Аналитические отчеты
«Лаборатории Касперского»

Значимые утечки данных в 2023

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Содержание

Ключевые результаты

Общие сведения о значимых[1] утечках данных в российских компаниях в 2023 году[2]:

факта утечек данных за 2023 год

За 2022 год

141 факт утечек данных

>230 млн пользовательских данных

>33 млн записей с паролями

За 2023 год

133 факта утечек данных

>310 млн пользовательских данных

>47 млн записей с паролями

23% — представители крупного бизнеса

от общего числа жертв

Топ-10 утечек

содержат 74% всех скомпрометированных данных

54% утечек

содержали парольную информацию

17 фактов утечек из 133

были подтверждены пострадавшими компаниями публично

4,5% утечек

содержали пароли в открытом виде

md5 (pass+salt)

самый популярный алгоритм хеширования паролей

Ритейл и интернет-сервисы — лидеры по числу фактов утечек

Ритейл и финансы — лидеры по объему утечек пользовательских данных

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

2 С января по октябрь 2023 года

Тренды 2023

Telegram — основной канал распространения публичных утечек

67%

всех публикаций

Смещение фокуса на публикацию данных компаний крупного бизнеса

58%

рост в 2023 году

Увеличение количества утечек в организациях сфер:

Здоровье

x9

Финансы

x7

IT

x3,5

Компании выбирают «осторожную» позицию при публичном комментировании произошедшего инцидента или полностью отрицают факт утечки данных

Атаки на 1C-Bitrix — один из основных векторов кражи данных

47% опубликованных утечек, содержащих парольную информацию, указывают на использование данной CMS в целевой системе

Введение

Аналитический отчет содержит информацию о значимых утечках данных в российских компаниях, публикация которых произошла в период с января по октябрь 2023 года. Команда Kaspersky Digital Footprint Intelligence отслеживает 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.

В отчете представляем результаты нашей аналитики, на основании которой мы можем отследить изменения, произошедшие в сфере утечек данных российских компаний, и ответить на вопросы:

- Участились ли инциденты, связанные с публикацией скомпрометированных данных компаний и их клиентов в 2023 году?
- Какие отрасли в первую очередь попали под удар злоумышленников?
- Сколько пользовательских данных было скомпрометировано?
- Сколько и в каком виде парольной информации стало доступно атакующим?
- 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, опубликованные в свободном доступе в интернете.

Как отличить фейковую утечку от реальных данных?

Подтвердить факт утечки пользовательских данных может только владелец данных, поэтому наличие комментария в СМИ или на официальном сайте / форуме / Telegram-канале компании является единственным однозначным признаком достоверности опубликованных материалов.

Во всех остальных случаях можно только сделать предположительное заключение, основанное на анализе:

Уникальности

Проверяется сопоставлением данных из утечки с предыдущими утечками, опубликованными в свободном доступе.

Адекватности

Оценка структуры опубликованных данных и их формата, путем сопоставления значений отдельных колонок таблицы. Во внимание берутся такие значения, как ФИО, дата рождения, технические даты, адрес электронной почты и т. д.

Структуры данных

Вероятность подделки json или sql файла ниже, чем обычного текстового документа. Явные признаки редактирования, изменения документа вызывают дополнительные подозрения.

Комментариев

Анализ комментариев в Telegram-сообществах и теневых площадках является неотъемлемой частью анализа утечек данных. Также стоит обращать внимание на экспертные мнения насчет уникальности и достоверности данных.

Источника публикации

Регулярный анализ опубликованных материалов от отдельных группировок или пользователей с теневых площадок позволяет составить их репутацию и сформировать их паттерн поведения, «подчерк», который может также помочь сделать вывод о достоверности данных.

Ресурса

Проверить наличие регистрации определенного пользователя можно через форму восстановления пароля на предположительно скомпрометированном ресурсе.

Зачем анализировать факты утечек данных?

1

Скомпрометированные учетные записи, находящиеся в публичных утечках данных, также могут использоваться злоумышленниками для получения доступа к корпоративным ресурсам компаний-жертв. Даже если утечка является не самой новой, наличие публично скомпрометированного аккаунта, подходящего под парольную политику, может привести к компрометации привилегированного аккаунта через неопределенное время. Сотрудники часто используют корпоративные адреса электронной почты для регистрации на сторонних сервисах, поэтому информация из сторонних утечек дает возможность узнать о скомпрометированных учетных записях сотрудников.

Таблица 1

Как атакующие проникают внутрь организаций[1]

	2019	2020	2021	2022
Эксплуатация уязвимостей в публично доступных приложениях	37,0%	53,6%	53,6%	42,9%
Скомпрометированные учетные записи	13,0%	53,6%	17,9%	23,8%
Вредоносные письма	30,0%	23,7%	11,9%	11,9%

2

Не все утечки остаются в поле зрения СМИ и экспертов сообщества информационной безопасности. Поэтому важно предоставить всем организациям и пользователям возможность получать информацию о компрометации данных как можно быстрее. Для первых — это возможность минимизировать репутационные или регуляторные риски, для других — это повышение цифровой осведомленности и возможность узнать о компрометации парольной информации.

