→ GROUP-IB

DIGITAL RISK INSIGHTS

ТЕНДЕНЦИИ РАЗВИТИЯ ИНТЕРНЕТ-МОШЕННИЧЕСТВА

GROUP-IB

group-ib.ru

Дисклеймер

1. Отчет подготовлен специалистами Group-IB без какого-либо финансирования третьими лицами.
2. Целью отчета является предоставление сведений о тактике, инструментах и особенностях инфраструктуры различных групп для минимизации риска дальнейшего совершения таких противоправных деяний, их своевременного пресечения и формирования у читателей должного уровня правосознания. В отчете приведены рекомендации от экспертов Group-IB по превентивным мерам защиты от атак групп. Описание деталей угроз в отчете приведено исключительно для ознакомления с ними специалистов по информационной безопасности с целью предотвращения возникновения подобных инцидентов в дальнейшем и минимизации возможного ущерба. Опубликованная в отчете информация об угрозах не является пропагандой мошенничества и/или иной противоправной деятельности в сфере высоких технологий и/или иных сферах.
3. Отчет подготовлен в информационных и ознакомительных целях, ограничен в распространении и не может использоваться читателем в коммерческих и иных, не связанных с образованием или личным некоммерческим использованием целях. Group-IB предоставляет читателям право использовать отчет на территории всего мира путем скачивания, ознакомления с отчетом, цитирования отчета в объеме, оправданном правомерной целью цитирования, при условии, что сам отчет, включая ссылку на сайт правообладателя, на котором он размещен, будет указан как источник цитаты.
4. Отчет и все его части являются объектами авторского права и охраняются нормами права в области интеллектуальной собственности. Запрещается его копирование, распространение полностью или в части, в том числе путем копирования на другие сайты и ресурсы в сети Интернет, или любое иное использование информации из отчета без предварительного письменного согласия правообладателя. В случае нарушения авторских прав на отчет Group-IB вправе обратиться за защитой своих прав и интересов в суд и иные государственные органы с применением к нарушителю предусмотренных законодательством мер ответственности, включая взыскание компенсации.

Оглавление

Все уходит в диджитал

×2

рост количества
онлайн-предложений

40%

продаж приходится
на соцсети

4,6 млрд пользователей

сети Интернет

5,2 млрд пользователей

мобильных устройств

4,2 млрд пользователей

соцсетей

Все процессы, которые сейчас происходят в интернете, напрямую связаны с таким явлением, как цифровизация. И точно так же неотрывно с ним связано интернет-мошенничество, так как интерес пользователей, компаний и мошенников возник по одной и той же причине. С неё и начнем.

Впервые термин «цифровизация» появился в 1995 году, когда американский информатик Николас Негропонте из Массачусетского технологического университета озвучил понятие «цифровая экономика». На сегодняшний день цифровизация стала неотъемлемой частью экономики во всем мире. Развитие информационных технологий позволило бизнесу выйти на новый, ранее недосягаемый, уровень социальных и деловых взаимодействий.

Только за последние пять лет количество пользователей сети Интернет во всем мире увеличилось на 1,24 млрд, а социальных сетей – на 2,91 млрд. Такой рост ведет к появлению множества как мировых корпораций и крупных компаний, так и небольших фирм и предприятий.

Конечно, такие масштабы внедрения цифровых технологий в нашу жизнь, помимо большого количества плюсов, имеют и некоторые минусы, главный из них – безопасность людей и бизнеса и их персональных данных в цифровом пространстве.

Мировая цифровизация является драйвером экономического развития. По данным IDC, к 2023 году больше половины ВВП составит цифровая экономика, новые продукты и приложения будут создаваться в 50–100 раз быстрее, количество их достигнет 500 миллионов.

Любой бизнес, неважно, насколько глубоко он связан с интернетом, подвержен цифровом рискам, так как:

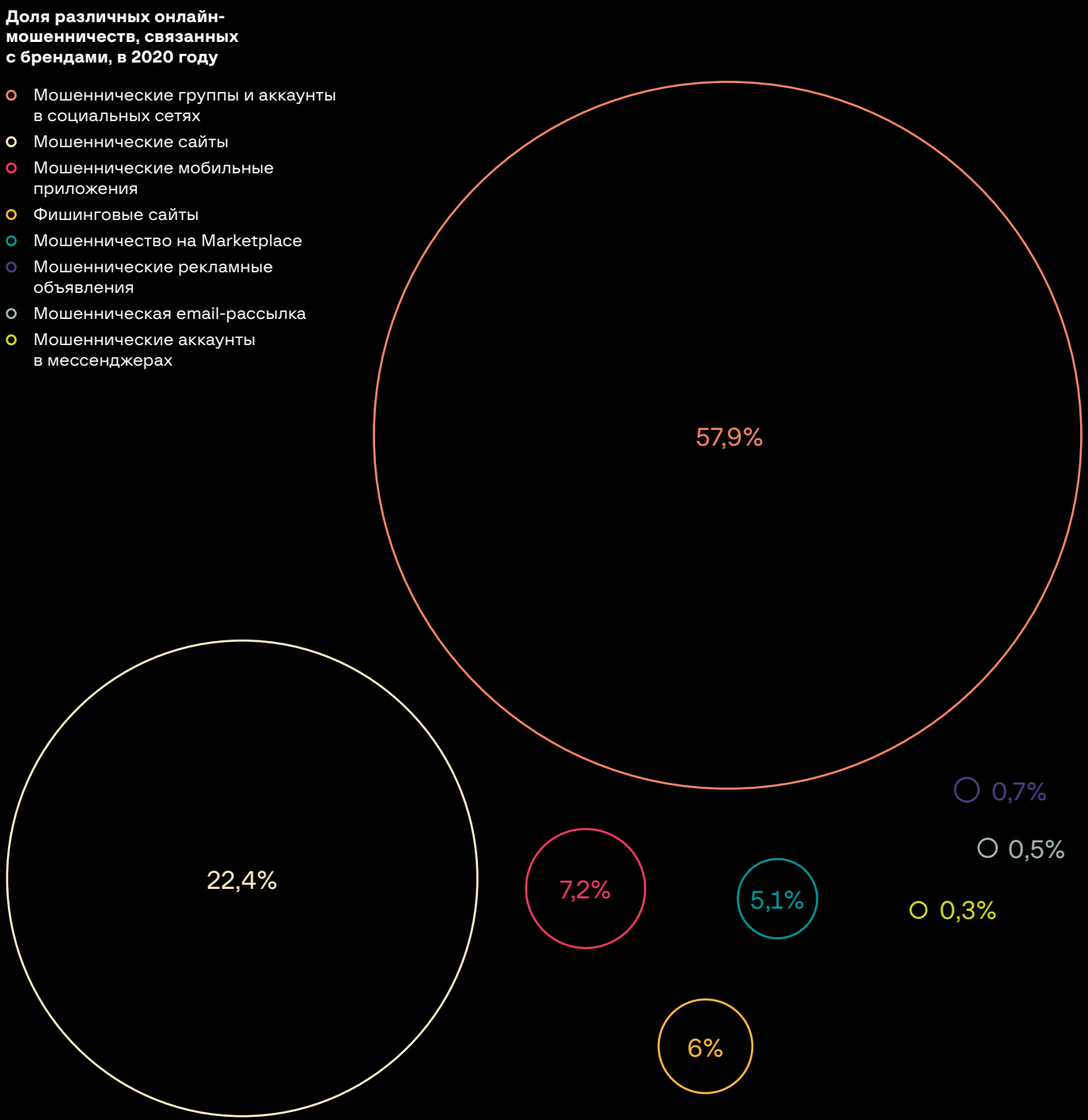
- Растет необходимость создавать безопасные цифровые платформы и экосистемы для масштабирования и расширения цифрового охвата;
- Кросс-канальные коммуникации формируют сложный цифровой отпечаток;
- Бизнесу становится сложнее контролировать свои цифровые активы;
- Все меньше защищенность цифровых активов, которые становится сложнее контролировать.

Ландшафт угроз

Типы атак

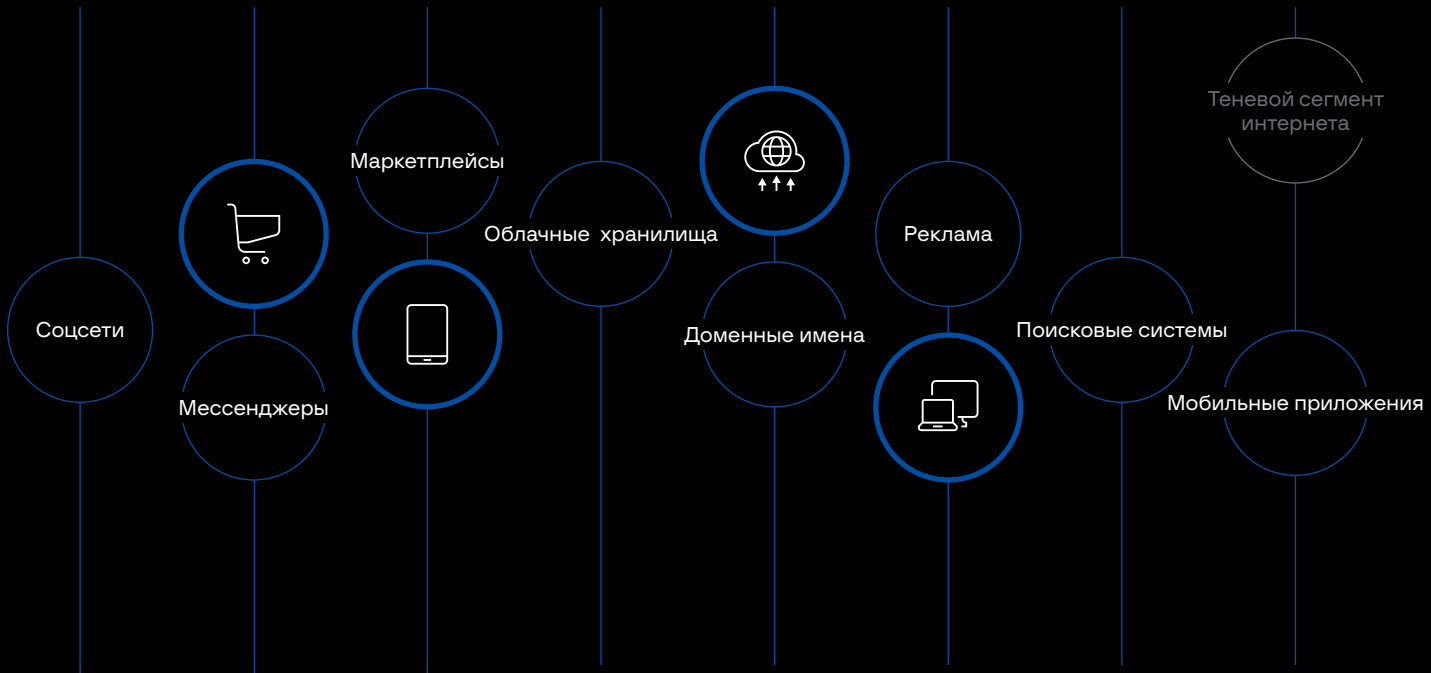
По данным Group-IB, больше всего мошенничеств с брендами в социальных сетях: на эту категорию пришлось 57,86%. На втором месте – мошеннические сайты (22,38%), на третьем – фишинговые сайты (6%).

Доля различных онлайн-мошенничеств, связанных с брендами, в 2020 году



Области цифрового присутствия

Компаниям важно анализировать все возможные точки контакта с аудиторией и защищать свои активы на всех платформах.



Ландшафт цифровых угроз

В онлайн-пространстве компании сталкиваются с множеством угроз, которые могут привести к ущербу данным, доходам и репутации.

Ландшафт угроз для любой компании довольно большой. Рассмотрим наиболее распространенные:

Фишинг – фальшивые страницы, которые воруют данные вашей карты, логины, пароли, чтобы заполучить доступ ко всем деньгам или данным.

Скам – сайты, которые снимают деньги сразу в виде конкретных платежей/переводов.

Контрафакт – предоставление поддельной, контрабандной продукции.

Пиратство – незаконно используемый контент, нарушающий авторское право, из-за чего недополучают прибыль легальные каналы дистрибьюции.

Ложное партнерство – сторонний сервис или продукция сомнительного качества, которая продается под вашим брендом, что ведет к снижению лояльности пользователей.

Неавторизованные мобильные приложения могут нести в себе все перечисленные выше риски: кражу данных, денег, доступа к устройству.

Неавторизованная реклама – захват части рекламного трафика брендовых запросов с последующим обманом вышеперечисленными способами.

Несогласованное использование товарного знака можно приравнять к ложному партнерству.

Утечка информации может привести к получению несанкционированного доступа.

Использование личностей VIP-персон – захват трафика из соцсетей, используя личность топ-менеджмента компаний.

Обсуждение вашей компании в дарквебе – публикация сведений об уязвимостях и вариантов заработка на вашем бренде, а также повышение внимания к компании в среде злоумышленников.

В большинстве случаев жертвами злоумышленников становятся клиенты компаний. Но тем не менее риски несет именно бизнес, так как он не только теряет часть выручки и получает претензии от пользователей, то есть несет финансовые и репутационные потери, но и может лишиться своего цифрового присутствия в целом.

Цифровым рискам подвержены все компании, независимо от индустрии, размера и географии.

Инструменты злоумышленников и последствия их действий

Привлечение трафика

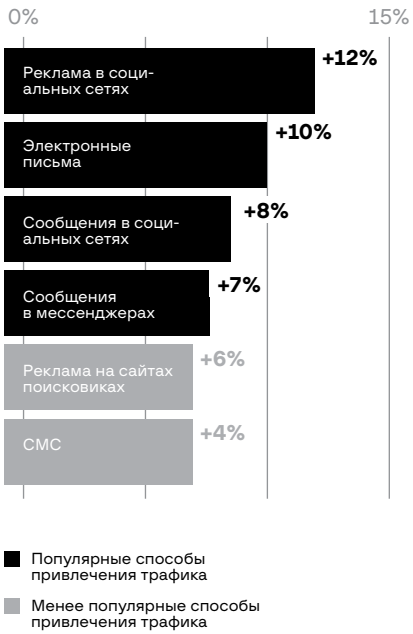
В своих схемах для привлечения трафика на мошеннические ресурсы злоумышленники используют интеллектуальную собственность правообладателей.

Способы привлечения пользователей в мошеннические схемы можно поделить на четыре вида:

1. **Поисковая оптимизация (SEO)** – раскрутка интернет-ресурса мошенников в топ выдачи поисковых систем.
2. **Реклама**
   - → Контекстная – текстово-графический или текстовый блок, который отображается с учетом контента рекламной площадки. Публикуется на страницах поисковых систем и на площадках, которые участвуют в рекламных сетях,
   - → баннерная – размещение текстовых или графических материалов на сайтах, форумах и порталах,
   - → в социальных сетях – размещение рекламных объявлений на страницах групп и аккаунтов,
   - → через Adware – ПО, предназначенное для показа рекламы на ПК пользователя, перенаправления запросов поиска на рекламные веб-сайты и сбора маркетинговой информации о пользователе для персонализации рекламных предложений.
3. **Продвижение в социальных сетях**
   - → С помощью поддельных аккаунтов бренда,
   - → разгон ботами,
   - → через лидеров мнений.
4. **Спам-рассылка с использованием купленных слитых баз данных**
   - → По email,
   - → в мессенджерах,
   - → СМС.

