

Аналитика ПОТОКОВ ДАННЫХ

Разбор трафика приложений

Александр Полунин



Применение DPI Engine

- Основные классы решений ИБ: NTA, NGFW, DPI и др.
- Решения для тарификации трафика абонентов: PCRF и др.
- Сетевые устройства, отвечающие за балансировку нагрузки на сеть, управление качеством обслуживания и др.

Бизнес задачи и сценарии

- Как идентифицировать видеозвонок в Telegram?
- Как получается, что AppleMusic содержит трафик Google?
- Как качественно разделить трафик экосистем (напр. Яндекс) на сервисы?

Методы классификации

от **port-based** до **Machine Learning** ...

Реализационные аспекты

Метод

Описание

Комментарий

Explicit

Классификация
по **порту** или
коду протокола

Определение номера порта
из контекста потока (5-tuple)
или поиск явного указания
кода протокола в заголовке
протокола нижележащего
уровня

Реализационные аспекты

Метод

Описание

Комментарий

**Port-based
classification
over SSL**

Классификация
по **ALPN-полям**
для SSL/TLS

Определение имени
протокола в полях ALPN
заголовка SSL/TLS.
Различает HTTPS, IMAPS,
POP3S и др.

Реализационные аспекты

Метод

Описание

Комментарий

**Pattern
matching**

Классификация
по **сигнатурам**
в пакете

Синтаксический анализ
содержимого пакета – поиск
конкретных сигнатур
(последовательностей байтов)
в самом идентифицируемом
пакете

Реализационные аспекты

Метод

Описание

Комментарий

**Protocol
Data
Signature**

Классификация
по значениям полей
в заголовке протокола
нижележащего уровня

Поиск конкретных значений полей
и их комбинаций в заголовке
протокола нижележащего уровня.
Например:
server, uri, user_agent (HTTP),
page_url (RTMP),
common_name (SSL)

Реализационные аспекты

Метод

Описание

Комментарий

DNS Caching

Классификация
по информации из **кэша**
протокола **DNS**

Использование информации,
полученной из DNS-обменов
и накопленной в кэше в ходе
обработки

Реализационные аспекты

Метод	Описание	Комментарий
Session Correlation	Классификация по информации из связанных сеансов	Использование информации, извлеченной из другого потока, в котором явно анонсировано выделение IP-адреса и порта для открытия идентифицируемого потока

Реализационные аспекты

Метод

Описание

Комментарий

**Session
Behavior**

Классификация
по **действиям** в рамках
сеанса

Анализ метрик потока,
специфичных для конкретного
приложения.

Определяет тип трафика
сервисов мгновенного обмена
сообщениями, зашифрованного
или обфусцированного трафика

Реализационные аспекты

Метод

Описание

Комментарий

**Statistical
Protocol
Identification**

ML-классификация
трафика на основании
структурно-временных
характеристик

Статистическое сравнение
с эталонной моделью трафика
данного вида

Источники признаков

- Специализированные сервисы (netify.ai, censys.io, WhoIs, 2ip и др.)
- Community (ndpi, Netify DPI и др.)
- Инструменты разработчика (роботы, scanner-revdns*, scanner-tls** и др.)
- **Аналитики**

Пространства признаков. Тюнинг

- Исключение дубликатов
- Приоритет доменных имен по длине совпадения
- Приоритет конкретного IP-адреса перед маской
- Приоритет между масками
- **Категоризация сервисов**

Категоризация трафика сервисов



Категоризация трафика сервисов

Специфичный трафик

для конкретного приложения
и имеющий специфические функции,
тесно связанные с основным
предназначением приложения / сервиса

Системный трафик,

генерируемый ОС устройства, или трафик
доступа к услугам общедоступных сервисов,
предоставляемых системами iOS и Android