3

Анализ жертв данных дает представление о текущих трендах, не только связанных с изменением фокуса злоумышленников, но и о потенциальных векторах атак, использующихся атакующими, а значит, позволяет выстроить защиту и минимизировать риски, связанные с применением этих атак.

1 Аналитический отчет Kaspersky: Природа инцидентов информационной безопасности 2022

Распространение утечек данных

За январь — октябрь 2023 года установлено 133 факта публикаций значимых баз данных, относящихся к российским компаниям, что на 6% меньше, чем за аналогичный период 2022 года.

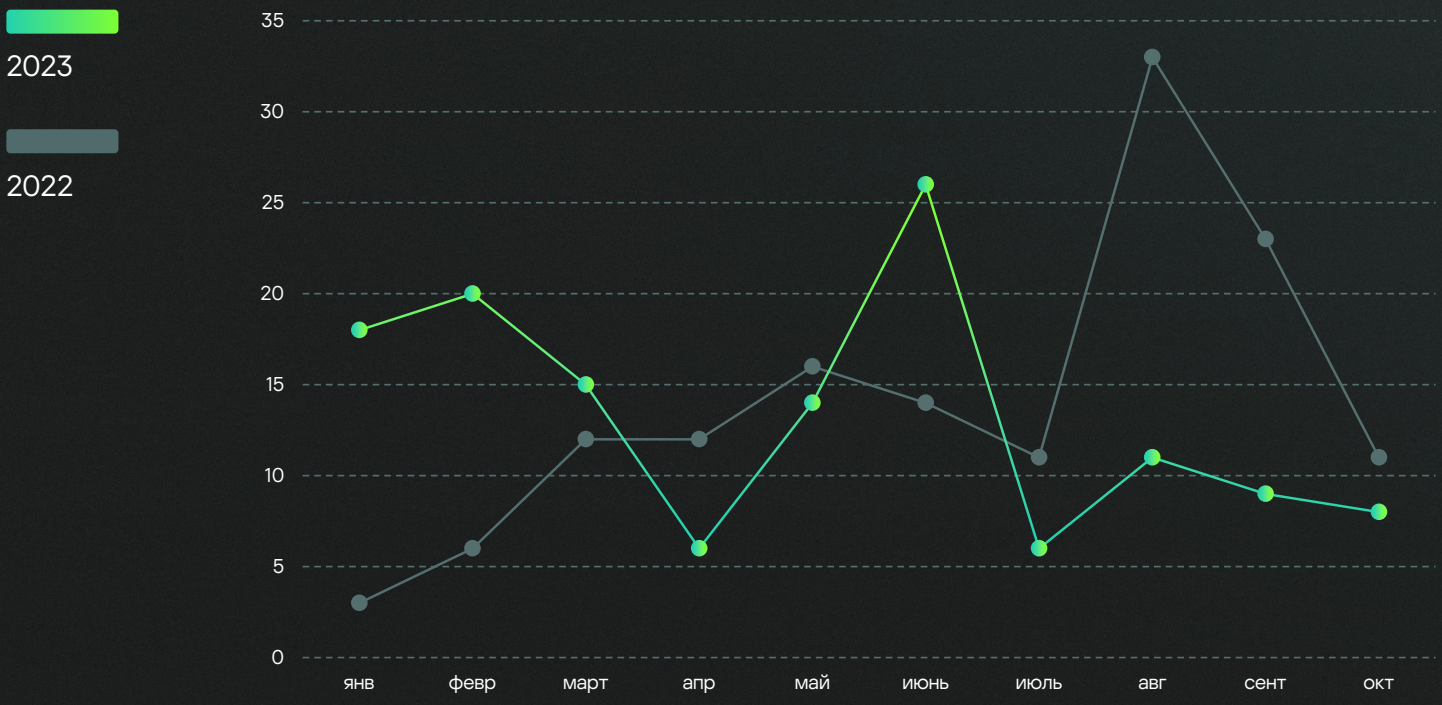
В большинстве случаев повышение или понижение активности публикаций не прогнозируемо и в первую очередь зависит от желания злоумышленников разместить имеющийся материал в конкретный момент времени.

Однако мы наблюдали как минимум 2 фактора, которые могут свидетельствовать о возможной активизации злоумышленников в части размещения скомпрометированных пользовательских данных:

1. Наличие громких публикаций у противоборствующих группировок
2. Обострение общемировой политической обстановки

