ИССЛЕДОВАНИЕ GROUP-IB: АКТУАЛЬНЫЕ КИБЕРУГРОЗЫ ДЛЯ ПАРФЮМЕРНЫХ БРЕНДОВ В 2019 ГОДУ

group-ib.com

GROUP IB

СОДЕРЖАНИЕ

01 АННОТАЦИЯ

ИССЛЕДОВАНИЕ СОДЕРЖИТ:

результаты исследования онлайн-рынка контрафактной парфюмерии и интернет-мошенничества

список рекомендаций для производителей, как реагировать на подобные нарушения

ЦЕЛЬ ДАННОГО ИССЛЕДОВАНИЯ:

изучить способы мошеннического использования брендов парфюмерных компаний и их популярных продуктов

оценить объем и денежный эквивалент продаваемых фальсифицированных продуктов

Распространение фальсифицированной парфюмерной продукции ставит под угрозу атакованные бренды. Возникает риск «размытия» — потери премиальности и стратегически определенной ниши на рынке. В итоге неправомерное использование парфюмерного бренда злоумышленниками в целях наживы может привести к снижению покупательского спроса и уровня доверия потребителей

Массовая миграция покупателей, а вслед за ними и продавцов в онлайн-сектор поднимает на новый уровень вопрос обеспечения информационной безопасности брендов. Любой переход на e-commerce влечет за собой возрастание риска цифрового мошенничества и проведения кибератак.

Мошенники активно используют все доступные им онлайн-каналы для распространения поддельной парфюмерной продукции или привлечения дешевого трафика. Пока производители конкурируют между собой, разрабатывая новые формулы духов и отвечая за качество готовой продукции — мошенники зарабатывают, паразитируя на чужом имени, зарекомендованном качестве и популярности.

Мошеннические ресурсы, использующие бренд официальной компании, опасны не только распространением контрафакта. Они также представляют угрозу репутации компании и значительно влияют на размер выручки, которую недополучают владельцы брендов.

Принимая во внимание важность описанной проблемы, команда Group-IB Brand Protection проанализировала каналы распространения и объемы фальсифицированной парфюмерной продукции, распространяемой через интернет. В ходе исследования были проверены сотни тысяч таких ресурсов, как:

— доменных имён,

— мобильных приложений,

— страниц в социальных сетях,

— ресурсов, направленных на продажу продукции под именами известных брендов.

Проведя подробный сбор данных, мы сфокусировались только на тех ресурсах, которые предположительно осуществляли торговлю контрафактной продукцией.

02 МЕТОДИКА ИССЛЕДОВАНИЯ

Объем выборки:

5

крупнейших производителей парфюмерии

Данные были получены в ходе мониторинга открытых источников в интернете и сети Deep Web.

Что мы анализировали:

- методы распространения и привлечения трафика,
- площадки для сбыта фальсифицированной продукции.

Для исследования мы выбрали «бренды-гиганты», известные во всем мире. Их целевая аудитория — весь международный рынок.

Объекты

Мы проанализировали упоминания и объявления о продаже парфюмерии, размещенные в интернете.

Были охвачены следующие типы ресурсов:

- поисковые системы Yandex и Google,
- социальные сети,
- интернет-магазины,
- тематические форумы,
- доски объявлений,
- теневой интернет.

Специфика

Специалисты Group-IB проанализировали взаимосвязи между регистрационными и контактными данными, IP-адресами и доменными именами. В результате чего вычислили аффилированность рассматриваемых ресурсов.

Ограничения:

Важно отметить, что достоверность объявлений имеет ряд ограничений, которые влияют на конечные результаты исследования. Невозможно с точностью проверить:

- наличие товара у продавца и соответствие тому, что указано в объявлении;
- происхождение продукта, выставленного на продажу;
- наличие документов, подтверждающих оригинальность продукта и легитимность его продажи.

Все количественные оценки реального оборота контрафактной парфюмерии носят приблизительный характер. Отсутствие точной информации не дает полного представления о теневых процессах и объемах.

03 ОБЪЕМ НАРУШЕНИЙ НА РАЗНЫХ РЕСУРСАХ

Площадки неправомерного использования брендов

Мошеннические ресурсы появляются и исчезают каждый день. В большинстве своем они объединены в сети, имеют идентичный бренду дизайн и конкретные признаки.

В рамках исследования мы выделили три категории мошеннических ресурсов, которые представляют наибольшую опасность для брендов:

1. Посвященные конкретному бренду

Полностью или частично скопированные с официальных ресурсов сайты с измененными ценами на товар и контактными данными.

2. Посвященные категории товара

Ресурс с различными товарами одного типа. Ассортимент таких сайтов – это, как правило, самые популярные модели внутри одного товарного сегмента.

3. Осуществляющие мультибрендовую продажу различных категорий товаров

Таким образом мошеннический ресурс маскируется под обычный интернет-магазин и создает иллюзию массовых продаж, тем самым вводит в заблуждение потребителя, который даже не догадывается, что может стать жертвой мошенников.

