Часов П.С. Маштаков Н.С. Целесообразность использования антифрод-системы для обеспечения безопасности // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 2 с. 62–67

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ЦЕЛЕСООБРАЗНОСТЬ ИСПОЛЬЗОВАНИЯ АНТИФРОД-СИСТЕМЫ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

[1] Часов П.С., Маштаков Н.С.
МИРЭА-Российский технологический университет (РТУ МИРЭА), Институт информационных технологий, Москва, Россия (119454, г. Москва, проспект Вернадского, д. 86, с2), e-mail: [1] pasha_chasov@mail.ru

Для противостояние мошенничеству необходимо знать уже существующие схемы обмана, на основе анализа которых можно распознать их дальнейшее использование. В качестве инструмента обработки этих данных может выступать антифрод-системы.

Ключевые слова: антифрод, мошенничество, прокси, метрика

FUNDAMENTALS OF INFORMATION SECURITY AND WAYS TO PROTECT INFORMATION TECHNOLOGIES

[1] Chasov P. S., Mashtakov N. S.
MIREA-Russian Technological University (RTU MIREA), Institute of Information Technology, Moscow, Russia (119454, Moscow, Vernadskogo Avenue, 86, p2), e-mail: [1] pasha_chasov@mail.ru

Abstract: in order to resist fraud, it is necessary to know already existing schemes of deception, based on the analysis of which it is possible to recognize their further use. Anti-fraud systems can act as a tool for processing this data

Keywords: anti-fraud, fraud, proxy, metric.

Существует множество способов противостояния мошенничеству, но чем больше находится этих возможностей, тем больше появляется и самих схем мошенничества — это закономерный процесс. Новые технологии порождают новые способы обойти системы безопасности. А поскольку технологическое развитие процесс непрерывный и в наше время быстроразвивающийся, то необходимо постоянно анализировать возможные новые методы мошенничества.

Для данное задачи хорошо подойдет машинное обучение — будет получено определенное количество сценариев, на основе которых можно будет вычислять с определенной вероятностью, считается ли какая-нибудь операция подозрительной с точки зрения мошенничества.

Существует реализация подобной идеи — антифрод-система. Данная система строится на основе ее прикладных задач. Основными ограничениями для большинства решений основываются на данных параметрах:

- Лимит на количество операций за определенный временной промежуток;
- Лимит на сумму разовой операции;

- Лимит на количество выпущенных банковских карт, которые используются для проведения операций одним физическим лицом в течение определенного временного промежутка.

Ссылаясь на исследования FraudScore были выделены категории на которые можно разделить мошенничества, при проверке антифрод-системой, если речь идет о ее стандартных настройках:

1. PROXY — самая детектируемая метрика: Трафик, который направляется через промежуточное прокси-устройство или сеть, где реклама отображается на устройстве пользователя, где есть реальный пользователь. IP-адреса, связанные с известными ботнетами и рекламным ПО.
2. Далее следует IP. В эту категорию попадают все аномалии, связанные с IP-мошенничеством. Например, несколько преобразований с одного и того же IP-адреса или несколько преобразований из одной и той же IP-подсети.
3. Мошенничество с атрибуцией занимает третье место. Мошенничество с атрибуцией все еще растет, поскольку это утверждение также подтверждается различными глобальными отчетами:

- Clickspamming — было обнаружено, что установки приложений, ранее приписываемые рекламным кликам, являются установками приложений, сгенерированными пользователями.
- Вставка файлов cookie — процесс, при котором клиенту предоставляются файлы cookie из других доменов, как если бы пользователь посетил эти другие домены, взяв теги объявлений с сайта издателя и поместив их на другой сайт без ведома издателя.
- Внедрение кликов (только для Android) — Android уникально уязвим для мошенничества с внедрением кликов, когда рекламная сеть берет на себя ответственность за обычные установки приложений.

Маркетологам хорошо известно, что есть регионы по всему миру, которые требуют более пристального внимания к трафику и источникам, которые его обрабатывают. FraudScore разделяет данные и по мобильному, и по веб-трафику — рейтинги показывают, что фрод-лидеры практически одинаковы, но цифры различаются. Ниже представлено графическое представление данных [1-2].