График 1

Распределение количества утечек данных по годам

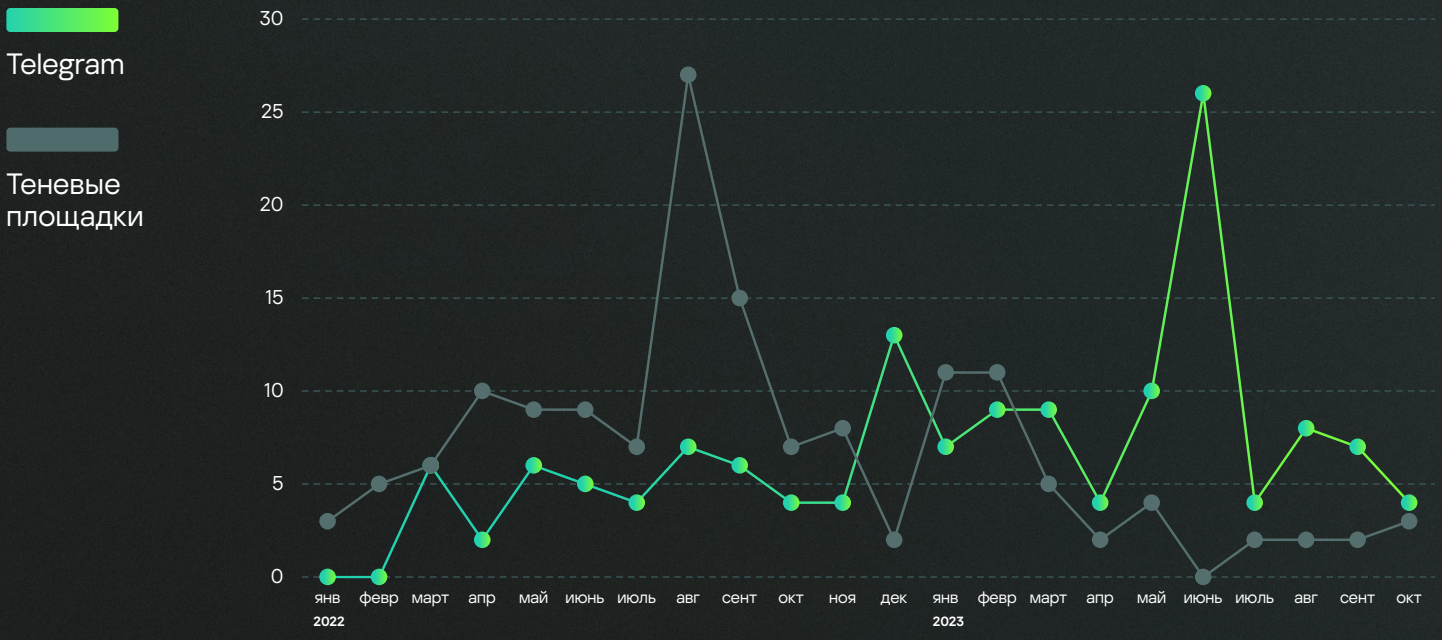


Одним из факторов снижения количества публикаций в 2023 году стала приостановка работы международной теневой площадки Breached в марте, на которой активно публиковались утечки данных российских пользователей и компаний. В результате закрытия форума часть злоумышленников на какое-то время потеряла доверенное место для размещения скомпрометированных данных.

Помимо краткосрочного снижения количества публикаций, объем опубликованных утечек в марте окончательно закрепил за Telegram статус основной площадки по распространению скомпрометированных данных (67% публикаций против 29% в 2022 году).

График 2

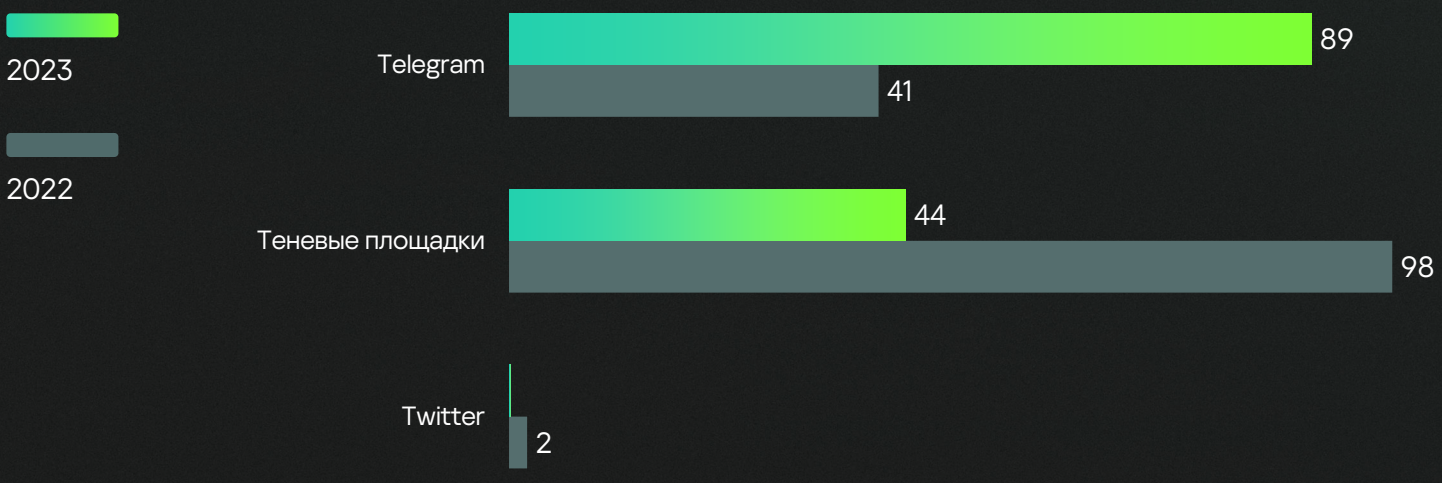
Распределение публикаций утечек данных и каналы распространения



Ситуация с распространением публичных баз данных в 2023 году кардинально противоположная 2022 году, когда основным каналом распространения утечек были теневые площадки. Предпосылок к снижению популярности Telegram, основного канала бесплатного распространения утечек, в ближайшее время не предвидится, несмотря на периодические блокировки отдельных сообществ, связанных с киберпреступными группировками.

