Отчет

«Кибератаки на российские компании в 2022 году»

Москва, 2023

rt-solar.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, IdM-систему Solar inRights и анализатор кода Solar appScreener. 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

2022 год показал, насколько кибермир восприимчив к изменениям, происходящим в реальности. Начало СВО сильно повлияло на ландшафт киберугроз. Интенсивность атак выросла, а хакерским ударам стали подвергаться абсолютно все компании, независимо от масштаба и сферы деятельности. Массовость атак сопровождалась их постоянным опубличиванием: сообщения о новых взломах и сливах регулярно появлялись в информационном поле. Активную позицию заняли хактивисты, цель которых заключалась в создании всеобщей паники. Но, несмотря на массовость, новых инструментов и уникальных тактик у киберпреступников за год скорее не появилось: они использовали фишинг с ВПО, уязвимости в софте, которые было сложно закрывать на фоне ухода вендоров из РФ, веб-атаки, компрометацию учетных записей и т. п.

В настоящем отчете приведены данные об инцидентах, выявленных командой Solar JSOC[1] в IV квартале 2022 года, и их сравнение со статистикой предыдущих периодов. Также представлены общие выводы по итогам всего 2022 года. 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 3350** внешних сервисов, опубликованных в интернете;
- **более 168 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 за III и IV кварталы

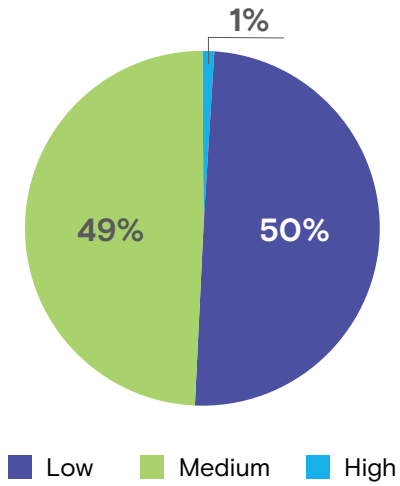
В октябре – декабре 2022 года была зафиксирована **281 тыс.** событий ИБ – подозрений на инцидент после обработки первой линией мониторинга и фильтрации ложных срабатываний. Это на треть превышает аналогичный показатель III квартала прошлого года (214 тыс. инцидентов), и это самый высокий квартальный показатель за весь 2022 год. При этом число подтвержденных инцидентов в IV квартале показало падение – почти на **20%** (речь о сложных инцидентах, которые подтвердил заказчик).

В целом картина типична для конца года: четвертый квартал, особенно декабрь, характеризуется резким всплеском событий ИБ. С одной стороны, предновогодняя суета и распродажи, с другой – поспешное закрытие финансового года, подготовка отчетов, финальные поставки. Все это активно используют злоумышленники в надежде на то, что в ворохе задач их действия останутся незамеченными.

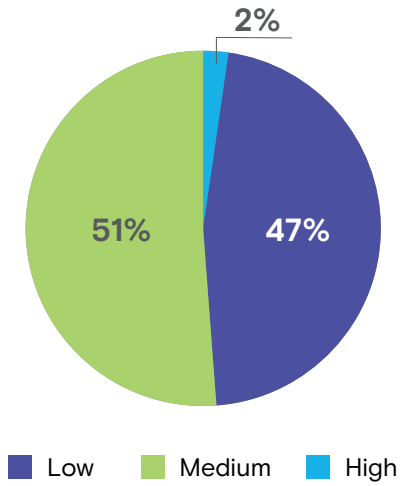
Однако такая поспешность и ситуативность сказывается на уровне подготовки: в основном это низкоквалифицированные атаки, имеющие массовый характер. В итоге мы видим снижение доли подтвержденных инцидентов. К тому же за год организации усилили защиту ИТ-периметра, и реализовывать несложные атаки хакерам стало сложнее.

Распределение инцидентов по критичности

III квартал 2022



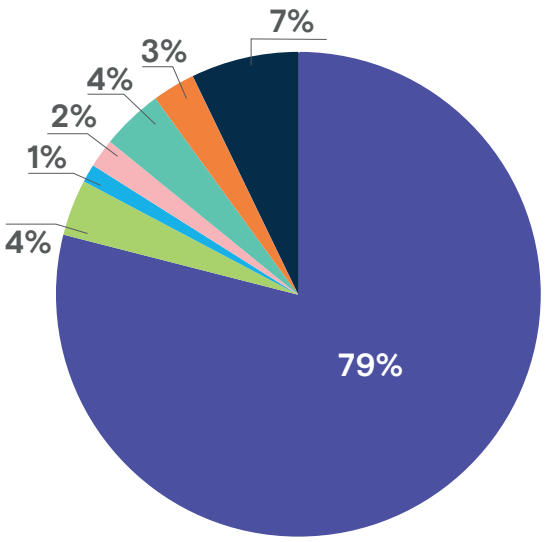
IV квартал 2022



Удельный вес каждого уровня инцидентов за квартал существенных изменений не претерпел. Произошедшее увеличение доли критических инцидентов не является опасным, так как данные показатели остаются в своих средних значениях.