Рейтинг лидеров мошенничества с веб-трафиком:

- Азиатско-Тихоокеанский регион — 50%
- США и Канада — 45%
- Ближний Восток — 44%

Рейтинг лидеров мошенничества с мобильным трафиком:

- Россия и СНГ — 48%
- Азиатско-Тихоокеанский регион — 38%
- Ближний Восток — 37%

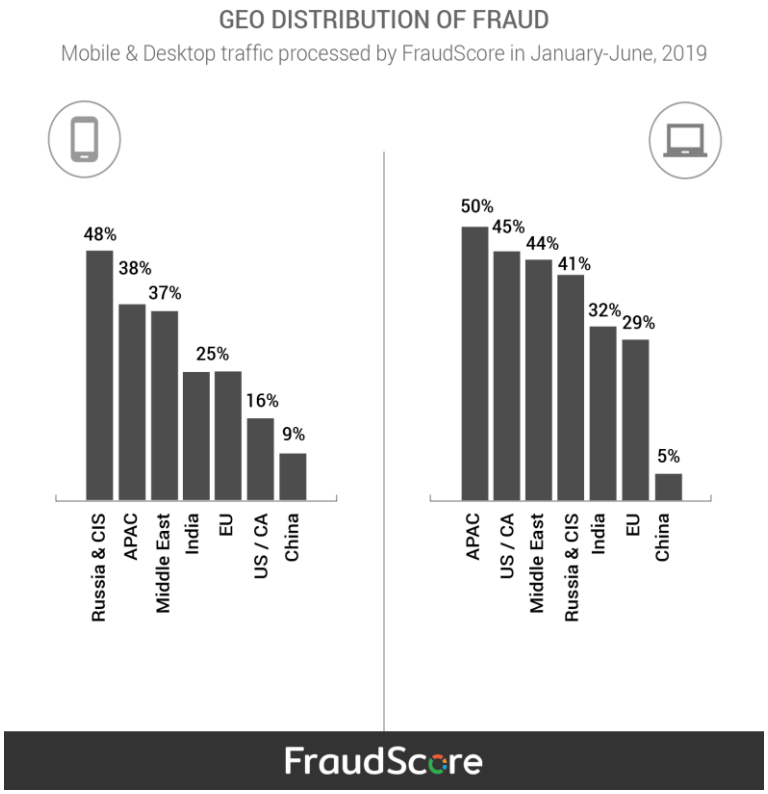

Рисунок 1 – Географическое распределение мошеничества на 2019 год
Источник: данные исследования FraudScore

Дальнейшее исследование было направлено на анализ трафика, который прежде был разделен на веб и мобильный.

Веб-трафик, исследуемый FraudScore представлен ниже.

