OONI

На шаг позади РКН

Мониторинг ковровых блокировок

Леонид Евдокимов

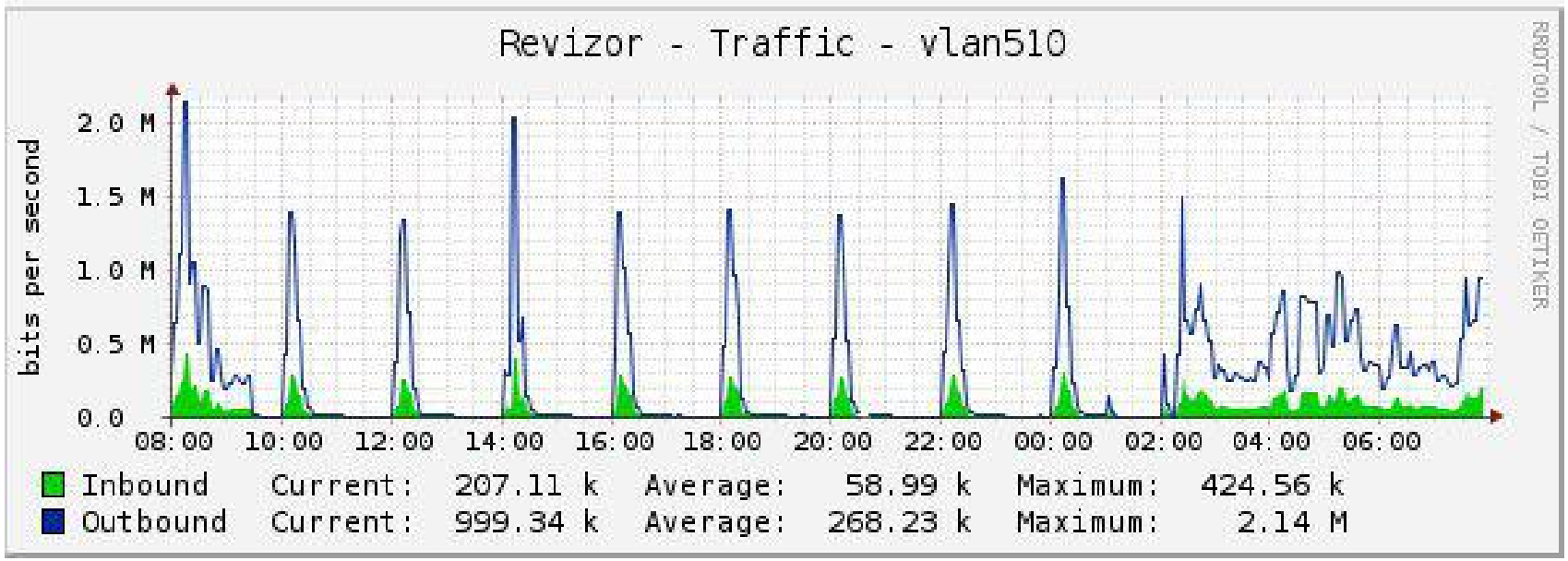
ENOG 15

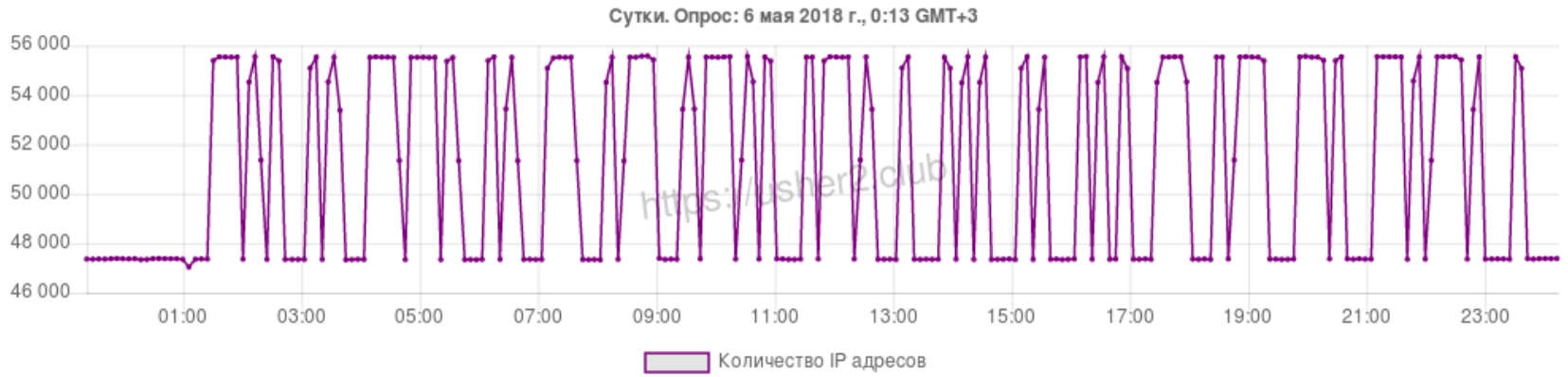
Москва, 5 июня 2018

Как же начинает надоедать. Сейчас клиент 10 минут жаловался коллеге, что не может играть в world of trucks. Ещё и извинений требует от нас лично!