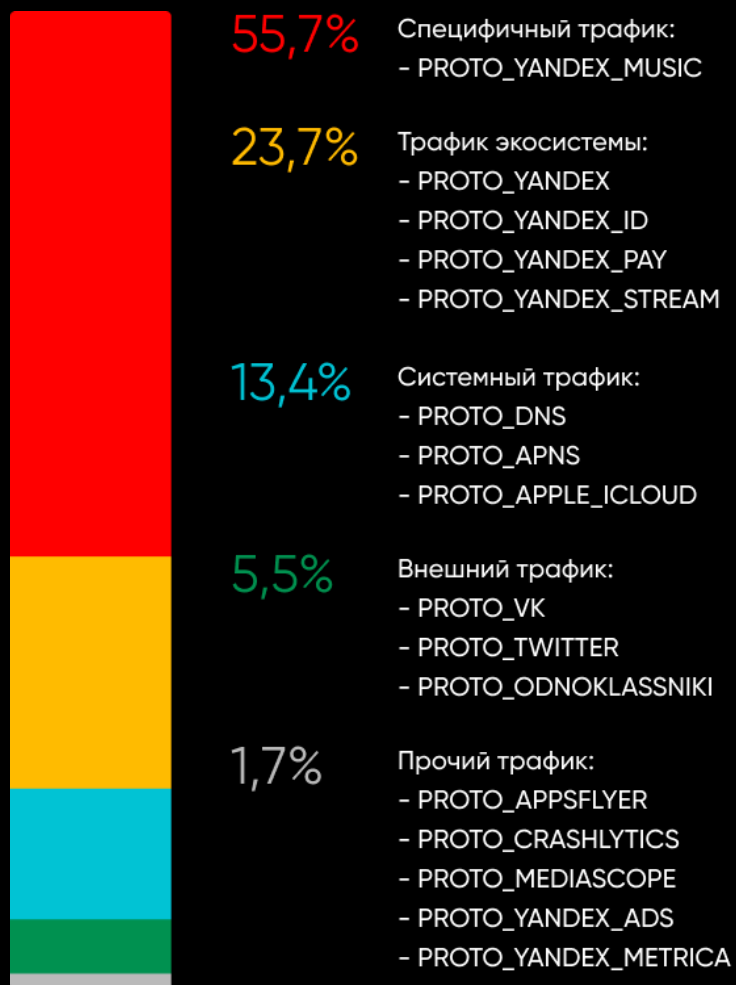
Внешний трафик

сторонних сервисов, которые не имеют
отношения к целевому приложению, но
генерируется через доступ ко внешним
ссылкам или через вызовы интерфейса

Трафик экосистемы

Трафик общедоступных служб, включая трафик
приложений экосистемы и общедоступных
серверов хранения CDN

