SOLAR

ОТЧЕТ

ОТЧЕТ ОБ АТАКАХ НА ФИНАНСОВЫЙ СЕКТОР В 2023 ГОДУ

W: RT-SOLAR.RU

МОСКВА 2024

СОДЕРЖАНИЕ

О КОМПАНИИ

Группа компаний «Солар» — архитектор комплексной кибербезопасности. Ключевые направления деятельности — аутсорсинг ИБ, разработка собственных продуктов, обучение ИБ-специалистов, аналитика и исследование киберинцидентов.

С 2015 года предоставляет ИБ-решения организациям от малого бизнеса до крупнейших предприятий ключевых отраслей. Под защитой «Солара» — более 850 крупнейших компаний России. Продукты и сервисы «Солара» объединены в домены экспертизы: Безопасная разработка программного обеспечения, Управление доступом, Защита корпоративных данных, Детектирование угроз и хакерских атак. Домены экспертизы закрывают все потребности заказчиков и включают собственные разработки, решения партнеров, услуги по созданию стратегии и архитектуры ИБ, консалтинг, обучение персонала.

Компания предлагает сервисы первого и крупнейшего в России коммерческого SOC — Solar JSOC, экосистему управляемых сервисов ИБ — Solar MSS. Линейка собственных продуктов включает DLP-решение Solar Dozor, шлюз веб-безопасности Solar webProxy, межсетевой экран нового поколения Solar NGFW, IdM-систему Solar inRights, PAM-систему Solar SafeInspect, анализатор кода Solar appScreener и другие.

ГК «Солар» развивает платформу для практической отработки навыков защиты от киберугроз «Солар Кибермир». Работа центра исследования киберугроз Solar 4RAYS нацелена на изучение тактик киберпреступников. Полученные аналитические данные обогащают разработки Центра технологий кибербезопасности.

Группа компаний «Солар» инвестирует в развитие отрасли кибербезопасности и помогает решать проблему кадрового дефицита. Совместно с Минцифры в рамках национального проекта «Цифровая экономика» реализует всероссийскую программу кибергигиены, направленную на повышение цифровой грамотности населения.

Штат компании — более 2000 специалистов. Подразделения «Солара» расположены в Москве, Санкт-Петербурге, Нижнем Новгороде, Самаре, Ростове-на-Дону, Томске, Хабаровске и Ижевске. Технологии компании и наличие распределенных по всей стране центров компетенций позволяют ей работать в режиме 24/7.

АРХИТЕКТОР КОМПЛЕКСНОЙ КИБЕРБЕЗОПАСНОСТИ

2000+
экспертов
по кибербезопасности

850+
организаций
под защитой

600+
реализованных
проектов в год

180+ МЛРД
анализируемых
событий ИБ в сутки

ОБ ОТЧЕТЕ

Настоящий отчет посвящен анализу состояния кибербезопасности в финансовом секторе в 2022-2023 гг.

ИССЛЕДОВАНИЕ ВКЛЮЧАЕТ:

01

Данные об атаках на инфраструктуры клиентов ГК «Солар»:

- центра противодействия кибератакам Solar JSOC
- сервисов защиты WAF и Anti-DDoS экосистемы Solar MSS

02

Данные мониторинга внешних киберрисков:

- центра мониторинга внешних цифровых угроз Solar AURA

03

Результаты исследования экономики ИБ в финансовом секторе

КЛЮЧЕВЫЕ ТЕЗИСЫ

- В 2023 году Solar JSOC зафиксировал 6,8 тыс. киберинцидентов в кредитно-финансовом секторе. Большая их часть связана с эксплуатацией уязвимостей и несанкционированным доступом к системам и сервисам.
- Попытки взлома баз данных и использования учетной записи сотрудника третьими лицами — сценарии кибератак, свойственные именно банковской отрасли.
- Количество фишинговых атак на банки выросло в полтора раза с начала 2023 года. Этот вектор по-прежнему остается достаточно эффективным, несмотря на высокую степень защищенности отрасли.
- За 2023 год в общий доступ попало более 161 млн строк, содержащих персональные данные клиентов финорганизаций.
- Количество кибердаров по банковским веб-ресурсам (DDoS- и веб-атаки) постепенно сокращается, что объясняется высокой защищенностью организаций и неэффективностью массовых атак.
- Финансовая отрасль занимает первое место по размеру бюджетов на ИБ: в 2023 году на эти цели организации потратили 18 млрд рублей.

6,8 ТЫС.

киберинцидентов в кредитно-финансовом секторе в 2023 году зафиксировал Solar JSOC

161+ МЛН

строк, содержащих персональные данные клиентов финорганизаций, попало в общий доступ в 2023 году

18 МЛРД РУБ.

российские финорганизации потратили на ИБ в 2023 году

40%

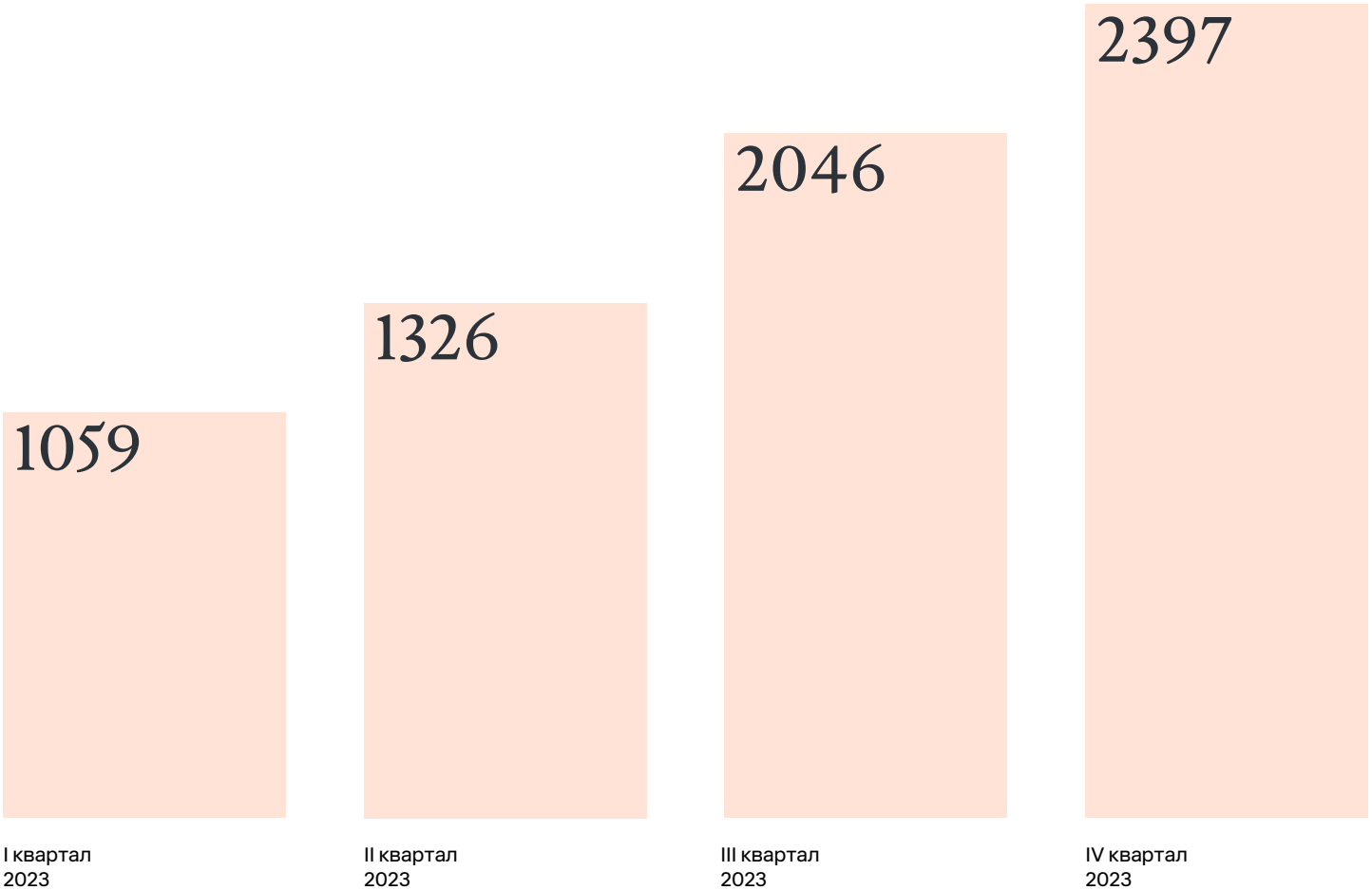
объявлений о нелегальных услугах в даркнете связано с банками

