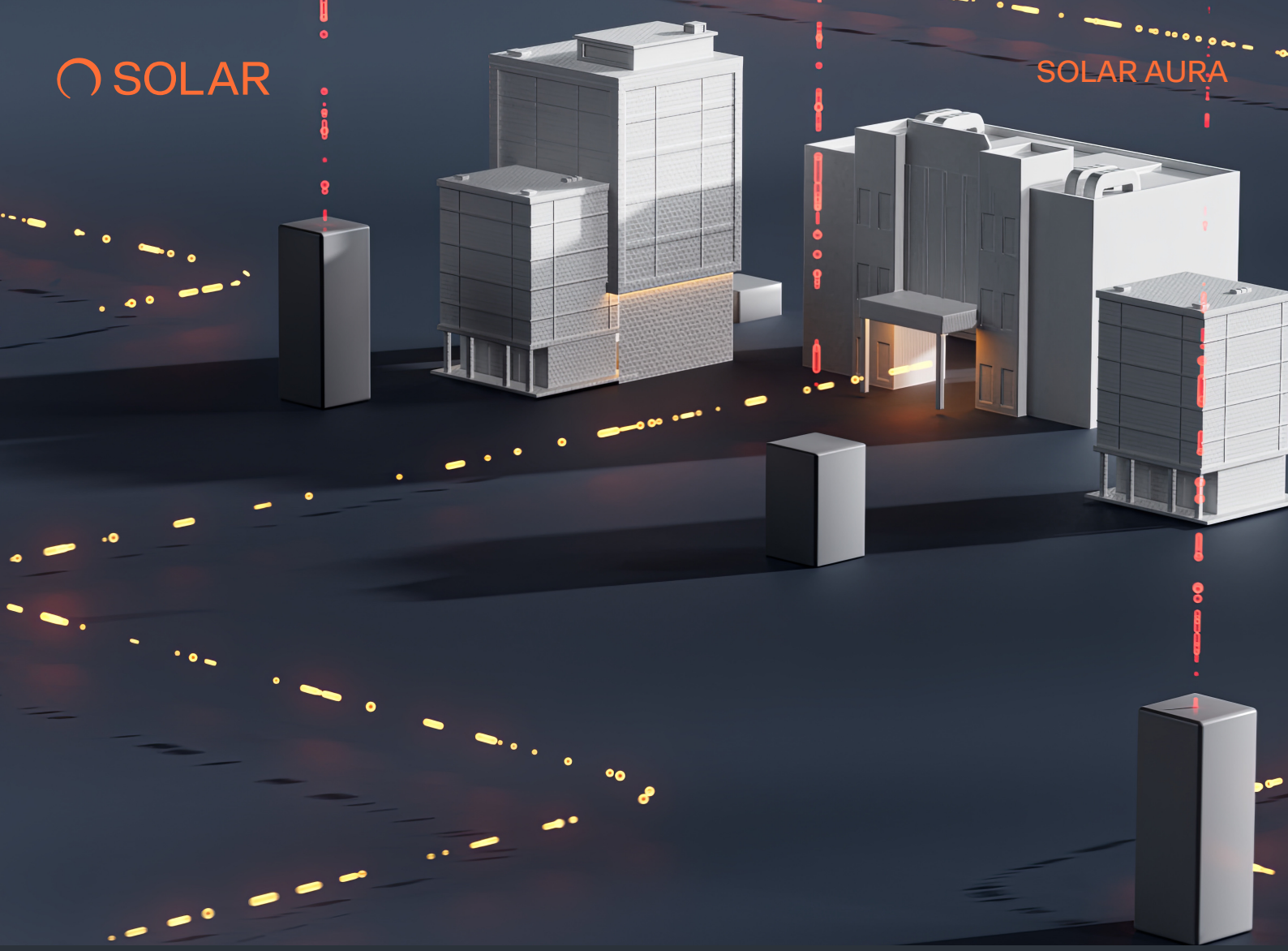
SOLAR

SOLAR AURA



ОТЧЕТ SOLAR AURA

Ключевые внешние цифровые угрозы для российских компаний в I-III кварталах 2024 года

W: RT-SOLAR.RU

I-III кв. 2024

СОДЕРЖАНИЕ

ОБ ОТЧЕТЕ

Отчет составлен на основе данных DRP-сервиса мониторинга внешних цифровых угроз Solar AURA ГК «Солар». Аналитика базируется на результатах мониторинга публичных и закрытых сегментов интернета по клиентам и пилотным проектам центра Solar AURA:

1,2+ МЛН

доменных имен и выданных SSL-сертификатов (пул источников динамически обновляется каждые сутки)

>2500

telegram-каналов противоправной тематики и даркнет-форумов

50 МЛН

DNS-запросов в сутки

Отчетный период включает январь – сентябрь 2024 года

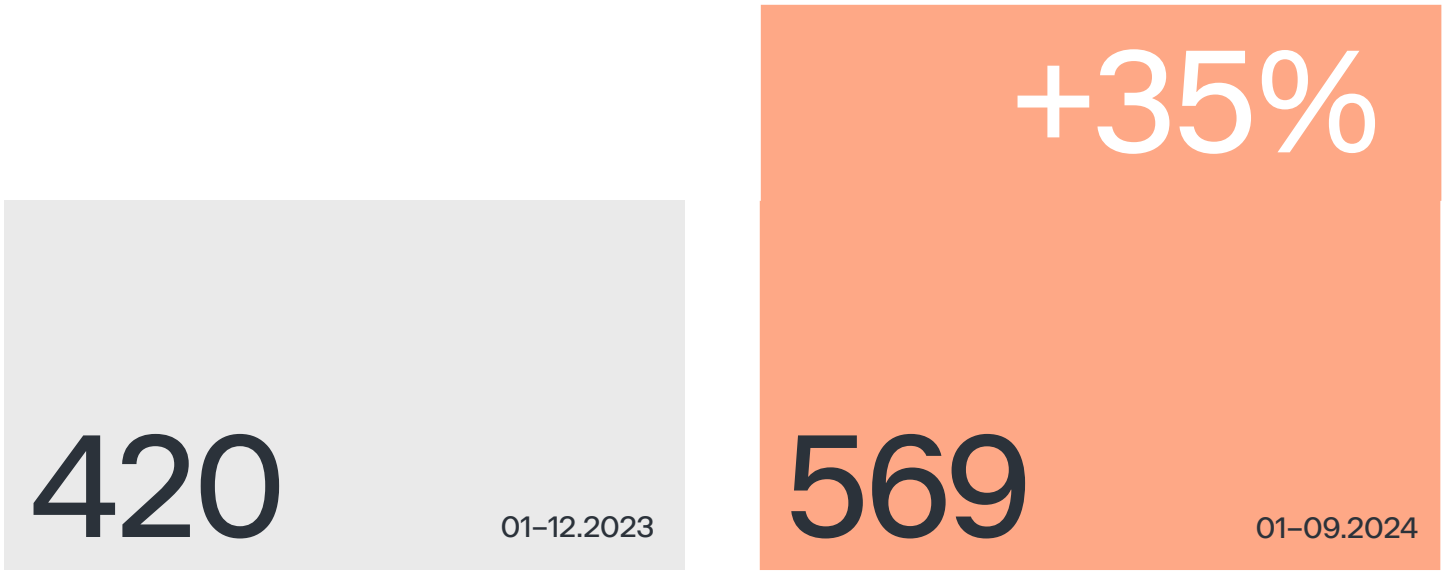
О СЕРВИСЕ SOLAR AURA

Сервис Solar AURA состоит из 8 модулей, которые могут подключаться отдельно или в комплексе:

АНТИФИШИНГ	Обеспечивает полный цикл противодействия фишингу: от выявления доменных имен и интернет-ресурсов, которые могут быть использованы в противоправных действиях в отношении заказчика или от его имени, до реализации комплекса мер по оперативной блокировке подобных ресурсов.
УТЕЧКИ	Помогает оперативно выявлять факты компрометации чувствительной для компании информации в публичных источниках.
ДАРКНЕТ	Помогает оперативно выявлять в даркнете и на иных ресурсах признаки угроз, нацеленных на компанию, таких как случаи публикации в Сети документов ограниченного доступа, баз данных, сведений о скомпрометированных аккаунтах, а также различного рода нелегальных услугах и готовящихся кибератаках.
БРЕНД КОМПАНИИ	Выявляет широкий перечень нарушений, затрагивающих бренд компании: от фейковых страниц в соцсетях и мессенджерах до мобильных приложений, использующих название и логотип организации или ее продукты.
ЛИЧНЫЙ БРЕНД	Отслеживает появление фейковых личных аккаунтов в соцсетях, случаи компрометации личных и корпоративных учетных данных, оценивает информационный фон вокруг персоналий компании, фиксирует появление негативных или компрометирующих публикаций.
МЕДИАПОЛЕ	Выявляет в открытом доступе публикации, способные негативно повлиять на информационную или экономическую безопасность компании, в частности сведения об используемых средствах защиты информации, регламентах работы, особенностях ИТ-инфраструктуры и т. п.
БЕЗОПАСНОСТЬ ФИНАНСОВ	Обнаруживает факты использования интернет-эквайринга банка для оплаты запрещенных в РФ услуг; собирает сведения о банковских картах, используемых при отмывании или обналичивании нелегальных денег; мониторит сайты с интернет-эквайрингом защищаемого банка на соответствие заявленному виду деятельности; предоставляет сведения для проверки контрагентов.
МОНИТОРИНГ ПЕРИМЕТРА	Сканирует корпоративные сервисы на наличие уязвимостей; ищет новые опубликованные в интернете ИТ-активы компании; контролирует контент сайта на предмет нелегитимных изменений.

КЛЮЧЕВЫЕ ФАКТЫ

Число инцидентов, связанных с утечкой данных, за 9 месяцев 2024 года в сравнении с аналогичным периодом 2023 года достигло 569, что на 35% превышает показатели всего прошлого года.



Украденные данные попадали в Сеть в частичном или полном объеме лишь в 55% случаев.

Число строк опубликованных данных уменьшилось на 85%, а общий объем – на 95%, до 5,4 терабайта.

В ряде случаев злоумышленники публиковали базы данные, полученные в прошлом году.

Число выявленных фишинговых ресурсов за 9 месяцев выросло на 116% в сравнении с тем же периодом прошлого года.

УТЕЧКИ ДАННЫХ

Утечки данных продолжают оставаться ключевой угрозой для российских организаций. Количество инцидентов, связанных с успешными атаками на российские организации, которые повлекли дефейс ресурсов, проникновение в инфраструктуру или кражу данных, за девять месяцев 2024 года выросло на 80% по сравнению с аналогичным периодом 2023 года.

С января по сентябрь 2024 года было зафиксировано 569 инцидентов – сообщений об утечках, включая случаи публикации баз данных российских компаний и сервисов. За 9 месяцев 2023 года количество инцидентов равнялось 315, а за весь предыдущий год было зафиксировано 420 таких случаев. Это означает, что количество инцидентов только за первые девять месяцев 2024 года уже превысило показатели всего 2023 года на 35%.

Отметим, что украденные данные попали в Сеть в частичном или полном объеме лишь в 55% случаев (316 инцидентов) – о ряде инцидентов можно судить лишь по фрагментам опубликованных баз, архивов или по отчетам хакерских группировок. Также зафиксированы случаи публикации в общем доступе баз данных, которые были получены злоумышленниками в 2023 году, но до 2024 года не фигурировали в свободном доступе. Помимо этого было зафиксировано 120 случаев дефейса сайтов российских организаций.

Отдельно отметим, что за отчетный период значительно уменьшилось количество строк опубликованных данных – на 83%: с 4,7 млрд за девять месяцев прошлого года до 800 млн в этом году.