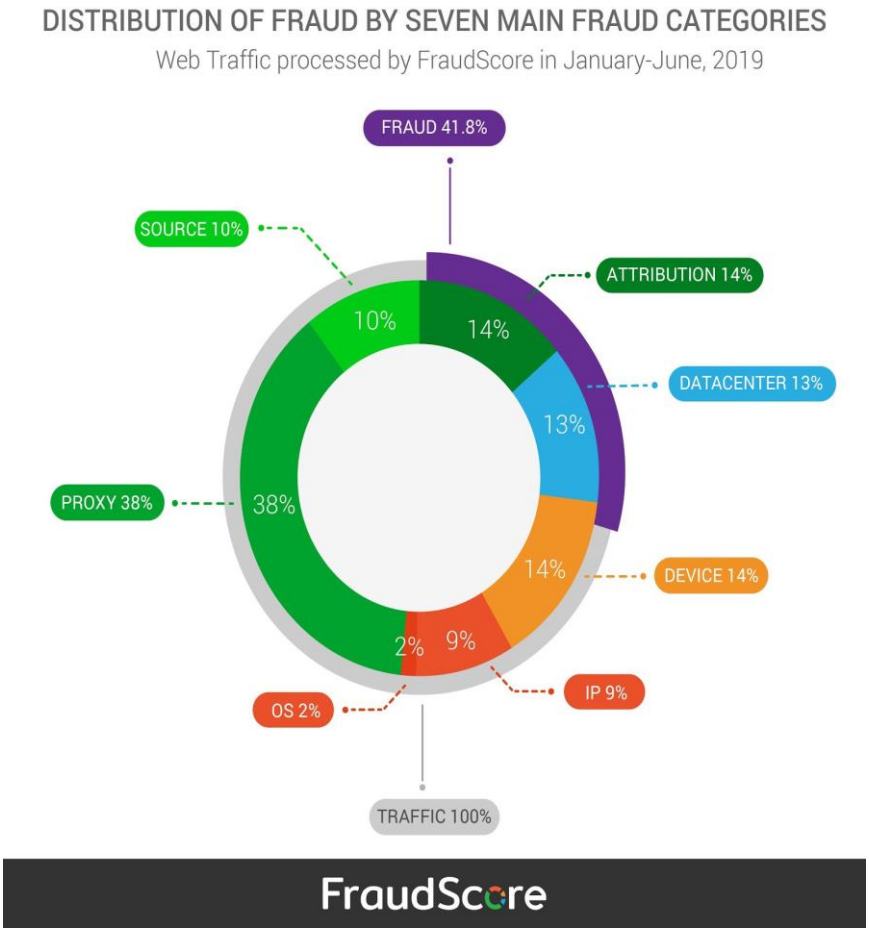

Рисунок 2 –Веб-трафик исследования

Источник: данные исследования FraudScore

За первые шесть месяцев 2019 года FraudScore обнаружил, что 41,8% всего обработанного десктопного трафика является мошенническим.

- Прокси-мошенничество и атрибуция лидируют с 38% и 14% соответственно.
- Далее следует мошенничество с устройствами — все аномалии, связанные с параметрами пользовательских устройств.
- APAC — регион с самым высоким уровнем мошенничества. Мошенничество с прокси и атрибуцией как наиболее выявляемые показатели.
- США и Канада делят второе место среди расположения, наиболее подверженных мошенничеству с центрами обработки данных, устройствами и прокси-серверами.
- Ближний Восток занимает третье место в рейтинге мошенничества с использованием прокси-серверов, атрибуции и мошенничества с устройствами [3].

Далее рассмотрим мобильный трафик.