СВОДНАЯ СТАТИСТИКА ИНЦИДЕНТОВ В ИНФРАСТРУКТУРАХ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

В этом разделе представлены данные мониторинга киберинцидентов в инфраструктурах клиентов центра противодействия кибератакам Solar JSOC.

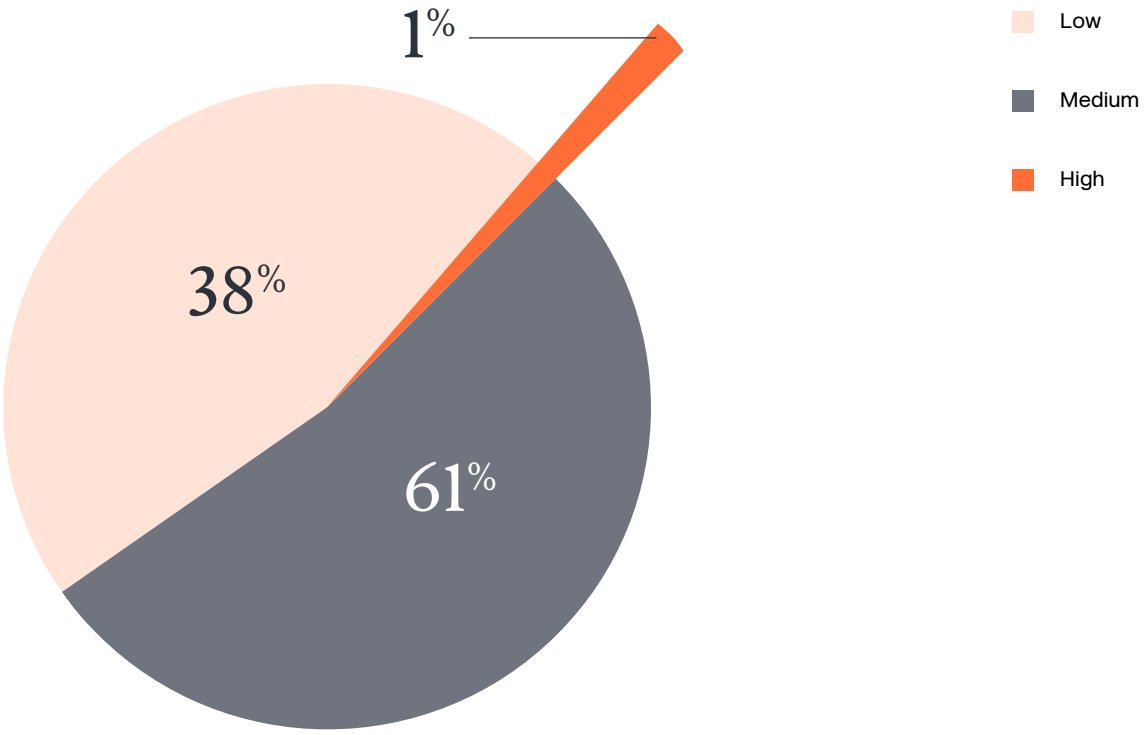
В 2023 году Solar JSOC зафиксировал 6,8 тыс. киберинцидентов в кредитно-финансовом секторе, что составляет пятую часть (20%) от общего числа выявленных инцидентов ИБ. При этом за последние два года количество событий ИБ в банках выросло на 75%, что немного ниже средних показателей в других отраслях (где рост составил 90%).

Распределение инцидентов ИБ
в финансовом секторе в 2023 году



За год количество инцидентов в банковской отрасли увеличилось более чем на четверть, что объясняется возросшей квалификацией злоумышленников. Как мы помним, в 2022 году большинство киберинцидентов в разных отраслях было связано с массовыми атаками, которые редко были направлены на такие хорошо защищенные организации, как банки. Целевых атак, которые требуют от хакеров технической подкованности и финансовых вложений, было меньше. Сейчас же мы видим более тщательную подготовку со стороны хакеров и, как следствие, рост сложных атак. В частности, кибердарам предшествует киберразведка и первичное проникновение в инфраструктуру (возможно, с посредничеством внутреннего нарушителя). Этому также способствует большое количество утечек, произошедших за последние полтора года, когда в открытый доступ попало множество данных, включая сведения о корпоративных аккаунтах.

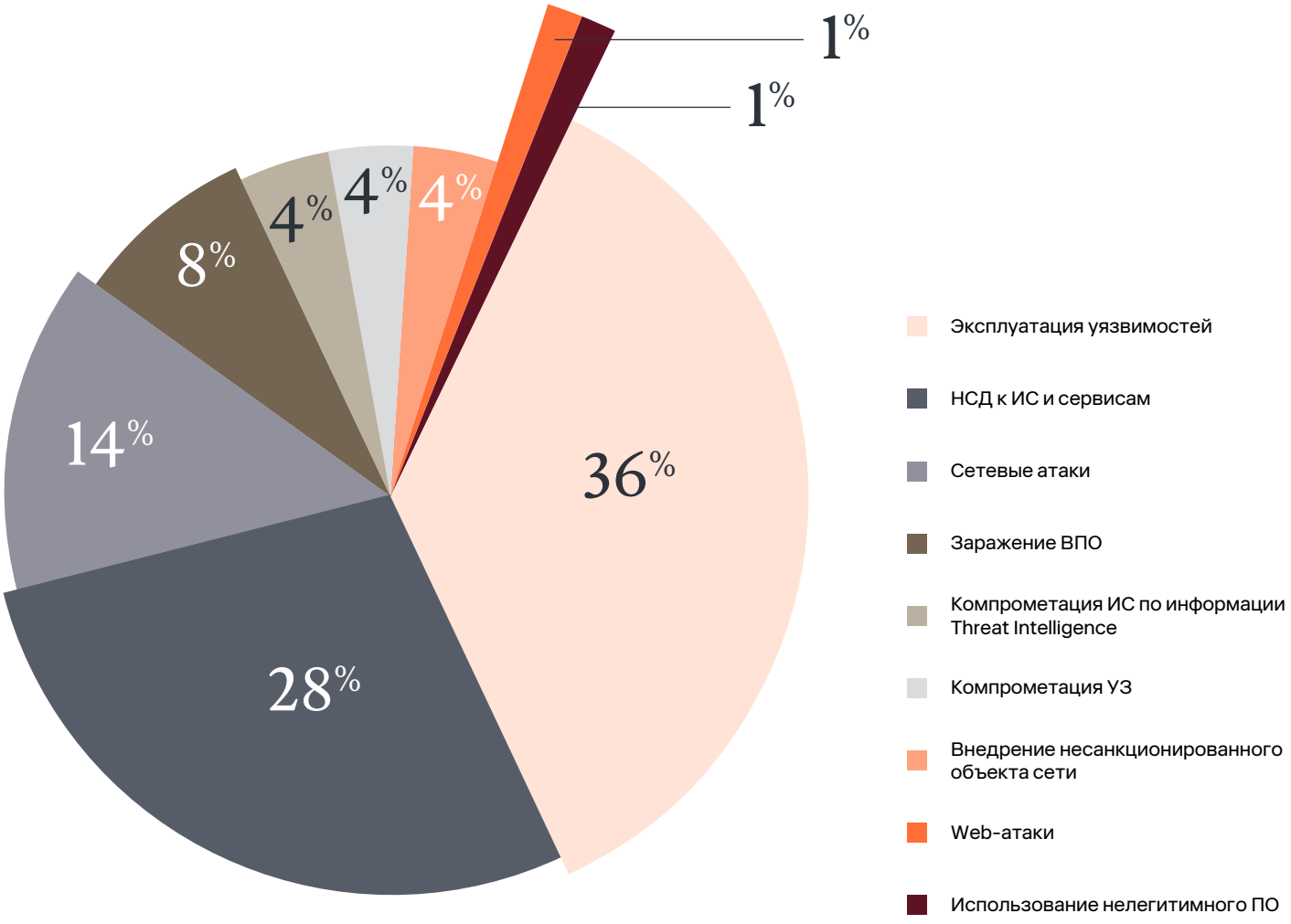
Распределение инцидентов
в финсекторе по критичности в 2023 году