Благодаря увеличению числа пользователей социальных сетей и мобильных устройств привлечение трафика через эти каналы пользуется наибольшим спросом.

Динамика роста популярности методик атак в 2020 году



Способы заработка

Способы монетизации действий злоумышленников можно разделить на четыре типа:

1. **Захват логинов и паролей.**
   Для данного типа монетизации в качестве инструмента используются фишинг-компоненты.
2. **Прием платежей на поддельные реквизиты с помощью сайтов-клонов.**
   Для данного типа монетизации в качестве инструмента используются поддельные сайты, аккаунты в социальных сетях, фальшивые промоакции.
3. **Привлечение трафика на собственные сторонние сервисы.**
   Для данного типа монетизации в качестве инструмента используются ложное партнерство, неправомерное использование товарного знака.
4. **Заражение ВПО (вредоносное программное обеспечение).**
   Для данного типа монетизации в качестве инструмента используются поддельные сайты, мобильные приложения, аккаунты в социальных сетях.

Риски для бизнеса

Противоправная активность несет для брендов компаний множество рисков, которые можно выделить в три обобщенные категории:

Финансовые риски

- Недополученная прибыль,
- растущий объем обращений, компенсации.

Репутационные риски

- Репутационные потери,
- потеря клиентов и сотрудников,
- недоверие к рекламе бренда,
- трудности с информированием пользователей.

Инфраструктурные риски

- Использование утечек для целевых атак,
- подготовка атак в даркнете.

Решения по противодействию угрозам, связанным с цифровыми рисками

От всех перечисленных угроз можно защититься с помощью современных технологий. Одним из решений по противодействию угрозам, связанным с цифровыми рисками, является Digital Risk Protection (DRP) компании Group-IB.

Group-IB предоставляет своим клиентам лучшие инструменты и технологии для отражения атак и борьбы с любыми цифровыми рисками. Они основаны на уникальных данных Group-IB Threat Intelligence & Attribution и опыте борьбы с киберпреступностью по всем направлениям с 2003 года.

Обзор Group-IB Digital Risk Protection

11+ лет

опыта в сфере защиты брендов

70+ человек

международная команда аналитиков

85% нарушений

в среднем устраняются в досудебном порядке

Group-IB Digital Risk Protection (DRP) — это комплексная платформа управления цифровыми рисками на основе технологий искусственного интеллекта и нейронных сетей, которая осуществляет:

- оперативное выявление неправомерного использования цифровых активов,
- автоматическую классификацию и оценку критичности обнаруженных нарушений на основании собственной системы скоринга рисков,
- приоритизацию нарушений,
- рекомендации по оперативному устранению угроз.

Защиту от цифровых рисков поддерживает также специализированная команда технических и юридических экспертов с более чем **11-летним опытом защиты брендов** и другой интеллектуальной собственности. Связь и взаимодействие с клиентом осуществляются с помощью выделенной команды клиентского сервиса, что позволяет нам всегда быть в курсе возникающих угроз.

После выявления нарушений по согласованию с клиентом запускается процедура их устранения. Group-IB Digital Risk Protection реализует поэтапную процедуру реагирования, **что позволяет устранять в досудебном порядке в среднем 85% нарушений**.

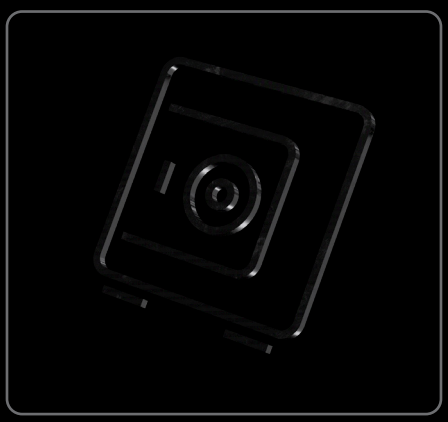
Сегодня Group-IB **защищает более 450 брендов** по всему миру.

Модули продукта Group-IB Digital Risk Protection:

АНТИМОШЕННИЧЕСТВО ↗

АНТИКОНТРАФАКТ ↗

АНТИПИРАТСТВО ↗



ОБНАРУЖЕНИЕ УТЕЧЕК ДАННЫХ ↗

ЗАЩИТА VIP-ПЕРСОН ↗

АНТИМОШЕННИЧЕСТВО

54%

доля мошеннических схем от общего числа высокотехнологичных преступлений за 2020 год

5000

пострадавших в одной из наиболее заметных мошеннических схем в 2020 году

Защита от неправомерного использования бренда

Защита пользователей от мошенничества в интернете и незаконного использования бренда. Система оперативно выявляет нарушения, наносящие репутационный и финансовый ущерб вашему бренду и пользователям, и принимает меры по блокировке.

Что можно обнаружить и устранить:

- фишинговые и мошеннические сайты,
- недостоверные сообщения о партнерстве с брендом,
- мошенническую рекламу с использованием бренда,
- поддельные аккаунты и группы в социальных сетях,
- поддельные и вредоносные мобильные приложения.

Угрозы:

- захват связки логинов и паролей,
- прием платежей на поддельные реквизиты с помощью сайтов-клонов,
- раскрутка мошеннических сервисов,
- заражение вредоносным ПО.

Реагирование и устранение нарушений:

- Определение и устранение случаев неправомерного использования бренда на отдельных порталах посредством мониторинга фишинговой и мошеннической активности, баз данных доменных имен регистраторов, поисковых систем и любых других возможных источников (соцсети, мессенджеры).
- Мониторинг рекламных сетей (контекстная и реклама в соцсетях) для выявления и устранения любой рекламы, затрагивающей бренд клиента.
- Отслеживание в легальных (Google Play, App Store) и полулегальных магазинах для устранения измененных или нелегально использующих бренд приложений сразу же после их появления.
- Поиск групп и постов в соцсетях для предотвращения попыток маскировки под бренд.
- Автоматическое построение связей между найденными и ранее зафиксированными нарушениями для прогнозирования угроз на ранних стадиях.
- Получение богатого опыта и знаний для обеспечения осведомленности о самых новых мошеннических техниках.

АНТИКОНТРАФАКТ

$1,9 трлн

прогнозируемый объем мирового рынка контрафакта товаров к 2022 году

До 40%

доля контрафакта в некоторых группах товаров

Защита от подделок и нелегальных онлайн-продаж

Борьба с контрафактной продукцией в интернете, предотвращение неправомерного распространения продукции, контроль соблюдения партнерской политики.

Что можно обнаружить и устранить:

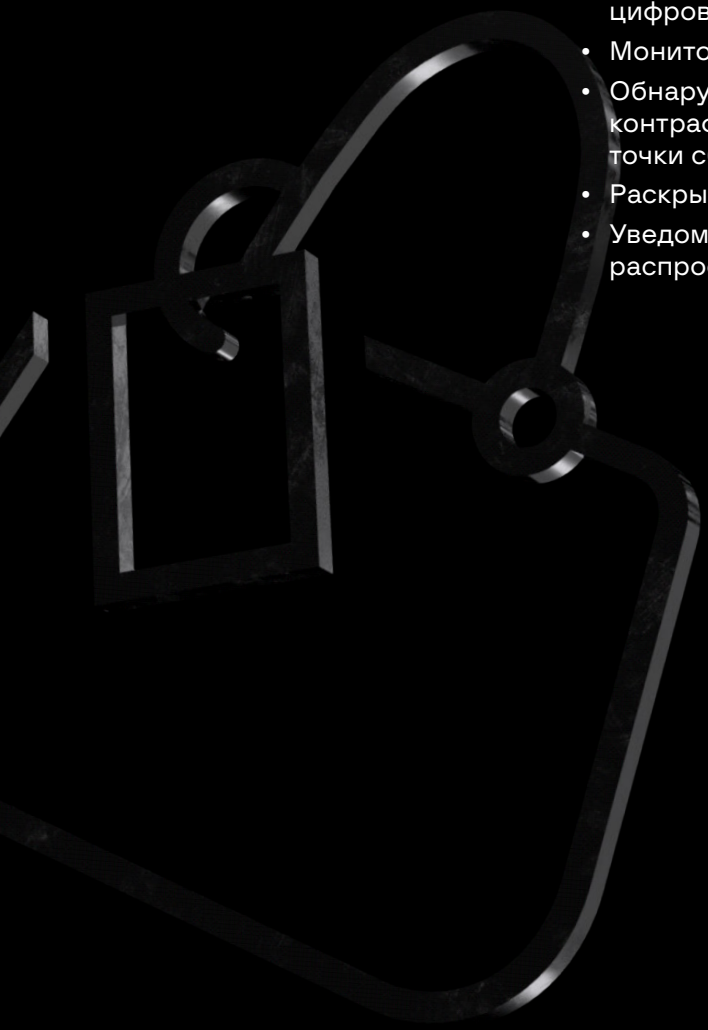
- незаконную продажу товаров в интернете,
- серый импорт,
- ложное партнерство,
- контрафакт.

Ущерб:

- Размытие бренда — потеря статуса бренда и его ниши на рынке.
- Ущерб репутации из-за риска низкокачественного контрафакта и вытекающего из этого вреда здоровью покупателя.
- Падение психологической цены продукта.
- Потеря клиентов и недополучение выручки.

Реагирование и устранение нарушений:

- Блокировка предложений контрафактных товаров на всех цифровых платформах.
- Мониторинг нарушений партнерских соглашений.
- Обнаружение нелегальных каналов распространения контрафакта в сети Интернет: производство — хранение — точки сбыта.
- Раскрытие всей цепочки распространения контрафакта.
- Уведомления о нарушениях точкам продаж и компаниям, распространяющим нелегальные товары.



АНТИПИРАТСТВО

$89 000

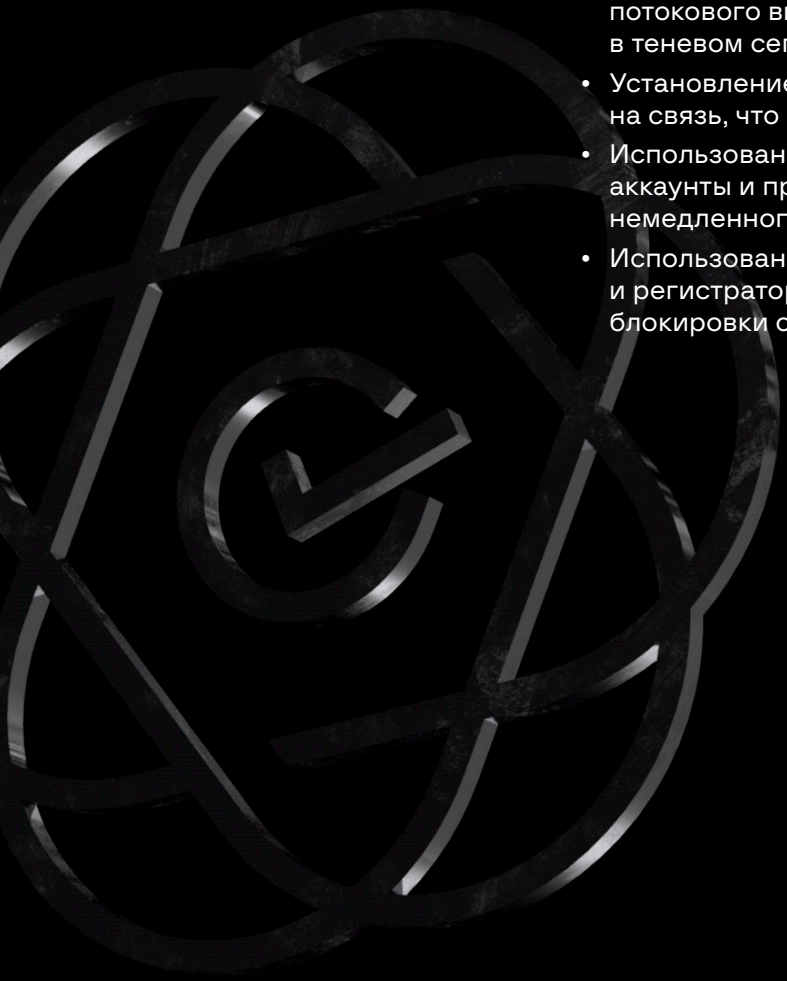
средний доход пиратского кинотеатра в год от нелегальной продажи контента и др.

80%

ссылок было заблокировано уже через 7 дней после появления первой нелегальной копии в сети Интернет

30 минут

требуется в среднем для обнаружения первой пиратской копии в Интернете



Защита от незаконного распространения цифрового контента

Мы используем передовую технологию digital fingerprinting, которая позволяет сравнивать цифровые копии по целому набору параметров и выявлять пиратский контент, даже подвергшийся значительным изменениям.

Что можно обнаружить и устранить:

- видеоконтент;
- онлайн-трансляции;
- программное обеспечение, компьютерные игры;
- книги, газеты, статьи;
- музыку.

Ущерб:

- недополучение выручки,
- упущенный трафик,
- упущенные клиенты,
- ущерб репутации из-за плохого качества пиратских копий.

Реагирование и устранение нарушений:

- Мониторинг по всей сети от торрент-трекеров и сервисов потокового видео до групп в соцсетях и пиратских платформ в теневом сегменте Интернета.
- Установление владельцев ресурса и прямой выход с ними на связь, что гарантирует доставку уведомлений модераторам.
- Использование таких преимуществ, как модераторские аккаунты и программы для доверенных вендоров для немедленного удаления контента.
- Использование нашей репутации среди хостинг-провайдеров и регистраторов доменов по всему миру для оперативной блокировки опасных ресурсов.

ОБНАРУЖЕНИЕ УТЕЧЕК ДАННЫХ

36 млрд

записей было скомпрометировано в 2020 году

75%

компаний считают, что не защищены от утечек данных

55%

компаний не уверены в уровне безопасности своих данных

Мониторинг утечек конфиденциальной информации и кода

Group-IB Digital Risk Protection отслеживает различные источники для обнаружения нелегальных репозиториев кода и другой неправомерно распространяемой информации.

Что мы мониторим:

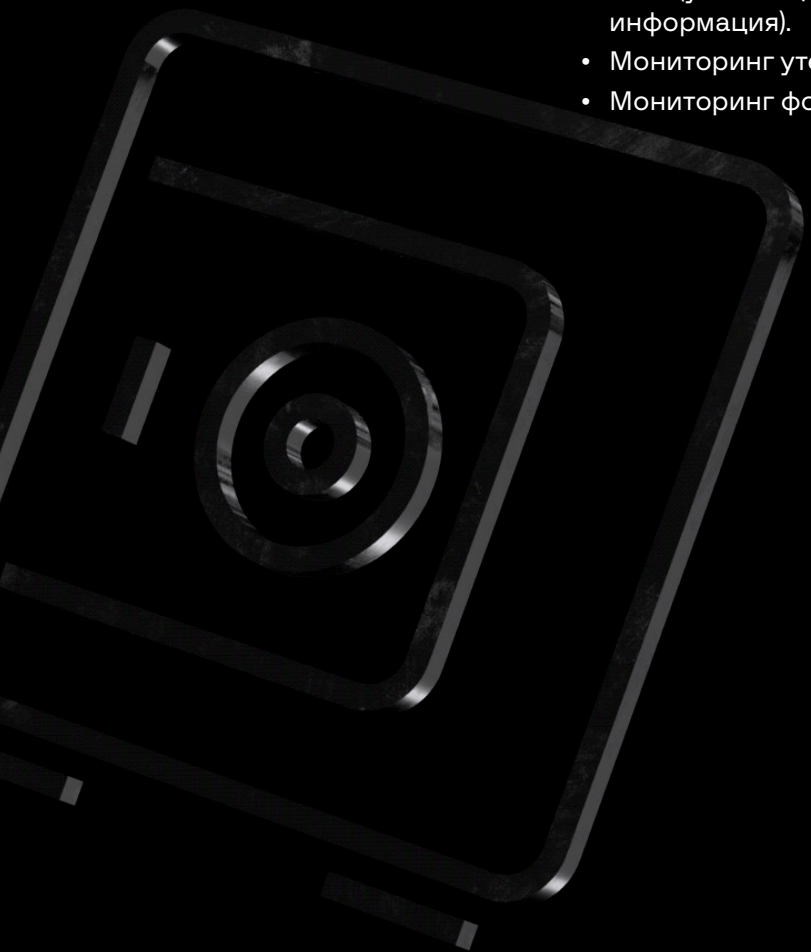
- публичные массовые базы данных,
- репозитории кода,
- dark/deep web.