ВЫСОКИЙ

уровень угрозы

> 6 000

ресурсов, созвучных с названиями парфюмерных компаний

Доменные имена

Специалисты Group-IB Brand Protection зафиксировали множество схожих с официальными доменных имен, которые потенциально могут использоваться в мошеннических целях.

При этом не все ресурсы содержали противоправный контент. Так, например, кроме 1 домена, остальные 1 500, обнаруженные по одной из парфюмерных компаний, оказались «чистыми», то есть на них пока не было размещено никакого содержания. Впрочем, это не исключает возможного появления на них противоправного контента в любой момент.

Соотношения по группам следующие:

Как злоумышленники используют схожие доменные имена?

Рекламируют собственные сервисы

Мошенники мимикрируют под известные бренды для раскрутки собственных сайтов и привлечения трафика

Представляются партнерами известного бренда.

Мошенники используют чужой логотип или название компании в знак подтверждения делового партнерства, которое по факту является ложным. Некачественно или вообще не оказанные мошенниками услуги потребители начинают ассоциировать с известной компанией, что может повлечь за собой претензии, обращения в компанию, а также нанести репутационный ущерб

Указывают недостоверную информацию.

Ложные сведения могут вводить в заблуждение потенциальных клиентов и сотрудников компании-производителя. Кроме того, любые подделки могут быть опасны для здоровья человека

ВЫСОКИЙ

уровень угрозы

35

мобильных приложений
в неофициальных магазинах

Мобильные приложения

Существует большое количество разнообразных мобильных приложений, которые могут использовать или не использовать наименование и товарные знаки бренда.

Чем опасны неофициальные мобильные приложения?

Риск заразить пользовательское устройство вредоносным программным обеспечением.

Заражённое устройство может передавать все данные злоумышленнику, открывать доступ к управлению устройством и похищать персональные данные пользователя.

Введение потребителя в заблуждение.

Подобные приложения могут очень долго не обновляться или содержать недостоверную и неактуальную информацию, которая может нанести вред здоровью.

Указывают недостоверную информацию.

Ложные сведения могут вводить в заблуждение потенциальных клиентов и сотрудников компании-производителя. Кроме того, любые подделки могут быть опасны для здоровья человека.

ВЫСОКИЙ

уровень угрозы

> 3 000

групп и аккаунтов, которые помимо наименования препаратов используют средства индивидуализации парфюмерных компаний и осуществляют продажу

Социальные сети

Эксперты Group-IB Brand Protection проанализировали различные группы и аккаунты в социальных сетях, которые содержат средства индивидуализации парфюмерных компаний и популярных духов, а также занимаются продажами.

Их общая аудитория превышает 2 000 000 человек. Поэтому можно с уверенностью сказать, что эти площадки представляют серьезный риск для репутации компании.

Также мы собирали активные социальные сети, использовающие средства индивидуализации парфюмерных компаний: мультибрендовые и монобрендовые.

46	22	8

Количество групп в социальных сетях, специализирующихся на одном бренде

ВЫСОКИЙ

уровень угрозы

5 000 - 10 000

сайтов с продажей приходится на один бренд

Интернет-магазины

Анализ объявлений о продаже фальсифицированной парфюмерии показал: большая часть реализуется на общих агрегированных площадках. Мошенники активно используют мультибрендовые сайты из-за их доступности. И популярность духов идёт только им на руку.

ВЫСОКИЙ

уровень угрозы

1 800-20 000

объявлений приходится
на один бренд

Доски объявлений

Производился поиск по отечественным и зарубежным доскам объявлений:

- Авито, 9 150 объявлений.
- Tiu, 11 150 объявлений.
- Юла, 11 000 объявлений.
- Amazon, 970 объявлений.
- Ebay, 15 450 объявлений.
- AliExpress, —
- DHGate и др.

ВЫСОКИЙ

уровень угрозы

> 3 600

сообщений о продаже
парфюмерии за 2019 год

Теневые форумы

На теневых форумах производится продажа продукции под брендами, а также рекламируются существующие мошеннические ресурсы (в основном, в комментариях).

Часть продавцов распространяет товар сразу на нескольких форумах. Также встречались предложения оптовой продажи, в названии которых упоминается сразу несколько брендов.

04 МЕТОДЫ РАСПРОСТРАНЕНИЯ И ПРИВЛЕЧЕНИЯ ТРАФИКА

Предваряющий покупку поиск является идеальным моментом для мошенников — именно в этот момент проще всего привлечь потенциального покупателя выгодным предложением. Затраты мошенников в таком случае минимальны, ведь какой бы метод продвижения своих ресурсов они ни выбрали, он будет приносить результат и прибыль.

Анализ поисковой выдачи позволил выявить, что сайтов с продажей десятки тысяч, включая доски объявлений и социальные сети. Помимо выдачи по запросу, поисковые системы также предлагают аудитории контекстную рекламу мошеннических ресурсов, которая вводит неподготовленного пользователя в заблуждение.

Реклама

Для привлечения аудитории на свои ресурсы мошенники используют различные каналы, которые могут вести на мошеннические ресурсы злоумышленников:

- контекстную рекламу,
- таргетированные рекламные СМС-рассылки,
- рассылки в мессенджерах.

Подобная деятельность существенно влияет на отношение целевой аудитории к брендам и ведёт к репутационным потерям. Отдельно стоит учитывать рекламу мошеннических ресурсов, которые распространяют объявления о продаже контрафактной парфюмерии в комментариях и социальных сетях.

05 ПОТЕНЦИАЛЬНЫЙ УЩЕРБ

По данным Data Insight, конверсия в интернет-магазинах, рассчитанная как соотношение числа заказов в месяц к количеству посетителей, равна 4,4%.

Специалисты направления Brand Protection компании Group-IB подсчитали потенциальный ущерб парфюмерных компаний от продажи контрафакта в российских официальных интернет-магазинах.

Средний чек на духи популярных брендов, взятых нами для исследования, варьируется от 3 096 рублей до 9 970 рублей.

Средний чек	3 096	9 970
Количество интернет-магазинов	6 300	10 000
Оборот, мес.	**20 млн. ₽**	**100 млн. ₽**

Расчет убытка производился по формуле:

ПОТЕНЦИАЛЬНО НЕДОПОЛУЧЕННАЯ ПРИБЫЛЬ = (средний чек × конверсия × количество ресурсов, продающих монобренд × среднее количество посетителей + средний чек × конверсия × количество мультибрендовых ресурсов × среднее количество посетителей × среднее количество пользователей, пришедших за данным продуктом) × процент контрафактного парфюма

По нашей оценке, рассчитанной с использованием вышеуказанной формулы, годовой объем торговли поддельной продукцией по 5 исследуемым парфюмерным брендам варьируется от **3,7 до 22,5 млрд рублей.**

При этом такие крупные объемы практически не несут издержек — для мошенников интернет-каналы распространения фальсификата полностью бесплатны и просты в использовании.

06 РЕКОМЕНДАЦИИ GROUP-IB ДЛЯ ПАРФЮМЕРНЫХ КОМПАНИЙ

Провести первичный мониторинг информационного поля

Основная цель — оценить масштаб проблемы (количество нарушений) и определить приоритетные источники. Также первичный мониторинг укажет, необходимо ли предпринимать меры по реагированию. Даже если на данный момент нарушений нет, это не значит, что они не появятся в будущем. Одни нарушения временны, а другие выявляются только после глубокого анализа информации.

Запустить релевантную систему мониторинга

Чтобы знать ситуацию в точках сбыта фальсифицированной продукции, необходим систематизированный мониторинг интернет-пространства. Его цель — определить фронт работ для устранения нарушений.

Важно, чтобы система мониторинга учитывала интересы потребителей и параллельно анализировала ранее полученные результаты. Для этого нужно применять соответствующие пользовательские запросы и искать в самых популярных среди покупателей источниках.

Повышать уровень осведомленности покупателей

Потребители не всегда разбираются в технологиях производства фирменной продукции и в её отличиях от подделок. Большинство людей легко ввести в заблуждение. Поэтому крайне важно проводить кампании по осведомлению и обучению потенциальных потребителей.

Group-IB - международная компания по предотвращению, расследованию киберпреступлений и мошенничеств с использованием высоких технологий.

В основе решения Group-IB **Brand Protection** — собственные разработки для борьбы с киберпреступлениями и уникальные данные киберразведки. Постоянное развитие механизмов обнаружения нарушений позволили защитить более 200 российских и зарубежных брендов.

Модераторские аккаунты в социальных сетях и выстроенные отношения с крупными площадками гарантируют ускоренное рассмотрение запросов Group-IB Brand Protection администраторами крупных площадок для оперативного устранения нарушений.

GARTNER IDC FORRESTER

Threat Intelligence, который лежит в основе решения Group-IB Brand Protection, признан лучшим в мире по оценкам Gartner (2015), IDC (2016), Forrester (2017)

FIRST TI

CERT GIB — аккредитованный член международных сообществ команд реагирования FIRST и Trusted Introducer. Благодаря этому Group-IB Brand Protection имеет компетенции оперативно блокировать опасные интернет-ресурсы по всему миру.

IACC

Компетентная организация Координационного центра национального домена сети Интернет, Фонда развития интернета и международной коалиции по борьбе с контрафактной продукцией и пиратством IACC.

16 лет

опыта расследований и анализа хакерских атак

1000+

успешных расследований по всему миру

Узнайте больше о Group-IB Brand Protection

group-ib.ru/brandprotection
info@group-ib.com