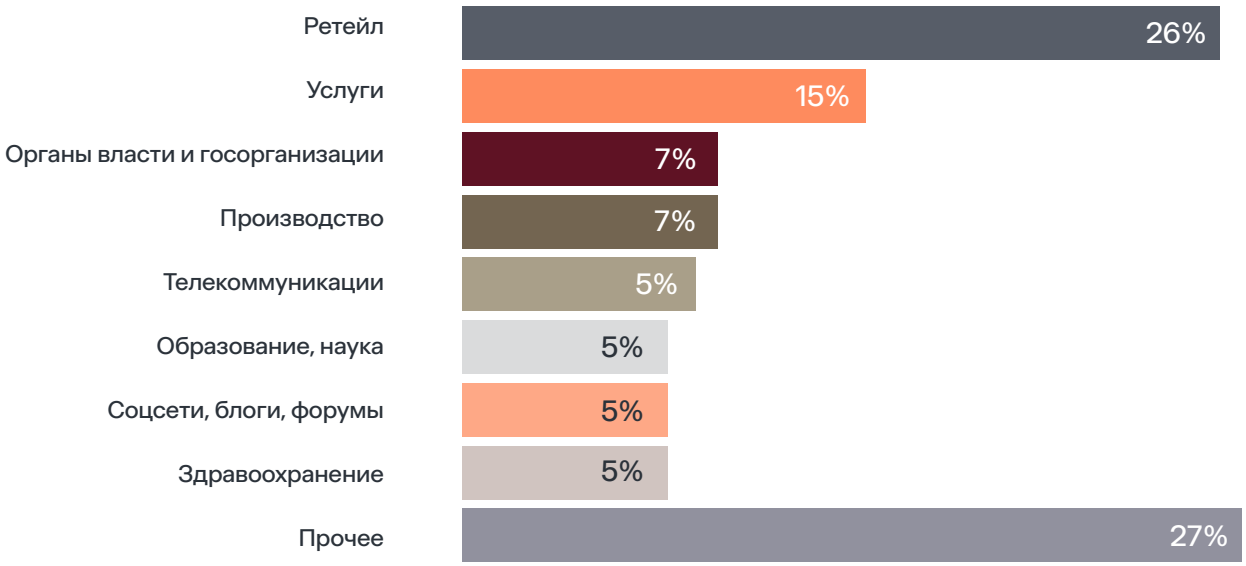
Означает ли это, что красть стали чаще, но меньше? В целом да, но здесь мы рискуем попасться на уловку статистики. Дело в том, что иногда один инцидент может в корне изменить общую картину, если мы говорим об объеме украденной информации. Так и произошло в 2023 году, когда в сентябре злоумышленниками была выложена всего одна база одной компании, содержащая 4 миллиарда строк с преимущественно технической информацией. Если мы исключим этот инцидент из статистики, то получим 700 миллионов строк в 2023 году и 800 миллионов – в 2024-м.

Объем попавших в открытый доступ конфиденциальных данных за 9 месяцев текущего года также уменьшился на 95% – 5,4 терабайта против 102,8 терабайта за тот же период прошлого года. Но к концу года ситуация может легко измениться, ведь впереди еще три месяца.

На первом месте по количеству инцидентов, связанных с утечками данных или успешными атаками на сетевые ресурсыорганизаций, находится ретейл – на данный сектор пришлось 182 зафиксированных случая. Второе место опять же традиционно занимает сфера услуг (101 инцидент). А вот на третьем месте обосновался государственный сектор, включающий как органы государственной власти, так и органы власти субъектов, а также местного самоуправления (45 инцидентов).

Далее с минимальным отрывом следует сегмент образования и науки (42 инцидента), а за ним – производственный сектор (38 инцидентов) и телекоммуникации (37 инцидентов).

РАСПРЕДЕЛЕНИЕ УТЕЧЕК ПО КОЛИЧЕСТВУ ИНЦИДЕНТОВ В ОТРАСЛЯХ



Распределение мест с третьего по шестое очень хорошо демонстрирует мотивацию злоумышленников в современных условиях, когда мы наблюдаем существенный всплеск хактивизма, основной целью которого является нанесение вреда экономике нашей страны, системе ее госуправления, а также высококритичным для государства отраслям, таким как наука и производство.

