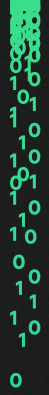
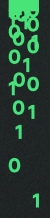
Аналитический
отчет «Лаборатории
Касперского»

Значимые утечки данных в 2022





kaspersky АКТИВИРУЙ БУДУЩЕЕ

Содержание

Ключевые результаты 3

Введение 4

Когда происходили утечки? 6

Сколько данных утекло? 8

Профиль жертвы 10

Каналы распространения 14

Реакция бизнеса 16

Что делать в случае утечки данных? 18

Налаживаем коммуникации 21

Рекомендации 23

Наши решения 24

Ключевые результаты

Общие сведения о значимых[1] утечках данных в российских компаниях в 2022 году:

168

фактов утечек данных

2 126 095 255 строк данных

290 933 531 пользовательских данных

47 663 767 записей с паролями

28% компаний

открыто прокомментировали факт утечки данных

64% пользовательских данных

были скомпрометированы в результате атак на крупный бизнес

Ритейл — лидер по количеству утечек (26%)

Доставка и Ритейл — лидеры по объему утечек пользовательских данных (34% и 14%)

СМИ — основной канал коммуникаций компаний по освещению факта утечки данных (75%)

Прогноз на 2023 год

На 20% увеличится количество утечек пользовательских данных

На 10% увеличится объем скомпрометированных пользовательских данных

Основной удар злоумышленников также будет направлен на сферу ритейла

[1] Значимая утечка данных — утечка данных, в результате которой было скомпрометировано более 5 тысяч строк пользовательских данных или которая получила резонанс в СМИ.

Введение

Аналитический отчет содержит информацию о значимых утечках данных в российских компаниях, публикация которых произошла в 2022 году. Команда Kaspersky Digital Footprint Intelligence на протяжении всего года отслеживала факты компрометации пользовательских данных, происходящие чуть ли не на ежедневной основе, предоставляя клиентам возможность в числе первых узнавать о произошедших инцидентах и оперативно реагировать на них.

Полученная аналитика представляет собой набор статистических показателей, на основании которых мы можем отследить изменения, произошедшие в течение года, и ответить на вопросы:

Как часто атаки на российские компании приводили к утечкам данных?

Сколько пользовательских данных было скомпрометировано?

Какие отрасли в первую очередь попали под удар злоумышленников?

Где публиковались утечки?

Как бизнес реагировал на утечки?

Что такое утечка данных?

Утечка данных – инцидент информационной безопасности, при котором конфиденциальная информация становится доступной для посторонних лиц. в контексте данного отчета под конфиденциальной информацией рассматриваются данные пользователей и сотрудников российских организаций, оказавшиеся в свободном доступе в интернете.

Стандартный набор скомпрометированных данных

ФИО

Адрес электронной почты

Номер мобильного телефона

Какие еще данные можно встретить в утечках

Логин / пароль

Дата рождения

Пол

Номера документов

Город и адрес проживания

Ссылки на социальные сети

Информация о членах семьи

Место учебы / работы

Информация о заказах товаров и услуг

Дата регистрации / последней активности

Последствия утечек данных для пользователей

Распространение приватной информации

Регистрируясь на интернет-ресурсе, мы верим, что наши данные под надежной защитой. Зачем кому-то знать не просто наш номер телефона, а адрес проживания, историю наших покупок или путешествий, увлечения и историю болезней? Любая личная информация, попавшая в публичное пространство, может использоваться против пользователя (насмешки, шантаж, запугивание, травля) и причинять как репутационный, так и моральный вред.

Взлом аккаунтов

Ни для кого не секрет, что большинство пользователей используют один пароль при регистрации на интернет-сервисах. Если один из сервисов становится жертвой утечки данных, злоумышленники могут использовать эту информацию для доступа к другим вашим аккаунтам.

Попадание в мошеннические базы

Надоели мошеннические звонки? Именно на основе утечек данных формируются мошеннические базы, из которых можно делать выборки по возрасту, местоположению, полу и другим параметрам. Также не стоит забывать об угрозе фишинговых писем, которые, на основе контекста скомпрометированной базы, могут стать еще более опасными.

Последствия утечек данных для компании

Репутационные риски

СМИ достаточно внимательно относятся к утечкам данным и быстро предают их огласке. Это может негативно повлиять на желание клиентов работать с компанией, в которой произошла утечка.

Регуляторные риски

Компания, подвергшаяся утечке, может быть оштрафована.

Подробнее

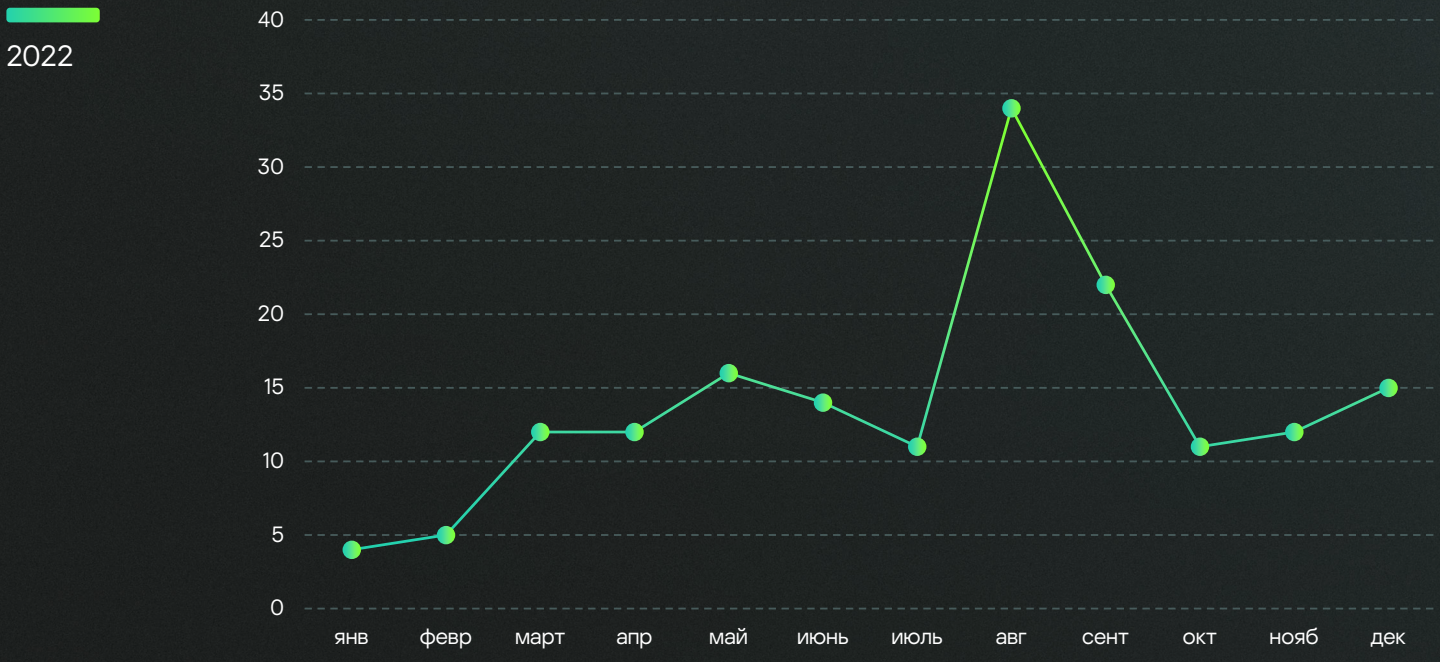
Материальные риски

Пользователи, чьи права были нарушены, могут подать коллективные иски против компании, в которой произошла утечка, и потребовать возмещения вреда, который был им причинен по ее вине.