График 3

Источник публикации утечки данных



Актуальность утечек данных

В 2023 году в результате 133 значимых утечек было опубликовано более 310 млн пользовательских данных:

315 337 785 пользовательских данных

Несмотря на небольшое снижение (6%), количества публикаций утечек в 2023 году, наблюдается рост 33% в объеме скомпрометированных данных.

Большинство опубликованных скомпрометированных данных (71%) датируется текущим годом, что говорит о том, что сами данные являются актуальными, а сами инциденты по компрометации этих данных произошли недавно.

2023

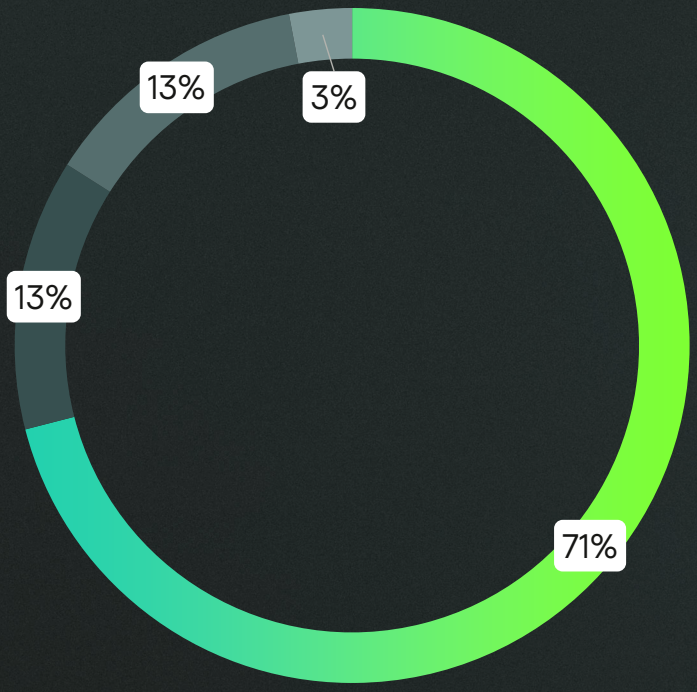
2022

2021

До 2021 (или не удалось установить)

Диаграмма 1

Предполагаемый год утечки



Действия злоумышленников носят системный характер, можно сказать, что атаки, направленные на компрометацию пользовательских данных, происходят регулярно.

55% опубликованных утечек размещались в свободном доступе в течение месяца после предполагаемой даты выгрузки из базы данных компании.

В течение месяца

До 2-х месяцев

От 2-х до 6 месяцев

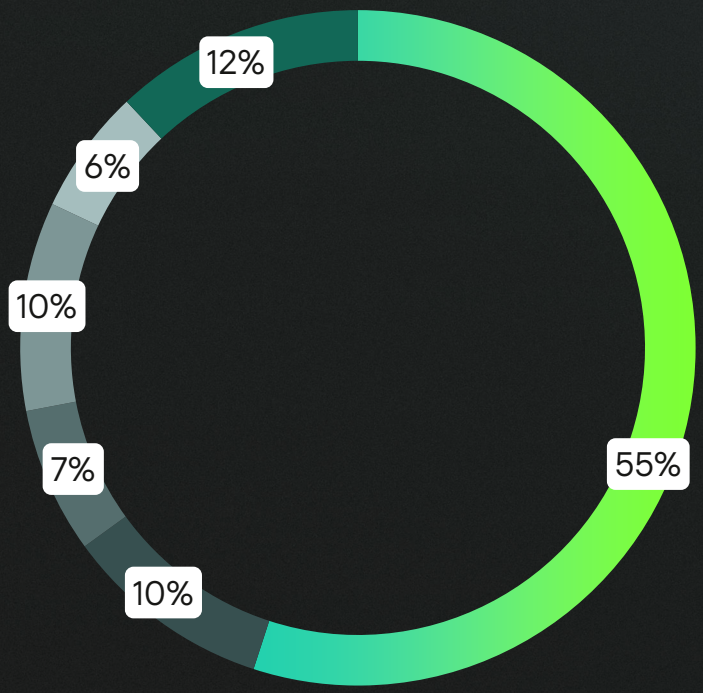
От 6 месяцев до года

Более года

Не установлено

Диаграмма 2

Интервал времени от утечки данных до публикации



Профиль жертвы

Как и в 2022 году, главный удар злоумышленников пришелся на компании из сферы «Ритейл» — 23% от всех опубликованных утечек. В первую очередь это объясняется преобладающим количеством организаций из данной сферы в российском бизнесе[1].