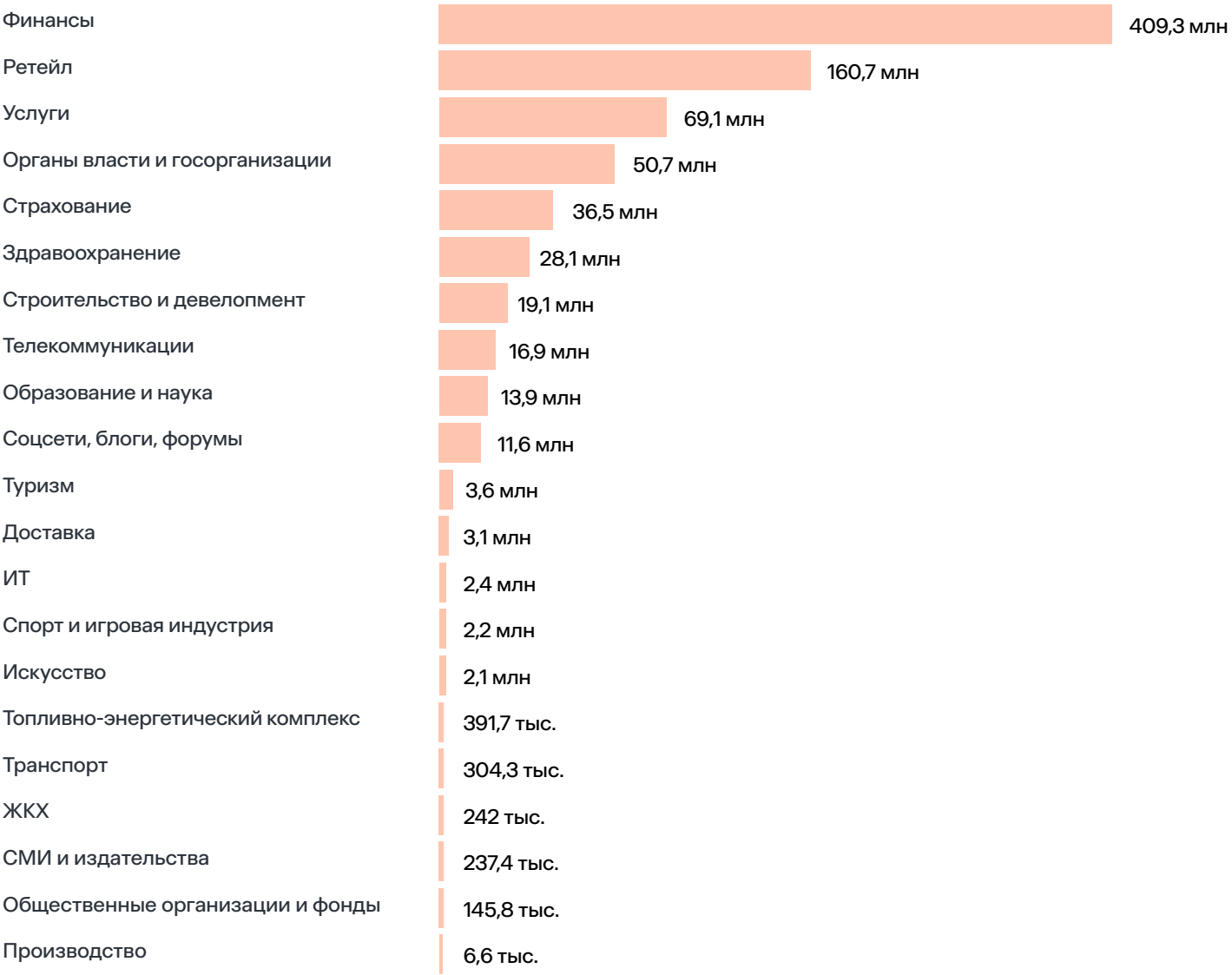
Как отмечалось выше, не все инциденты привели к публикации баз данных в общем доступе. Всего в даркнете было зафиксировано 316 случаев публикации баз данных или их фрагментов, причем в ряде случаев выставлялись базы, похищенные в 2023 году или ранее, а также некоторые базы являются результатом парсинга данных, а не злонамеренного воздействия на инфраструктуру. Среди этих случаев лидирует так же ретейл – 123 случая публикации баз данных. На втором месте (30 инцидентов) находится сфера услуг, далее следуют соцсети и блоги (27) и финансовый сектор (22). Пятое место делят наука и образование, а также здравоохранение (по 18 случаев на отрасль).

Если составить рейтинг по количеству утекших строк данных, то тут на первое место выйдет уже финансовый сектор с показателем в 409 млн строк. Впрочем, ретейл и здесь будет в тройке лидеров – 160 млн строк данных.