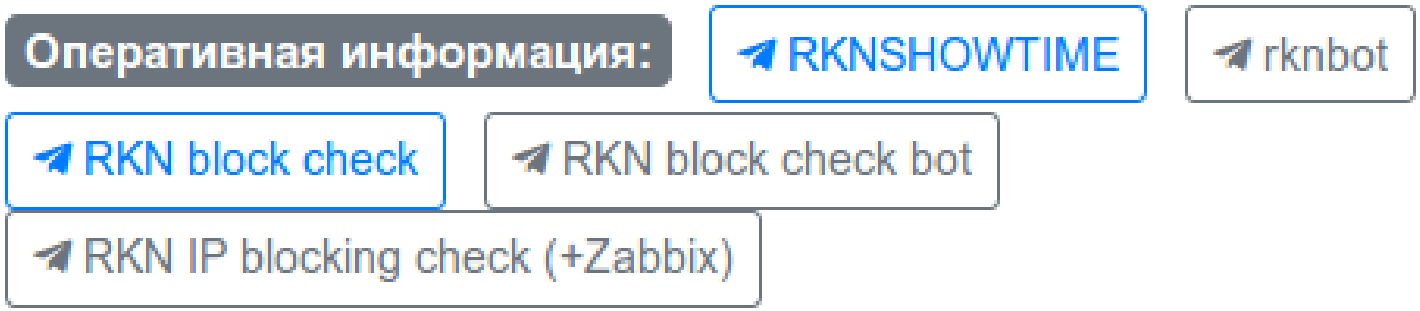
У нас клиенты воют! Гугл не работает, ютуб не работает, инстаграм не работает, твитч не работает, стим не работает. на некоторых сайтах просто белый экран.

Слушайте, а что там про инстаграм?





Знакомый график?



Клуб «Эшер II»: usher2.club

Зачем мониторинг?

Предотвращать инциденты

Уведомлять о проблемах первый уровень поддержки

В бане /10. Что «упало»?

О чём предупредить саппорт?...

Проверить AS.
Перебрать PTR?
Изучить кэш DNS-рекурсора?
Сканировать zmap http*, собрать GET / и commonName?

Не быстрее ли использовать открытые данные? :-)

SCANS.IO

Rapid7 Sonar, FDNS (A)

Сотни миллионов доменных имён

Еженедельные обновления

Простой *grep-friendly* json формат!

CNAME в комплекте

В бане 8 млн доменов...
ЧТО «упало»?!

РАНЖИРУЙ @ СОКРАЩАЙ

Сокращай: ~~до TLD~~, до public suffix

Ранжируй: Alexa API и top 1M, Cisco Umbrella

Это все дико, например

Блоб парсим грепом, например...

reddit.com, alexa #6

Интернет-сообщество

`out.reddit.com`, обёртка вншешних ссылок — 34.230.170.103

и ещё три домена

amazon.com, alexa #10

Инфраструктура?

`ns-3.amazon.com`, DNS сервер — 54.69.236.62

и ещё три NS, и ещё три домена

instagram.com, alexa #16

Соцсеть

`instagram.com`, перенаправление на www — 34.192.156.80 и 34.193.159.161

netflix.com, alexa #32

Онлайн-кинотеатр

`api-global.latency.prodaa.netflix.com`, кусочки инфраструктуры — 54.148.226.99 и др.

`netflix.com`, перенаправление на www — 54.70.73.70 и др.

полторы сотни доменов, три сотни IP адресов...

twitch.tv, alexa #33

Стриминговый сервис

`app.twitch.tv`, бэкенд для приложения? — 52.72.179.4

`download.twitch.tv`, `invite.twitch.tv` и десятки других RR

dropbox.com, alexa #86

Облачный сервис хранения

`paper.dropbox.com`, инструменты совместной работы — 34.198.178.230

и ещё четыре домена

mozilla.org, alexa #156

Браузер

`serviceapi.security.mozilla.org` — 35.160.155.26 и др.

`accounts.firefox.com` — 34.210.164.160

`screenshots.services.mozilla.com` — 54.148.151.221 и др.

и десятки других

slack.com, alexa #231

Корпоративный мессенджер

`upload.slack.com`, сервис загрузки файлов — 34.200.60.200 и др.

`slack-redir.net`, обёртка вншешних ссылок — 52.73.151.99 и др.

airbnb.com, alexa #280

Аренда жилья

`airbnb.com`, перенаправление на www — 34.236.9.133 и др.

а также .ru, .hu, .es, и десятки других

zendesk.com, alexa #391

Платформа для корпоративной службы тех.поддержки

`thumbtacktech.zendesk.com`, тех.поддержка омских Thumbtack Technology? — 35.167.245.158

и три тысячи других саппортов от zello до zvooq

hp.com, alexa #354

Производитель оборудования

cdn.ext.hp.com, наверняка, CDN — 54.153.34.102

и десятки других доменов

wix.com, alexa #439

Платформа для создания веб-сайтов

`dns1.wix.com` — 13.56.142.82

`dns2.wix.com` — 34.199.12.23

mit.edu, alexa #462

Университет

`zerorobotics.mit.edu`, соревнования по робототехнике — 34.236.164.47

и двадцать доменов

strava.com, alexa #855

Соцсеть для физкультурников и спортсменов

`strava.com`, перенаправление на www — 34.232.140.172

kaspersky.com, alexa #2512

Поставщик решений в области информационной безопасности

`ics-cybermap.kaspersky.com`, карта киберугроз — 54.154.231.219

`game.kaspersky.com`, проект "Game of Threats" — 34.231.45.170

и 7 других доменов, включая blog.kaspersky.com, business.kaspersky.com и др.

ted.com, alexa #1097

Образовательный портал

`api.ted.com`, интерфейс для приложений — 34.198.211.2 и др.

и десятки других доменов сервиса, который повествует о "достойных распространения идеях"...

Итого «задеты»:

41 тысяча доменов из Alexa Top 1M

7.8 млн. поддоменов из Alexa Top 1M

12 млн. поддоменов

0 социально значимых ресурсов

Спасибо!

- ooni.torproject.org
- slides.ooni.io/2018/enog-15

Контакты

- leonid@openobservatory.org
- contact@openobservatory.org