Когда происходили утечки?

В 2022 году обнаружено 168 случаев публикаций значимых баз данных, относящихся к российским компаниям. Если распределить утечки равномерно в течение года, выяснится, что практически каждый второй день в свободный доступ выкладывалась информация, затрагивающая российских пользователей интернета.

График 1 Распределение публикаций баз данных



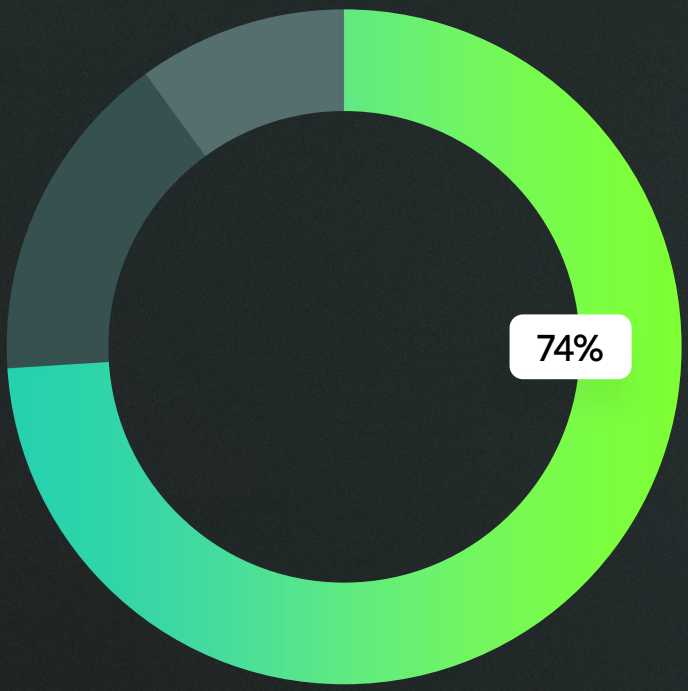
Активизация злоумышленников в части размещения скомпрометированных данных произошла в марте и августе 2022 года. В эти месяцы наблюдался значительный рост публикаций по сравнению с предыдущими (2,4 раза – февраль-март; в 3,1 раза – июль-август). И если мартовская активность связана в первую очередь с массовыми взломами ресурсов СМИ и служб доставки ресторанов, то август отметился публикацией объемного архива дампов небольших баз данных различных компаний, среди которых присутствовали в том числе значимые утечки.

Пик публикации значимых баз данных приходится на март и август 2022 года

Насколько публикуемые данные являлись актуальными?

Диаграмма 1 Предполагаемый год утечки данных

Хотелось бы сказать, что все утечки имели срок давности 10 и более лет, но это не так. Большая часть данных была выгружена в 2022 году (74%) и только 16% в 2021. Выгрузки до 2021 года (или неустановленного года) всего 10%.



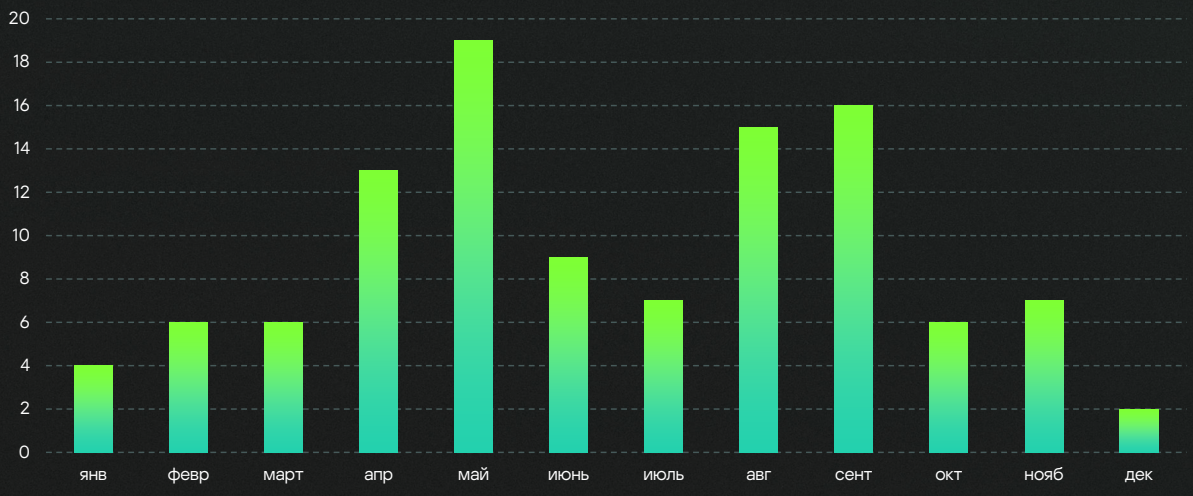
2022 2021 До 2021

Если рассматривать атаки, произошедшие только в 2022 году, то рост компрометаций баз данных пришелся на апрель 2022 года (рост более чем в 2 раза по сравнению с февралем), со значительным снижением в летние месяцы (июнь-июль) и осенне-зимний период. Предполагаем, что последствия декабрьских атак еще проявят себя в 2023 году.

В среднем за 2022 год 10 компаний в месяц подвергались атакам, результатом которых была значимая утечка пользовательских данных с последующим размещением в свободном доступе.