316

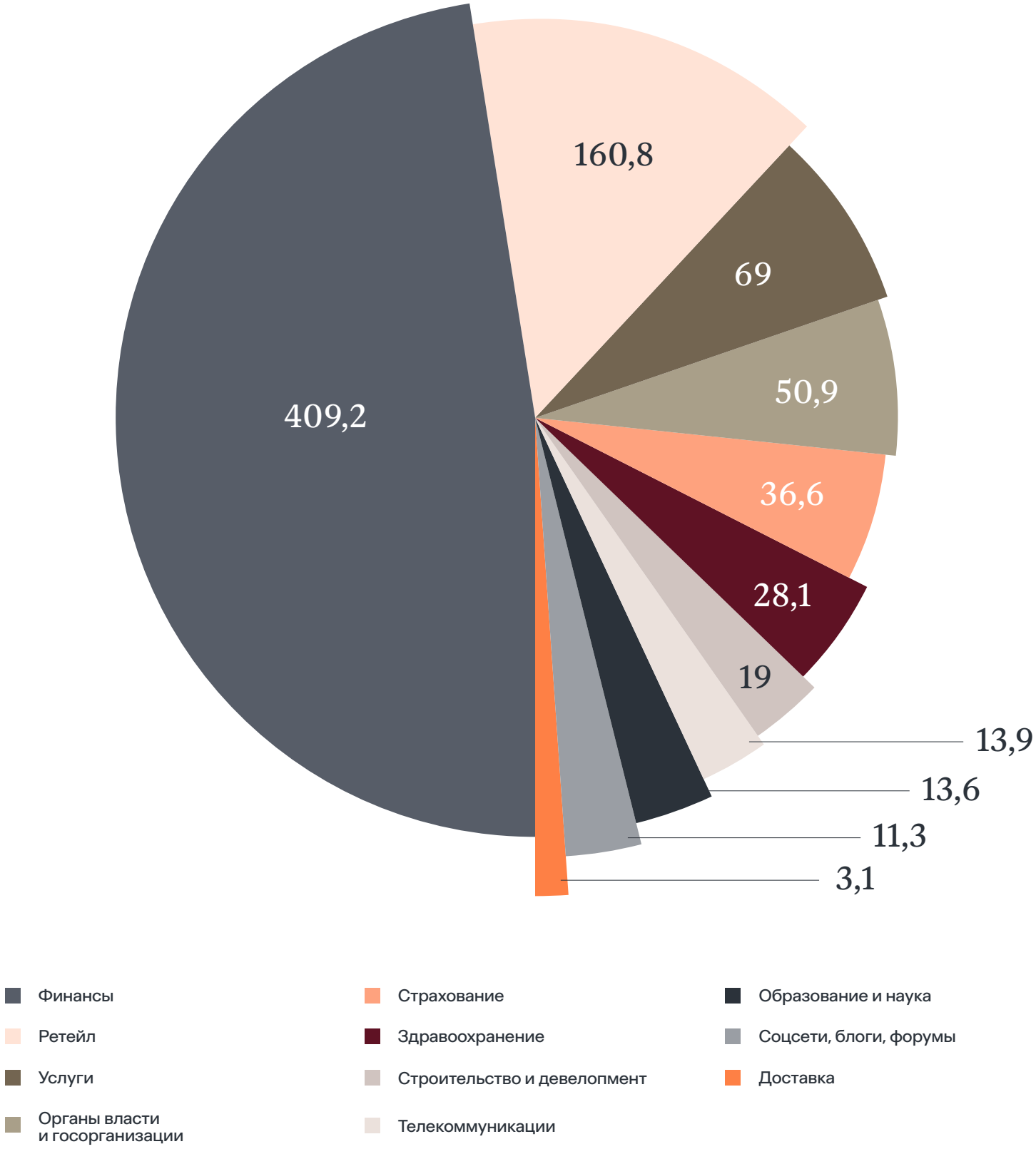
случаев публикации баз данных или их фрагментов было зафиксировано в даркнете