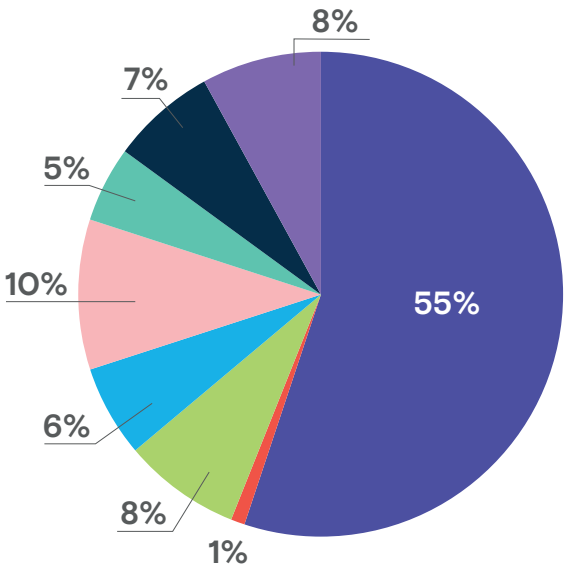
Распределение инцидентов с разным уровнем критичности по категориям

III квартал 2022



- Заражение ВПО
- Эксплуатация уязвимостей
- Сетевые атаки
- Компрометация УЗ
- НСД к ИС и сервисам
- Использование нелегитимного ПО

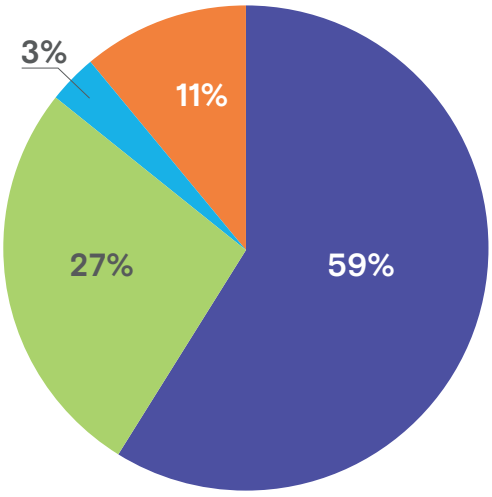
IV квартал 2022



- Заражение ВПО
- Эксплуатация уязвимостей
- Веб-атаки
- Сетевые атаки
- Компрометация УЗ
- НСД к ИС и сервисам

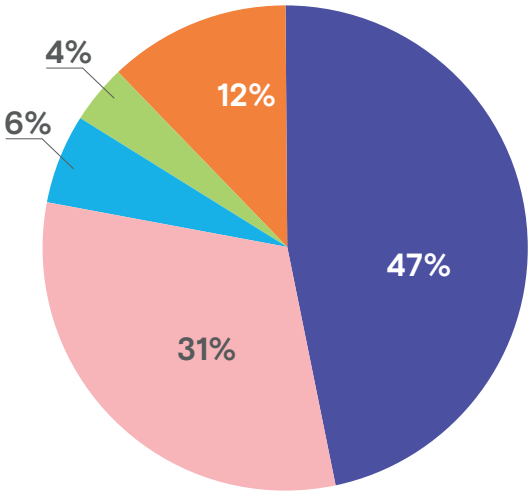
Распределение инцидентов с высокой долей критичности

III квартал 2022



- Заражение ВПО
- Компрометация УЗ
- Эксплуатация уязвимостей
- Остальное

IV квартал 2022



- Заражение ВПО
- Компрометация УЗ
- Веб-атаки
- Эксплуатация уязвимостей
- Остальное

Эти данные наглядно показывают следующее:

Вредоносное ПО остается бессменным лидером в инструментарии киберпреступников. Однако волна фишинга с рассылкой вредоносов пришлась на III квартал года и в IV квартале уже пошла на спад. Это может говорить о не совсем удачных попытках злоумышленников использовать социальную инженерию. Причины, скорее всего, в эффективной работе антивирусного ПО и повышении осведомленности сотрудников компаний в вопросах кибергигиены.