График 2 Предполагаемый месяц выгрузки данных в 2022 году

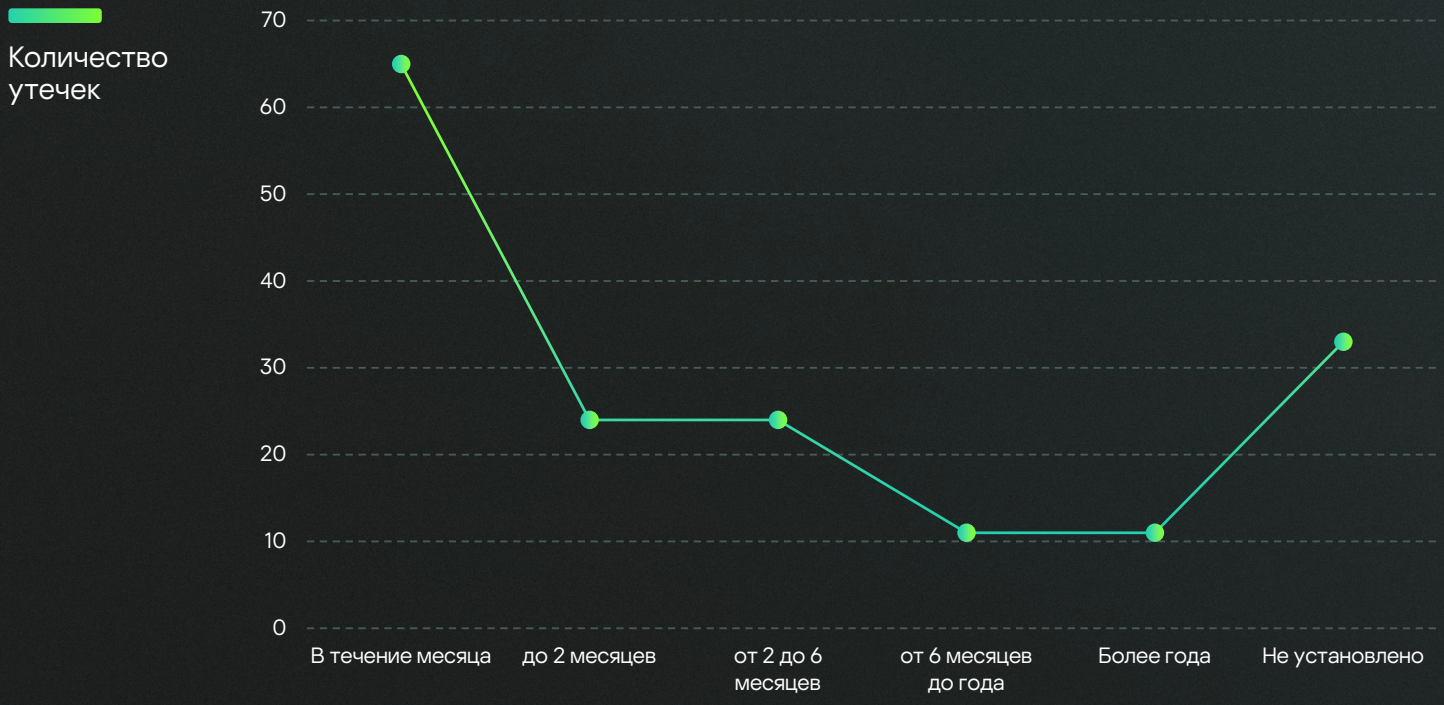
2022



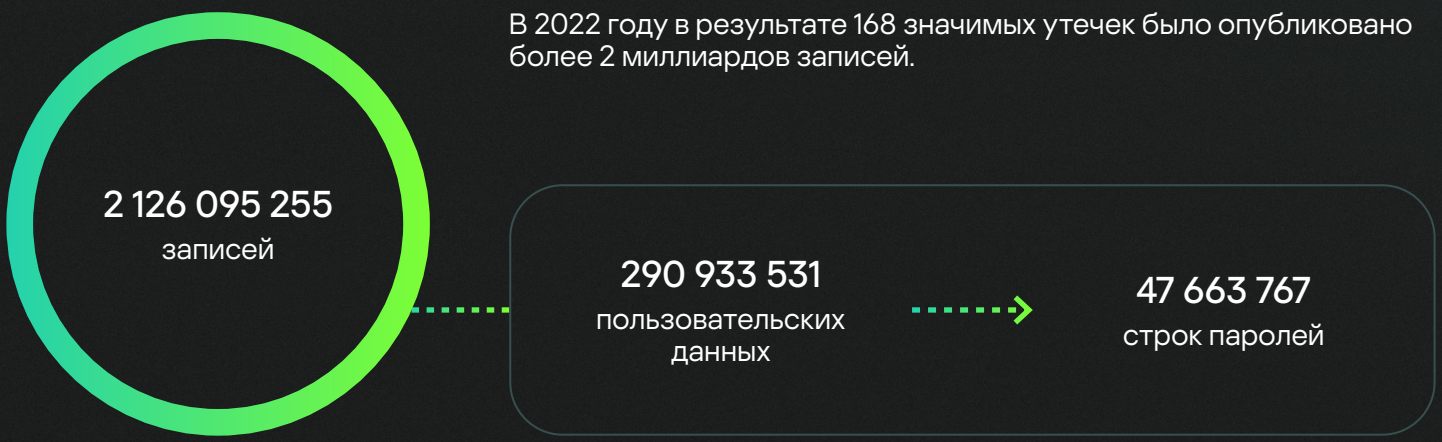
Сколько данных утекло?

Трендом 2022 года является изменение философии злоумышленников. Если раньше основным мотивом взломов являлось извлечение прибыли, то в 2022 году утечки носили преимущественно идейный характер. 39% утечек публиковались в течение месяца после выполнения выгрузки из базы данных компании.

График 3 Интервал времени от выгрузки данных до публикации



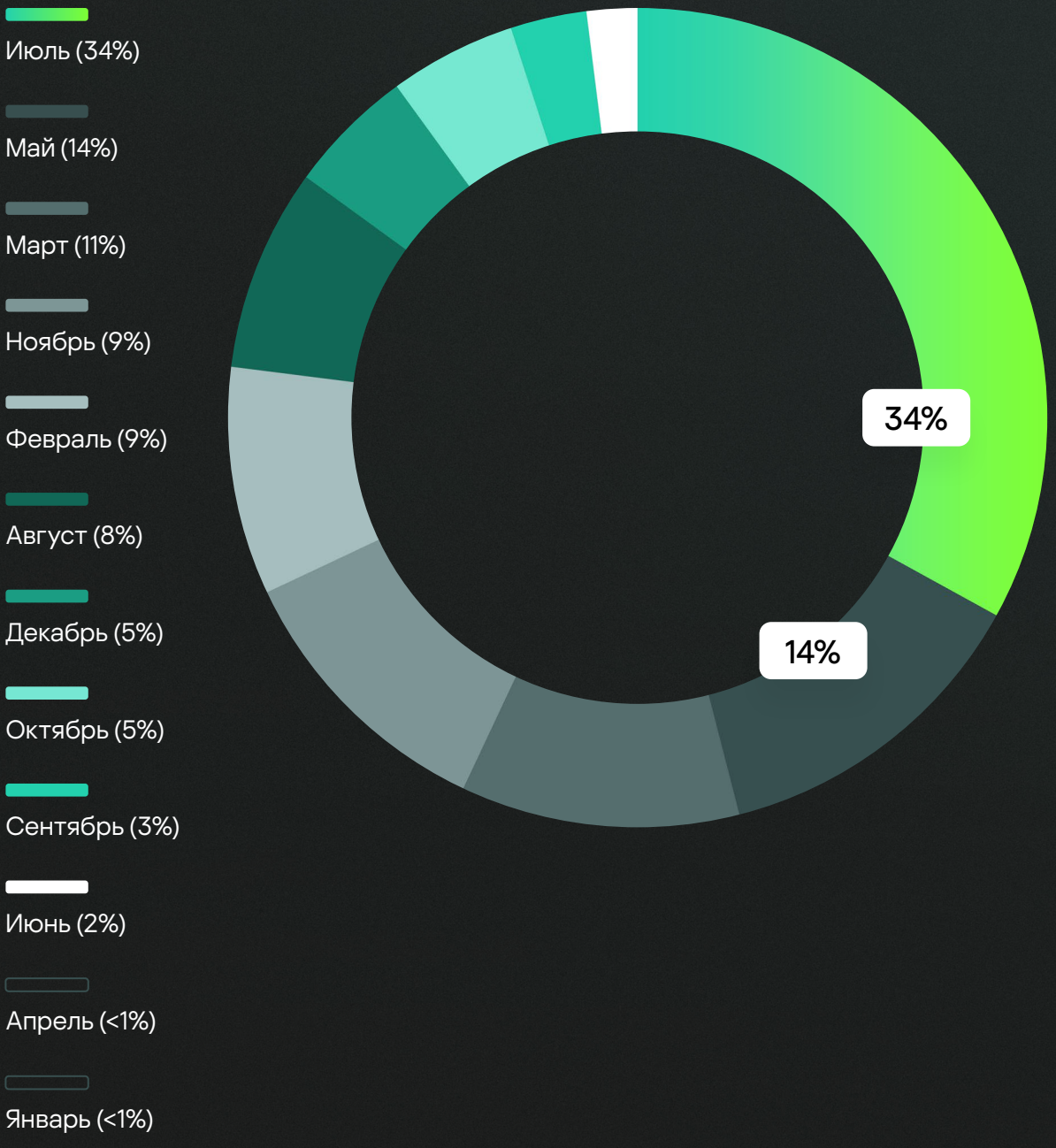
В 2022 году в результате 168 значимых утечек было опубликовано более 2 миллиардов записей.