РАСПРЕДЕЛЕНИЕ УТЕЧЕК ПО КОЛИЧЕСТВУ СТРОК

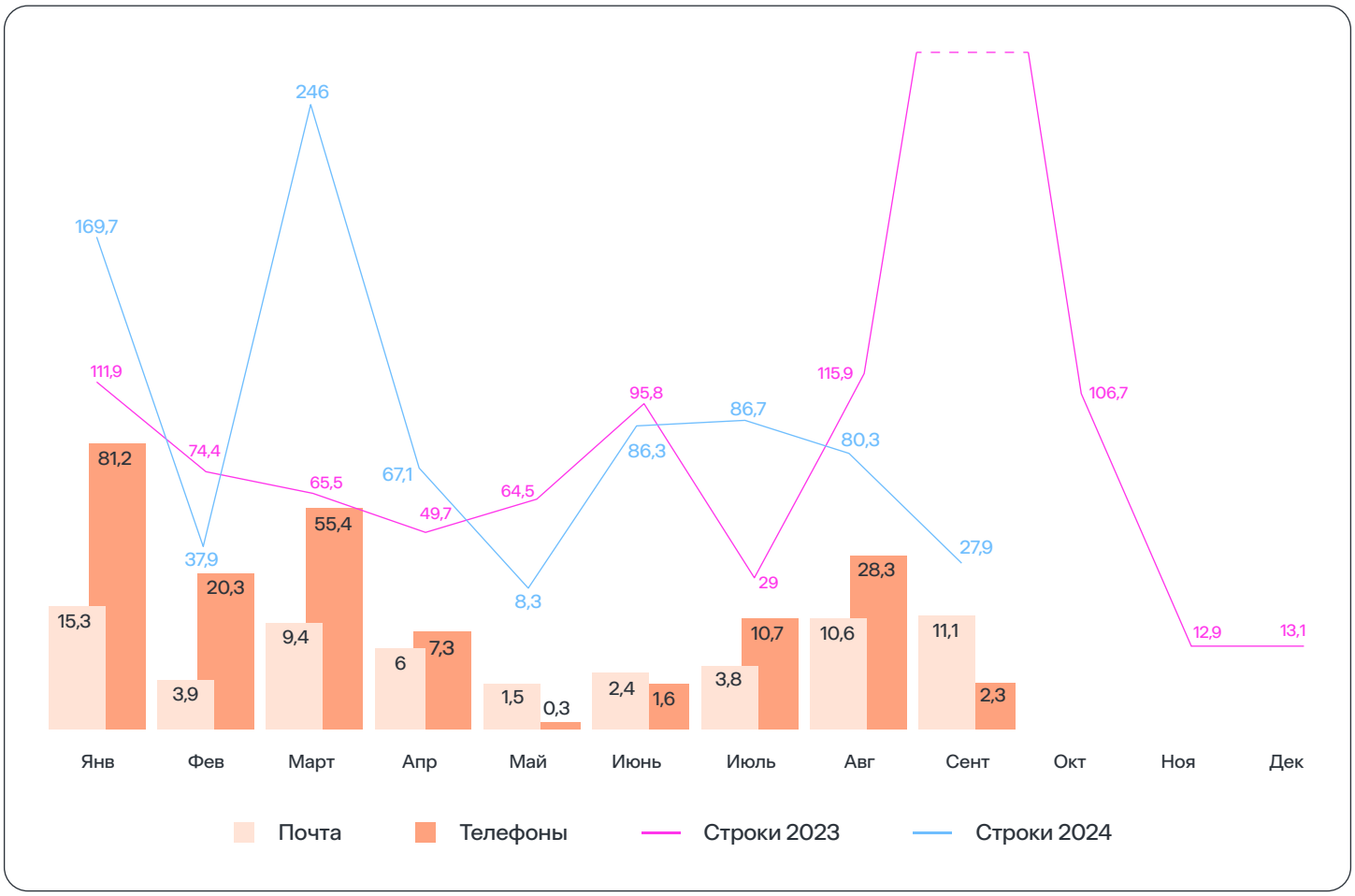


Для наглядности делимся двумя другими вариантами диаграммы

РАСПРЕДЕЛЕНИЕ УТЕЧЕК ПО ОТРАСЛЯМ, МЛН



РОССИЙСКИЕ УТЕЧКИ ПО МЕСЯЦАМ: СТРОКИ, ПОЧТА, ТЕЛЕФОНЫ, МЛН



АНТИФИШИНГ

В настоящий момент фишинг переживает свой расцвет. Количество фишинговых ресурсов существенно увеличилось по сравнению с предыдущим годом, а сложность фишинговых атак значительно возросла.

Одной из ключевых тенденций развития фишинга в 2024 году является массовое использование доменов 3-го и более глубоких уровней. Рекорд, который мы встречали, – 7 уровней. Так, например, в случае с фишингом от имени маркетплейсов, количество подобных доменных имен превышает 50%. Зачастую один домен второго уровня имеет несколько, а то и десятки поддоменов под разные маркетплейсы.

Другая важная тенденция – использование доменов без упоминания брендов, которые сложнее обнаружить. Если год назад количество доменов, не схожих с официальными доменными именами, от имени которых осуществляется атака, колебалось на уровне 16%, то в 2024 году до 40% фиксируемых нами фишинговых ресурсов не имеет смысловой связки с брендом. А в случае с теми же маркетплейсами процент внебрендовых доменов достигает 70%.

Подобная ситуация заставляет изобретать все новые механизмы анализа доменных имен и веб-сайтов в целях выявления фишинговых атак.