Массовые атаки со стороны хактивистов на фоне проведения СВО постепенно затухают. Это также влияет на снижение числа инцидентов, связанных с ВПО (примечательно, что за IV квартал не было выявлено ни одной атаки с использованием шифровальщиков). Это не значит, что злоумышленники потеряли интерес к России, – просто их удары стали более целевыми и осознанными. В частности, все больше инцидентов направлено на хищение клиентских данных и компрометацию учетных записей.

В IV квартале хакеры стали чаще **эксплуатировать уязвимости.** Это может указывать на то, что они поняли неэффективность фишинга и вернулись к взлому периметра. Но в то же время количество критических инцидентов подобного типа сократилось на 80%. В начале и середине года на фоне ухода зарубежных вендоров многие ИТ-продукты остались без поддержи и возможности обновления. Но со временем компании перешли на отечественные решения, нашли способы установить патчи и в целом стали вести регулярную работу с периметром на предмет выявления и закрытия нелегитимных сервисов и критических уязвимостей. Также организации стали уделять повышенное внимание к потенциальным точкам входа в инфраструктуру – публичным сервисам компаний на периметре. Все это усложнило для злоумышленников реализацию кибератак.

Веб-атаки вернулись в топ. Они лидировали в I и II кварталах, но в III их доля резко сократилась. К концу года мы увидели возвращение тренда на взлом веба. Всплеск подобных атак типичен для конца года: попытки взлома, дефейса сайтов (преимущественно это онлайн-магазины, маркетплейсы), получение доступа к конфиденциальным данным клиентов и сотрудников. Однако годом ранее в IV квартале не было зафиксировано ни одного критического инцидента, связанного с веб-атакой. Но в 2022 году все зафиксированные нами попытки взлома сайтов имели высокую степень критичности. Можно предположить, что хакеры хорошо подготовились к «жаркому» сезону и лучше продумали свои действия.

В отчетном периоде мы увидели увеличение числа **сетевых атак** и инцидентов, связанных с **компрометацией учетных записей** (УЗ). Последнее в большинстве случаев связано с брутфорсом (подбор пароля) публичных сервисов (почта, веб-порталы), используя утекшие в первой половине года учетные данные. Компрометация УЗ говорит о том, что в ряде случаев злоумышленники успешно проникали в инфраструктуру, но благодаря мониторингу SOC их удалось выявить на ранних этапах развития атаки.

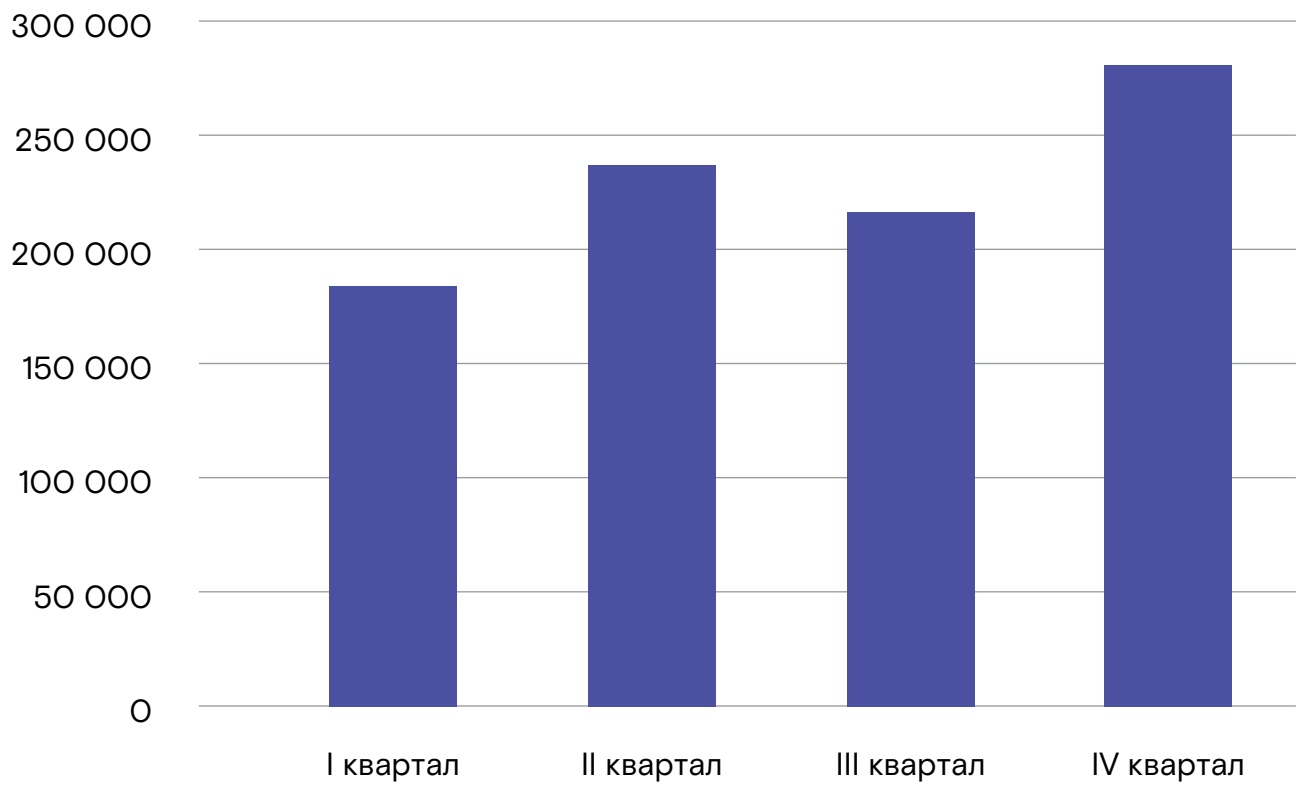
Зачастую сетевые атаки (сканирование периметра или веба) и попытки компрометации УЗ выполняются автоматизированными инструментами, которые хакеры используют для разведки в отношении клиента. Несмотря на низкий уровень критичности таких инцидентов, это опасный звонок для компаний, который указывает на то, что они привлекательны для злоумышленников. А значит, им необходимо продолжать тренд на усиление киберзащиты ИТ-периметров.