Есть ли зависимость от количества произошедших утечек и объема опубликованных данных?

Как оказалось – нет. Одна точечная утечка может полностью перекрыть множество более мелких. Это видно на диаграмме «Распределение объема публикаций пользовательских данных», где июнь и май, не являясь лидерами по количеству публикаций, в совокупности содержали 48% всех скомпрометированных пользовательских данных.

Диаграмма 2 Распределение объема пользовательских данных



Профиль жертвы

Основной удар злоумышленников пришелся на организации сферы «Ритейл» (27%). От 10 до 12% всех утечек произошли в организациях сфер «Карьера и образование», «Интернет-сервисы» и «Рестораны и доставка еды».

Наименьшему количеству взломов в 2022 году подверглись компании финансовой сферы, здравоохранения и недвижимости. Стоит отметить, что в перечисленных областях хранятся наиболее чувствительные пользовательские данные.

График 4 Количество утечек данных по отраслям

Лидерами по объему скомпрометированных пользовательских данных являются сферы «Доставка» (34%) и «Ритейл» (14%), которые исторически хранят колоссальные объемы информации. Наименьшее количество данных скомпрометировано у компаний сферы недвижимости, организаций производственной и финансовой отрасли (менее 1%).

График 5 Количество скомпрометированных пользовательских данных по отраслям

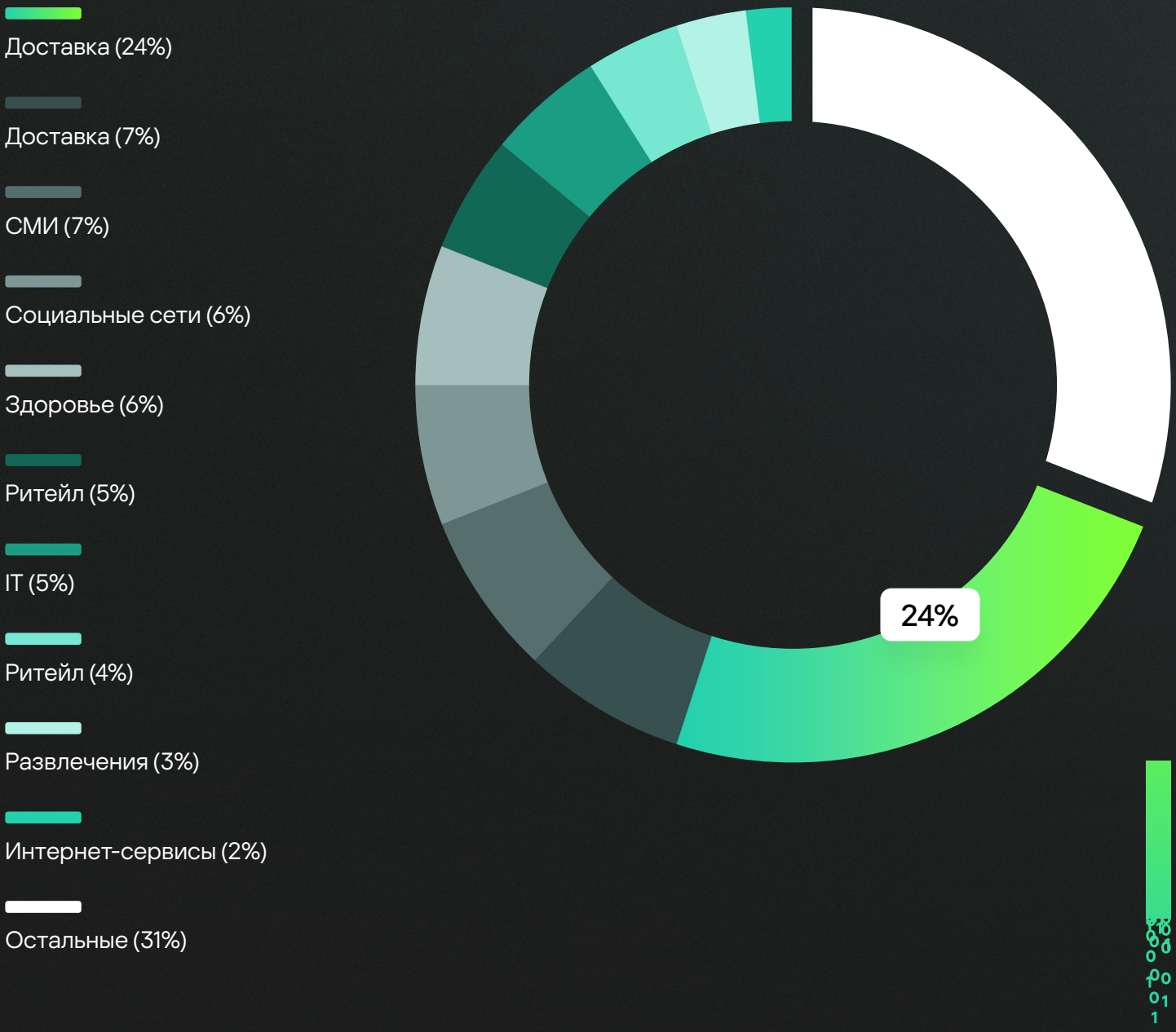
Большинство утечек публикуется в необработанном виде. Это означает, что в массиве данных присутствуют пустые, технические строки. Также стоит отметить, что различные форматы данных содержат разное количество строк для формирования информации об одном пользователе.
Этот факт может вводить читателей СМИ в заблуждение, потому что не всегда понятно, что означает в действительности утечка двухмиллионной базы данных.