116%

За 9 месяцев 2024 года сервисом AURA было выявлено и заблокировано на 116% больше фишинговых ресурсов, чем за аналогичный период 2023 года.

В то же время стоит отметить прогресс в прекращении функционирования выявленных фишинговых ресурсов. На сегодняшний день среднее время блокировки фишингового сайта сервисом Solar AURA составляет чуть более четырех часов, а более 50% вредоносных ресурсов блокируется еще быстрее.

Таких показателей удалось достичь как за счет применения широкого спектра технических решений и автоматизации работы с жалобами на фишинг, так и за счет повышения уровня взаимодействия с регистраторами доменных имен, хостинг-провайдерами, а также другими организациями, вовлеченными в процесс борьбы с фишингом.

Наиболее частые схемы неперсонифицированных фишинговых атак, нацеленных на физических лиц:

Кража аккаунтов Telegram и WhatsApp

Злоумышленники используют самые разные информационные подводки для того, чтобы убедить жертву перейти на фишинговую страницу, на которой потребуется ввести номер телефона, пароль и код из СМС от аккаунта в мессенджере. Такими подводками могут быть онлайн-голосования (например – за детский рисунок, подписание петиции и множество других информационных поводов). Получая доступ к аккаунту жертвы, злоумышленники выкачивают всю актуальную информацию, включая переписки, файлы, фотографии и прочее, а также рассылают веером сообщения с просьбой одолжить денег или ссылками на очередные фишинговые сайты. Отдельно отметим, что вариативность подобных схем крайне высока.

Фейковые инвестиционные платформы

Подвид схемы работы телефонных мошенников. Сначала мошенники создают сайты, предлагающие заработать на инвестициях. Если жертва соглашается и оставляет свои персональные данные, с ней связывается по телефону «персональный менеджер» и в дальнейшем делает все, чтобы жертва «инвестировала» как можно большую сумму.

Данная схема существует уже более 5 лет и ничуть не теряет своей актуальности. Ежедневно мы фиксируем появление нескольких десятков новых подобных сайтов.

«Помощь» пострадавшим инвесторам

Мошенники создают сайты, предлагающие оформить возврат похищенных денежных средств для тех, кто пострадал от действий фейковых инвесторов. После с жертвой связывается мошенник и под видом юриста или инвестиционного консультанта вытягивает из жертвы оставшиеся денежные средства.

Обман при покупке и продаже на маркетплейсах

Вариаций этой схемы довольно много: это и классическое мошенничество на сайтах объявлений, и различного рода схемы, когда продавец на маркетплейсе связывается с покупателем и просит его оформить возврат или переказать товар, а затем присылает фишинговую ссылку с просьбой ввести данные для оплаты, после чего клиент теряет деньги. Все варианты перечислить сложно. Но их объединяет один момент – в конечном счете жертва попадет на фишинговый сайт, на котором потребуется ввести данные карты, что приведет к потере денежных средств.

Фейковые розыгрыши и акции от известных брендов

Классические схемы с «коробочками» – открой подарок и выиграй приз. Имеются сотни подвидов данной схемы, существующей уже порядка десяти лет. Количество вредоносных ресурсов стремится к бесконечности и снижаться не намерено.

Фейковые лотереи

Мошенники создают фейковые сайты популярных существующих лотерей или якобы новых платформ. По традиции каждый пользователь оказывается победителем, а для получения приза необходимо либо ввести данные карты, либо оплатить несуществующую комиссию. Пользователь не получает выигрыша, а лишь теряет деньги.

Фейковые опросы и социальные выплаты

Очень часто фейковые сайты используются для взлома аккаунтов на Госуслугах. Суть заключается в том, что пользователь проходит опрос или ему предлагается выплата от государства, но для ее получения необходимо либо заплатить налог или комиссию, либо авторизоваться через портал госуслуг.

ВЫВОДЫ

Сохраняется тенденция к росту числа преступлений, совершаемых с использованием информационных или телекоммуникационных технологий

В современных условиях любая организация или любой человек могут быть атакованы, и нынешняя ситуация должна стать серьезным мотиватором, заставляющим нас пересмотреть отношение к информационной безопасности, как в разрезе бизнеса, так и в контексте частной жизни каждого человека.

SOLAR

W: RT-SOLAR.RU
W: RT.RU

T +7 (499) 755-07-70
E solar@rt-solar.ru

Центральный офис, 125009, Москва
Никитский переулок, 7с1