Наметившаяся в предыдущем квартале тенденция по снижению уровня критичности сетевых атак сохранилась – компании научились защищать свой периметр и уверенно движутся к повышению общего уровня защищенности.

Сводная статистика за год

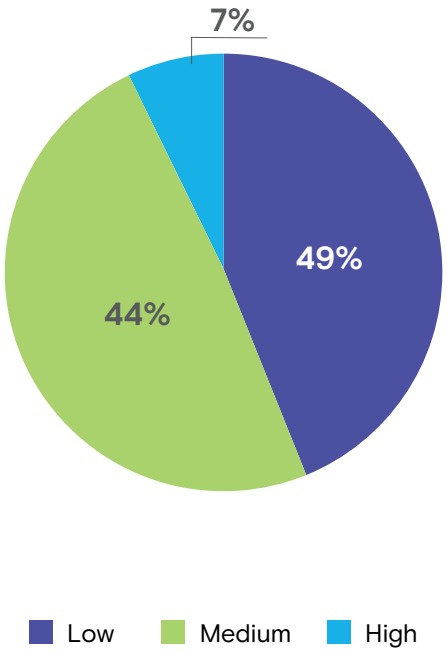
В I полугодии 2022 года было выявлено **416 тыс.** событие ИБ, и **495 тыс.** – во II, таким образом, рост составил 19%. Что же касается подтвержденных инцидентов, то здесь мы видим их резкий прирост на 73% во II полугодии. Однако доля критических инцидентов снизилась на 65%, что указывает на повышение способности российских компаний адекватно и своевременно реагировать на угрозы ИБ на фоне происходящего импортозамещения. Также мы видим более ответственный подход со стороны служб ИБ наших заказчиков – в условиях возросшей угрозы они стали активнее общаться с сервис-провайдерами и более четко выстраивать процессы реагирования на инциденты. Этот тренд виден и по росту спроса на решения класса IRP (Incident Response Platform), которые помогают выстроить и автоматизировать процесс реагирования на инциденты.