Третье место по количеству утечек занимают организации сферы «Финансов», где мы наблюдаем семикратный рост по сравнению с 2022 годом. Большой рост публичных инцидентов, связанных с утечками данных в 2023 году, произошел в организациях сферы «Здоровье» и IT-компаниях, когда в 2022 году данные сферы являлись менее пострадавшими от утечек.

Таблица 2

Топ-5 пострадавших отраслей от утечек данных

2022	2023
Ритейл	Ритейл
↓ Рестораны и доставки еды	↑ Интернет-сервисы
Интернет-сервисы	↑ Финансы (7 раз)
Карьера и образование	Карьера и образование
↓ Транспорт	↑ IT (3,5 раз)

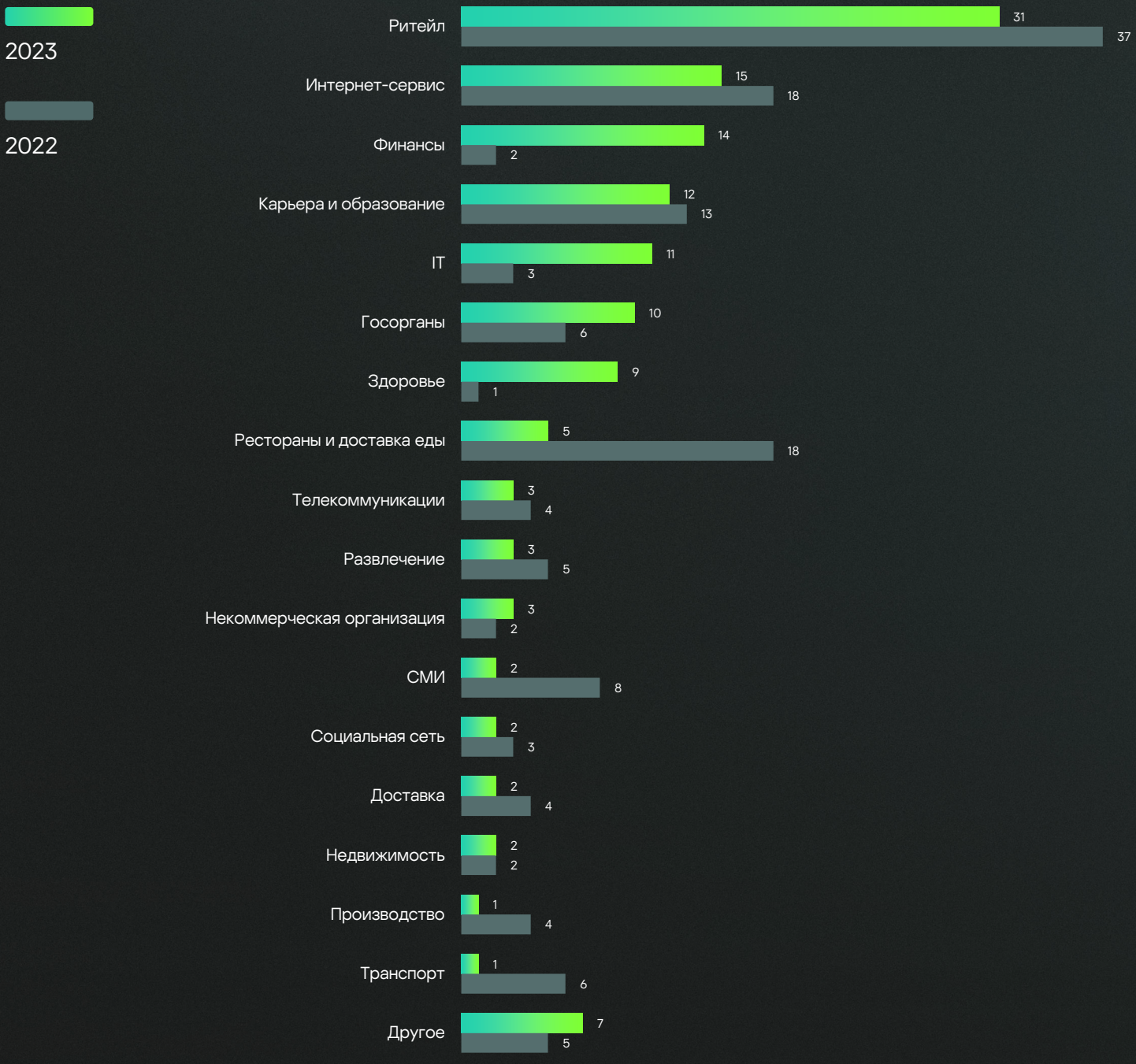
Увеличение количества атак на финансовые и IT-организации, в особенности на компании сферы «Здоровье», является неутешительным трендом 2023 года по причине критичности данных, которые обрабатываются и хранятся в этих компаниях.