Мы решили оценить приближенные к реальности значения и сопоставили необработанные массивы данных с количеством пользовательских данных, находящихся в них. Оказалось, что, в среднем, по всем утечкам треть данных не содержала в себе критичной для пользователей информации, однако в сфере доставки разница между необработанными и пользовательскими данными достигла 15 раз.

Крупные утечки в 2022 году

Крупные утечки в 2022 году происходили в разных отраслях российского бизнеса. Злоумышленники искали возможность нанести урон любой компании, находящейся на территории России. В Топ-10 по количеству опубликованных пользовательских данных вошли по две утечки компаний из сфер «Доставка» и «Ритейл». По одной крупной утечке произошло в сферах «Здоровье», «IT», «СМИ», «Развлечения», «Социальные сети» и «Интернет-сервисы». Стоит отметить, что Топ-10 включают в себя 69% всех данных.

Диаграмма 3 Топ-10 утечек в процентах от общего числа



Публикации баз данных в 2022 году затронули не только пользователей, но и сотрудников компаний.

Информация о 1 229 859 сотрудниках была размещена в свободном доступе

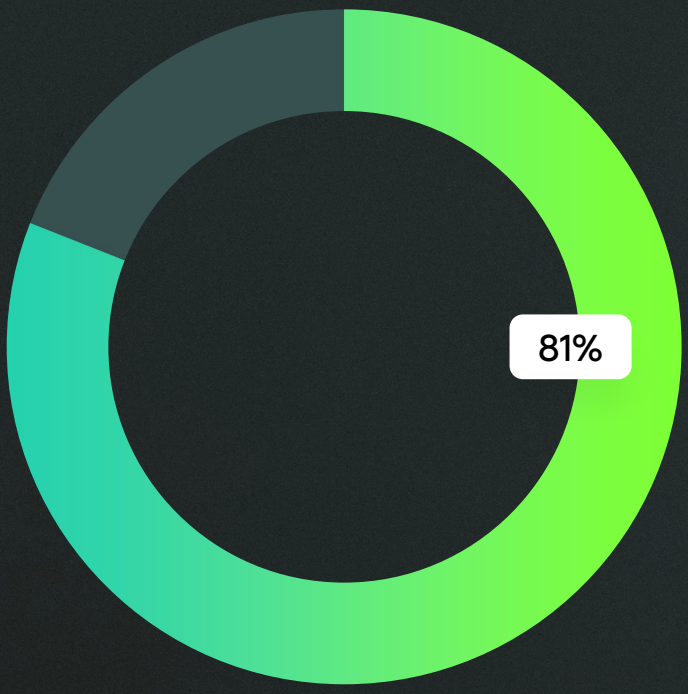
Стоит отметить, что подобные утечки не только раскрывают рабочие данные – должность, e-mail, принадлежность к группам Active Directory, что может использоваться злоумышленниками для проведения целенаправленных атак, но и личную информацию: номер мобильного телефона, финансовые данные, наличие декрета и т. д.

81% атак пришлись на организации малого и среднего бизнеса

Малый / Средний бизнес

Крупный бизнес

Диаграмма 4 Количество утечек по размерам бизнеса



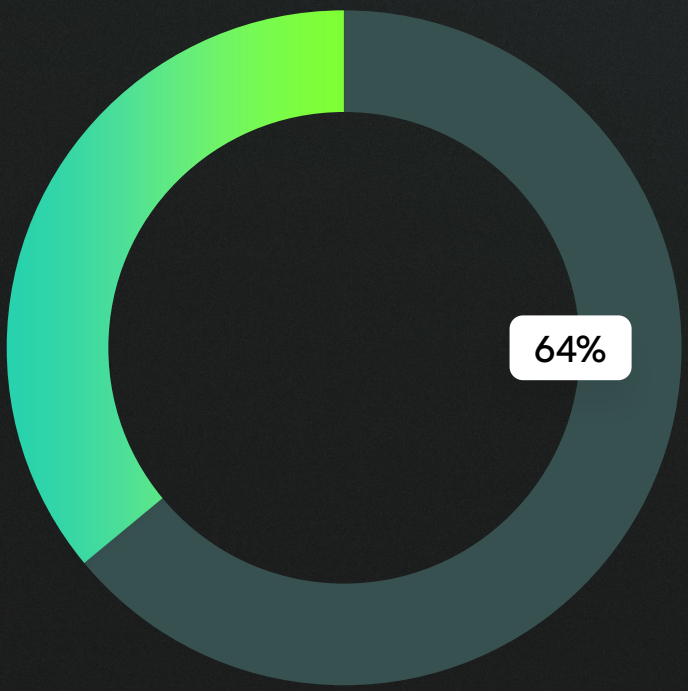
64% пользовательских данных были скомпрометированы в результате атак именно на крупный бизнес

Представители крупного бизнеса понимают риски, которые могут возникнуть в случае отсутствия организации защиты информации, имеют возможность тратить деньги на развитие систем защиты. Но обладание гигантскими объемами ценных данных, финансовая обеспеченность делают эти компании привлекательной целью злоумышленцников. В 2022 году, помимо перечисленных факторов, одну из основных ролей сыграл общественный резонанс, возникший после первых крупных утечек данных.

Малый / Средний бизнес

Крупный бизнес

Диаграмма 5 Объем утечек по размерам бизнеса

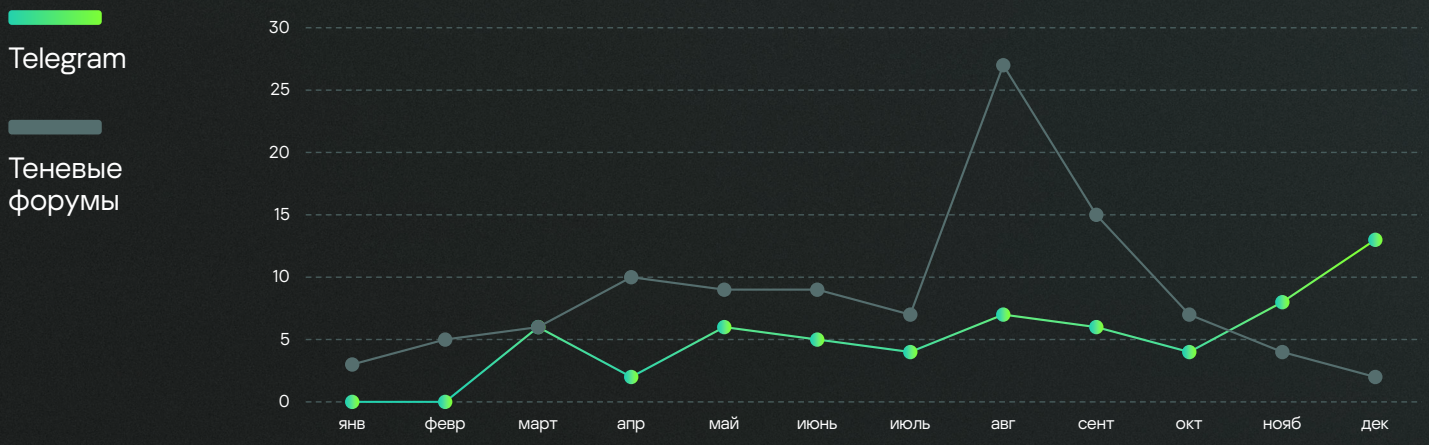


Каналы распространения

Исторически основным каналом распространения баз данных были даркнет-форумы, целью которых является привлечение пользователей, максимально заинтересованных в таких данных. Это, в свою очередь, ограничивало распространение информации о произошедших инцидентах.

