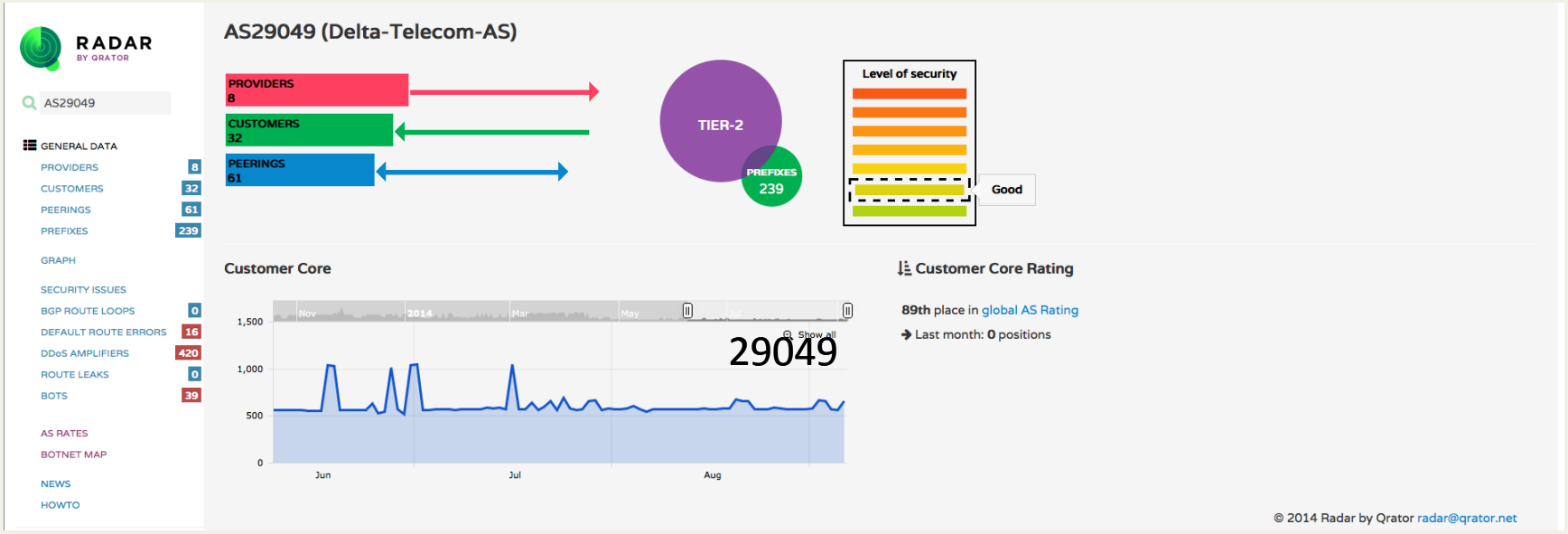


Radar: Azertelekom, AS196925



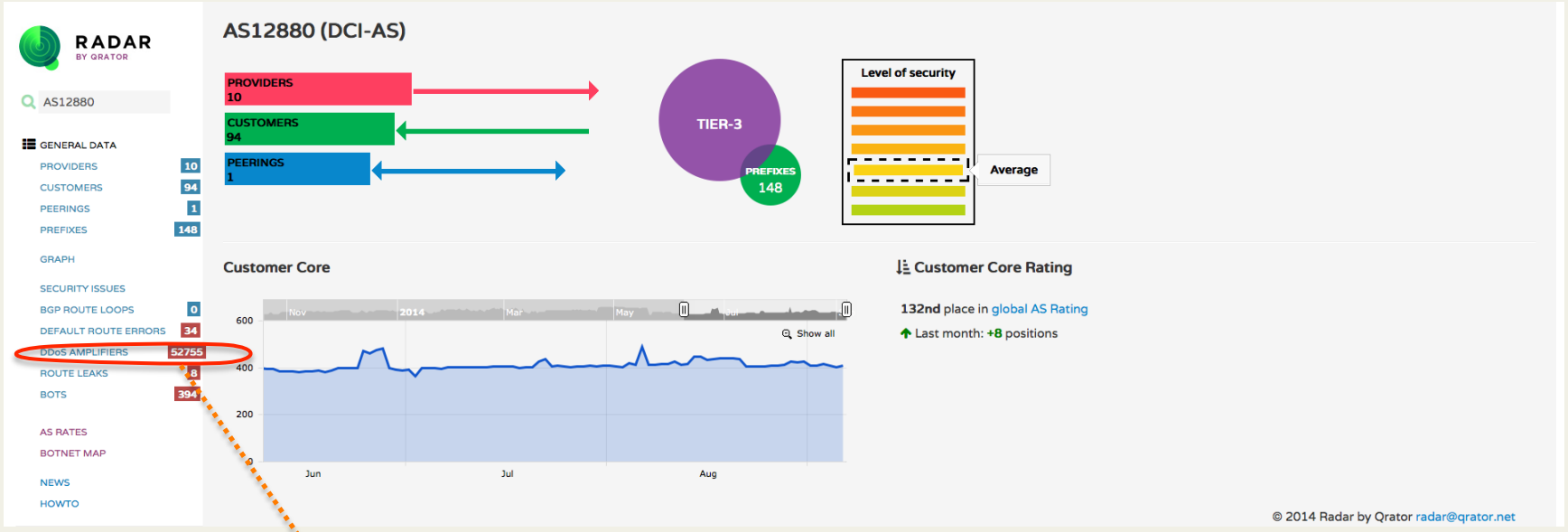
При потере связности с этим апстримом клиенты или перестанут быть видны из мира, или возрастет задержка до них.
В любом случае, оператор при этом будет пропускать через себя ненужный трафик.