Ущерб:

- потеря данных,
- нарушение бизнес-деятельности,
- недополучение выручки и потеря клиентов,
- правовые вопросы и штрафы,
- ущерб репутации.

Мониторинг и выявление:

- Мониторинг публичных утечек на paste-сайтах и репозиториях кода для обнаружения чувствительной информации любого типа (учетные данные, код и другая конфиденциальная информация).
- Мониторинг утечек данных в теневом сегменте интернета.
- Мониторинг форумов в теневом сегменте интернета.



ЗАЩИТА VIP-ПЕРСОН

120

фейковых аккаунтов было обнаружено в среднем в год по отношению к каждому из трех высших руководителей международного банка.

5 млн

просмотров поста фейкового аккаунта VIP-персоны в Instagram за 7 дней

Обнаружение и блокировка фейковых аккаунтов VIP-персон в социальных сетях

Решение Group-IB DRP защищает VIP-персон от угроз, связанных с распространением фейковых аккаунтов

Что можно обнаружить:

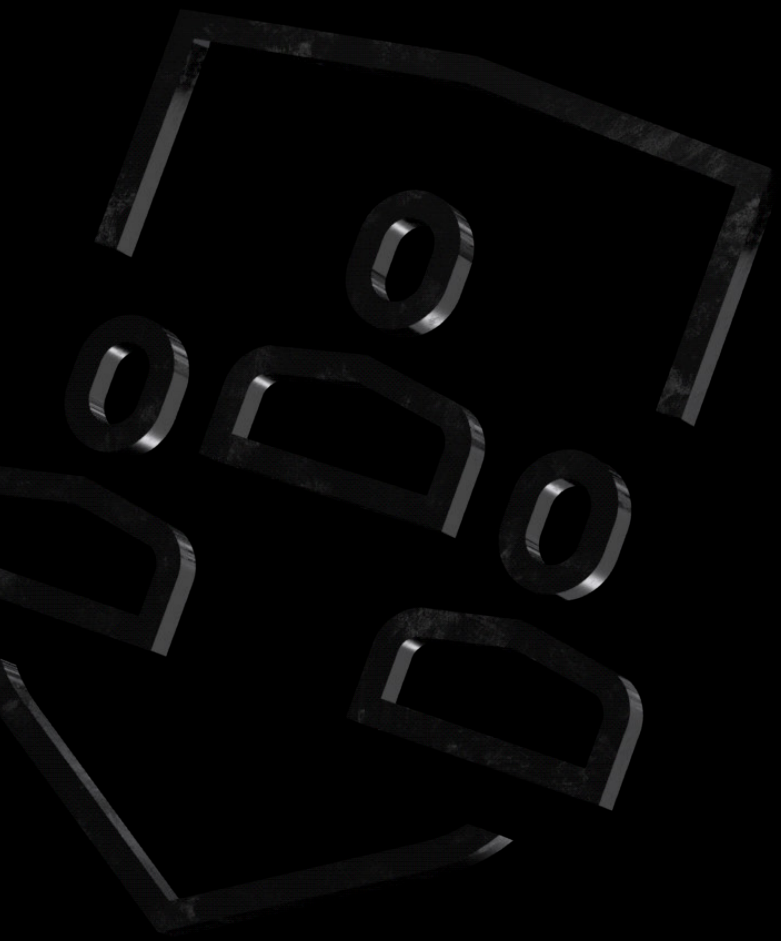
- фейковые аккаунты в социальных сетях.

Ущерб:

- ухудшение репутации руководства бренда,
- доступ к чувствительной информации компании посредством фишинговых схем,
- использование личности руководителя для дестабилизации бренда компании в онлайн-пространстве.

Мониторинг и реагирование:

- Мониторинг цифрового присутствия VIP-персон: репутации, фактов компрометации данных, любого инфополя, актуального для VIP-лица или его ближайшего окружения.
- Использование ежемесячных отчетов для формирования персонального цифрового бренда и корректировки цифровых активов.



Технологии решения

Анализ выявленных нарушений и приоритизация реагирования ↓

На основе заданных критериев система автоматически выявляет и фиксирует нарушения. Для исключения ошибок в нестандартных случаях ссылки верифицируются командой опытных аналитиков. Нарушения ранжируются по более чем 50 метрикам с учетом потенциального экономического ущерба, наиболее опасные устраняются в первую очередь.

Обнаружение нарушений

Мониторинг случаев незаконного использования бренда осуществляется с помощью комплекса технологий, собственных разработок нашей компании. Система применяет технологии киберразведки для обогащения данными и автоматически отслеживает в режиме 24/7/365 миллионы ресурсов.

Group-IB Digital Risk Protection использует машинное обучение для обнаружения нарушений на самых ранних этапах. Приоритетным направлением работ является выявление нарушений до начала привлечения трафика и предотвращение таким образом ущерба.

- Благодаря технологиям машинного обучения, система автоматически квалифицирует нарушения, опираясь на весь предшествующий опыт, изучает изображения, тексты и структуру миллиардов веб-страниц.
- На основе анализа больших данных система выявляет связанные с нарушением ресурсы, что позволяет проследить историю развития инцидента и заблокировать сразу всю инфраструктуру мошенника.
- Собственные технологии киберразведки позволяют быстро и эффективно, точечными воздействиями устанавливать инфраструктуру злоумышленников и останавливать ее.

Уникальный модуль визуализации Graph, основанный на данных системы киберразведки Group-IB, наглядно отображает каждое нарушение, позволяя связывать инциденты с их источником. Эта технология выявляет всю инфраструктуру злоумышленника и осуществляет комплексные действия по блокировке.

Мониторинг и обнаружение ↓

Мониторинг ресурсов

Средства мониторинга:
- Парсеры
- Веб-краулеры
- API

Способы мониторинга:
- Proxy scheduler
- User-agent scheduler
- Специально созданные аккаунты

Анализ данных

Выявление случаев нелегального использования бренда и контента

Упоминания названия бренда:
- Анализ логотипа
- Распознавание текста
- Распознавание изображений
- Регулярные выражения

Выявление нарушений

Регулярное обновление информации и статусов в системе, проверки на предмет повторного появления угроз

Идентификация
- Сигнатурный анализ (фишинг/мошенничество)
- Нейронные сети
- Общий скоринг
- Скоринг доменных имен

Фиды данных ↓ **Облако тегов** ↓ **Связи на графе** ↓

ОБЛАКО ПОТЕНЦИАЛЬНЫХ НАРУШЕНИЙ

Устранение нарушений

Group-IB Digital Risk Protection реализует трехэтапный процесс удаления, что максимально увеличивает вероятность устранения нарушений.

1. **Извещение.** Идентификация владельца ресурса и отправка запроса на устранение обнаруженного нарушения.
2. **Эскалация.** Использование партнерской сети для принудительного устранения нарушения.
3. **Досудебная претензия.** Отправка официального досудебного уведомления о блокировке выявленного нарушения.

Комплексное реагирование ↓

Уведомление (1)

Установление владельца ресурса и запрос на устранение обнаруженного нарушения

Эскалация (2)

Использование партнерских связей для исполнения требования устранить нарушение

Устранение нарушения (3)

Получение официального разрешения на устранение выявленного нарушения в досудебном порядке

Прямое реагирование (блокировка ресурса)

→ Обращение к администратору ресурса
→ Обращение к хостинг-провайдеру
→ Обращение к регистратору доменного имени
→ Обращение к ассоциациям и партнерам (CERT, ICANN и др.)

Блокировка ресурсов | Устранение нарушений | Удаление контента

Дополнительные меры (минимизация нарушений)

→ Добавление ресурса в базы мошеннических и фишинговых ресурсов
→ Удаление из поисковой выдачи и блокировка контекстной рекламы
→ Блокировка мошеннических аккаунтов в соцсетях
→ Блокировка на уровне DNS-серверов

Пользователи увидят предупреждающий баннер | Пресечение трафика из социальных сетей и поисковой выдачи | Недоступность ресурса для большинства пользователей

Компетенции и партнеры

CERT-GIB – это первая в России частная аккредитованная группа оперативного реагирования на инциденты информбезопасности, член международных сообществ FIRST, Trusted Introducer, компетентная организация Координационного центра национального домена сети Интернет и Фонда развития Интернета.

Быстро и эффективно реагировать на нелегальное использование бренда в Сети нам помогают:

- Квалифицированная помощь специалистов с многолетним опытом реагирования на киберпреступления.
- Специальные компетенции по блокировке мошеннических ресурсов в доменных зонах: .ru, .рф и .su.
- Реагирование за пределами Рунета благодаря сотрудничеству с центрами реагирования в других странах и международными ассоциациями по борьбе с киберпреступлениями.

Ключевые инновации ↓

Искусственный интеллект

Уникальное семейство нейронных сетей, разработанное на основе передовых запатентованных методов обнаружения, способное обнаруживать до 90% нарушений подобно тому, как это сделал бы высококвалифицированный специалист

Разведданные по мошенничеству

Революционный подход к расследованиям, изучению и прогнозированию поведения мошенников, а также разработка инструментов, позволяющих улучшать возможности по обнаружению и устранению нарушений

Адаптируемая скоринговая модель

Уникальный механизм оценки степени серьезности нарушения, основанный на машинном обучении, позволяет быстро и эффективно расставлять приоритеты при устранении нарушений

Графовый анализ

Сетевой анализ, который помогает выявить инфраструктуру киберпреступников и найти дополнительные методы для успешного устранения нарушений

Автоматическая атрибуция

Алгоритмическая корреляция связанных ресурсов и объектов для атрибуции и устранения мошеннических групп с целью предотвратить дальнейшую эскалацию атак

Экосистема Group-IB

Обогащение алгоритмов обнаружения за счет взаимодействия между решениями Group-IB и использование оригинальных методов мониторинга позволяет обнаружить даже самые сложные нарушения и неуловимых киберпреступников

Глобальная сеть партнеров для эффективного реагирования ↓

Модераторские аккаунты в социальных сетях и выстроенные отношения с крупными площадками

AliExpress ebay YouTube Google

Аккредитованный член международных сообществ команд реагирования

IACC CERTIFIED VENUE FIRST IMPACT TI

Лидер на рынке услуг Digital Risk Protection по версии аналитического агентства Frost & Sullivan

FROST & SULLIVAN

Комплексный подход ↓

Международная команда аналитиков

Высококвалифицированные аналитики специализируются на угрозах, актуальных для вашего бизнеса и региона, что позволяет осуществлять эффективное реагирование на нарушения по всему миру

Платформа для бизнеса и аналитиков

Возможность видеть основные показатели, самостоятельно согласовывать уведомления о нарушениях и получать статистику в режиме реального времени

Уникальный подход к реагированию

Сочетание автоматизированной системы и развитой партнерской сети позволяет устранить большинство нарушений в досудебном порядке

Платформа DRP

Доступ к информационным панелям и отчетам, которые дают полное и прозрачное представление о процессах обнаружения и устранения нарушений

Клиентский сервис

Персональный менеджер информирует вас об обнаруженных нарушениях и рисках, а также способствует их эффективному устранению

Защита в режиме 24/7/365

Автоматизированный мониторинг цифровых активов, круглосуточное обнаружение и устранение нарушений командой аналитиков

Применение продукта

Программное обеспечение по безопасности и отдел ИТ обычно отвечают за работу инфраструктуры компании, безопасность цифровых активов во всех их проявлениях, им релевантны блоки Антимошенничество, Защита VIP-персон, Обнаружение утечек.

Безопасность и IT ↓

Кто?

- Директор по информационной безопасности
- Директор по информационным технологиям
- Директор по разведке угроз (Threat Intelligence)
- Департаменты антифрода и антимошенничества
- Аппарат генерального директора (VIP-защита)

Что?

- Защита бизнеса от всех релевантных форм цифрового риска
- Реагирование, инновационный подход, цифровая трансформация
- Мониторинг неправомерного использование бренда, мониторинг и отображение цифрового следа, защита VIP-персон в цифровом пространстве
- Регулярные отчеты и поддержка аналитиков

Почему?

- Возврат цифровой активности в официальный канал
- Преимущества над конкурентами
- Мониторинг и минимизация последствий на стороне вендора
- Экспертиза и компетенции

Маркетинг ↓

Маркетинг отвечает за продвижение компании и продукта, а также за генерацию лидов и пользовательский опыт. Для этих целей наиболее актуальны блоки Антимошенничество, Антиконтрафакт, Антипиратство.

Кто?	Что?	Почему?
• Директор по маркетингу • Бренд-менеджер • Специалист по защите бренда • Менеджер социальных сетей	• Защищенное взаимодействие клиента с брендом во всех точках (каналах) онлайн-продаж • Регулярный мониторинг упоминаний бренда, продажи контрафактной продукции, мошеннических активностей • Сохранение эффективности маркетинговых инструментов для стимулирования роста продаж • Механизмы для выявления угроз для бизнеса в сети Интернет на ранних стадиях	• Высокий уровень защиты брендов от цифровых рисков • Широкий спектр источников для мониторинга и минимизации цифровых рисков • Улучшение показателей отдела • Высокий процент успешного реагирования: блокировка ресурсов, устранение нарушений

Юридический департамент ↓

Юридический департамент отвечает за защиту интеллектуальной собственности компании, защиту товарных знаков, для таких задач в первую очередь будут полезны блоки Антимошенничество, Антиконтрафакт, Антипиратство.

Кто?	Что?	Почему?
• Глава юридического департамента • Бренд-менеджер • Менеджер по защите интеллектуальной собственности	• Регулярный мониторинг упоминаний бренда, продажи контрафактной продукции, мошеннических активностей • Единое решение и комплекс мер для минимизации цифровых рисков на стороне поставщика • Применение комплекса досудебных мер для минимизации цифровых рисков	• Экономия времени и ресурсов на досудебном реагировании • Сокращение объема обращений, претензий со стороны пострадавших • Простота в использовании • Высокий процент успешного реагирования: блокировки ресурсов, устранения нарушений • Фокус на корпоративной юридической и стратегически важной работы

Юридический комплаенс ↓

Комплаенс-департамент отвечает за безопасность взаимодействия клиента, ему релевантны модули антимошенничество и антиконтрафакт.

Кто?	Что?	Почему?
• Директор по соответствию • Директор по рискам	• Защищенное взаимодействие клиента с брендом во всех точках (каналах) онлайн-продаж • Регулярный мониторинг упоминаний бренда, продажи контрафактной продукции, мошеннических активностей • Единое решение и комплекс мер для минимизации цифровых рисков на стороне поставщика	• Запрос от ЦБ о необходимости выполнения локальных или глобальных требований • Внутреннее соответствие для конкурентоспособности • Соответствие глобальному рынку • Минимизация рисков мошенничества в отношении клиентов и сотрудников

Тренды и Use Cases

Общие тренды и тенденции

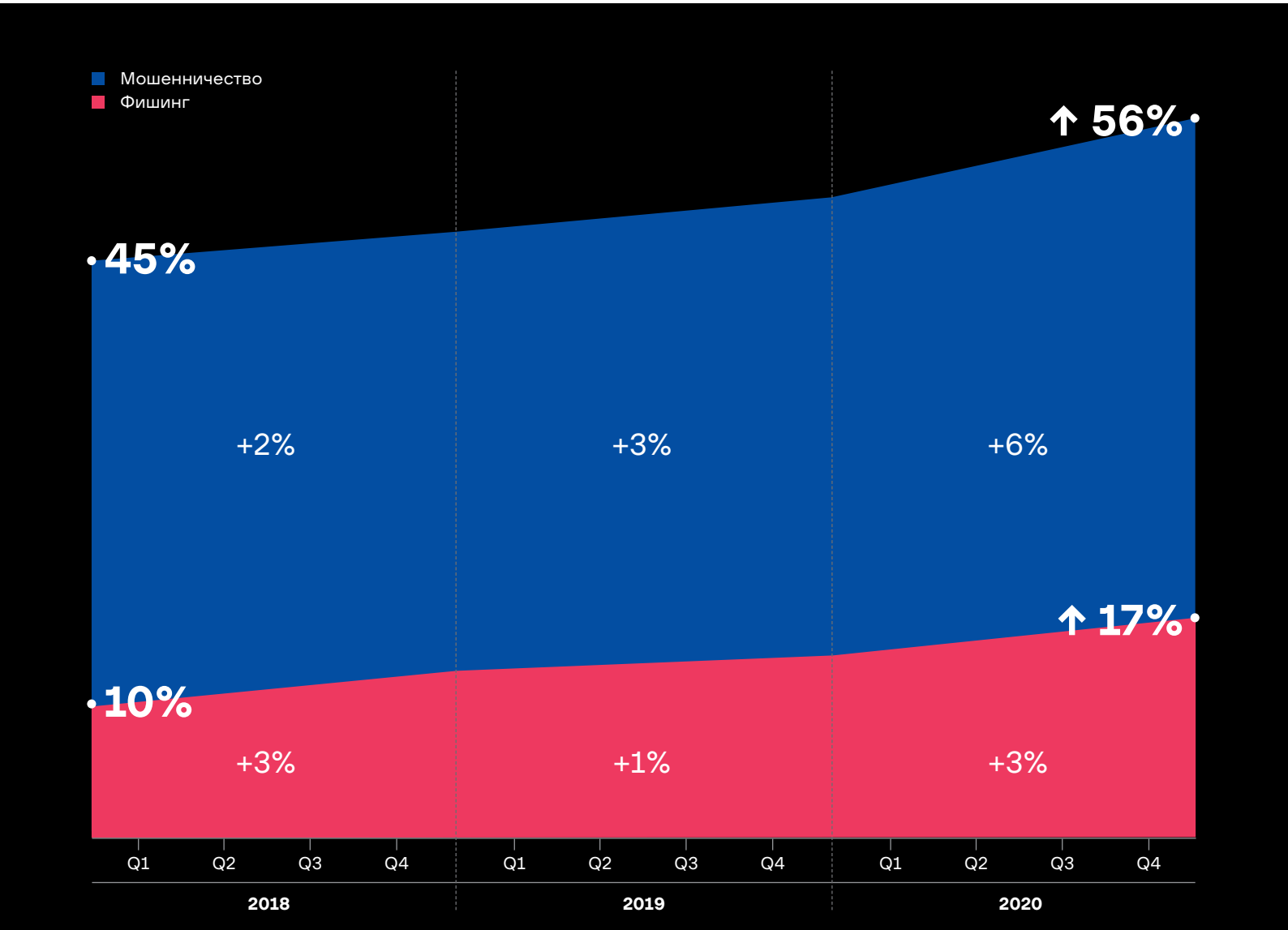
Пандемия коронавирусной инфекции вынудила компании цифровизировать свой бизнес, а офлайн-мошенников уйти в онлайн. Все это повлияло на рост онлайн-мошенничества во всем мире. Помимо этого, естественный рост онлайн-мошенничества обусловлен повышением доступности интернета.

По данным Group-IB, 73% процента всех кибератак приходится на скам и фишинг. Остальные 27% – на высокотехнологичные преступления, такие как Android-трояны, вирусы-шифровальщики, атаки на интернет-банкинг и т.д.

В 2020 году доля онлайн-мошенничества в общем объеме онлайн-атак увеличилась на 6% по сравнению с прошлым годом и составила 56%. Доля фишинга увеличилась на 3% и составила 17%.

Динамика роста количества нарушений, связанных со скамом и фишингом и зафиксированных Group-IB в России, составила 35% в сравнении с прошлым годом. В Европе этот показатель равен 39%, в Азиатско-Тихоокеанском регионе – 88%, на Ближнем Востоке – 27,5%

Процентная составляющая онлайн-мошенничеств ↓



Новая парадигма мошеннического бизнеса

Сегментирование, таргетирование, персонализация

Как и специалисты по интернет-маркетингу, ранее злоумышленники в первую очередь обращали внимание на охват аудитории. Их главной задачей было привлечь на ресурс как можно большее количество пользователей, чтобы в дальнейшем кого-то из них обмануть. Но интернет-сообщество уже давно понимает, что это просто прожигание бюджетов, все стали считать конверсию и оценивать эффективность своих промокомпаний. Злоумышленники тоже начали сегментировать пользователей, таргетировать промо-компании и персонализировать предложения – все для того, чтобы получить как можно больше жертв и прибыли при минимальных вложениях.

Более того, новая парадигма интернет-мошенничества уже успела модернизироваться. Ниже показаны сравнительные характеристики и изменения за последние 2 года:

Сравнительная характеристика интернет-мошенничества ↓

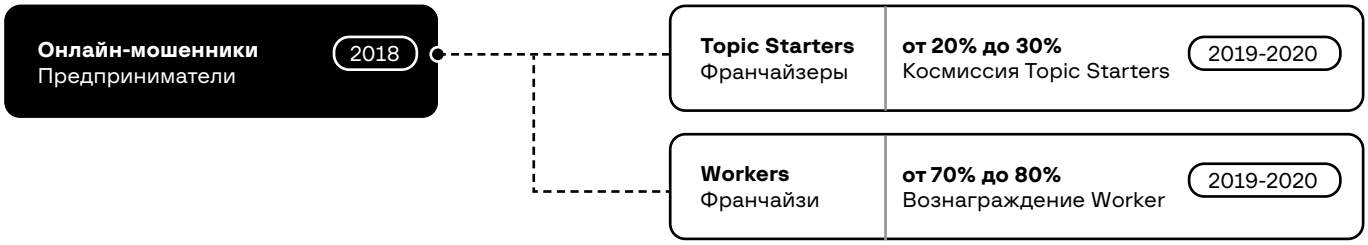
Таргетированное привлечение ①	**Персональная ссылка** ②	**Персональный контент** ③
2019	**2019**	**2019**
Нецелевой пользователь попадает на ресурс с легитимным контентом	Ссылка работает только один раз и только у одного конкретного пользователя	Контент сгенерирован под таргетированного пользователя
2020	**2020**	**2020**
Привлечение конкретных групп жертв, чтобы повысить конверсию	Сбор аналитических данных для реферальных программ	Автозаполнение формы с данными жертвы

Потенциальные жертвы теперь выбираются обдуманно, а когда они переходят по ссылке, происходит множество редиректов, где попутно собираются данные о пользователе, его провайдере, местоположении и IP-адресе, модели устройства и пользовательском агенте, подбирается наиболее подходящий вид мошенничества (язык, бренд, индустрия). В конце создается персонализированная ссылка, открывающаяся только у этого пользователя. Это позволяет мошенникам адаптировать контент к конкретной жертве и усложняет отслеживание начальной стадии схемы.

SaaS (Scam-as-a-Service)

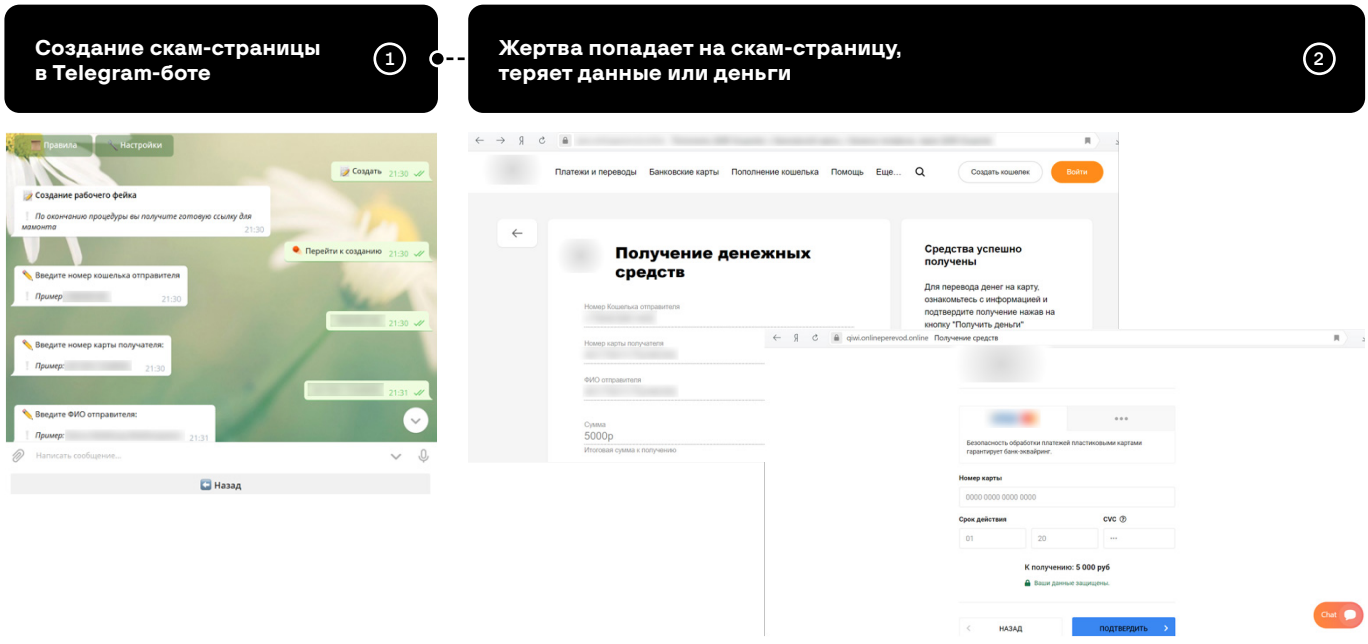
Второе важное изменение – разделение труда в мошеннических группировках. Чтобы иметь больший охват, злоумышленники, которые умели придумывать мошеннические схемы и создавали технологии для реализации схем, теперь сами не занимаются обманом пользователей и привлечением трафика на создаваемые ресурсы. Мы называем эту модель SaaS (Scam-as-a-Service) – в ней есть Topic Starters (создатели франшизы и технологий) и Workers (исполнители).

Схема SaaS ↓



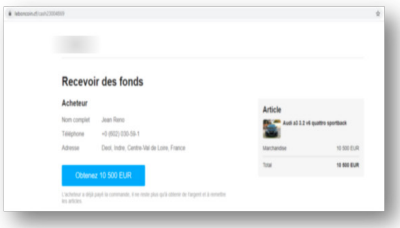
Это в корне меняет масштабы проблемы, так как обычным исполнителям, желающим подзаработать в интернете на обмане, теперь ничего не мешает – им не нужны идеи и специальные знания, за них все уже сделано – создание сайтов для обмана происходит автоматически, им нужно просто начать привлекать на них жертв и делать отчисления франчайзерам.

Последовательность SaaS ↓

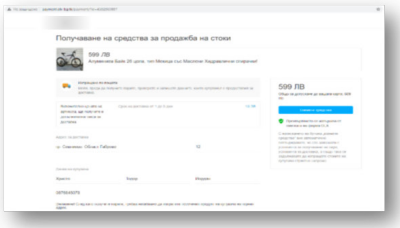


Данный подход также позволяет реализовать такие схемы на международном уровне. Создание типовых сайтов на разных языках автоматизировано, технологии можно использовать по всему миру, что существенно увеличивает заработок злоумышленников. Мы видим огромное количество типовых страниц мошеннических сайтов на разных языках для любых индустрий, которые были созданы автоматически с использованием одних и тех же технологий.

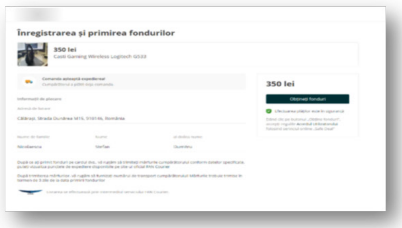
Разнообразие SaaS ↓



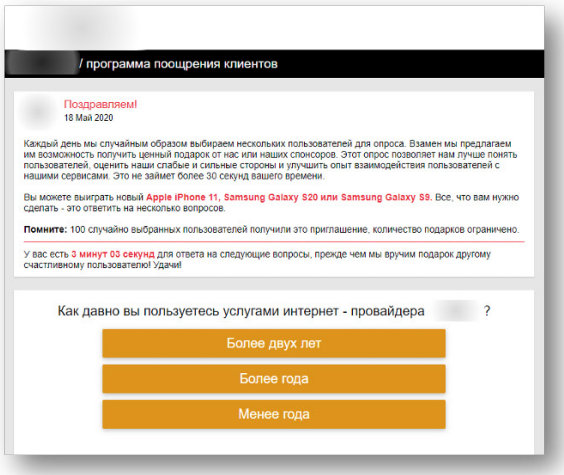
Франция

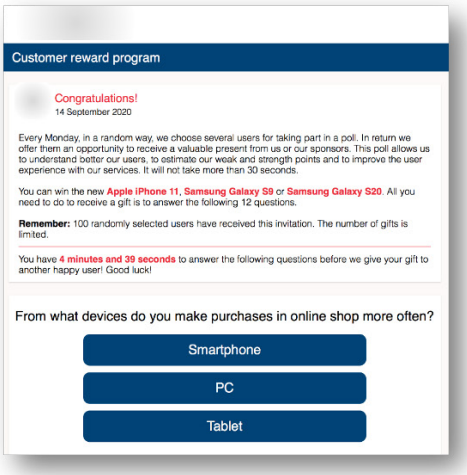


Болгария



Румыния





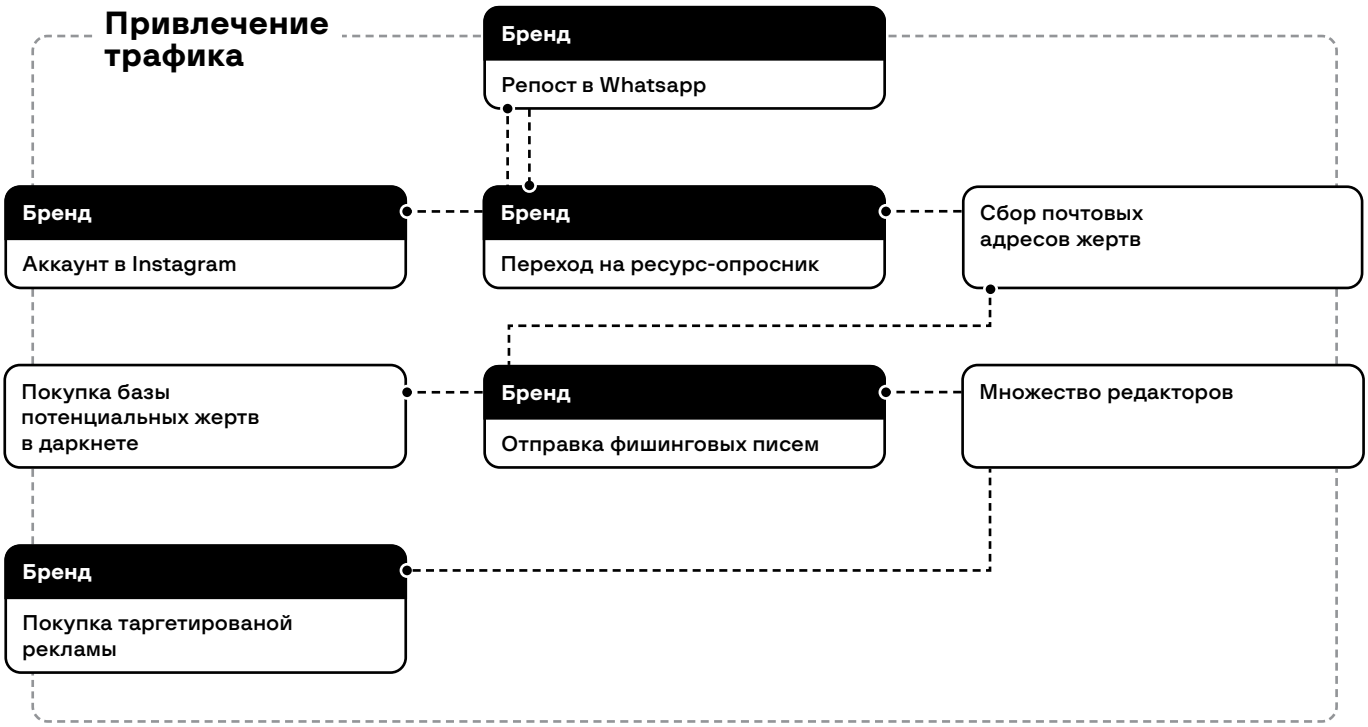
Подходы, схемы, атаки

Развитие многоступенчатого мошенничества

В 2019 году Group-IB обнаружила новую схему многоэтапного мошенничества, которую назвали «схема белого кролика» или «кроличья нора». Это эфемерная схема привлечения трафика, суть которой заключается именно в многоступенчатости, когда все начинается с безобидных маркетинговых касаний жертвы, а заканчивается настоящим мошенничеством. Жертва теряет бдительность из-за множественных взаимодействий, не приводящих ни к какому обману, а на финальной стадии все же решается довериться и теряет свои деньги или платежные данные.

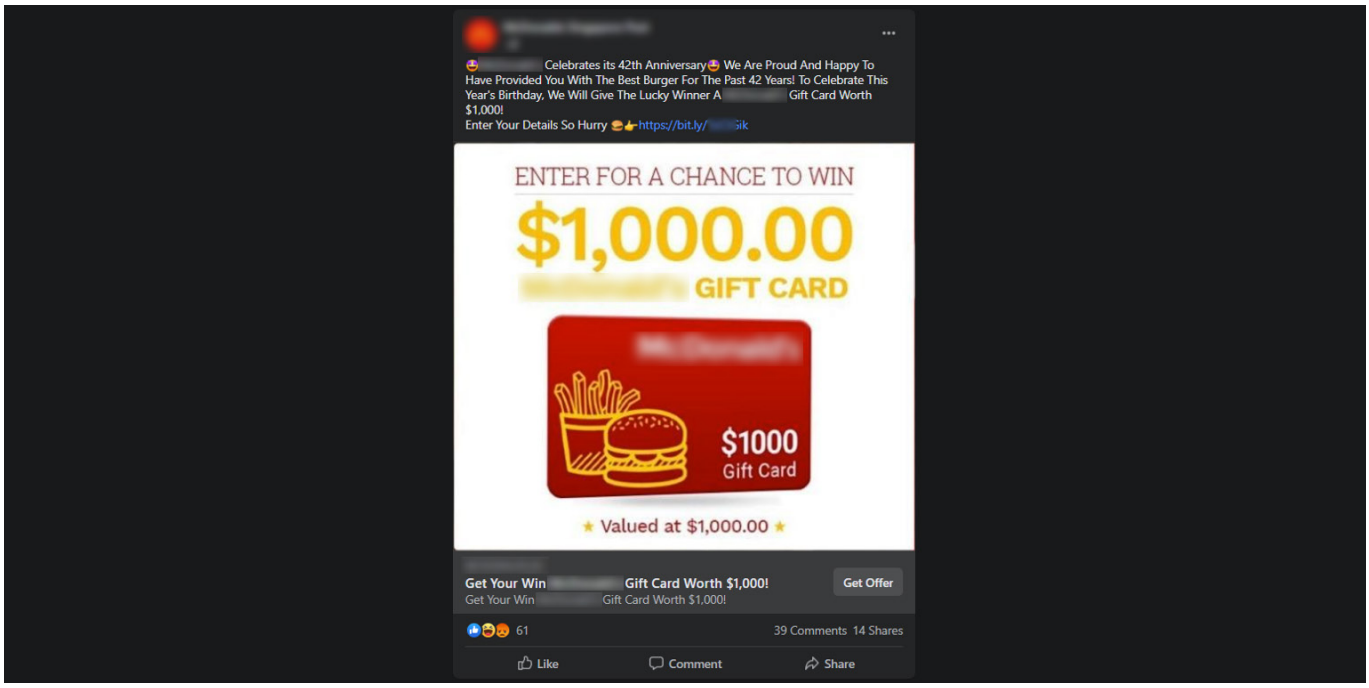
Команда DRP Group-IB разделила схему на две основные части: привлечение трафика – этап, на котором мошенники привлекают трафик через социальные сети, SMS или дорвеи, и атака, которая включает в себя кражу денег, личной информации или перехват платежных данных. Для традиционных автоматизированных систем обнаружения разные этапы схемы таргетированного многоступенчатого мошенничества выглядят как отдельные независимые нарушения, что не позволяет полностью искоренить этот вид мошенничества.

Привлечение трафика
в многоступенчатой таргетированной
мошеннической схеме ↓



На первом этапе мошенники обычно используют громкие имена в фейковой рекламе в качестве приманки. Они либо выдают себя за местных знаменитостей, предпринимателей, политиков, либо используют бренды крупных компаний в качестве приманки и объявляют раздачи, специальные предложения или опросы с крупными призами и дорогими подарками (например, подарочные карты, смартфоны, наушники, билеты), также часто используются глобальные и локальные инфоповоды.

Реклама на Facebook, запущенная
с поддельного аккаунта, эксплуатирующего бренд McDonald's ↓



Примечательно, что как только пользователь реагирует на наживку, в данном случае фальшивую рекламу в социальных сетях с логотипом известного бренда, и переходит по ссылке, то он попадает, например, на опрос, где его просят ответить на ряд простых вопросов и иногда поделиться удачей с друзьями через мессенджеры или социальные сети. Таким образом, мошенники обеспечивают вирусное распространение схемы и увеличивают трафик на свои ресурсы. В то же время жертве предлагается ввести свой телефон или адрес электронной почты, который впоследствии может быть использован для фишинговых рассылок или заражения вредоносным ПО. Но на данной стадии пользователь еще не потерял деньги, он еще доверяет этой промо-акции.

Пример атаки в многоступенчатой таргетированной мошеннической схеме ↓

После того, как эти подготовительные шаги будут завершены, мошенники переходят к следующему этапу.

Все жертвы, клюнувшие на наживку на первом этапе, получают электронные письма или личные сообщения, в которых им предлагают забрать выигрыш или товар, их приглашают принять участие в новом опросе или викторине со «значительным денежным вознаграждением».

Ключевой частью схемы является то, что пользователей просят перевести определенную сумму в качестве сбора или налога или произвести тестовый платеж в конце опроса. Жертвы, конечно, не получают вознаграждения, а вместо этого теряют свои деньги, платежные данные или все вместе.

Опасность схемы многоступенчатого таргетированного мошенничества заключается в том, что страдают не только частные лица. Крупные бренды и знаменитости, чьи имена используются мошенниками, несут репутационный ущерб. По данным исследователей рынка, почти 64% пользователей, столкнувшихся со злоупотреблением торговой маркой в интернете, никогда не вернутся к ней – их доверие к ней было подорвано.

2019

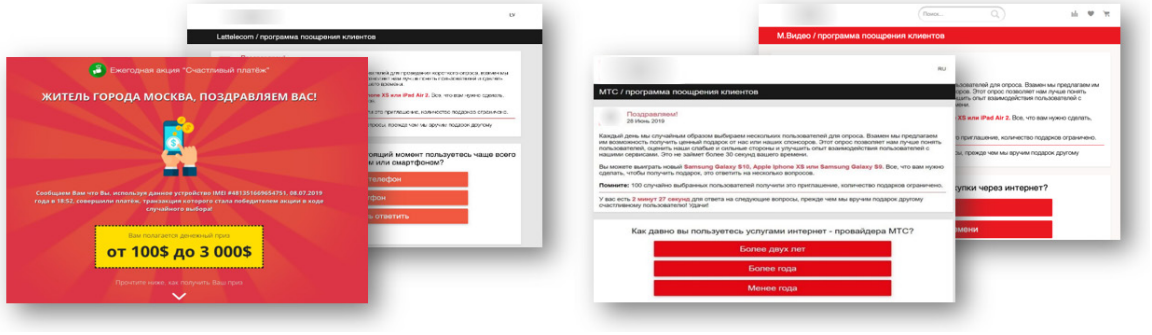
7,000 активных переходов

незначительное использование известных брендов

2020

40,000 активных переходов

активное использование известных брендов



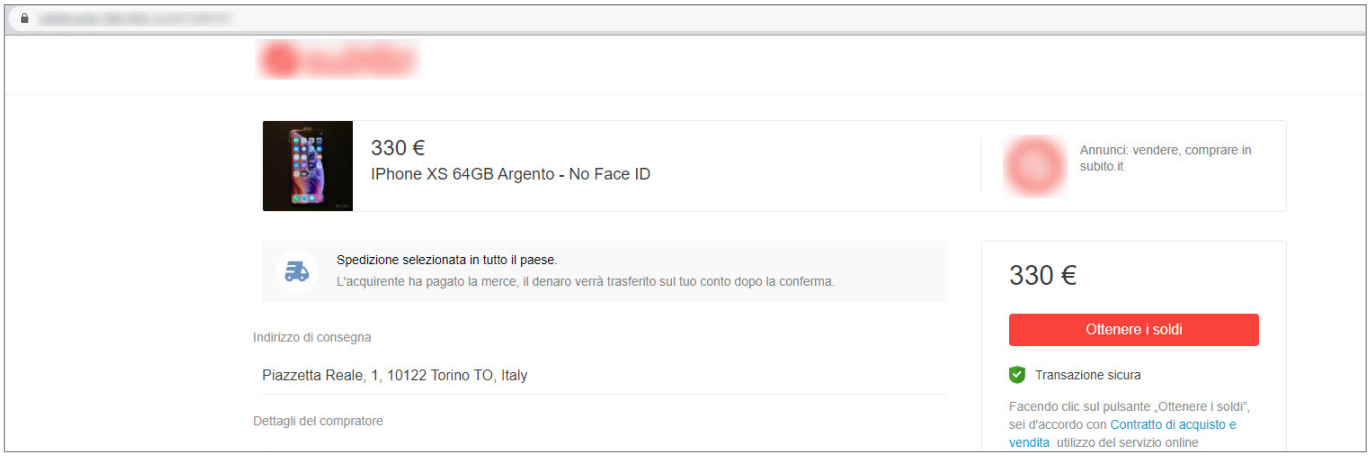
По данным Group-IB, на сегодняшний день в схеме многоступенчатого таргетированного мошенничества используются более 1000 брендов со всего мира.

Развитие схемы Classiscam

Режим карантина, введенный для борьбы с распространением COVID-19, по разным оценкам, увеличил спрос на услуги курьерской доставки на 30%– 40%. Покупатели все чаще заказывают товары в интернете, стараясь не выходить из дома и при этом экономить. Этим решили воспользоваться злоумышленники, активировав мошенническую схему с поддельным сервисом курьерской доставки.

На популярных сервисах бесплатных объявлений злоумышленники размещают так называемые лоты-приманки – объявления о продаже по заниженным ценам товаров, рассчитанных на разные целевые аудитории – фотоаппараты, игровые приставки, ноутбуки, смартфоны, бензопилы, звуковые системы для авто, швейные машинки, коллекционные вещи, товары для рыбалки, спортпит и другие. Сервисы борются с подобными типами мошенничества, однако лжепродавцы постоянно создают способы обхода блокировок своих сообщений.

Пример поддельной страницы по оформлению доставки, эксплуатирующей бренд сервиса бесплатных объявлений ↓



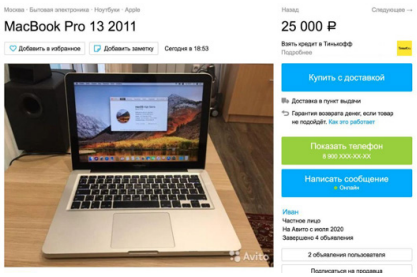
Покупатель, заинтересовавшись выгодным предложением, связывается с продавцом во внутреннем чате сервиса. «Продавец» предлагает продолжить обсуждение покупки и доставки товара в одном из популярных мессенджеров якобы для удобства клиента. На самом деле, мошенник умышленно уводит покупателя на стороннюю площадку, чтобы служба безопасности сервиса не могла его отследить и помешать «сделке».

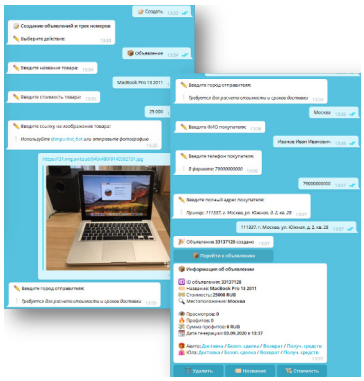
Заманив жертву в чат мессенджера, злоумышленники запрашивают у нее контактные данные (ФИО, адрес и номер телефона) для оформления доставки через курьерскую службу. Затем жертве присылают ссылку на один из сайтов популярных курьерских служб. На деле сайт оказывается фишинговой страницей, полностью копирующей дизайн курьерского или почтового бренда и использующей доменное имя, похожее на оригинальное. Естественно, подлинные сервисы доставки не имеют к этим сайтам никакого отношения.

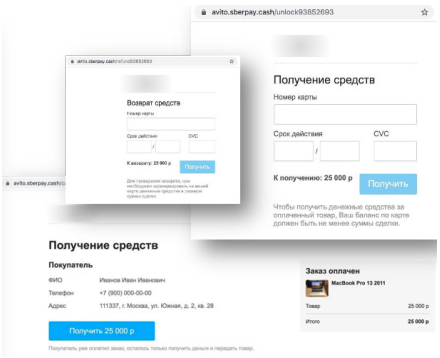
Здесь, на фейковой странице заказа, злоумышленник сам заполняет форму для отправки посылки, используя полученные от покупателя данные. Жертве предлагается проверить корректность информации и совершить оплату товара, введя данные своей банковской карты. Цель мошенника достигнута: покупатель теряет и деньги, и данные карты, при этом оставаясь без товара. Средний чек одной такой «покупки» составляет примерно 120 долларов.

Пример применения мошеннической схемы на сервисах бесплатных объявлений ↓

Подбор жертвы ① — **Создание скам-страницы в Telegram-боте** ② — **Жертва попадает на скам-страницу и теряет данные** ③







Зачастую на этом мошенники не останавливаются. Часть жертв обманывают повторно – «разводят на возврат». Через некоторое время после оплаты товара покупателю сообщают, что на почте произошло ЧП. Легенда может быть любой, например, сотрудник почты пойман на краже, а заказанный товар конфисковала полиция, поэтому для компенсации перечисленной суммы необходимо оформить возврат средств. Понятно, что на деле с карты происходит повторное списание той же суммы.

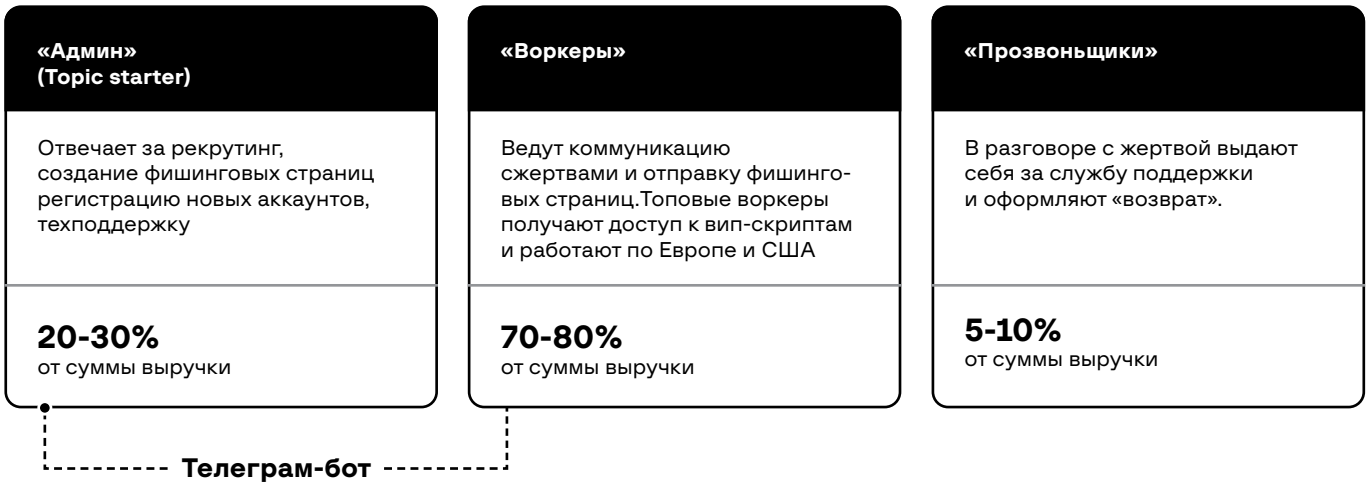
Одной из главных причин популярности причины этой схемы является автоматическое управление и расширение с помощью специальных чат-ботов Telegram. К концу 2020 года в 40 самых популярных чатах Telegram было зарегистрировано более 5000 пользователей (мошенников).

В настоящее время достаточно отправить ссылку с продуктом-приманкой в чат-бот, который затем генерирует полный набор для фишинга, включая URL-адрес курьера, оплату и возврат. Существует множество типов ботов Telegram, которые создают поддельные страницы брендов не менее 44 стран. Для каждого бренда и страны мошенники пишут сценарии, которые помогают новичкам заходить на зарубежные сайты и общаться с жертвами на местном языке.

У чат-ботов также есть магазины, где вы можете приобрести учетные записи на различных торговых площадках, электронные кошельки, целевые рассылки и руководства или даже нанять юриста, который будет представлять вас в суде.

Вся информация о совершаемых сделках, включая сумму, номер платежа и имя пользователя, отображается в боте Telegram. Вот так эксперты Group-IB смогли рассчитать предполагаемый месячный улов.

Пирамида мошенничества. Распределение ролей в типичной преступной группе ↓



Развитие способов привлечения трафика

Злоумышленники используют весь функционал интернет-сети в продвижении своих мошеннических схем. Помимо самостоятельного привлечения трафика, в некоторых случаях они прибегают к услугам черных арбитражников – вебмастеров, которые приводят пользователей на заведомо мошеннические ресурсы.

Особенность комбинированного привлечения трафика в схеме многоступенчатого таргетированного мошенничества позволяет многократно увеличить число потенциальных жертв.

Редиректы

Данный вид привлечения трафика обычно используется в элементах взаимодействия – ссылках на мошеннических сайтах, после нажатия на которые происходит перенаправление на сторонние интернет-ресурсы. Особенностью таких редиректов является множество перенаправлений, которые в случае блокировки мошеннического сайта позволяют открыть пользователю действующий мошеннический сайт.

Особенности привлечения трафика

Большинство мошеннических схем используют вышеописанный способ привлечения трафика, однако в некоторых схемах используют особенные методы. Так, в мошеннической схеме Classiscam злоумышленники создают объявления по продаже товара или услуги на официальных интернет-сервисах. Мошенник якобы хочет приобрести товар или услугу, и взаимодействие с жертвой происходит на самой интернет-площадке, либо через мессенджеры.

Use-cases (по регионам, индустриям и угрозам)

MEA

	Фишинг ①	Скам ②	Контрафакт ③	Пиратство ④	Ложное партнерство ⑤	Мобильные приложения ⑥	Реклама ⑦	Товарные знаки ⑧	Утечки ⑨	VIP-персоны ⑩	Теневые форумы ⑪
Финансы и страхование	+	+			+	+	+	+	+	+	+
Производство	+	+	+			+	+	+		+	
Нефтегазовая промышленность		+			+	+		+	+	+	
Ритейл и E-commerce	+	+			+	+	+	+		+	+
Телекоммуникации и медиа	+	+		+	+	+	+	+		+	+
Здравоохранение			+			+		+		+	
Транспорт и логистика	+	+				+		+		+	
Государственный сектор		+				+	+	+	+		+
Информационные технологии		+			+	+	+	+	+		+
Образование						+	+	+			+

APAC

Финансы и страхование	+	+				+	+	+	+		+
Производство			+			+		+		+	
Oil and gas		+						+			
Ритейл и E-commerce	+	+			+	+	+	+	+	+	+
Телекоммуникации и медиа	+	+		+		+	+	+			
Здравоохранение		+				+	+	+	+		+
Транспорт и логистика		+					+	+			
Государственный сектор	+	+			+	+		+	+	+	
Информационные технологии	+					+	+	+		+	
Образование		+									

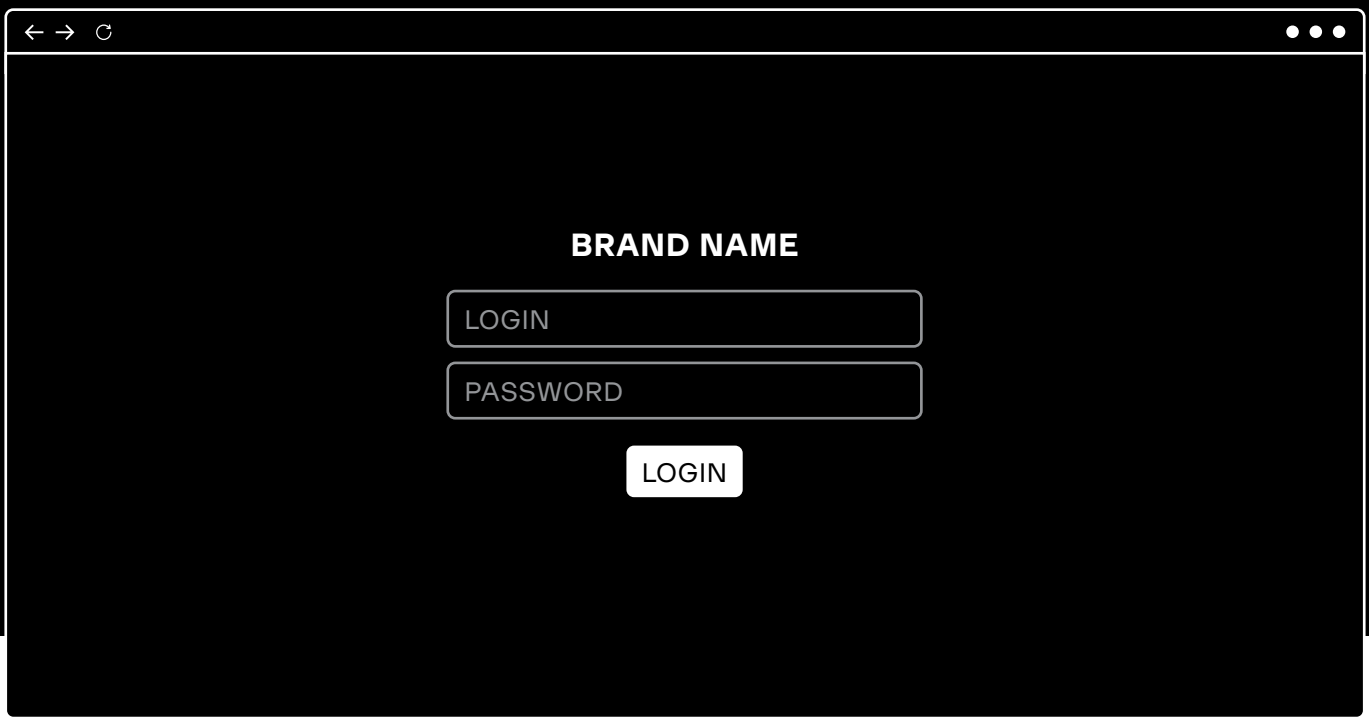
EU

Финансы и страхование	+	+			+	+	+	+	+	+	+
Производство	+	+	+		+	+		+		+	
Нефтегазовая промышленность	+	+			+	+		+	+	+	
Ритейл и E-commerce	+	+			+	+	+	+		+	+
Телекоммуникации и медиа	+	+		+	+	+		+	+	+	+
Здравоохранение	+	+				+	+	+	+	+	+
Транспорт и логистика	+	+				+	+	+	+	+	+
Государственный сектор	+	+				+	+	+	+	+	+
Информационные технологии	+	+				+		+	+	+	
Образование		+				+		+		+	

CIS

Финансы и страхование	+	+			+	+	+	+	+	+	+
Производство		+	+		+	+	+	+			
Нефтегазовая промышленность	+	+			+	+	+	+		+	+
Ритейл и E-commerce		+			+	+	+	+		+	+
Телекоммуникации и медиа	+	+		+		+		+	+		
Здравоохранение					+	+		+			+
Транспорт и логистика	+	+			+	+	+	+			+
Государственный сектор	+	+			+	+	+	+	+	+	+
Информационные технологии	+	+				+		+	+		
Образование		+				+		+			

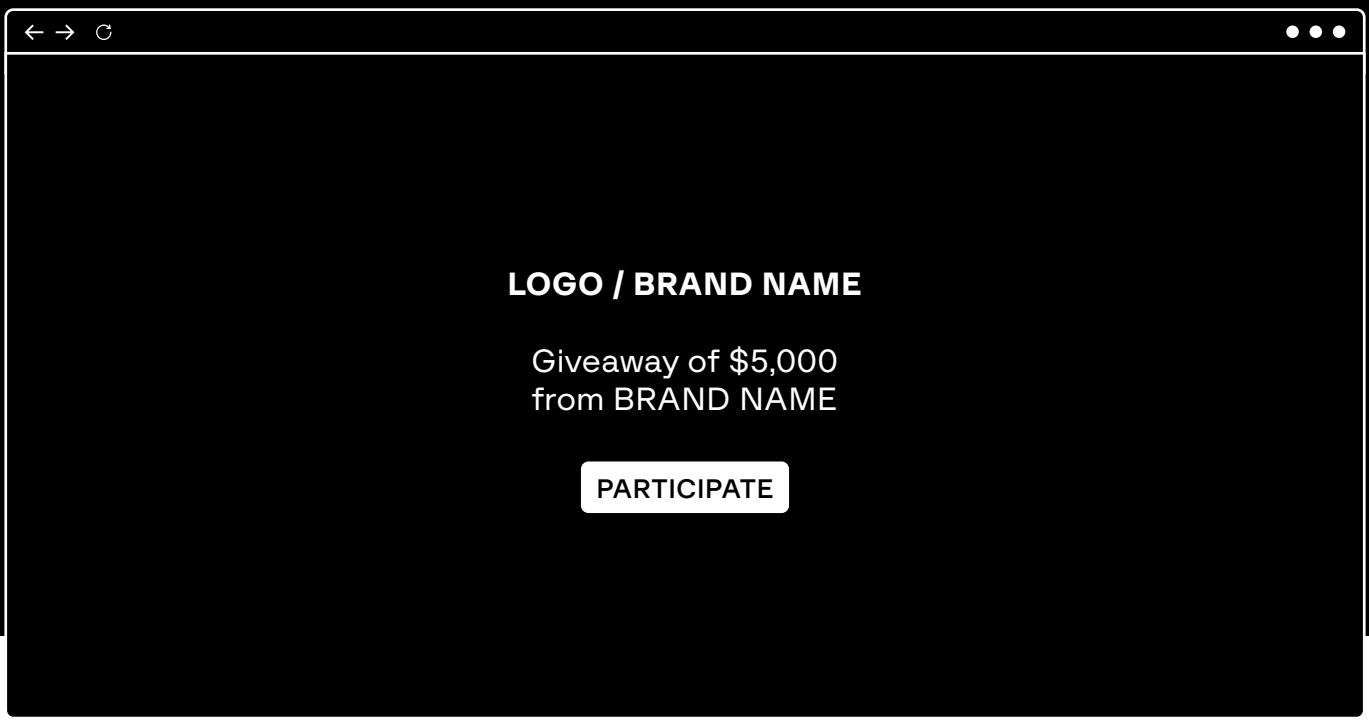
Фишинг



Страницы-клоны, крадущие данные вашей карты, логины, пароли, для получения доступа ко всем деньгам или данным.

Затронутые индустрии	MEA	APAC	EU	CIS
Финансы и страхование	⊕	⊕	⊕	⊕
Производство	⊕		⊕	
Нефтегазовая промышленность			⊕	⊕
Ритейл и E-commerce	⊕	⊕	⊕	
Телекоммуникации и медиа	⊕	⊕	⊕	⊕
Здравоохранение			⊕	
Транспорт и логистика	⊕		⊕	⊕
Государственный сектор		⊕	⊕	⊕
Информационные технологии		⊕	⊕	⊕
Образование				

Скам



Злоумышленники эксплуатируют бренды промышленных компаний для оказания мошеннических услуг. Подобные сайты создаются с целью хищения у интернет-пользователей конфиденциальных данных и денежных средств.

Затронутые индустрии	**MEA**	**APAC**	**EU**	**CIS**
Финансы и страхование	⊕	⊕	⊕	⊕
Производство	⊕		⊕	⊕
Нефтегазовая промышленность	⊕	⊕	⊕	⊕
Ритейл и E-commerce	⊕	⊕	⊕	⊕
Телекоммуникации и медиа	⊕	⊕	⊕	⊕
Здравоохранение		⊕	⊕	
Транспорт и логистика	⊕	⊕	⊕	⊕
Государственный сектор	⊕	⊕	⊕	⊕
Информационные технологии	⊕		⊕	⊕
Образование		⊕	⊕	⊕

Конрафакт

Мошенники используют интернет ресурсы для реализации продажи контрафактной продукции под брендом компании.

Затронутые индустрии	**MEA**	**APAC**	**EU**	**CIS**
Финансы и страхование				
Производство	⊕	⊕	⊕	⊕
Нефтегазовая промышленность				
Ритейл и E-commerce				
Телекоммуникации и медиа				
Здравоохранение	⊕			
Транспорт и логистика				
Государственный сектор				
Информационные технологии				
Образование				

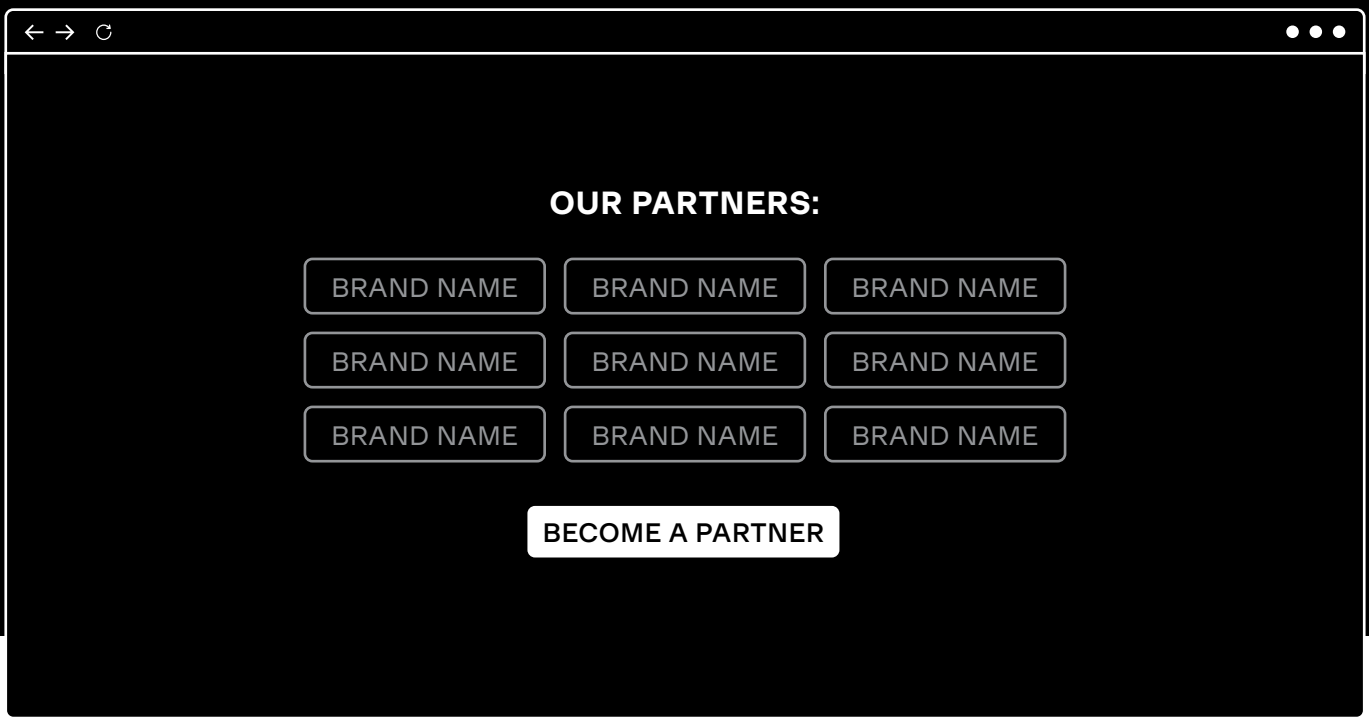
Пиратство

Незаконная трансляция контента, нарушающего авторское право бренда компании.

Затронутые индустрии	MEA	APAC	EU	CIS
Финансы и страхование				
Производство				
Нефтегазовая промышленность				
Ритейл и E-commerce				
Телекоммуникации и медиа	⊕	⊕	⊕	⊕
Здравоохранение				
Транспорт и логистика				
Государственный сектор				
Информационные технологии				
Образование				

Ложное партнерство

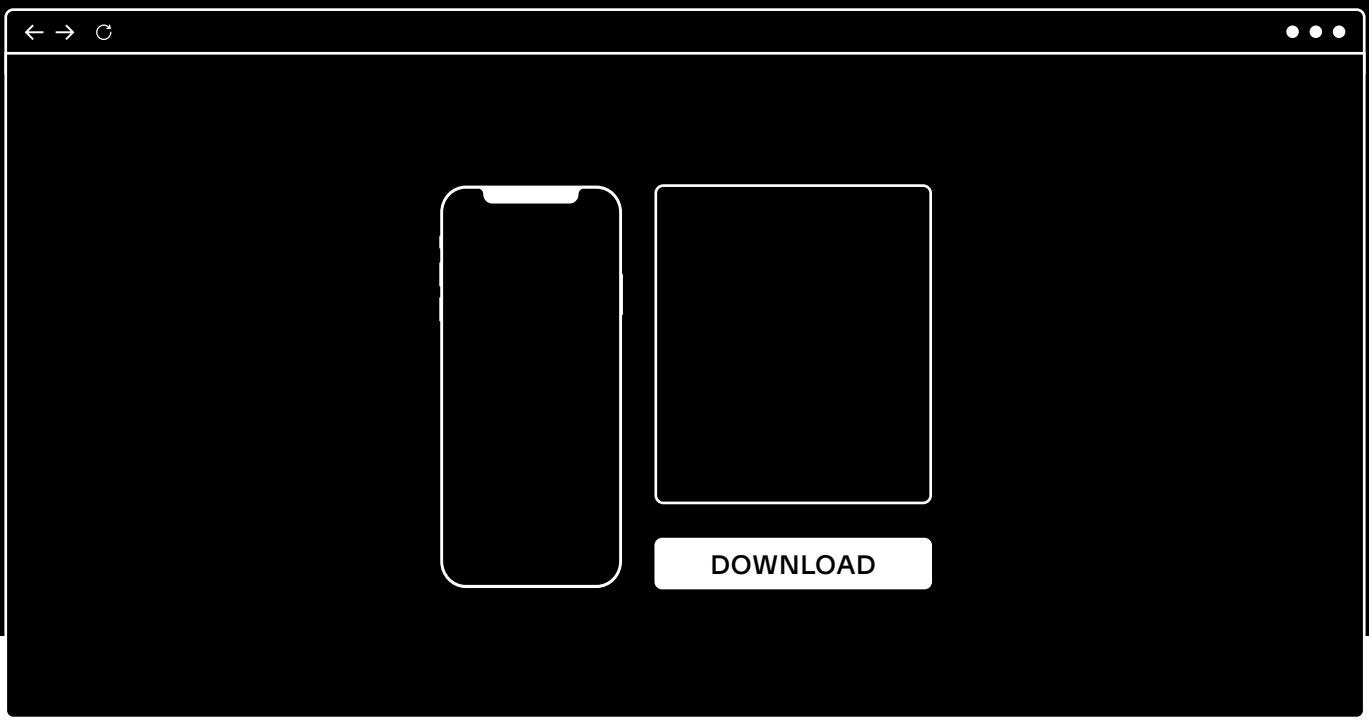
5 ↗



Мошенники используют бренд компаний в качестве своих партнеров, чтобы получить от пользователя дополнительное доверие и продать более выгодно свою продукцию или услуги.

Затронутые индустрии	**MEA**	**APAC**	**EU**	**CIS**
Финансы и страхование	⊕		⊕	⊕
Производство			⊕	⊕
Нефтегазовая промышленность	⊕		⊕	⊕
Ритейл и E-commerce	⊕	⊕	⊕	⊕
Телекоммуникации и медиа	⊕		⊕	
Здравоохранение				⊕
Транспорт и логистика				⊕
Государственный сектор		⊕		⊕
Информационные технологии	⊕			
Образование				

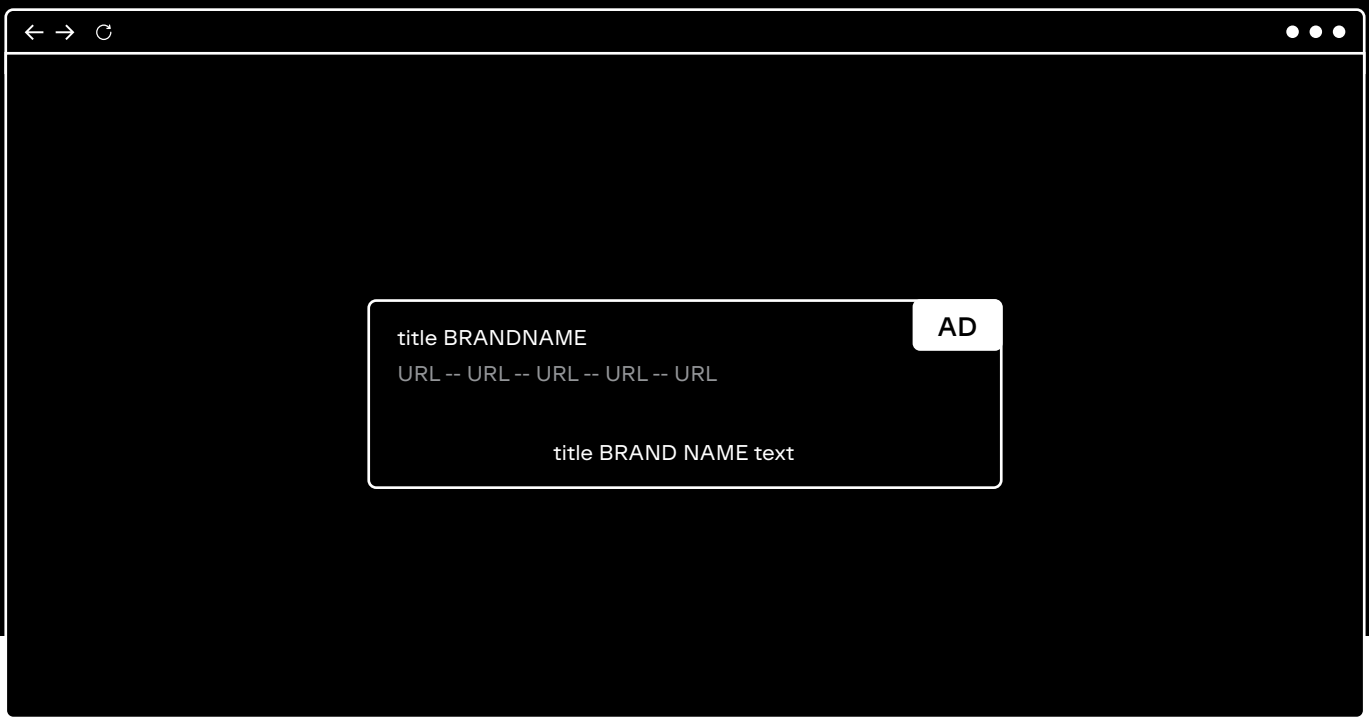
Неавторизованные мобильные приложения



Распространение неавторизованных приложений под брендом компании в официальных и неофициальных магазинах программного обеспечения, которые могут содержать вредоносный код или фишинговую форму.

Затронутые индустрии	**MEA**	**APAC**	**EU**	**CIS**
Финансы и страхование	⊕	⊕	⊕	⊕
Производство	⊕	⊕	⊕	⊕
Нефтегазовая промышленность	⊕		⊕	⊕
Ритейл и E-commerce	⊕	⊕	⊕	⊕
Телекоммуникации и медиа	⊕	⊕	⊕	⊕
Здравоохранение	⊕	⊕	⊕	⊕
Транспорт и логистика	⊕		⊕	⊕
Государственный сектор	⊕	⊕	⊕	⊕
Информационные технологии	⊕	⊕	⊕	⊕
Образование	⊕		⊕	⊕

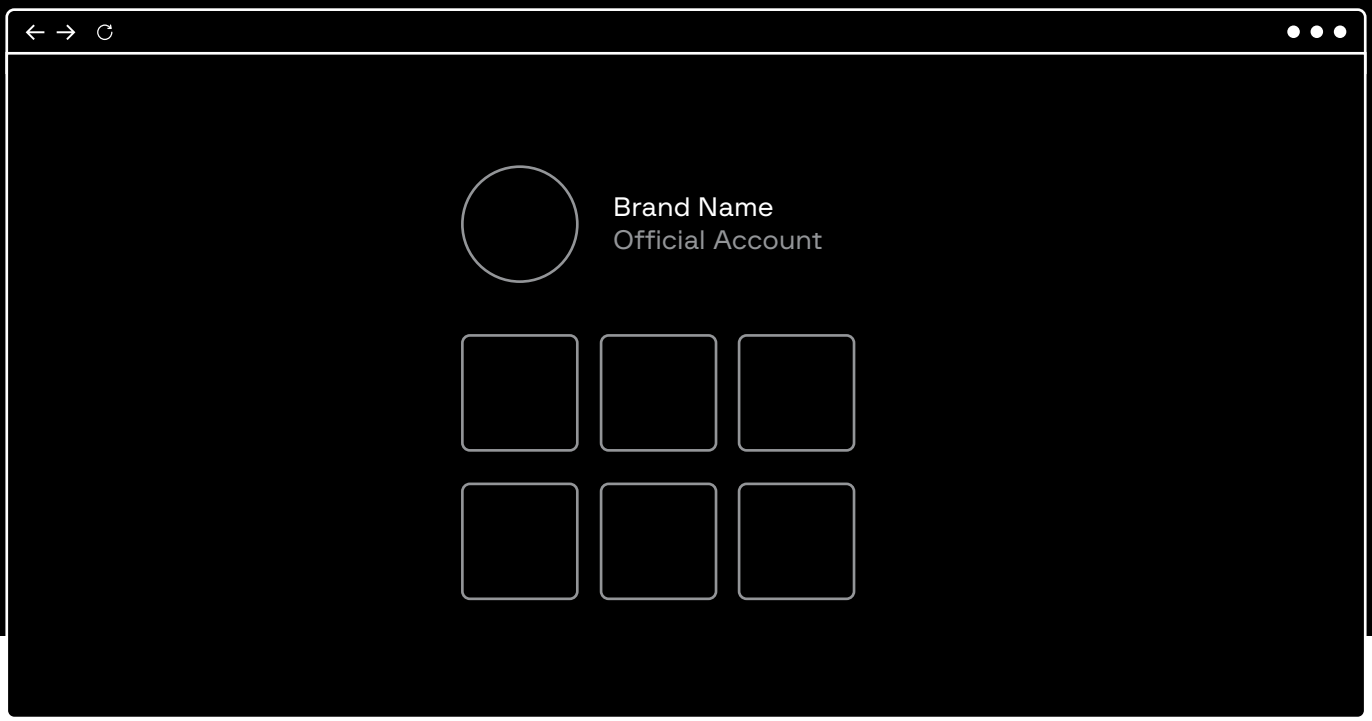
Неавторизованная реклама



Мошенники используют рекламные объявления с упоминанием бренда компании для привлечения трафика на сторонние мошеннические ресурсы.

Затронутые индустрии	MEA	APAC	EU	CIS
Финансы и страхование	⊕	⊕	⊕	⊕
Производство	⊕			⊕
Нефтегазовая промышленность				⊕
Ритейл и E-commerce	⊕	⊕	⊕	⊕
Телекоммуникации и медиа	⊕	⊕		
Здравоохранение		⊕	⊕	
Транспорт и логистика		⊕	⊕	⊕
Государственный сектор	⊕		⊕	⊕
Информационные технологии	⊕	⊕		
Образование	⊕			

Несогласованное использование товарного знака



Злоумышленники используют товарные знаки бренда компании с целью мошеннических финансовых операций или привлечения трафика на сторонние мошеннические ресурсы.

Затронутые индустрии	**MEA**	**APAC**	**EU**	**CIS**
Финансы и страхование	⊕	⊕	⊕	⊕
Производство	⊕	⊕	⊕	⊕
Нефтегазовая промышленность	⊕	⊕	⊕	⊕
Ритейл и E-commerce	⊕	⊕	⊕	⊕
Телекоммуникации и медиа	⊕	⊕	⊕	⊕
Здравоохранение	⊕	⊕	⊕	⊕
Транспорт и логистика	⊕	⊕	⊕	⊕
Государственный сектор	⊕	⊕	⊕	⊕
Информационные технологии	⊕	⊕	⊕	⊕
Образование	⊕		⊕	⊕

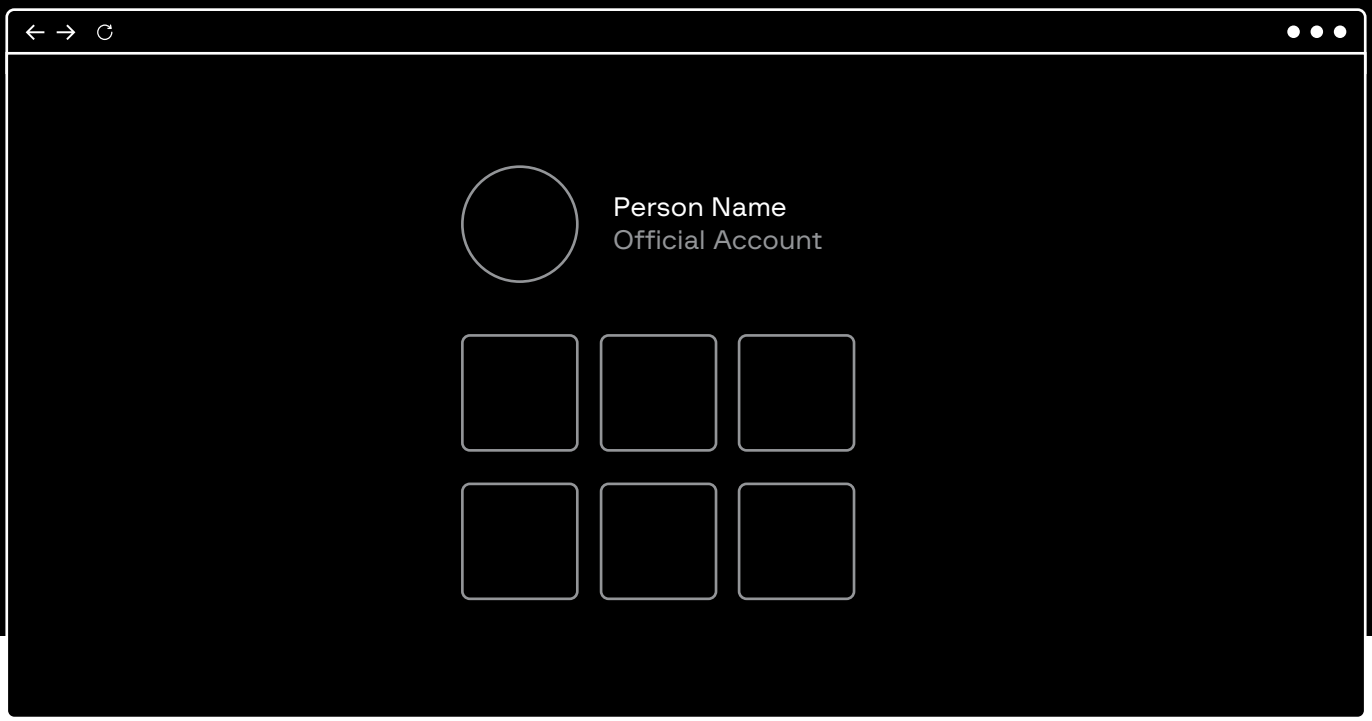
Утечка информации

9 ↗

Злоумышленники, завладевшие персональными данными, могут использовать их в преступных целях, например, с целью шантажа, продажи, взлома учетных записей сотрудников или финансовых махинаций.

Затронутые индустрии	**MEA**	**APAC**	**EU**	**CIS**
Финансы и страхование	⊕	⊕	⊕	⊕
Производство				
Нефтегазовая промышленность	⊕		⊕	
Ритейл и E-commerce		⊕		
Телекоммуникации и медиа			⊕	⊕
Здравоохранение		⊕	⊕	
Транспорт и логистика			⊕	
Государственный сектор	⊕	⊕	⊕	⊕
Информационные технологии	⊕		⊕	⊕
Образование				

Использование личностей VIP-персон



Фейковые аккаунты представителей бренда компании используются для вымогания денежных средств и конфиденциальных данных.

Затронутые индустрии	MEA	APAC	EU	CIS
Финансы и страхование	⊕		⊕	⊕
Производство	⊕	⊕	⊕	
Нефтегазовая промышленность	⊕		⊕	⊕
Ритейл и E-commerce	⊕	⊕	⊕	⊕
Телекоммуникации и медиа	⊕		⊕	
Здравоохранение	⊕		⊕	
Транспорт и логистика	⊕		⊕	
Государственный сектор		⊕	⊕	⊕
Информационные технологии		⊕	⊕	
Образование			⊕	

Обсуждение вашей компании в дарквебе

В дарквебе злоумышленники могут обсуждать бренд и представителей компании с целью продажи конфиденциальной информации и осуществления иной незаконной деятельности, направленной против бренда компании.

Затронутые индустрии	**MEA**	**APAC**	**EU**	**CIS**
Финансы и страхование	⊕	⊕	⊕	⊕
Производство				
Нефтегазовая промышленность				⊕
Ритейл и E-commerce	⊕	⊕	⊕	⊕
Телекоммуникации и медиа	⊕		⊕	
Здравоохранение		⊕	⊕	⊕
Транспорт и логистика			⊕	⊕
Государственный сектор	⊕		⊕	⊕
Информационные технологии	⊕			
Образование	⊕			

Команда технических и юридических экспертов Group-IB обладает более чем 11-летним опытом защиты брендов и другой интеллектуальной собственности. При подготовке данного отчета мы проанализировали более 100 мошеннических схем и их модификаций в разных странах для компаний из разных отраслей. Посмотреть больше кейсов по отдельным регионам, индустриям и угрозам вы можете на отдельной web-странице перейдя по одной из ссылок или отсканировав QR-код:

MEA

Use-cases арабского региона

APAC

Use-cases азиатского региона

EU

Use-cases европейского региона

CIS

Use-cases региона СНГ

Group-IB — один из ведущих разработчиков решений для детектирования и предотвращения кибератак, выявления мошенничества, расследования высокотехнологичных преступлений и защиты коммерческой и интеллектуальной собственности в сети.

INTERPOL И EUROPOL

Group-IB — партнер и участник совместных расследований

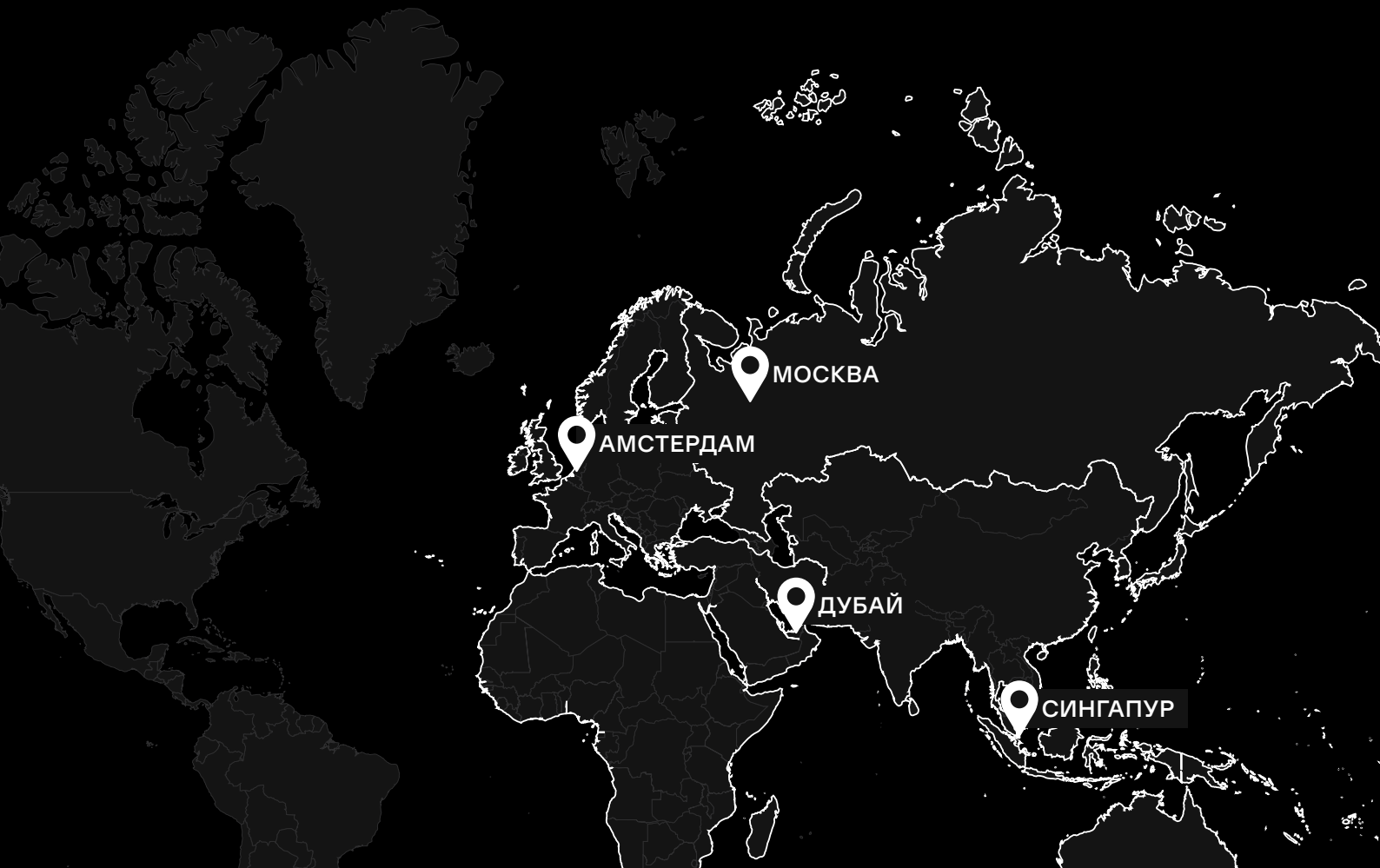
ТОП-10 В APAC

Group-IB вошла в топ-10 компаний по кибербезопасности в регионе APAC согласно APAC CIO Outlook

Центры исследования киберугроз Group-IB

- Европа
- Россия
- Ближний восток
- Азиатско-Тихоокеанский регион

- Распределенная по миру инфраструктура наблюдения за киберпреступностью
- Лаборатории компьютерной криминалистики
- Расследования киберпреступлений
- Круглосуточные центры мониторинга и оперативного реагирования CERT-GIB



Решения Group-IB

Опыт Group-IB в международных расследованиях, киберразведке и выявлении преступлений на разных уровнях подготовки был интегрирован в экосистему решений, объединившую чрезвычайно сложное программное и системное обеспечение, с целью мониторинга, обнаружения и предотвращения кибератак и мошенничества. Миссия Group-IB — защищать наших клиентов в киберпространстве, создавая и используя инновационные продукты и решения.

Решения Group-IB признаны мировыми агентствами в категориях:

— Innovation Excellence,
— Product Leader,
— Innovation Leader.

IDC
Gartner
FORRESTER
kuppingercole ANALYSTS
FROST & SULLIVAN

GARTNER IDC FROST & SULLIVAN FORRESTER

Threat Intelligence & Attribution

Система исследования и атрибуции кибератак, охоты за угрозами и защиты сетевой инфраструктуры на основании данных о тактиках, инструментах и активности злоумышленников

KUPPINGERCOLE ANALYSTS AG

Threat Hunting Framework

Реактивная защита и проактивная охота за угрозами внутри и за пределами вашей сети

FROST & SULLIVAN

Digital Risk Protection

Выявление и устранение цифровых рисков на основе искусственного интеллекта

KUPPINGERCOLE ANALYSTS AG FORRESTER GARTNER

Fraud Hunting Platform

Выявление и предотвращение мошенничества и бот-активности в режиме реального времени

NEW

Atmosphere: Cloud Email Protection

Облачная защита электронной почты от целевых атак, детонация полезных нагрузок и атрибуция угроз

550+	70 000+	1 300+	18 лет
экспертов международного класса	часов реагирования на инциденты информационной безопасности	успешных расследований по всему миру	практического опыта

Intelligence-driven services

FORRESTER
GARTNER

В основе технологического лидерства компании и возможностей в сфере научных исследований и разработки — 18-летний практический опыт расследования киберпреступлений по всему миру и более 70 000 часов реагирования на инциденты информационной безопасности, аккумулированные в распределенной по миру инфраструктуре наблюдения за киберпреступностью.

РАССЛЕДОВАНИЯ И КРИМИНАЛИСТИКА

Компьютерная криминалистика.
Анализ вредоносного кода.
Расследования:

- сложных высокотехнологичных преступлений;
- утечек информации;
- финансовых, корпоративных киберпреступлений;
- сложных атак на объекты КИИ и другие.

АУДИТ И ОЦЕНКА РИСКОВ

Тестирование на проникновение.
Анализ исходного кода.
Выявление следов компрометации сети.
Киберобучение в формате Red Teaming.
Проверка готовности к реагированию на инциденты.
Оценка соответствия.

THREAT HUNTING И РЕАГИРОВАНИЕ

24/7 Центр реагирования CERT–GIB.
Проактивный хантинг угроз.
Выездное реагирование на сложные кибератаки.
Реагирование на инциденты по подписке.

ОБУЧАЮЩИЕ ПРОГРАММЫ

Курсы для технических специалистов:

- Реагирование на инциденты,
- Анализ вредоносного кода,
- Проактивный поиск угроз и другие.

Программы для широкой аудитории:

- Цифровая гигиена,
- Личная кибербезопасность,
- Управление репутацией в интернете и другие.

Мастер-классы для школьников и студентов.