На фоне растущей угрозы организации стремятся подключить к ИБ-мониторингу как можно больше объектов инфраструктуры, но зачастую это упирается в технологические ограничения SIEM-систем, поэтому с учетом повышения сложности атак все большую роль играют сенсоры и специализированные решения (такие, как NTA, EDR и проч.).

Отметим, что Solar JSOC ежегодно запускает порядка 20 новых сценариев выявления киберинцидентов в финансовых организациях. При том что в других отраслях этот показатель не превышает 10.

Распределение инцидентов
по типам в 2023 году



Больше трети инцидентов в банковском секторе связано с эксплуатацией уязвимостей. Уязвимости используются хакерами на всех этапах развития атаки: при попытках взлома веб-ресурсов, приложений и сервисов жертвы, при горизонтальном продвижении по сети и повышении привилегий на хосте, при попытках компрометации систем банка внутри инфраструктуры. Именно поэтому регулярный патч-менеджмент и налаженный процесс управления уязвимостями остается основой построения безопасной инфраструктуры.

Также все больше инцидентов происходит по причине несанкционированного доступа к системам и сервисам. В контексте банка это, например, компоненты автоматизированной банковской системы (АБС) и дистанционного банковского обслуживания (ДБО), внутренние системы документооборота, ключевые базы данных.

Примечательно, что на заражение вредоносным ПО приходится только 4% всех инцидентов в банковской сфере.Это показывает высокий уровень зрелости финансовых организаций, благодаря которому обеспечивается высокий уровень базовой защиты ИТ-инфраструктуры: антивирусная защита и соблюдение политик ИБ сотрудниками. Именно они чаще всего являются причиной срабатывания данного сценария выявления инцидентов.

Далее рассмотрим топ-10 сигнатур[1] за 2023 год в финансовой отрасли и сравним с аналогичной статистикой во всех отраслях.

Топ-10 сигнатур в финсекторе

8%	Отсутствие в профиле аутентификации
7%	Внутреннее сетевое сканирование
7%	Экспорт данных виртуальной машины
6%	Срабатывание критичной сигнатуры СЗИ
4%	Использование УЗ сотрудника
3%	Многочисленные блокировки учетной записи
3%	Отключение антивирусного ПО на критичном хосте
3%	Отклонение от профиля использования служебных УЗ СУБД ORACLE
3%	Обнаружение индикатора компрометации Threat Intelligence
3%	Отключение антивирусного ПО на хосте

[1] Сигнатура — конкретный сценарий выявления инцидентов.

Топ-10 сигнатур во всех отраслях

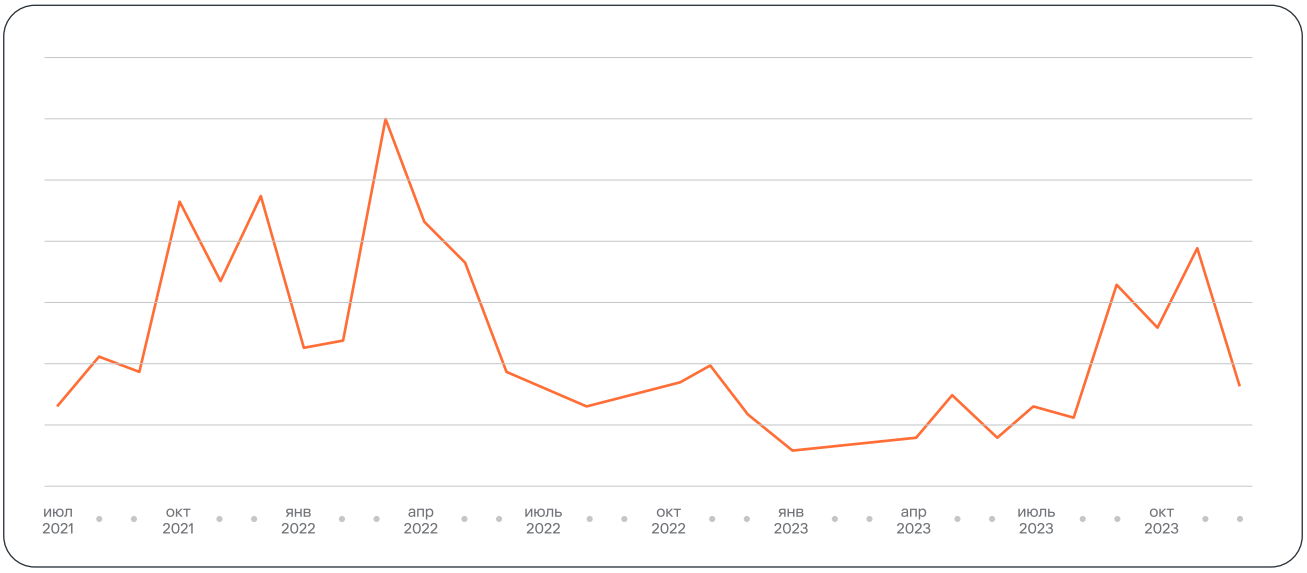
6%	Отсутствие в профиле аутентификации
4%	Попытка подбора пароля на критичных системах
4%	Обнаружен вирус на хосте
4%	Срабатывание критичной сигнатуры СЗИ
3%	Обнаружение индикатора компрометации Threat Intelligence
3%	Попытка подбора пароля
3%	Внутреннее сетевое сканирование
2%	Установка ПО на критичном хосте
2%	Модификация критичных веток реестра
2%	Обнаружение сетевой атаки средствами АВПО

Распределение долей наиболее популярных типов инцидентов в финансовом секторе практически совпадает со статистикой по остальным отраслям. Однако в аналитике по банкам в явном виде присутствуют сценарии, связанные с базами данных (СУБД), которые используются в основных банковских приложениях (ДБО, АБС и др.). Это нетиповые сценарии, реализуемые именно в банковской сфере, ведь все значимые конфиденциальные данные отрасли (персональные, финансовые) находятся именно в базах.
В итоге СУБД — это наиболее критичные системы, инциденты в которых особенно контролируются.

Еще одной особенностью атак на отрасль являются попытки использования учетных записей сотрудников третьими лицами, что связано с исключительной важностью проводимых сотрудниками операций. Поэтому именно банки чаще других организаций просят запустить такие сценарии в рамках мониторинга.