[1] Раздел «Отрасли и экономика»

Подробнее

График 4

Количество утечек данных по отраслям



Большая часть данных включает информацию о пользователях ресурсов и/или их историю заказов. Базы данных сотрудников в 2023 году публиковались реже (2 публикации против 5 в 2022 году).

Лидерами по объему скомпрометированных данных являются компании из сферы «Ритейл» (49%) и «Финансы» (23%). На графике 5 показано соотношение опубликованных пользовательских данных год к году, где можем видеть значительный рост в таких сферах, как «Финансы», «Карьера и образование». Несмотря на значимость в количественном соотношении, что показывает интерес злоумышленников к определенным сферам, количество опубликованных данных в первую очередь зависит от размеров компаний и объемов хранимой информации, где произошла утечка.

График 5

Соотношение скомпрометированных пользовательских данных по отраслям

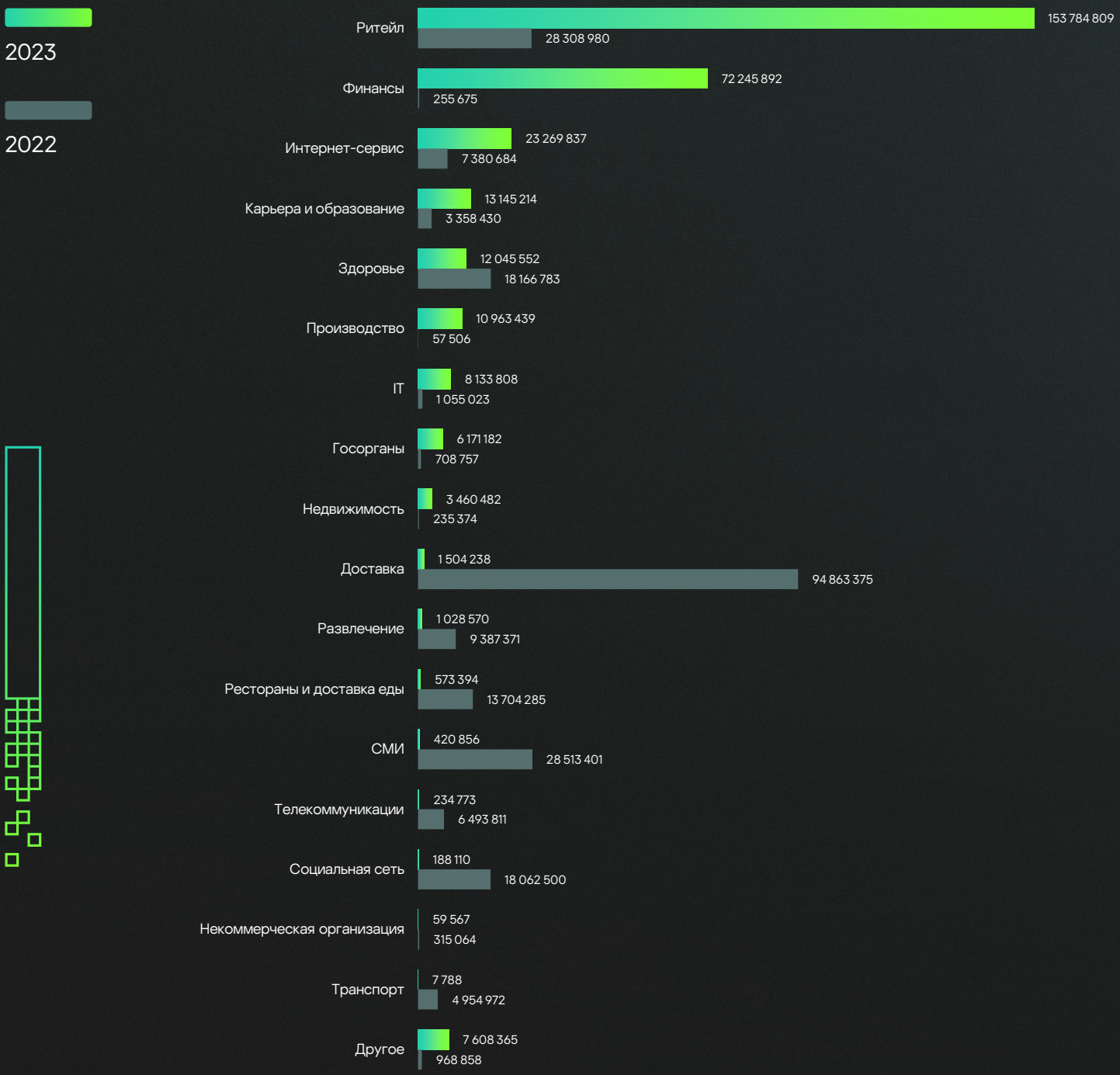


Таблица 3

Топ-5 отраслей по объемам скомпрометированных данных

2022	2023
Доставка	↑ Ритейл (5 раз)
СМИ	↑ Финансы (282 раза)
Ритейл	↑ Интернет-сервисы (3 раза)
Здоровье	↑ Карьера и образование (4 раза)
Социальные сети	↓ Здоровье

Топ-10 утечек по объемам данных содержат в себе 74% всех скомпрометированных данных, опубликованных в 2023 году.