2022 год внес свои изменения в устоявшийся порядок, а именно – в марте часть злоумышленников, целью которых является поднятие общественного резонанса, поняли, что Telegram больше подходит для осуществления идеологических задач. В связи с высокой активностью подобных группировок к концу году заметна полная переориентация публикаций утечек исключительно в Telegram-каналы.

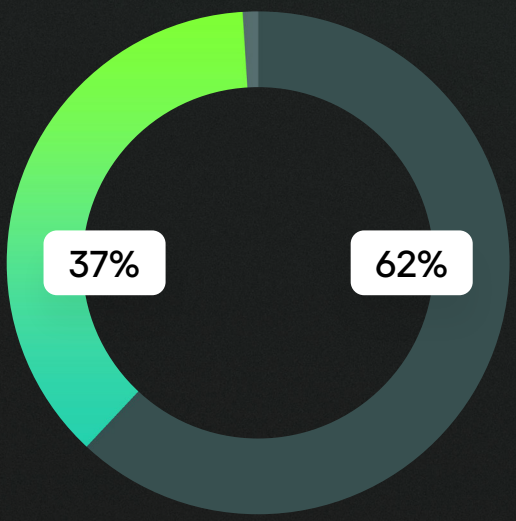
График 6 Распределение публикаций по месяцам и каналам распространения

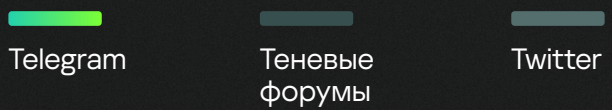


62% баз опубликованы на даркнет-форумах. 37% баз опубликованы в Telegram-каналах

Стоит отметить, что активность злоумышленников на даркнет-форумах никуда не пропала. Ценные базы данных также передаются внутри небольших сообществ, продаются на форумах; менее ценные выкладываются в свободном доступе для повышения репутации на теневых площадках.

Диаграмма 6 Источники публикации утечки данных





Чем же так популярен Telegram?

Мы проанализировали количество просмотров постов в Telegram-каналах и на одном из популярных англоязычных даркнет-форумов.

Посты в Telegram-каналах просматриваются в среднем в 20 раз больше, чем публикации, доступные на даркнет-форумах

Максимальное количество просмотров в Telegram достигает сотни тысяч, на даркнет-форумах исчисляется десятками тысяч.

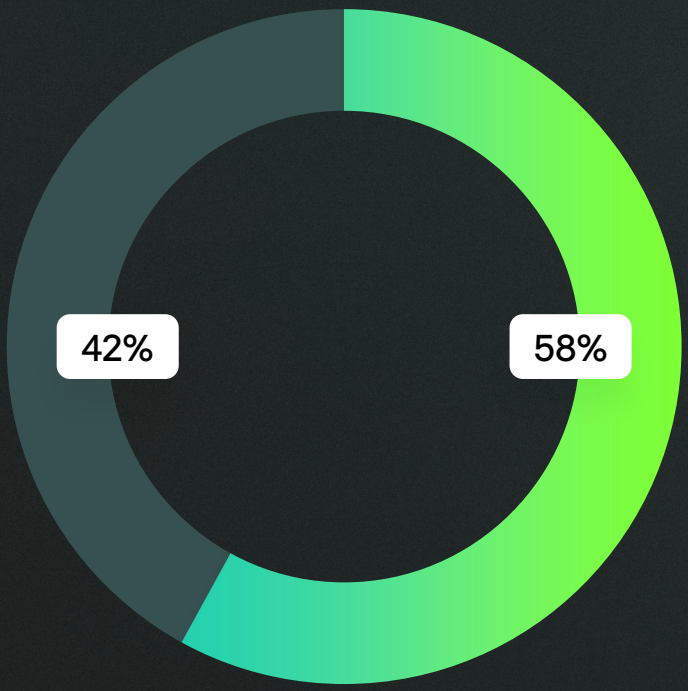
Именно поэтому резонансные базы данных публиковались в первую очередь в Telegram-каналах. Эта закономерность отражена на диаграмме 7, где показывается распределение каналов публикации баз данных объемом 1 млн строк и более.

Telegram

Теневые форумы

Диаграмма 7

Источник публикации базы данных (больше 1 млн строк)



Реакция бизнеса

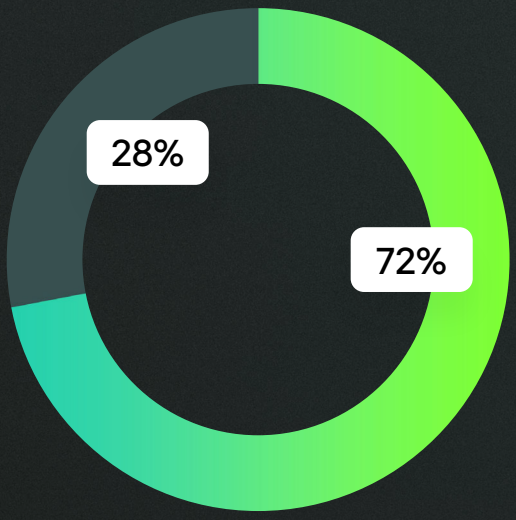
К сожалению для бизнеса, инциденты, результатом которых стали утечки данных, очень быстро расходятся в публичном пространстве; реагировать на них приходится тоже публично. По нашим наблюдениям, на наличие комментария влияет статус и публичность компании, а не объем скомпрометированных данных.