При этом статистика по подтвержденным инцидентам выглядит следующим образом:

Динамика подтвержденных инцидентов



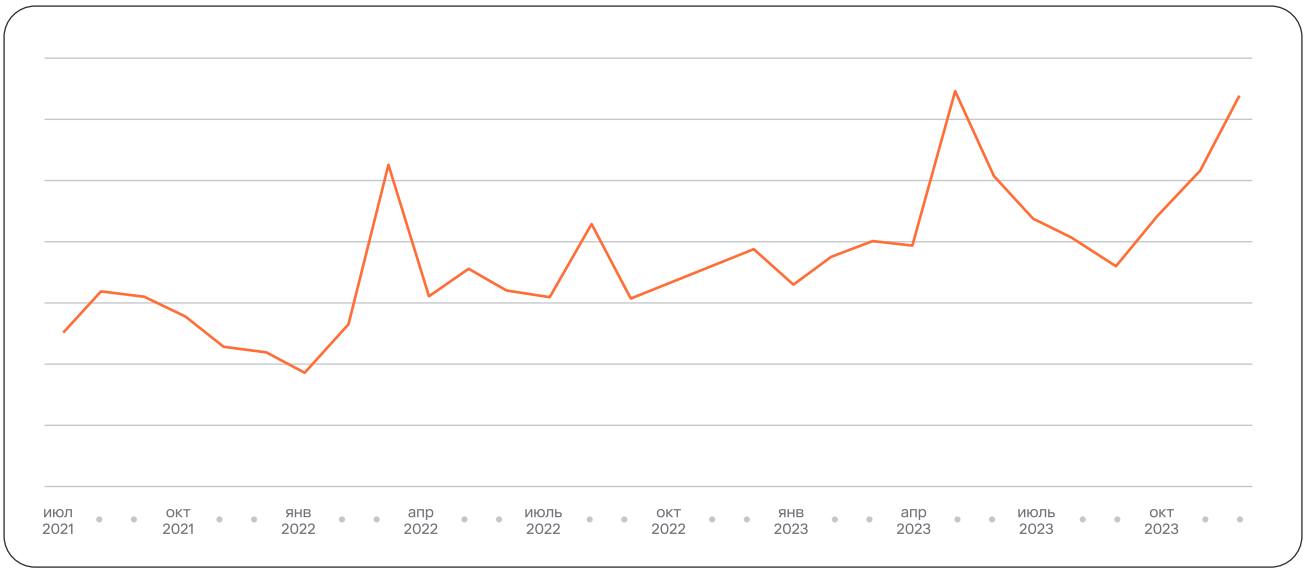
Здесь мы наблюдаем очевидные всплески в 1 квартале 2022 года, когда банки стали одной из ключевых целей злоумышленников. Тогда массовым атакам подверглись все сферы, имеющие ключевое значение для населения (банки, госсервисы, ретейл, СМИ). Кибердары по ним вызвали широкий общественный резонанс. С сентября 2023 года после длительного спада снова наблюдается рост подобных атак.

Также за год злоумышленники сменили вектор кибератак на банки. Явственно увеличилось количество хакерских утилит (в том числе средств разведки) и средств удаленного администрирования. Основной вектор — фишинговые письма, рассылки которых на банки производятся все интенсивнее. С начала 2023 года их количество увеличилось в полтора раза. Этот вектор сохраняет свою эффективность, так как даже в банковской сфере все еще недостаточен уровень киберграмотности сотрудников, поэтому требуется активнее использовать такие средства борьбы с ВПО, как песочницы.

x1,5 РАЗА

увеличилось количество фишинговых атак на банки с начала 2023 года

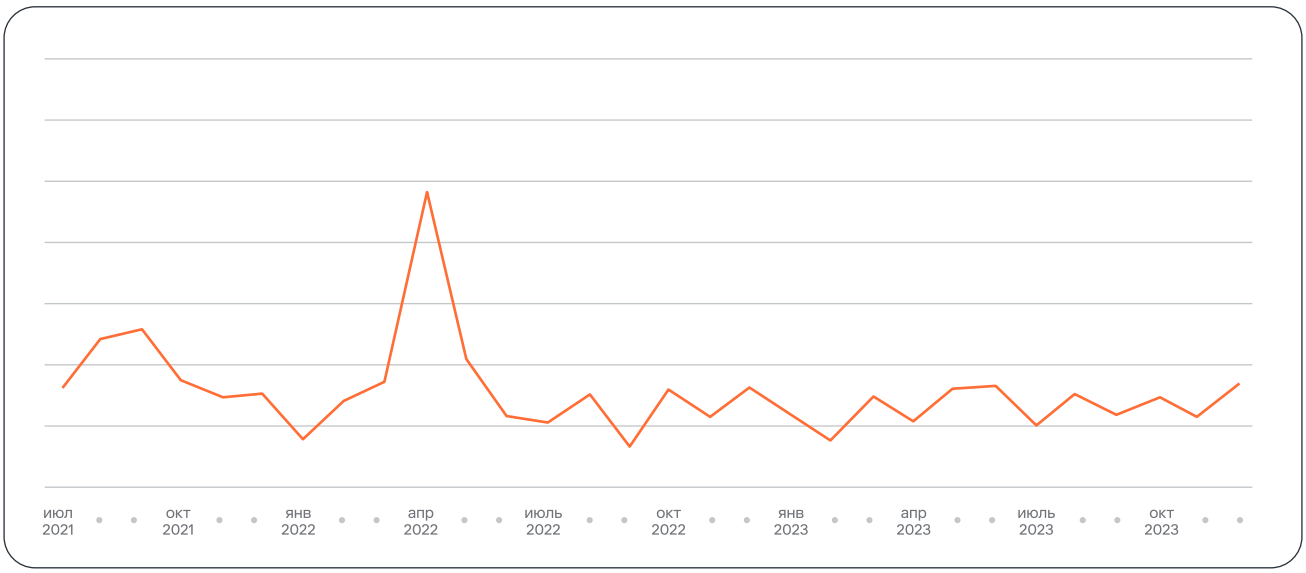
Динамика атак на финсектор с применением фишинга



В начале 2022 года мы наблюдали всплеск кибератак на ИТ-периметры и веб-ресурсы финорганизаций. Однако злоумышленники быстро осознали низкую эффективность таких действий в отношении банков.

Объясняется это высоким уровнем зрелости последних в части управления ИТ-периметром и распространенностью решений класса WAF.

Динамика атак на веб-ресурсы и ИТ-периметр



СТАТИСТИКА ВЕБ-АТАК В ФИНАНСОВОМ СЕКТОРЕ

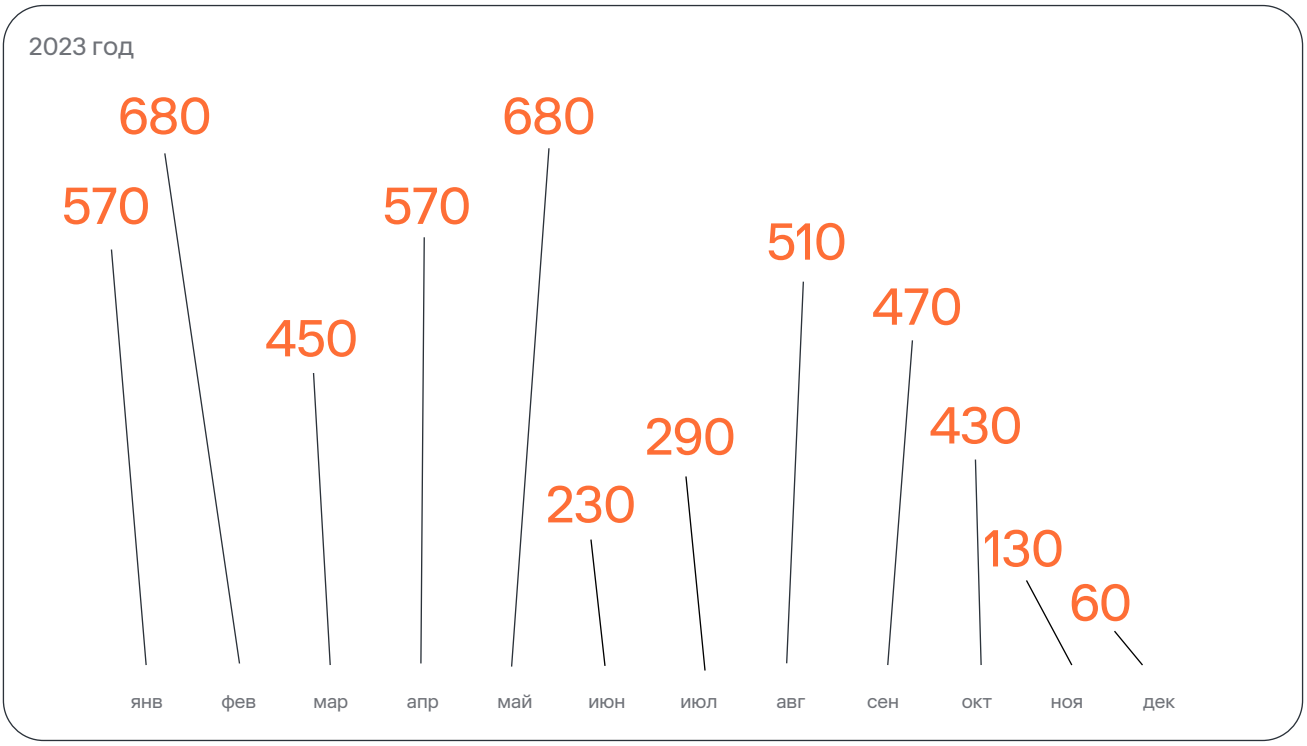
В этом разделе отражена динамика атак на веб-ресурсы финансовых организаций в 2023 г. Аналитика базируется на данных сервиса защиты WAF экосистемы Solar MSS.

Несмотря на сокращение объема веб-атак в кредитно-финансовом секторе, они остаются серьезной угрозой для отрасли. Недоступность банковских веб-приложений крайне чувствительна для пользователей и вызывает широкий общественный резонанс. А взлом сайта может привести хакеров к базам данных, в которых содержится чувствительная финансовая информация и персональные данные клиентов.

ОКОЛО 5 МЛН

веб-атак на ресурсы представителей финансовой отрасли зафиксировал и отразил сервис WAF в 2023 г.

Количество атак на финсектор по месяцам, тыс.



Основная доля веб-атак на банки в 2023 году — это атаки высокого уровня сложности. В частности, это SQL-инъекции (позволяют внедрить произвольный код в запросы к базам данных), эксплуатация LFI-уязвимостей (позволяют через браузер запускать файлы на сервере) и RCE-уязвимостей (позволяют внедрить вредоносный код в серверную часть приложения). Такие уязвимости дают возможность злоумышленникам получить доступ к управлению веб-приложением и к его данным.

Также мы видим рост числа сканирований веб-приложений, то есть попыток поиска уязвимостей автоматизированными инструментами. Это еще раз указывает на то, что хакеры, осознавая высокий уровень защищенности банков, уже не пытаются атаковать их простыми инструментами (например, с помощью ботов).

Злоумышленники нацелены на поиск слабых мест в приложениях, чтобы получить над ними максимальный контроль.

УЯЗВИМОСТИ, КОТОРЫЕ ДАЮТ ДОСТУП К УПРАВЛЕНИЮ ВЕБ-ПРИЛОЖЕНИЯМ И ЕГО ДАННЫМ

01

SQL-ИНЪЕКЦИИ

Позволяют внедрить произвольный код в запросы к базам данных

02

LFI-УЯЗВИМОСТИ

Позволяют через браузер запускать файлы на сервере

03

RCE-УЯЗВИМОСТИ

Позволяют внедрить вредоносный код в серверную часть приложения

СТАТИСТИКА DDOS-АТАК В ФИНАНСОВОМ СЕКТОРЕ

В этом разделе отражена динамика DDoS-атак на финансовые организации в 2022-2023 гг. Аналитика базируется на данных о сетевых атаках уровней L3/L4, отраженных сервисом Anti-DDoS экосистемы Solar MSS.

В 2022 году наблюдался широкий охват DDoS-атаками компаний из различных сфер экономики. Финансовый сектор входил в топ-5 наиболее атакуемых отраслей наряду с телекомом, ИТ-сегментом, логистикой и медициной.

Однако в 2023 году ситуация изменилась: наряду с общим снижением количества DDoS-атак во всех секторах экономики в среднем в 3 раза в финансовой сфере наблюдалось падение почти в 9 раз и перемещение отрасли по этому показателю с 4-го на 11-е место. Эта ситуация свидетельствует о том, что в целом финансовые организации достаточно хорошо защищают свои каналы уровней L3/L4 — на этом фоне злоумышленники предпочитают прицельно атаковать более легкие мишени в других отраслях.

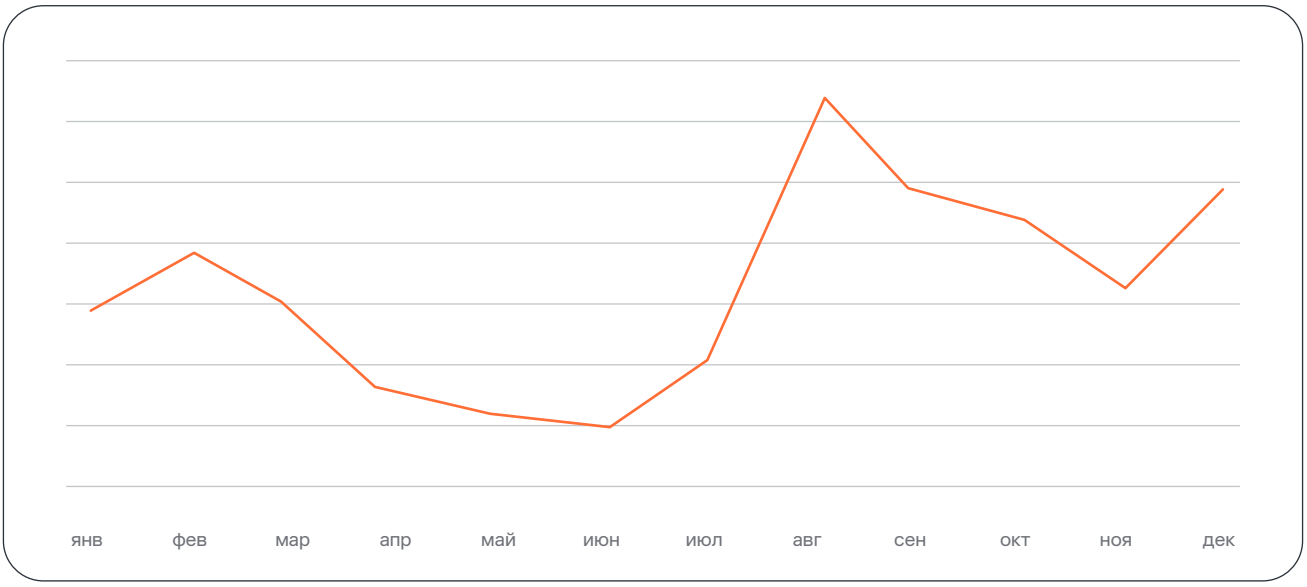
Топ-5 атакуемых отраслей в 2022 г.

Топ-5 атакуемых отраслей в 2023 г.

[1] Количество DDoS-атак на одну организацию за год.

В то же время динамика атак на финсектор за 2023 год выявила очевидный восходящий тренд: период относительного затишья в мае-июне сменился ростом числа DDoS-атак во второй половине года.

Динамика атак на финсектор в 2023 г.

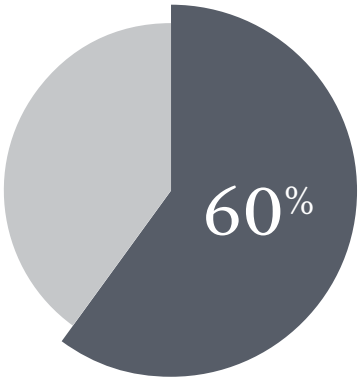


В целом похожий восходящий тренд по DDoS-атакам в 2023 году наблюдался во многих других секторах экономики: от небольшого количества атакуемых компаний отрасли в начале года к существенному его расширению во второй половине года, особенно в период с августа по октябрь.

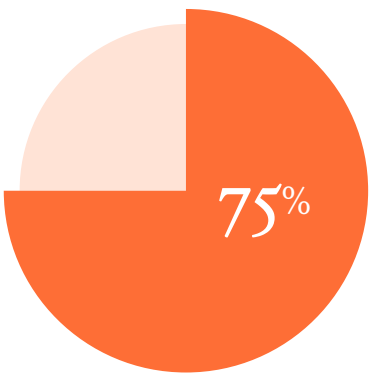
То есть в 2023 году все больше отраслей стали подвергаться большему количеству атак типа "отказ в обслуживании". Это подтверждает гипотезу о том, что злоумышленники ищут незащищенные от DDoS-атак организации, чтобы оказать максимально негативное влияние на бизнес.

Доля атакуемых компаний увеличилась с 60% в 2022 г. до 75% в 2023 г. от клиентской базы сервиса Anti-DDoS.

2022



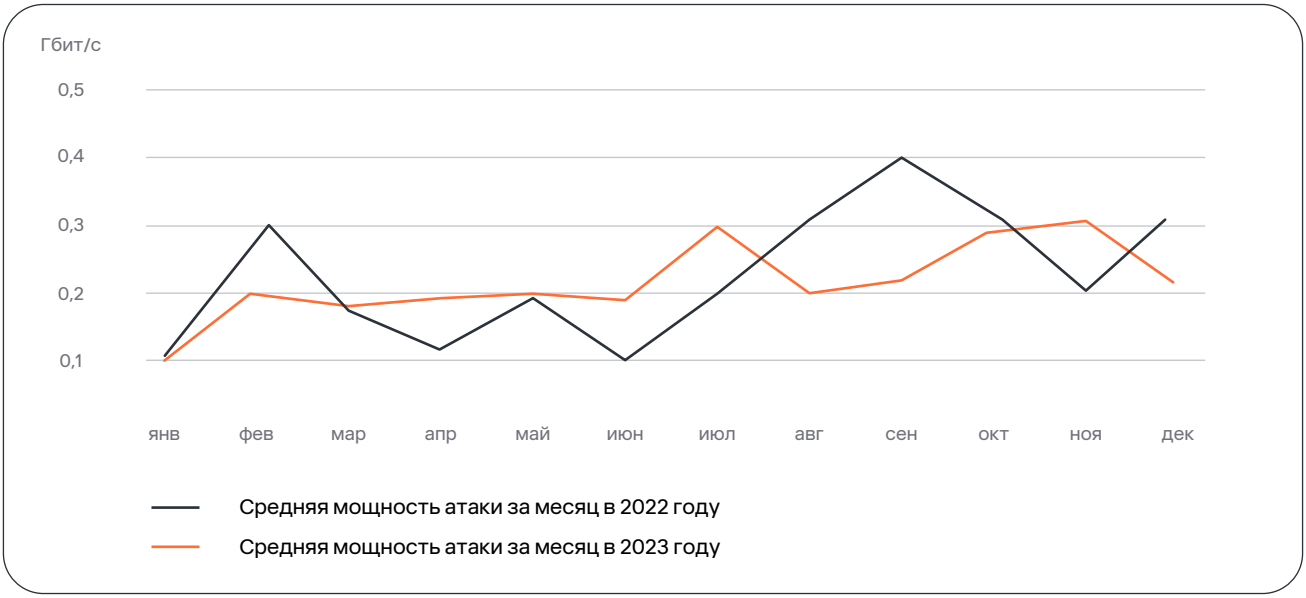
2023

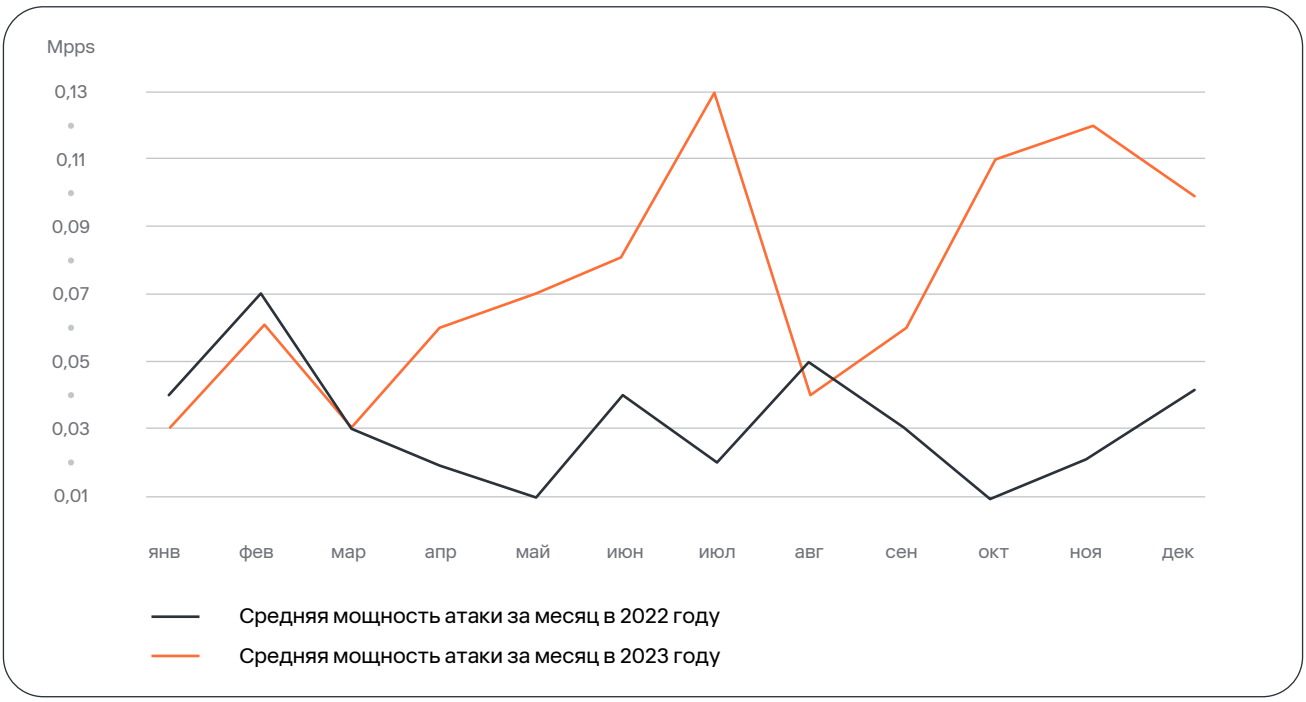


Анализ средней мощности атак в финсекторе выявляет еще одну тенденцию: если мощность в Гбит/с на протяжении 2023 года оставалась стабильно невысокой, как и в 2022 г., то показатель MPPS (millions of packets per second) демонстрировал всплески, заметно превышающие аналогичный параметр предыдущего года.

То есть атаки с целью забить нелегитимным трафиком каналы связи не претерпели существенных изменений. В то же время злоумышленники все чаще выбирают в качестве целей не просто каналы, а интернет-сервисы в рамках каналов — для этого они манипулируют количеством пакетов, идущих на серверы во время атак. Как следствие — средняя мощность в MPPS носит нестабильный характер в течение года.

Сервисы Anti-DDoS и WAF являются источником большого количества информации, которую рекомендуется передавать в SIEM, так как система имеет более гибкие инструменты по составлению сценариев. Это позволяет повысить эффективность обнаружения комплексных атак, ведь под прикрытием DDoS-атак уровня L3 и L4 зачастую реализуются более сложные сценарии проникновения в инфраструктуру, а также ищутся слабые места на периметрах организаций. Вместе с тем именно информация с WAF и Anti-DDoS позволяет точно определить период, в который необходимо анализировать логи с веб-серверов для выявления векторов сложных атак в обход средств защиты.





ВНЕШНИЕ ЦИФРОВЫЕ УГРОЗЫ В ФИНАНСОВОМ СЕКТОРЕ

В 2023 году активность злоумышленников в отношении организаций финансовой сферы была крайне высокой.

По данным сервиса мониторинга внешних цифровых угроз Solar AURA, чаще всего отрасль сталкивалась:

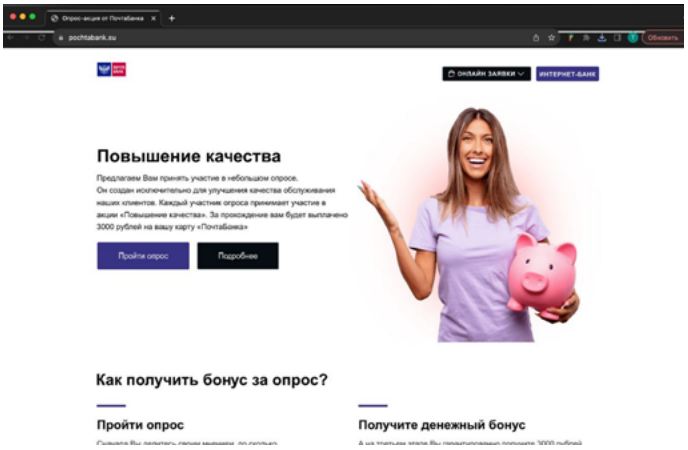
- с фишинговыми атаками;
- публикацией утечек данных;
- продажей банковских карт;
- открытием расчетных счетов;
- вербовкой сотрудников банков;
- пробивом данных.

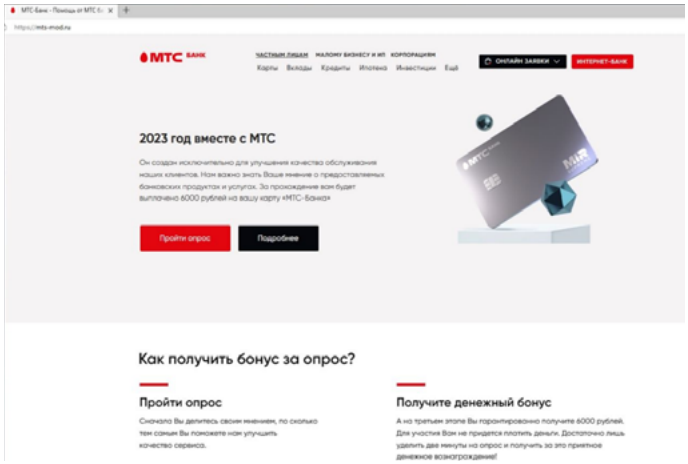
ФИШИНГ

Фишинговые атаки претерпели ряд изменений. Так, более 40% фишинговых ресурсов, имитирующих сайты кредитных организаций, не использовали в наименовании домена бренд конкретной организации. До этого таких сайтов были единицы. Кроме того, резко увеличилось количество вредоносных ресурсов, располагающихся на доменах третьего и четвертого уровней. Это предъявляет новые требования к механизмам выявления незаконных ресурсов и делает обнаружение фишинговых сайтов «по старинке», путем анализа созвучных доменов, малоэффективным.

Основной акцент злоумышленников сместился с хищения данных банковской карты на получение доступа в личный кабинет клиента. При этом 8% выявленных фишинговых сайтов использовались для распространения вредоносного ПО (программ удаленного администрирования компьютера, закамуфлированных под программы техподдержки банка). Такого рода ресурсы встречаются даже при телефонном мошенничестве — в процессе разговора злоумышленники направляют на них свою жертву.

Наиболее популярная фишинговая схема в 2023 году — акция или опрос от имени банка.





В 2023 году нами было зафиксировано 38 инцидентов, связанных с публикацией в общем доступе данных клиентов кредитных организаций. Общий объем опубликованных сведений превысил 161 млн строк, включая 130 млн телефонных номеров и 28 млн адресов электронных почт.

Серьезный вклад в эту копилку внесли инциденты, связанные с утечкой данных крупных российских страховых компаний: суммарно в сеть попало более 33 млн строк данных.

При этом стоит отметить, что данные далеко не всегда утекают из самих кредитных учреждений, ведь последние уделяют большое внимание вопросам информационной безопасности. Немалая часть сведений о клиентах банков попадает в общий доступ через третьих лиц — благодаря использованию троянов-стилеров, через фишинговые сайты, а также вследствие инцидентов, затрагивающих сторонние организации, например интернет-магазины. Также на протяжении года мы фиксировали инциденты, связанные с публикацией фейковых данных, приписываемых той или иной кредитной организации.

38

инцидентов было связано с публикацией данных клиентов кредитных организаций в 2023 году

130+ МЛН

строк, содержащих данные телефонных номеров

33+ МЛН

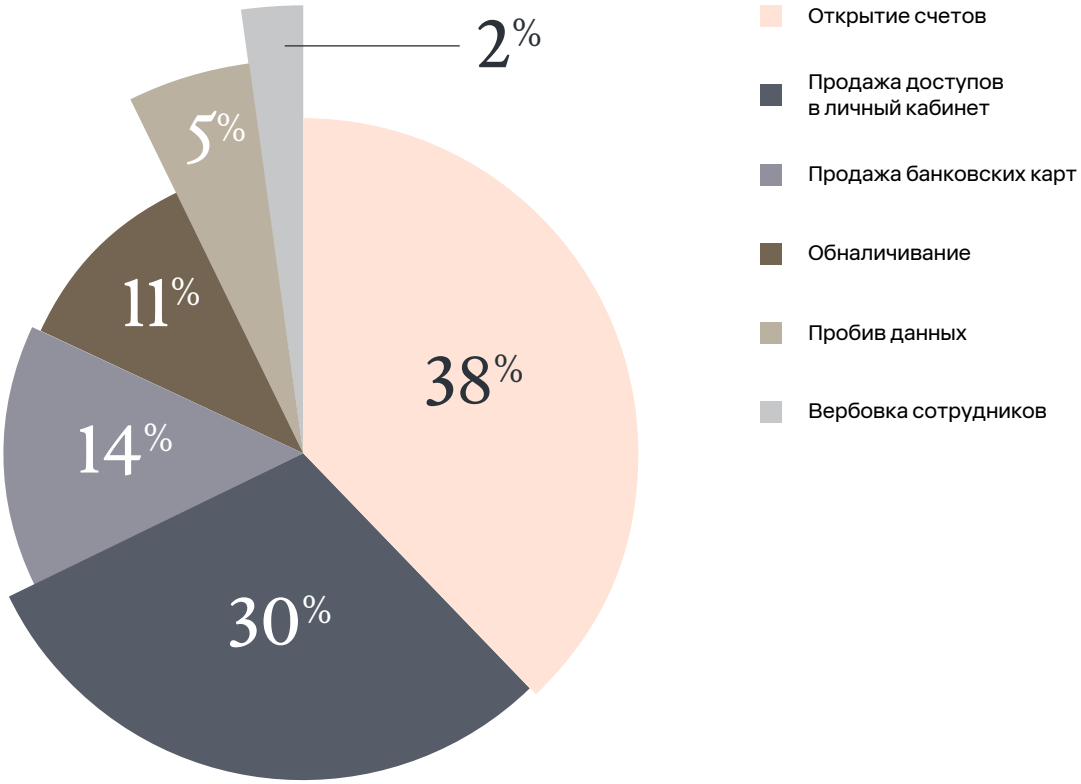
строк, содержащих данные клиентов крупных российских страховых компаний в 2023 году

28+ МЛН

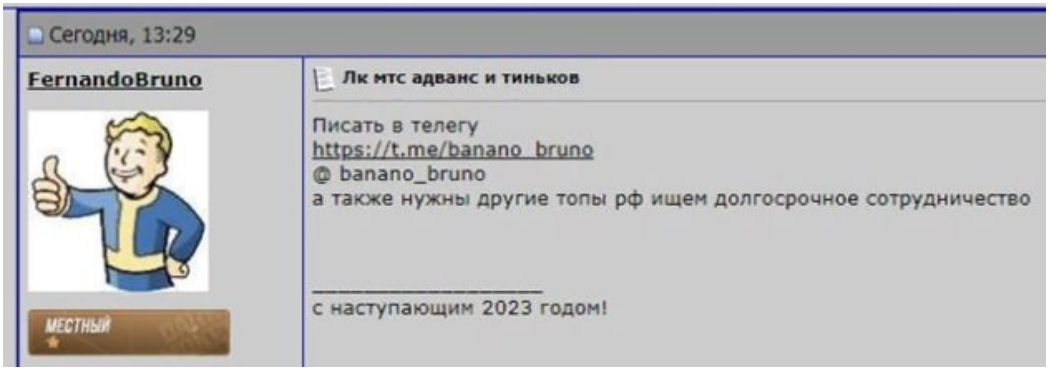
строк, содержащих данные адресов электронных почт

Большое количество запросов в даркнете традиционно связано именно с кредитно-финансовым сектором. Эту отрасль затронуло 40% проанализированных нами публикаций. Перечень запрашиваемых нелегальных услуг не меняется уже много лет.

Распределение нелегальных услуг по категориям



Так выглядит объявление в даркнете:



В 2023 году мы зафиксировали 5376 вредоносных интернет-ресурсов, принимающих электронную оплату от пользователей. Всего в копилке сервиса имеются ретроспективные сведения о 13 тыс. банковских картах и мерчантах, задействованных в противоправных операциях.

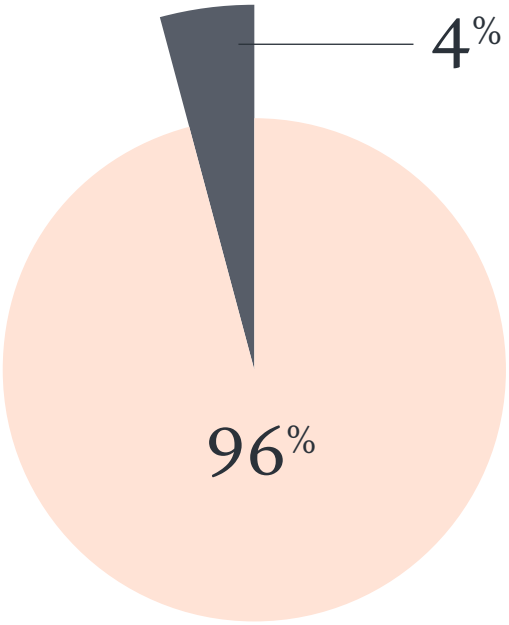
Большинство вредоносных сайтов связано с незаконным игорным бизнесом (96%), оставшиеся 4% приходятся на фишинг, различного рода мошеннические ресурсы, а также фейковые криптообменники.

Выявленные ресурсы можно разделить на 2 категории:

- использующие интернет-эквайринг для приема платежей от клиентов (12% от общего числа);
- использующие карты дропов для приема платежей (88% от общего числа).

Процесс работы с картами дропов автоматизирован. Например, некоторые платежные шлюзы, обслуживающие онлайн-казино, используют пулы из нескольких десятков карт, выпущенных различными банками.

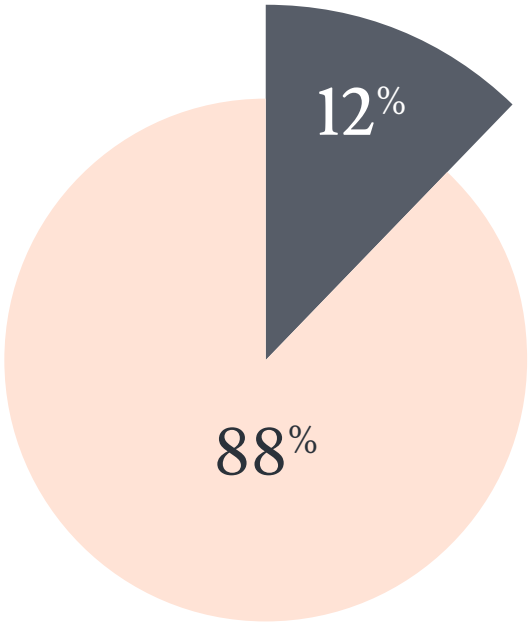
Распределение вредоносных интернет-ресурсов



Незаконный игорный бизнес

Фишинг, мошеннические ресурсы, фейковые криптообменники

Распределение мошеннических ресурсов по категориям



Использование интернет-эквайринга

Использование карты дропов

ЭКОНОМИКА ИБ В ФИНАНСОВОМ СЕКТОРЕ

Исследование проводилось на основе данных Росстата о размере отраслевой выручки, затратах на ИТ и средней численности сотрудников с применением методики, признанной российскими и международными аналитиками для оценки ИБ-бюджетов. Анализ включал оценку затрат на ИБ в зависимости от бюджетов на ИТ, средних затрат на одного сотрудника и выручки компаний. Для дополнительных расчетов применялся анализ закупок и результаты маркетинговых исследований.

По данным группы аналитики ГК «Солар», финансовый сектор, наряду с телекомом, ИТ, нефтегазовой, химической и нефтехимической, энергетической и транспортной отраслями, входит в список ключевых заказчиков ИБ-вендоров, образуя 67% рынка среди коммерческих компаний и 44% всего рынка, включая ФОИВ и РОИВ. Непосредственно финансовая сфера занимает 13% всего ИБ-рынка. Для сравнения, на нефтегазовую отрасль, химию и нефтехимию приходится 6,4% рынка, телекоммуникации и ИТ — по 5%. В 2023 году затраты компаний финансовой отрасли на СЗИ составили 18 млрд рублей. Бюджеты финансовых организаций превышают только бюджеты ФОИВ — 20 млрд рублей в 2023 году.

Несмотря на то, что кредитные организации, страховые компании, биржи, компании, предоставляющие финансовые и инвестиционные услуги, одними из первых озаботились вопросами обеспечения безопасности, финансы остаются недофинансированной с точки зрения средних мировых показателей отраслью.
В России доля ИБ в ИТ-бюджетах компаний финансовой сферы — 5%, в то время как в мире она достигает 8-10%.

По оценке аналитиков ГК «Солар», к 2030 году затраты финансовых компаний на ИБ могут составить 30 млрд рублей при среднегодовом темпе роста (CAGR) в 8%, что соответствует росту рынка ИБ в целом.

13%

Доля рынка финансовой сферы среди коммерческих организаций заказчиков ИБ-вендоров

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