В каких сферах были самые крупные утечки?

- 4 Ритейл
- 2 Финансы
- 1 Интернет-сервисы
- 1 Здоровье
- 1 Карьера и образование
- 1 Производство

Несмотря на то, что большинство атак, как и в прошлом году, направлено на представителей малого и среднего бизнеса, именно атаки на крупный бизнес оставляют больший общественный резонанс и значительную часть пользовательских данных (71%). Возможно, по этой причине количество публичных инцидентов, связанных с утечками данных, у представителей крупного бизнеса в 2023 году на 58% больше.

График 6

Количество утечек по пострадавшим компаниям

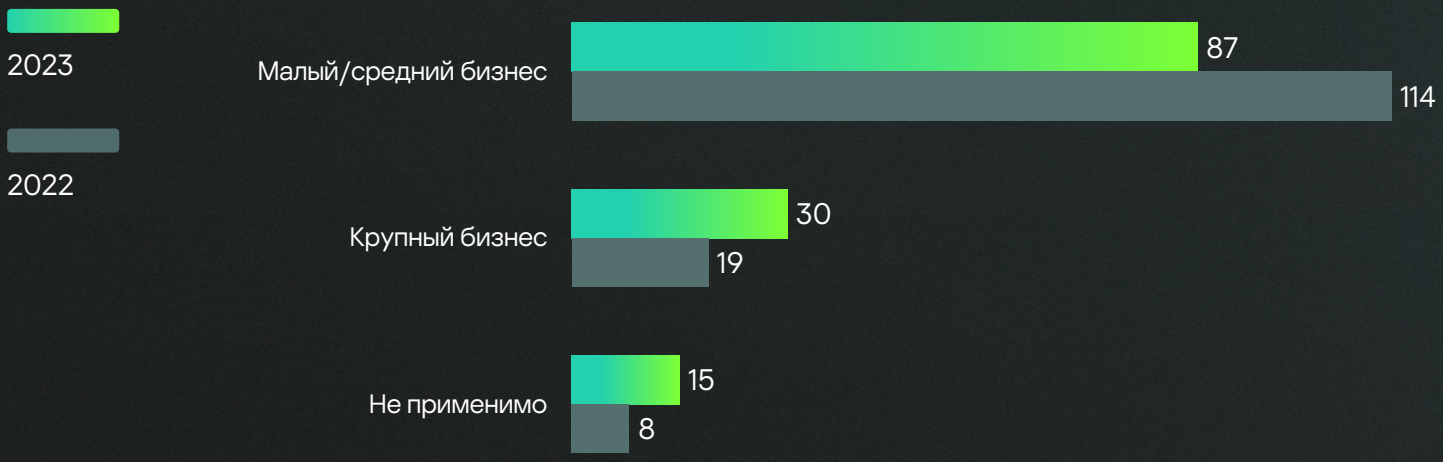


График 7

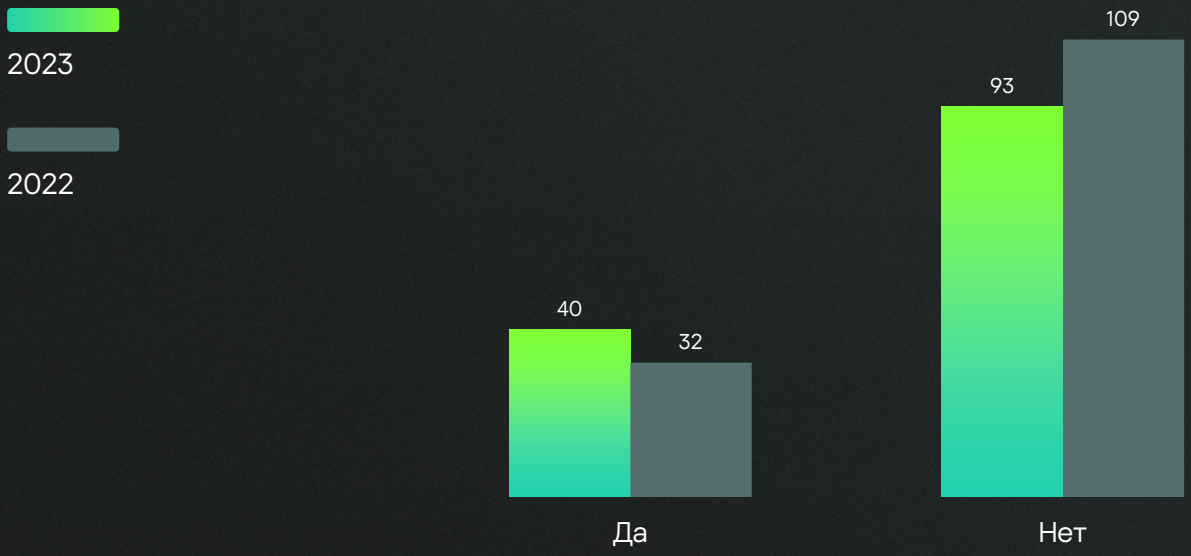
Объем утечек по пострадавшим компаниям

Реакция бизнеса

Мы наблюдаем положительную тенденцию в части наличия публичных реакций бизнеса на утечки данных. Но несмотря на предметный интерес СМИ к данной теме, наличие публичной реакции более свойственно представителям крупного бизнеса в случае масштабной или резонансной утечки.