Категоризация трафика сервисов



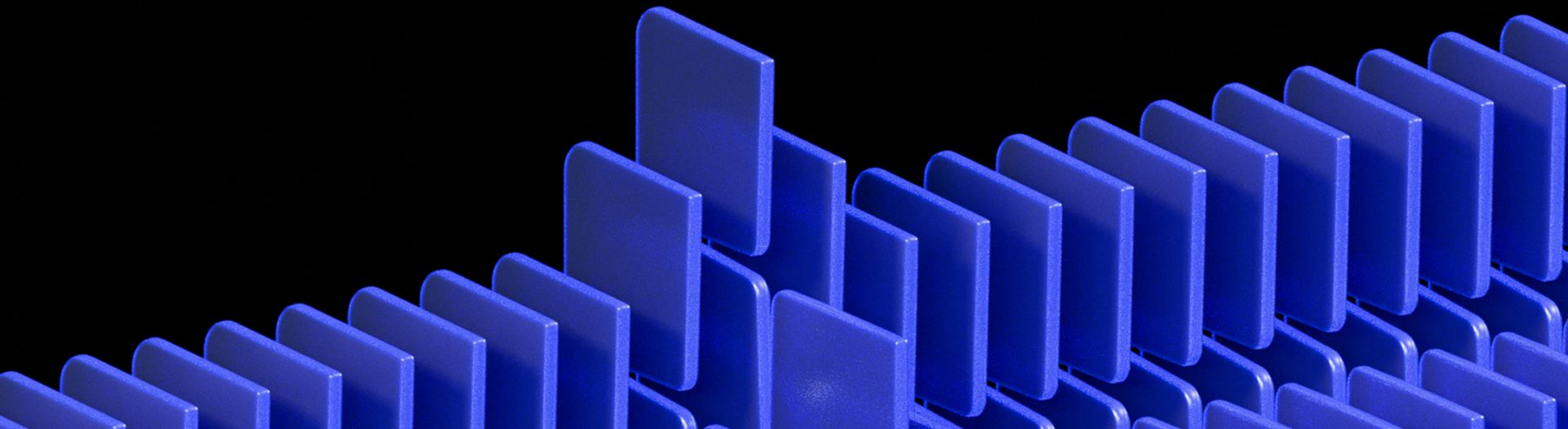
Яндекс  Музыка

Актуализация признаков



TrACE

SDK для анализа и классификации сетевого пакетного трафика



Ключевые преимущества

Собственная разработка

Разработка решения и обновление признаков выполняются собственными силами

Оперативность обновления

Обеспечивается комплексное сопровождение продукта с оперативной обратной связью и обновлением

Широкий спектр методов

Поддерживаются все основные существующие группы методов классификации трафика

Отечественные сервисы

Особое внимание уделяется распознаванию российских сервисов

600+

протоколов и сервисов

>95%

доля распознаваемого трафика



Instagram



WhatsApp

Яндекс



LinkedIn



Gmail



ВКонтакте

NETFLIX



YouTube



Facebook



Pinterest



TikTok

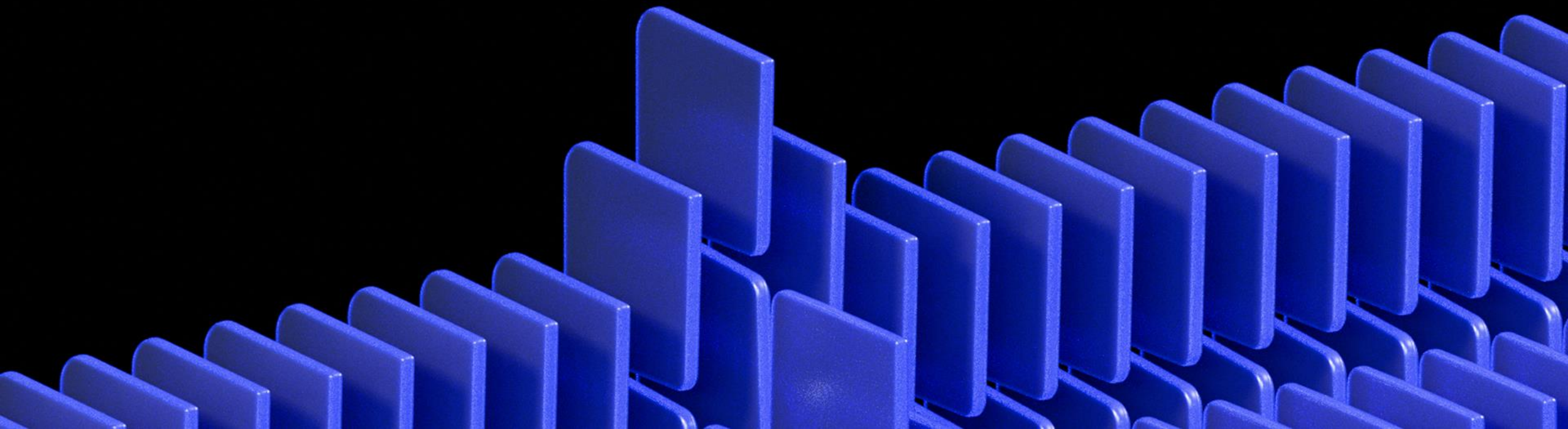


Twitter

Стенд №2



- Особенности использования в Ваших продуктах из первых уст
- Опыт применения решения в конкретных сценариях
- «Живая» демонстрация работы DPI Engine TrACE



Спасибо за внимание

Офис г. Москва

ДЦ "Дмитровский"

ул. Новодмитровская, д. 2Б, 5

Сайт

t-argos.ru

Почта

mail@t-argos.ru