Распределение событий ИБ по кварталам

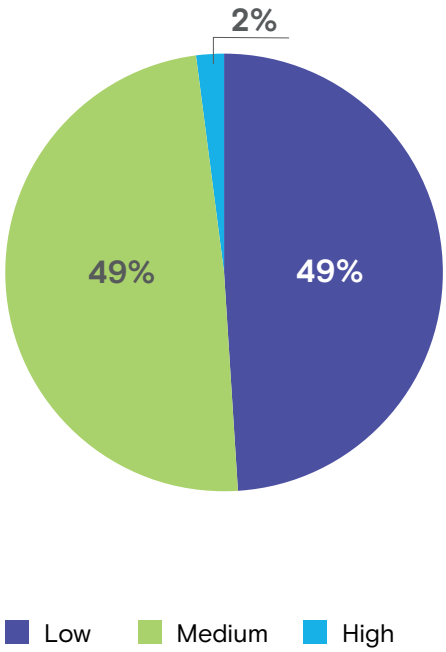


Распределение инцидентов по степени критичности

I полугодие 2022



II полугодие 2022

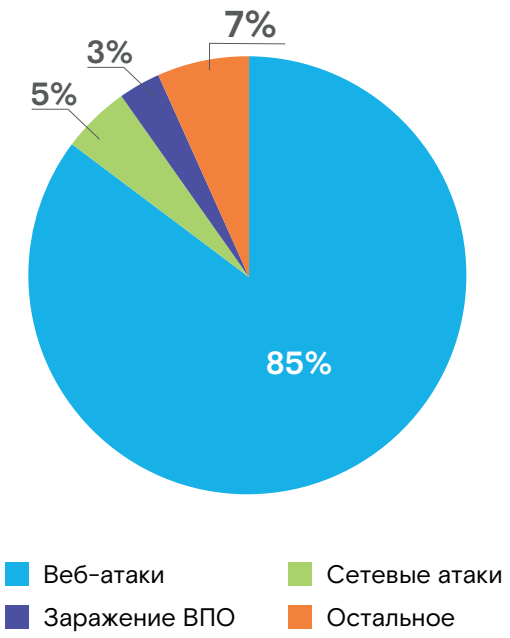


Примечательно, что в I полугодии доля критических инцидентов снизилась (на 7%) в сравнении со II полугодием 2021 года. Во II полугодии 2022 мы видим продолжение этого тренда. Это может показаться парадоксальным на фоне активного роста числа атак. Но стоит понимать, что с момента начала СВО российский бизнес серьезно озаботился вопросами собственной киберзащиты. В частности, мы видим кастомизацию сценариев детектирования инцидентов и реагирования на них, что в итоге и дает положительную динамику на общем фоне. Чтобы не допустить роста числа критических инцидентов, компаниям важно вовремя выстроить эффективный процесс выявления угроз и реагирования на них. Инструменты (такие как SIEM, IRP) – это лишь часть решения. Важно не забыть про экспертную команду и настроенные процессы.

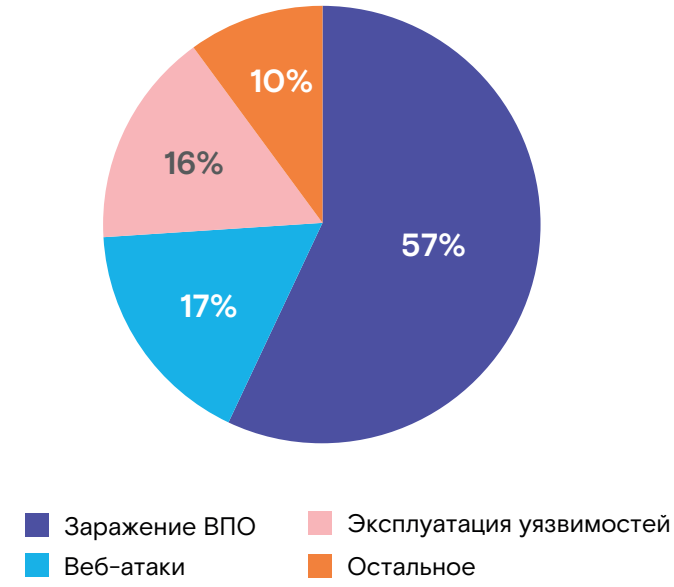
Самые популярные типы атак в течение года менялись. Инциденты с высокой степенью критичности в I полугодии были связаны в основном с веб-атаками, далее следовали ВПО и сетевые атаки. Во втором полугодии вектор сменился: сетевые атаки в принципе утратили свою критичность, удельный вес веб-атак снизился, а лидирующие позиции заняло ВПО.