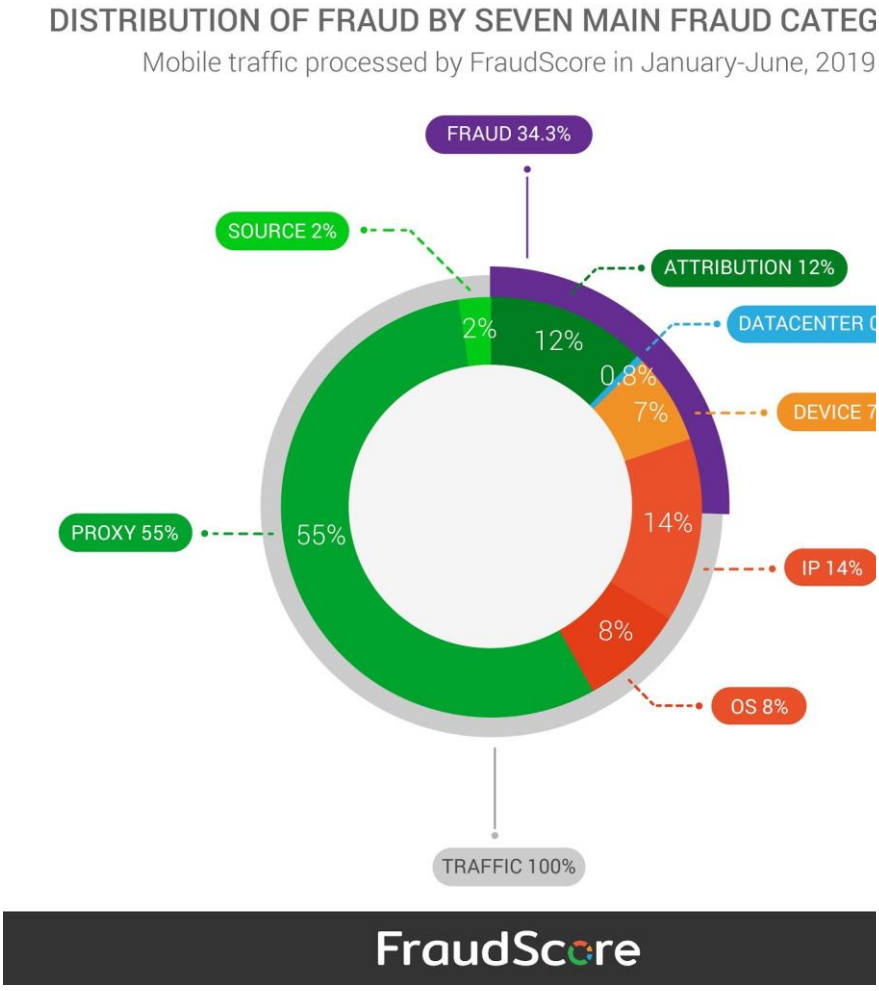

Рисунок 3 – Мобильный трафик исследования

Источник: данные исследования FraudScore

- По данным FraudScore за первые шесть месяцев 2019 года, 34,3% всего обрабатываемого мобильного трафика являются мошенническими.
- Прокси-мошенничество и IP лидируют с 55% и 14%.
- Далее следует мошенничество с атрибуцией — различные виды мошенничества с атрибуцией, в том числе наиболее широко известные — клик-спам, инъекция кликов и заполнение файлов cookie.
- Россия и СНГ — регионы с самым высоким уровнем мошенничества, при этом чаще всего выявляются категории мошенничества с использованием прокси-серверов и IP-адресов.
- Азиатско-Тихоокеанский регион занимает второе место с лидерами в категориях мошенничества с прокси-серверами, IP-адресами и ОС.
- Ближний Восток находится на третьем месте с мошенничеством с прокси-серверами, атрибуцией, IP-адресами и операционной системой.
- С конца 2018 года количество случаев мошенничества с iOS заметно увеличилось. Доля трафика iOS в мошенничестве составила 35,42%.

- Android-трафик на 28,16% мошеннический. Обе ОС становятся одинаково мошенническими с точки зрения рекламного трафика.

Приведенные данные показывают актуальность систем, противостоящих мошенничеству. Антифрод-системы являются главным рубежом проверки действий на предмет мошенничества. Полученные ею данные позволяют выявлять действия мошенников, так как система будет знать какие методы существуют на данный момент и статистическую возможность их применения.

Список литературы

1. Исследовательский материал «FraudScore» [Электронный ресурс] – URL: https://fraudscore.ai/blog/ad-fraud-report-global-statistics (Дата обращения: 04.11.2022)
2. Ознакомительный материал «Как работает антифрод» [Электронный ресурс] – URL: https://new-retail.ru/tehnologii/kak_rabotaet_antifrod6645 (Дата обращения: 05.11.2022)
3. Ознакомительный материал «ЧТО ТАКОЕ АНТИФРОД: ЗАДАЧИ И МЕТОДЫ» [Электронный ресурс] – URL: https://fisgroup.ru/blog/antifraud-zadachy-i-metody (Дата обращения: 05.11.2022)

References

1. Research material «FraudScore» [Electronic resource] – URL: https://fraudscore.ai/blog/ad-fraud-report-global-statistics (Date of access: 04.11.2022)
2. Introductory material «Kak rabot antifrode» [Elektronnyi resurs] – URL: https://new-retail.ru/tehnologii/kak_rabotaet_antifrod6645 (Date of access: 05.11.2022)
3. Introductory material «WHAT IS ANTIFRAUD: TASKS AND METHODS» [Electronic resource] – URL: https://fisgroup.ru/blog/antifraud-zadachy-i-metody (Date of access: 05.11.2022)