Radar: Delta, AS29049

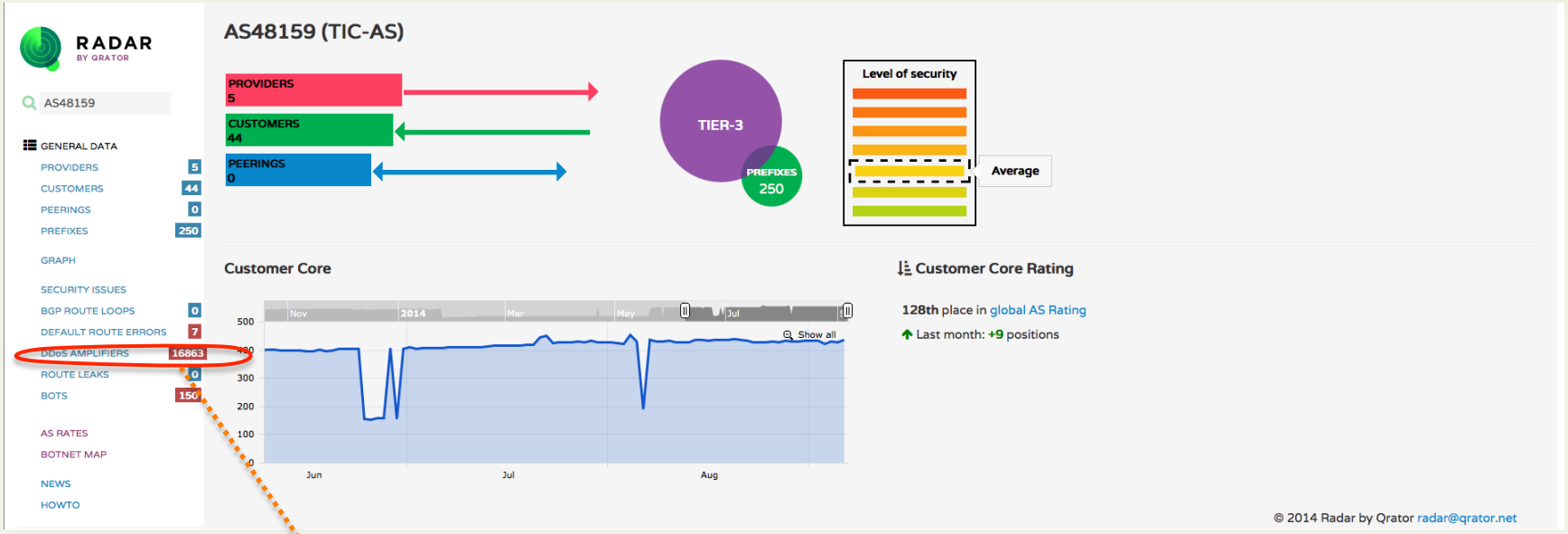


Выглядит не очень плохо... но есть одно «НО»: **клиенты**.
Иранские AS12880 и AS48159.

Radar: AS12880



Radar: AS48159



Немного [очевидных] выводов

- AZ – пока что небольшой сегмент, отсюда проблемы роста.
- И у разных транзитов они разные.
- Но эти проблемы легко могут выйти за пределы региона.
- Исправляться стоит начать прямо сейчас ☺

Комментарии? Вопросы?

Alex Semenyaka, Highload Lab, alex.semenyaka@gmail.com