28% компаний открыто прокомментировали произошедшую утечку данных. 72% компаний воздерживаются от комментариев или попросту не знают о существовании утечки

Нет

Да

Диаграмма 8 Наличие публичной реакции компании на утечку данных



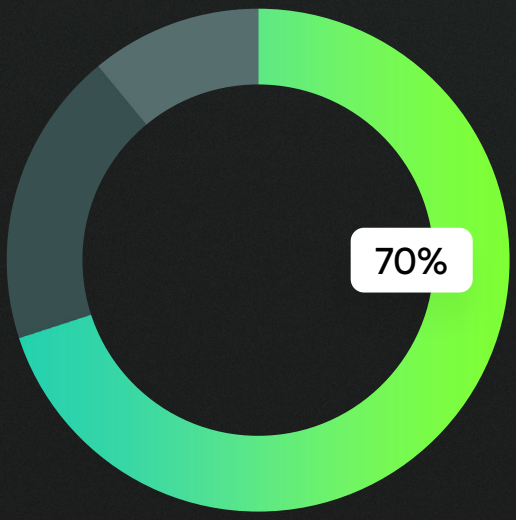
В 70% случаев компании признавали факт того, что скомпрометированные данные относятся к пользователям их ресурсов. в 19% случаев однозначно опровергли предъявленные обвинения, а в 11% случаев решили ограничиться заявлением о проверке инцидента

Подтвердили

Опровергли

Проводят проверку

Диаграмма 9 Реакция бизнеса на утечку данных

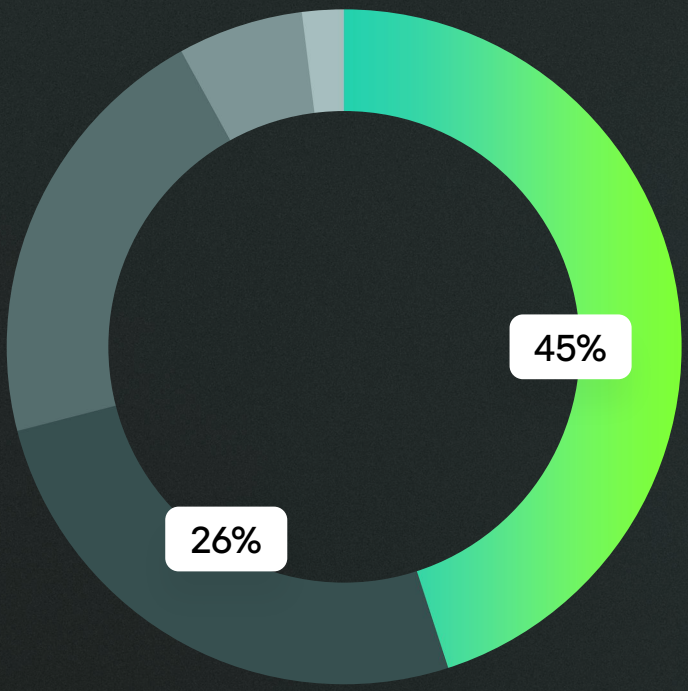


45% заявлений были опубликованы уже в течение дня после размещения утечки. 26% на следующий день. 8% позже чем через 7 дней

Компании старались прокомментировать случившийся инцидент как можно раньше.

- В течение дня
- 1 день
- от 2 до 7 дней
- от 7 до 14 дней
- Более месяца

Диаграмма 10 Интервал времени публичной реакции бизнеса

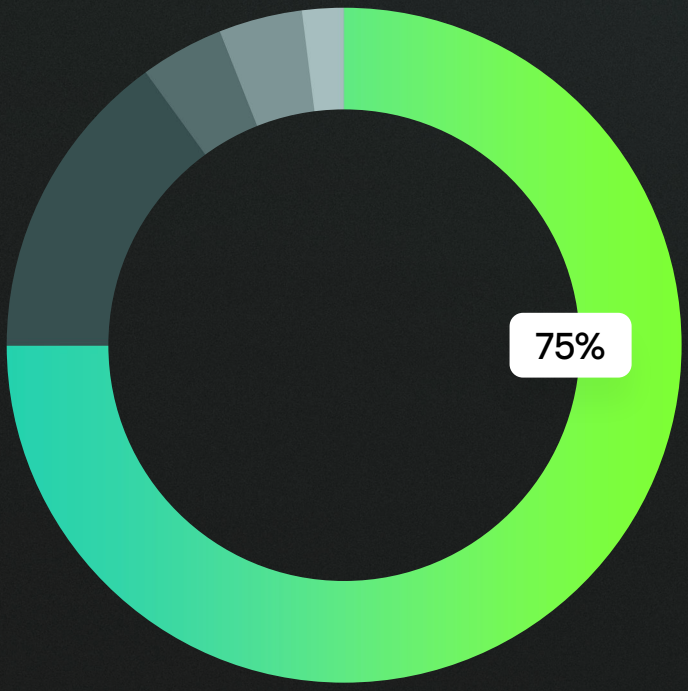


В 75% случаев каналом публикации комментария компании по поводу утечки данных являлось СМИ. 15% решили разместить информацию у себя на сайте, а 10% компаний выбрали наиболее публичные источники связи с пользователями (блоги, Telegram-каналы)

Если вы решили публиковать заявление об утечке данных на площадке с возможностью комментариев, необходимо максимально открыто подойти к освещению процесса и постараться отвечать на публикации пользователей. в противном случае велик шанс получить волну негатива и превратить открытость в антирекламу компании.

- СМИ
- Сайт
- Telegram
- Форумы
- Habr

Диаграмма 11 Источник публикации реакции



Что делать в случае утечки данных?

Утечка данных может затронуть любую компанию. Но все ли компании готовы к такому инциденту? Представьте, что сегодня тот день, когда ваше утро начинается не с чашки кофе, а с публикации в профильном Telegram-канале, что на даркнет-форуме выложили базу данных пользователей вашей компании. Что делать и куда бежать? Предлагаем вам поэтапно разобраться в этом вопросе.

1. Идентификация инцидента
2. Коммуникации
3. Устранение инцидента

1 Подтвердите или опровергните факт компрометации данных

1.1 Определите источник

Определите первоначальный источник информации об утечке данных. В большинстве случаев для построения исходной гипотезы достаточно свободно публикуемого примера данных.

1.2 Верифицируйте

Верифицируйте полученный пример скомпрометированных данных, сравнив с данными, хранящимися в информационных системах организации. При необходимости свяжитесь с партнерами, осуществляющими обработку / хранение / передачу данных, для верификации на их стороне.

1.3 Проведите анализ

В случае подтверждения валидности данных проведите анализ затронутых IT-систем, пользователей для понимания объемов утечки данных.

Важно

Ни в коем случае не переводите деньги злоумышленникам для сокрытия факта утечки данных / выкупа базы данных.

2 Организуйте коммуникации с заинтересованными сторонами

2.1

Топ-менеджмент компании

Оповестите руководство о предполагаемом факте утечки данных, принятых и планируемых шагах для устранения инцидента.

2.2

Регулятор

Сообщите надзорным организациям о факте обнаружения инцидента, результатах проведенного расследования.

2.3

СМИ

В случае необходимости подготовьте публичные заявления, согласованные с юридическим отделом.

Коммуникация №1: оповестить о проведении расследования, если информации, имеющейся на момент анализа, недостаточно для подтверждения или опровержения компрометации данных.

Коммуникация №2: по результатам проведенного расследования опровергнуть либо подтвердить факт утечки данных, обозначить список принятых мер.

2.4

Пользователи

Оповестить пользователей, затронутых утечкой данных, о факте компрометации, возможных последствиях и предпринятых действиях.

2.5

Партнеры

В случае необходимости оповестите партнерские организации о факте компрометации данных и результатах расследования.

Важно

Не раскрывайте предпринимаемые меры, пока не завершится расследование и устранение инцидента. Публичные коммуникации необходимо проводить через одно лицо / канал (в идеале PR-департамент). Проведите перекрестную проверку всех внешних коммуникаций, чтобы не было противоречий.