Распределение инцидентов с высокой долей критичности

I полугодие 2022

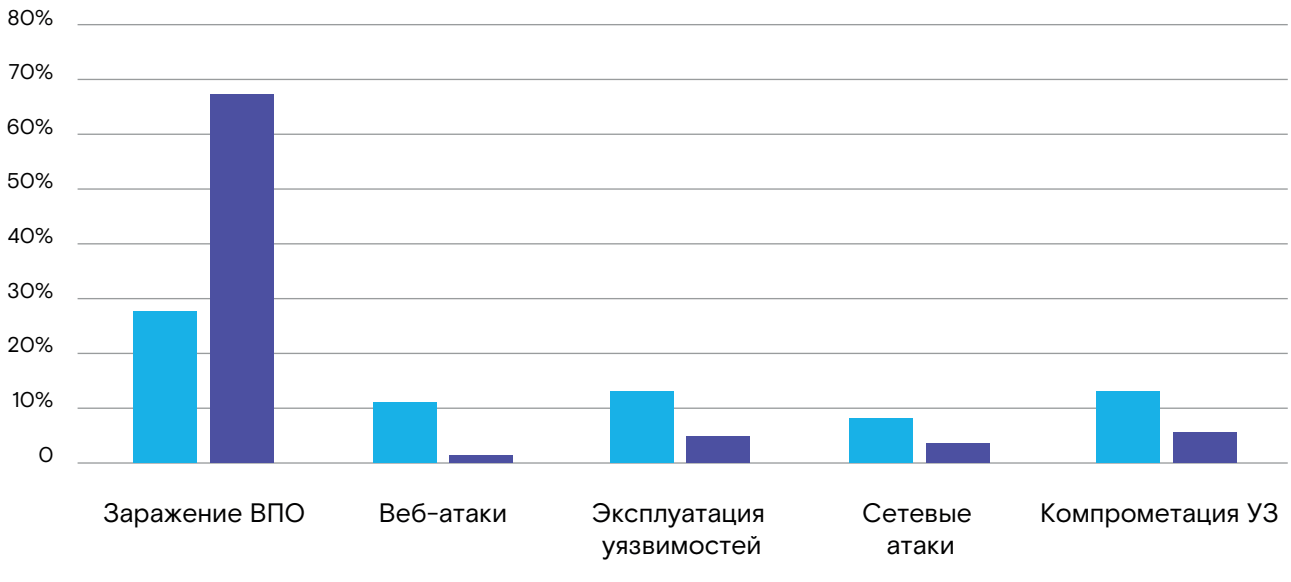


II полугодие 2022



Если же смотреть на весь пул инцидентов, то видно увеличение почти на 40% доли ВПО во II полугодии, в то время как остальные типы самых популярных атак, наоборот, теряют свой удельный вес.

Распределение инцидентов с разным уровнем критичности



Общие выводы

- Кибермир является отражением реального – все изменения в нем происходят зеркально и с максимально быстрой обратной связью. В 2022 году киберландшафт трансформировался как никогда стремительно, а тренды сменяли друг друга из квартала в квартал.
- За 2022 год общее количество событий ИБ увеличилось практически в 2 раза.
- Эксплуатация уязвимостей, несмотря на некоторое снижение удельного веса во втором полугодии, по-прежнему остается своеобразной брешью во многих российских компаниях, на закрытие которой направлены процедуры перехода на российское ПО.

Прогнозы

- Злоумышленники постоянно изобретают новые способы обхода средств защиты, поэтому без анализа событий обнаружить подозрительную активность становится крайне затруднительно. А значит, без центров мониторинга (SOC) выявлять атаки в 2023 будет сложнее.
- Массовые злоумышленники (хактивисты) либо пропадают, либо повышают квалификацию и объединяются под руководством более профессиональных хакеров. Последние координируют реализацию конкретных задач и целенаправленно атакуют российские компании.
- Кибермразведка активно используется злоумышленниками для профилирования векторов атак под заказчика – этот же инструмент должен использоваться компаниями для понимания своих уязвимых мест. Например, можно находить и блокировать фишинговые сайты, выявлять уязвимости на периметре с помощью Shodan, искать утекшие базы данных или фейковые аккаунты топ-менеджеров в социальных сетях. Также с помощью кибермразведки можно мониторить новостной фон и отслеживать негатив в отношении бренда. Это поможет понять, находится ли компания в поле зрения злоумышленников.
- Мы видим, что компании выстраивают более тесное взаимодействие с сервис-провайдерами. Решения класса IRP в компаниях станут необходимым инструментом базового SOC на фоне необходимости быстрого и четкого реагирования.
- Решения класса Sandbox (песочница) станут важным элементом кибербеза, потому что вектор фишинга будет только усложняться и совершенствоваться. В том числе злоумышленники будут использовать вредоносы, не детектируемые антивирусами.

Ростелеком
Солар

rt.ru | rt-solar.ru

solar@rt-solar.ru

+7 (499) 755-07-70