График 8

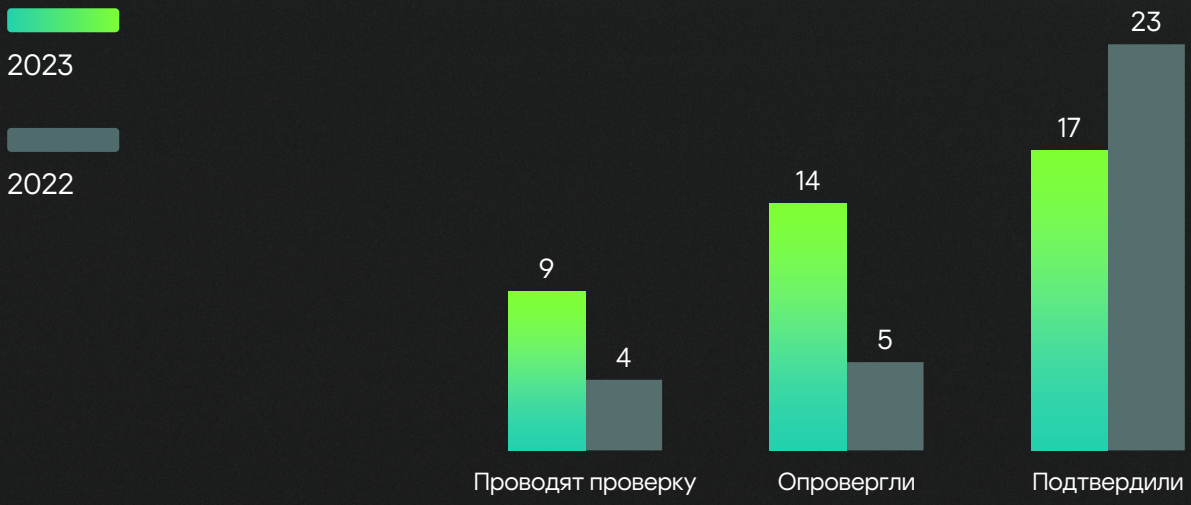
Наличие реакции на утечку данных



В 2023 году уменьшилось количество публично подтвержденных инцидентов; как результат — все больше компаний выбирают «осторожную» позицию либо полностью отрицают какой-либо факт утечки.

График 9

Реакция бизнеса на утечку данных



Облако тегов «Типовые комментарии представителей компаний по инцидентам об утечке данных»

Подрядчик
Проверкой занимаются правоохранительные органы
Фейк
Информация не соответствует действительности
Сгенерированные сведения
Не было никакого слива
Проводится внутреннее расследование
Скомпрометированный аккаунт
Компрометация ресурса
Подверглись хакерской атаке
Сторонний сервис
Проходит проверка
Материалы направлены в правоохранительные органы
Необходима проверка
Необходимо все проверить
Причины утечки устранены
Атака на сайт
Постороннего доступа к базам данным не зафиксировано
Взлом админ-панели
Причины утечки устранены
Атака на тестовый сервер
Сбоев не было
Персональные данные находятся в безопасности

Парольная информация

Компрометация парольной информации является одним из основных последствий утечек баз данных. Под угрозой находятся как личные аккаунты пользователей, так и корпоративные. Несмотря на проведение программ повышения осведомленности, пользователи часто используют корпоративные почтовые адреса для регистрации на сторонних ресурсах.

47 976 727

Строк, содержащих парольную информацию, было скомпрометировано злоумышленниками

Действительно пароли хранятся в базах данных преимущественно в хешированном виде, но в случае использования слабого алгоритма хеширования злоумышленник без труда может получить пароль в открытом виде, задействовав как свои вычислительные мощности, так и обратившись к специализированным сервисам, предоставляющим услуги расхеширования паролей.

Стоит отметить, что в части публикуемых баз данных злоумышленники целенаправленно удаляли столбцы, связанные с парольной информаций, что может говорить либо о параллельной/будущей продаже данных или намерении использовать их в других целях.

В 54%
опубликованных баз данных

содержалась парольная информация

В 8%
баз данных, содержащих парольную информацию,

пароли хранились в открытом виде. Преимущественно это небольшие интернет-сервисы, реализованные с использованием PHP.

Самым популярным алгоритмом хеширования является:

md5 (pass+salt)

- в 35% утечек, содержащих пароли
- используется в CMS 1C-Bitrix до версии 20.5.400

sha512-crypt

- в 13% утечек, содержащих пароли
- более защищенный алгоритм
- используется в современных версиях CMS 1C-Bitrix

md5

- в 18% утечек, содержащих пароли
- менее защищенный алгоритм

Kaspersky Digital Footprint Intelligence

Подробнее

Kaspersky Threat Intelligence

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее