Кибератаки на российские компании в I квартале 2023 года

Отчет

rt-solar.ru
rt.ru

Ростелеком
Солар

Оглавление

О компании

«РТК-Солар» – национальный провайдер сервисов и технологий кибербезопасности. Под защитой – 750+ компаний и госструктур. Ключевые направления – аутсорсинг ИБ, разработка собственных продуктов, интеграционные ИБ-проекты. Компания предлагает сервисы первого и лидирующего в РФ коммерческого SOC (Security Operations Center) – Solar JSOC, а также экосистему управляемых сервисов ИБ – Solar MSS. Линейка собственных продуктов включает DLP-решение Solar Dozor, шлюз веб-безопасности Solar webProxy, систему управления доступом Solar inRights, решение контроля привилегированных пользователей Solar SafeInspect, анализатор кода Solar appScreener, межсетевой экран нового поколения Solar NGFW и систему повышения эффективности труда Solar addVisor. Предоставляются compliance-услуги, в том числе по защите АСУ ТП. Штат компании – 1600+ специалистов. Офисы компании расположены в Москве, Нижнем Новгороде, Самаре, Ростове-на-Дону, Хабаровске, Томске, Санкт-Петербурге, Ижевске. Деятельность компании лицензирована ФСБ России, ФСТЭК России и Министерством обороны России.

Список сервисов Solar JSOC:

- Мониторинг и анализ инцидентов ИБ
- Анализ угроз и внешней обстановки
- Комплексный контроль защищенности
- Расследование и реагирование на инциденты
- Построение SOC и консалтинг

Введение

Количество кибератак продолжает расти, однако уже не так активно, как в 2022 году. Киберландшафт постепенно стабилизируется, хотя очевидно, что к состоянию, которое было до СВО, он в обозримом будущем не вернется. Атаки продолжают усложняться, а хакеры все чаще прибегают к исследованию периметров своих жертв и киберразведке. Массовые атаки (рассылка ВПО, веб-атаки) остаются в топе инструментов, но их популярность постепенно сокращается и место занимают сетевые атаки, компрометация учетных записей, попытки несанкционированного доступа к корпоративным системам.

В настоящем отчете приведены данные об инцидентах, выявленных командой Solar JSOC[1] в I квартале 2023 года, и их сравнение со статистикой предыдущих периодов. В исследовании отражена приоритизация инцидентов по степени критичности, а также процентное соотношение различных типов кибератак, которые наблюдались в отчетный период.

В фокус внимания экспертов попало около 280 компаний и организаций из разных отраслей экономики: госсектор, финансы, нефтегаз, энергетика, телекоммуникации, крупный ретейл. Все компании представляют сегмент Large Enterprise и Enterprise с количеством сотрудников от 1000 человек, оказывают услуги в разных регионах страны и, как правило, являются крупнейшими в отрасли по своему региону или по стране в целом.

Совокупно в рамках оказания сервиса Solar JSOC обеспечивает контроль и выявление инцидентов для:

- более 3400 внешних сервисов, опубликованных в интернете;
- около 170 тыс. серверов общего, инфраструктурного и прикладного назначения.

[1] В отчет вошли агрегированные данные об атаках на компании, подключенные к сервису мониторинга киберинцидентов Solar JSOC. Аналитика не учитывает информацию о клиентах управляемых сервисов кибербезопасности Solar MSS (включая магистральный Anti-DDoS и WAF), результаты услуг по расследованию киберинцидентов и данные с сенсоров и ханипотов.

Сводная статистика по инцидентам

В январе – марте 2023 года было зафиксировано около **290 тыс.** событий ИБ – подозрений на инцидент после обработки первой линией мониторинга и фильтрации ложных срабатываний. Это на **60%** превышает показатель аналогичного периода 2022 года. Если же сравнивать данные отчетного периода с показателями последней четверти 2022 года, то они выросли на **3%**.

Динамика числа кибератак по кварталам (тыс. событий ИБ)

Резкие изменения киберландшафта произошли после начала СВО, то есть под конец I квартала прошлого года. А январь-февраль 2022 были относительно спокойными. Именно поэтому мы видим резкое увеличение числа кибератак. Сейчас же тенденции роста существенно замедлились, и на текущий момент являются скорее незначительными, но очевидно, что возврат к показателям до начала СВО едва ли возможен в обозримой перспективе. Отчет о кибератаках за IV квартал и весь 2022 год вы можете найти по ссылке.

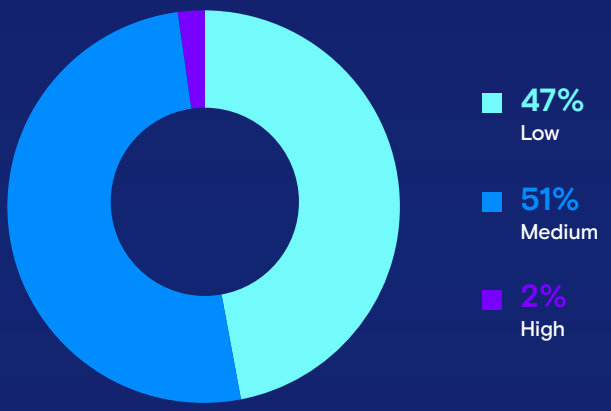
Если смотреть квартальную динамику, то тенденция на увеличение числа событий ИБ сохраняется. Хотя темпы роста существенно сократились: **31%** в IV квартале против нынешних **3%** в отчетном периоде. Это может объясняться в том числе и тем, что в конце года хакеры традиционно проявляют активность, а в начале, напротив, их активность снижается, постепенно нарастая уже ко II кварталу.

При этом число подтвержденных инцидентов продолжает снижаться. В III квартале показатель упал на **20%,** а в отчетном периоде – еще на **23%**. Это напрямую указывает на то, что уровень защищенности российских компаний растет, и они могут успешно противостоять кибератакам, сократив число инцидентов с реальными последствиями.

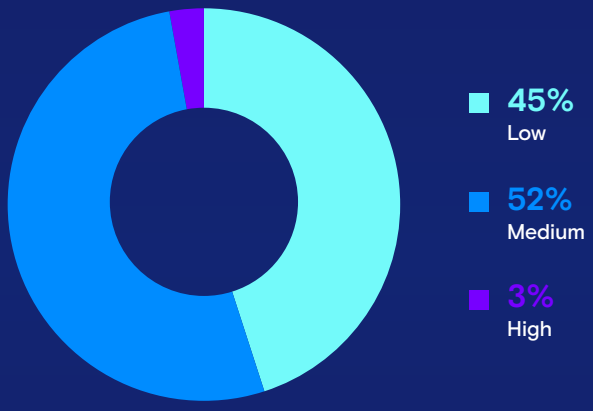
Поведение киберпреступников также играет важную роль. Во-первых, принципиально новых тактик и техник они пока не применяют, предпочитая атаковать по проверенным векторам. Во-вторых, успешность массовых атак снижается, а вместе с тем падает и их интенсивность. Однако в явном виде наблюдаются точечные кампании против конкретных организаций, координируемые квалифицированными злоумышленниками. Последние объединяют под своим началом хактивистов, желающих повысить свою квалификацию и участвовать в более сложных, чем обычный DDoS или дефейс, атаках. Этот тренд сформировался еще в предыдущем квартале, и сейчас мы видим его подтверждение.

Распределение инцидентов по критичности:

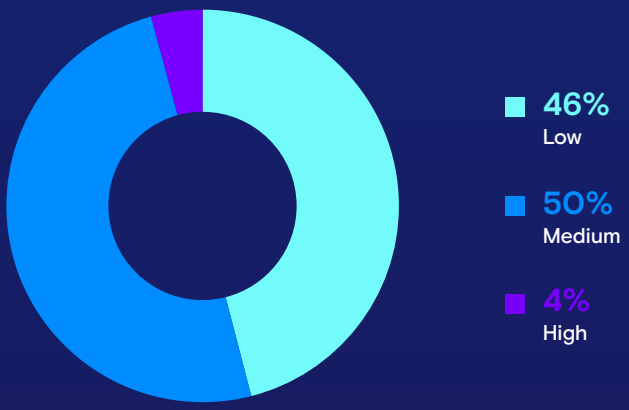
IV квартал 2022



I квартал 2023



I квартал 2022



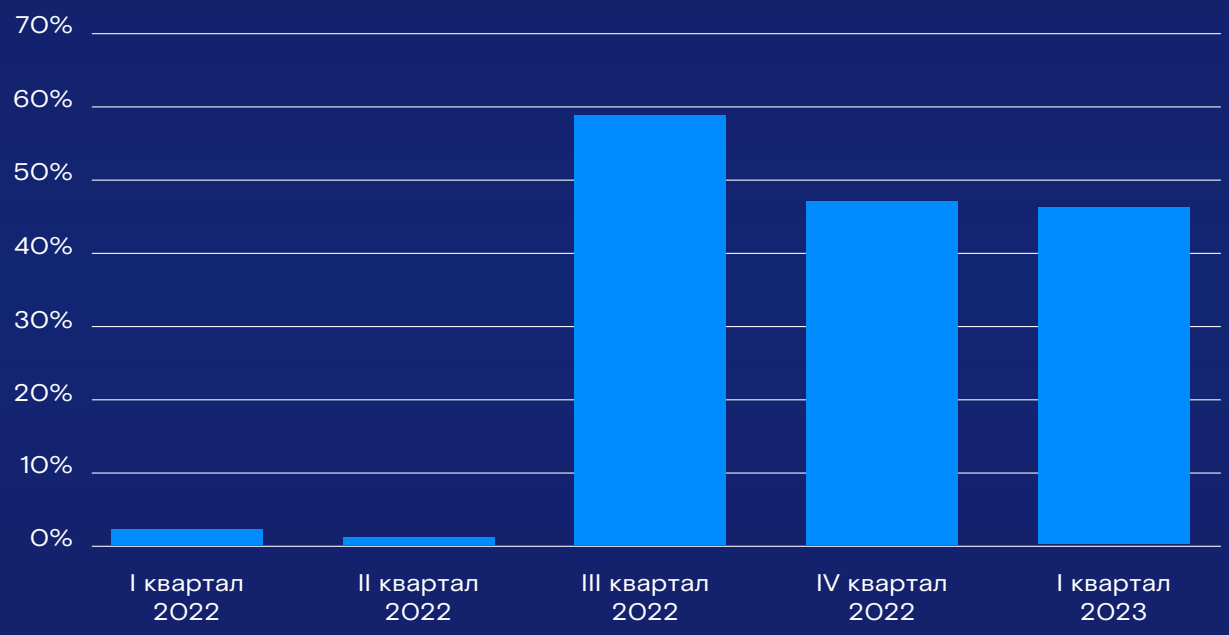
В целом удельный вес каждого типа инцидента по сравнению со значениями предыдущих периодов существенных изменений не претерпел.

Статистика по инцидентам с высокой степенью критичности

Инциденты с высокой степенью критичности чаще всего были связаны с применением вредоносного ПО, веб-атаками, эксплуатацией уязвимостей или сетевыми атаками – в зависимости от квартала.

Вредоносное ПО

Доля ВПО в общем объеме высококритичных инцидентов



В отчетном периоде **46%** высококритичных инцидентов связано с применением вредоносного ПО, а **10%** из них – с попытками использования шифровальщиков. Примечательно, что в конце 2022 года инцидентов с шифрованием зафиксировано не было. «Возвращение» шифровальщиков говорит о том, что атаки становятся более точечными. Тренд на направленное шифрование прослеживается уже давно, так как более внимательный выбор жертвы скорее гарантирует злоумышленникам получение выкупа, чем массовая рассылка ВПО.

Основным каналом доставки ВПО (в том числе и шифровальщиков) по-прежнему остается фишинг. И несмотря на то, что его эффективность падает на фоне роста уровня защищенности ИТ-инфраструктур, это один из самых простых и доступных большинству злоумышленников методов доставки вредоносов.

Годовая динамика показывает, что доля этого вектора атак менялась существенно. В первой половине прошлого года этот показатель был незначительным, так как злоумышленники сконцентрировались на более простых и массовых ударах (DDoS, дефейс), а также попытках проникнуть в инфраструктуру компаний, используя уязвимости и атаки на веб. Однако уже в III квартале они стали практиковать технику проникновения, используя человеческий фактор, либо ВПО для закрепления в инфраструктуре, – мы отчетливо увидели резкий рост доли этого вектора. Но уже в следующем квартале активность ВПО стала снижаться, этот тренд продолжается и в 2023 году. Скорее всего, это указывает на то, что попытки использования вредоносов оказались не так эффективны, как планировали хакеры, ведь за минувший год компании научились противостоять таким атакам.

Веб-атаки

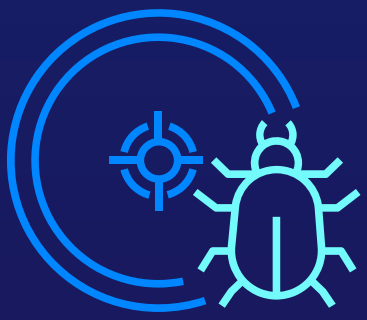
Доля веб-атак в общем объеме высококритичных инцидентов

В течение года динамика этого вектора была достаточно интересной: в первой половине года на него приходилось подавляющее большинство высококритичных инцидентов. Как говорилось выше, это связано с массовыми атаками на публичные онлайн-ресурсы. Но после «провала» в III квартале веб-атаки стали вновь набирать вес.

В отчетном периоде доля веб-атак составила **24%**, что немного ниже показателя предыдущего квартала. Такая ситуация весьма типична, так как в канун Нового года мы всегда сталкиваемся с увеличением попыток взлома и дефейса сайтов онлайн-магазинов, получения доступа к конфиденциальным данным клиентов и сотрудников – то есть со всем пулом веб-атак. А в начале года подобная активность всегда падает.

Другие векторы

Статистика по другим типам инцидентов демонстрирует, что в отчетном периоде злоумышленники использовали те же векторы атак, что и кварталом ранее: эксплуатацию уязвимостей, компрометацию учетных записей, сетевые атаки. При этом злоумышленники стали готовиться к кибератакам более тщательно: они активнее прощупывают периметр и публичные сервисы на предмет уязвимостей (за квартал рост составил 1,9%), а также предпринимают попытки компрометации публичных сервисов с авторизацией через утекшие ранее данные. Здесь стоит отметить проблему с парольной политикой и отсутствием второго фактора авторизации. Сотрудники часто используют одинаковые пароли в публичных (соцсети, форумы, онлайн-магазины) и корпоративных сервисах. Это позволяет злоумышленникам использовать утекшие ранее пароли для взлома онлайн-ресурсов компаний через беспечных работников.



Статистика по инцидентам с разной степенью критичности

В целом анализируемый период не характеризуется какими-либо аномалиями, вызванными резкими спадами или всплесками того или иного типа атак. Можно сказать, что ситуация остается стабильной.

Интересно, что число инцидентов, спровоцированных компрометацией учетных записей (УЗ), снизилось. Безусловно, 2022-й запомнился нам рядом громких утечек, что заставило компании всерьез задуматься о безопасности учетных данных своих сотрудников. Они усовершенствовали свои подходы к безопасности, ввели новую парольную политику, провели обучение сотрудников навыкам ИБ. Тем не менее слабые и повторяющиеся пароли часто встречаются в компаниях. И хотя повышенное внимание к ИБ затрудняет злоумышленникам совершение таких атак, как брутфорс публичных сервисов (подбор пароля к почте, веб-порталам), угроза все равно остается актуальной.

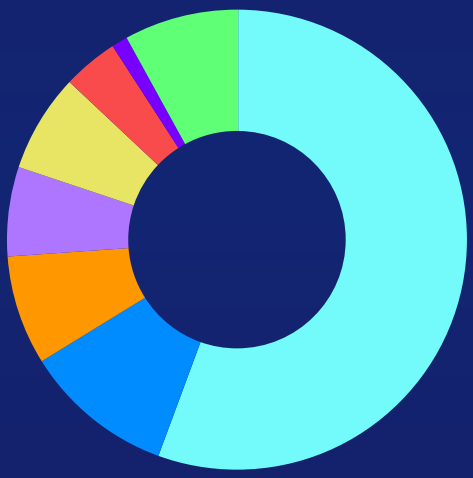
Рост доли инцидентов, связанных с несанкционированным доступом (НСД к ИС и сервисам), в этом квартале связан с внутренними злоумышленниками и подрядчиками. В 2022 году мы увидели значительный рост атак типа supply chain, который опять же связан с повышением уровня защищенности атакуемых организаций. На этом фоне злоумышленники ищут либо подрядчиков, менее защищенных, чем их основные жертвы, либо неучтенные или забытые точки входа этих подрядчиков в инфраструктуру. Поэтому компании должны следить за тем, насколько надежен партнер, которого они выбирают, а также позаботиться о средствах для контроля и ограничения доступа подрядчиков и привилегированных сотрудников.

Количество сетевых атак также продолжает расти. Это еще раз подтверждает, что в 2023 году киберразведка будет активно применяться злоумышленниками для поиска уязвимостей на периметре компаний. Такие атаки являются довольно простыми, но они указывают на то, что конкретная компания попала в поле зрения хакеров и, возможно, на нее готовится более серьезное нападение.

I квартал 2022

- 25% Заражение ВПО
- 18% Компрометация УЗ
- 16% НСД к ИС и сервисам
- 10% Веб-атаки
- 7% Использование нелегитимного ПО
- 7% Сетевые атаки
- 17% Остальное

IV квартал 2022



- 56% Заражение ВПО
- 10% Компрометация УЗ
- 8% Эксплуатация уязвимостей
- 6% Использование нелегитимного ПО
- 7% Сетевые атаки
- 4% НСД к ИС и сервисам
- 1% Веб-атаки
- 8% Остальное

I квартал 2023

- 56% Заражение ВПО
- 9% Использование нелегитимного ПО
- 8% Сетевые атаки
- 7% Эксплуатация уязвимостей
- 6% НСД к ИС и сервисам
- 4% Компрометация УЗ
- 1% Веб-атаки
- 9% Остальное

Выводы

За отчетный период киберландшафт не претерпел существенных изменений, общий фон остается скорее стабильным, а количество подтвержденных инцидентов продолжает снижаться. Важно учитывать, что до СВО атаки были проще и хакеры действовали не так точечно. Вместе с ростом квалификации нападающих компании также закрыли ИТ-периметры, что помогло скорректировать ситуацию после скачка подтвержденных инцидентов середины прошлого года. Это говорит о том, что организации фактически научились защищаться от более сложных кибератак.

Укрепление киберзащиты российских организаций усложняет реализацию низкоквалифицированных атак. Сегодня от злоумышленников требуется более серьезная подготовка и большие финансовые вложения, а также проведение подготовительных мероприятий. Все популярнее у киберпреступников становится и кибербразведка. Мы видим рост атак, связанных с публичными сервисами (эксплуатация уязвимостей, брутфорс учетных данных на внешних порталах, VPN, почте). Опасности ситуации добавляют утечки, которые происходили в 2022 году. Поиск ненадежных подрядчиков и незащищенных доступов также становится для хакеров все более выигрышной стратегией. Именно поэтому компаниям необходимо не только заниматься базовой защитой периметра, но и самим обращаться к услугам кибербразведки. Это позволит нивелировать риски, связанные с утекшими базами данных, скомпрометированными аккаунтами, адресами электронной почты и т. п. На основе этой информации компании смогут митигировать угрозы еще до эксплуатации найденных злоумышленниками уязвимостей.

В 2023 году станет еще более актуальным вопрос своевременного реагирования на киберинциденты на фоне общего роста числа событий ИБ. Поэтому крайне важно озаботиться вопросами автоматизации данного процесса, в том числе и с помощью применения решений класса IRP, что дополнит процесс работы с инцидентами.