3 Примите меры для устранения последствий инцидента

3.1 Проведите расследование инцидента

Проведите расследование инцидента, определив вектор атаки и факт закрепления злоумышленников в IT-инфраструктуре. Расследование инцидента является одним из самых важных этапов реакции на утечку данных. В случае закрепления злоумышленника в IT-инфраструктуре есть вероятность повторной компрометации. У внутренней команды, занимающейся информационной безопасностью в компании, может быть недостаточно ресурсов или даже компетенций в проведении расследования; в таком случае рекомендуется привлекать квалифицированных специалистов из внешних компаний.

3.2 Устраните угрозу

Устраните угрозу несанкционированного доступа к данным: удалите вредоносные файлы, устраните уязвимости, смените пароли затронутым учетным записям.

3.3 Подготовьтесь к возможным инцидентам

На основе полученного опыта подготовьте план реагирования в случае повторения инцидента, если у вас его еще нет. Надеемся, что это не так.

Важно

Партнеры организации являются одним из каналов утечек пользовательских данных. Старайтесь держать под контролем процесс обработки ваших данных сторонними компаниями, устанавливая приемлемые для вас требования в части хранения и обработки.

Налаживаем коммуникации

Организация коммуникации важна в случае утечки данных. Это позволяет уведомить заинтересованные стороны, включая пользователей, партнеров и законодательные органы, об инциденте и предпринятых мерах по его устранению. Также это помогает сохранить доверие к компании и предотвратить возможные негативные последствия для бизнеса.

План и шаблон коммуникаций необходимо подготовить заранее, чтобы определить – как, по какому каналу и в каком объеме следует передавать информацию при возникновении инцидента. В таблице ниже мы попытались агрегировать данную информацию, чтобы помочь вам правильно подготовиться к публичному взаимодействию с разными целевыми аудиториями.

Аудитория	Канал коммуникации	Предоставляемая информация	Подтверждение
Пользователи	Целенаправленные рассылки Сайт / форум СМИ Пресс-конференция	Факт инцидента Скомпрометированные данные Последствия для пользователей Принятые меры для недопущения повторения инцидента	
Партнеры	Согласованные каналы	Факт инцидента Затронутые системы / сервисы Скомпрометированные данные Возможные векторы атаки	Требуется
Регуляторы	Устанавливается регулятором	Устанавливается регулятором	Требуется
СМИ	Комментарий Сайт / форум Пресс-конференция	Факт инцидента Затронутые системы / сервисы Последствия для пользователей Принятые меры	

Регуляторы

Информация, которая должна быть предоставлена в случае возникновения инцидента, временные рамки оповещения, канал коммуникации строго определены руководством органа власти.

Команда, занимающаяся идентификацией инцидента, должна иметь предварительно подготовленный шаблон реагирования на подобные инциденты, иначе есть риск не успеть подготовить нужные материалы и получить штраф.

Стоит отметить, что оповещать нужно не только о факте инцидента, но и по результатам проведения расследования.

Пользователи и СМИ

Раскрытие информации для клиентов и общественности должно быть скоординировано PR-командой. Прежде всего необходимо определить, какая информация должна быть раскрыта. Не существует заранее определенных шаблонов, так как природа инцидента может быть различной.

Информация об инциденте, передаваемая пользователям и СМИ, требует согласования с юридическим отделом. В случае возникновения особо крупных инцидентов рекомендуем проводить коммуникации через руководство компании, а не PR-команду.

Не забывайте проводить повторные коммуникации даже после разрешения инцидентов.

Партнеры

Не существует определенного шаблона для обмена информацией об инциденте с партнерами, но основная структура определяется идеей обмена только ценной информацией, которая может снизить шансы развития атаки на инфраструктуру партнера.

Возможна обратная ситуация – когда есть подозрение, что данные или системы были скомпрометированы через компанию-партнера. Тогда необходимо провести взаимодействие для установления или опровержения гипотезы развития атаки.

Информация, переданная партнерам, должна быть подтверждена ими.

Общий перечень предоставляемой информации об инциденте:

Краткое описание инцидента

Масштаб воздействия

Рекомендуемые действия (если применимо)

Принятые меры по смягчению последствий инцидента

Планируемые меры по смягчению последствий таких же инцидентов в будущем

Возможный набор информации, подлежащей обмену:

Краткое описание начального вектора атаки и масштаба компрометации

Возможные пути развития атак на инфраструктуру партнеров или использование скомпрометированных сервисов против бизнес-процессов

Предпринятые действия по смягчению последствий инцидента

Рекомендации

Не хотите стать жертвой утечки пользовательских данных? Обратите внимание на наши рекомендации:

Права доступа

Внедрите разграничение прав доступа, чтобы быть уверенными, что доступ к данным ограничен, а источник активности идентифицируем.

Храните самое нужное

Храните только необходимые данные для реализации логики работы сервисов и приложений.

Не платите злоумышленникам

В случае подозрения на компрометацию данных не платите злоумышленникам за сокрытие информации. Во-первых, это уголовно наказуемо. Во-вторых, есть очень большой риск, что ваши данные через какое-то время будут преданы огласке, особенно это актуально в период массовых взломов по идеологическим мотивам.

Мониторинг поверхности атаки

Мониторинг поверхности атаки поможет выявить узкие места внешнего периметра организации.

Управление уязвимостями

Для оперативного устранения уязвимостей организуйте процесс «Управление уязвимостями».

Быть готовым ко всему

Будьте готовы, что вас могут взломать. План реагирования поможет уменьшить ущерб от инцидента.

Оперативность

Осведомлен — значит вооружен. Используйте средства Threat Intelligence для оперативного выявления инцидентов.

Помощь извне

Убедитесь, что злоумышленник больше не имеет доступа к инфраструктуре. В случае отсутствия компетенций обратитесь к внешним поставщикам услуг для проведения расследования инцидента.

Сбор и анализ событий

Внедрите систему сбора и анализа событий информационной безопасности для обнаружения попыток несанкционированного доступа на начальном этапе атаки.

Повышение осведомленности

Организуйте процесс «Повышение осведомленности» – для борьбы с вредоносной активностью и непреднамеренной публикацией конфиденциальной информации на уровне пользователей.

Наши решения

Kaspersky Digital Footprint Intelligence

Подробнее

Поиск внешних угроз, нацеленных на вашу компанию

Анализ сетевого периметра

Поиск потенциальных точек входа злоумышленников: доступных интерфейсов управления, неправильно сконфигурированных сервисов, интерфейсов сетевых устройств, уязвимого ПО

Активность киберпреступников

Мониторинг целевых угроз на ресурсах даркнета (форумах, мессенджерах, onion-ресурсах)

Анализ вредоносного ПО

Анализ фишинговых атак на компанию и активности ботнетов, обнаружение угроз

Утечки данных

Оперативное выявление данных компании, которые были скомпрометированы

Kaspersky Managed Detection and Response

Подробнее

Kaspersky Incident Response

Подробнее

Kaspersky Threat Intelligence

Подробнее

www.kaspersky.ru

#kaspersky
#bringonthefuture