Атаки на российские компании во II квартале 2023 года

Отчет

rt-solar.ru
rt.ru

Ростелеком
Солар

Оглавление

О компании

«РТК-Солар» – национальный провайдер сервисов и технологий кибербезопасности. Под защитой – 850+ 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
- Эксплуатация систем ИБ и реагирование на атаки
- Анализ угроз и внешней обстановки
- Комплексный контроль защищенности
- Реагирование на инциденты и техническое расследование
- Построение SOC или его частных процессов (в том числе центров ГосСОПКА)

Введение

Количество кибератак продолжает расти, при этом уже ко II кварталу обозначился тренд на рост эксплуатации уязвимостей. Переход компаний на отечественное ПО открыл хакерам новые возможности в этом направлении, однако такие инциденты в целом не наносили критического ущерба. В то же время по характеру критических инцидентов видно, что атаки становятся более точечными и высокопрофессиональными: хакеры все чаще используют киберразведку и вредоносы, способные обходить антивирусную защиту. Среди применяемого ВПО особенно заметно увеличение доли шифровальщиков, при этом хакерская активность направлена в первую очередь на оказание деструктивного воздействия.

В настоящем отчете приведены данные об инцидентах, выявленных командой центра противодействия кибератакам Solar JSOC[1] в I–II кварталах 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 более 290 компаний и организаций из разных отраслей экономики: госсектор, финансы, нефтегазовая отрасль, 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:

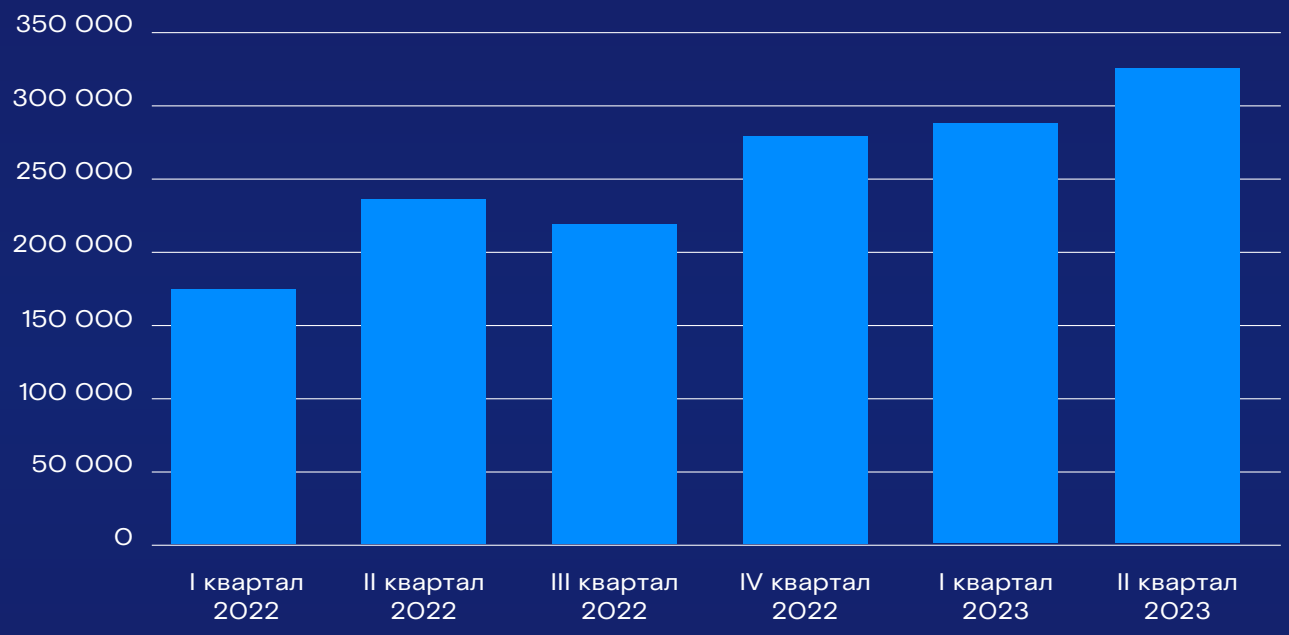
- более 3500 внешних сервисов, опубликованных в интернете;
- около 173 тыс. серверов общего, инфраструктурного и прикладного назначения.

[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 II квартала

За II квартал было выявлено **325 тысяч** событий ИБ – подозрений на инцидент после обработки первой линией мониторинга и фильтрации ложных срабатываний. Это на **12%** больше, чем в I квартале 2023 г., и на **38%** превышает показатель аналогичного периода прошлого года.

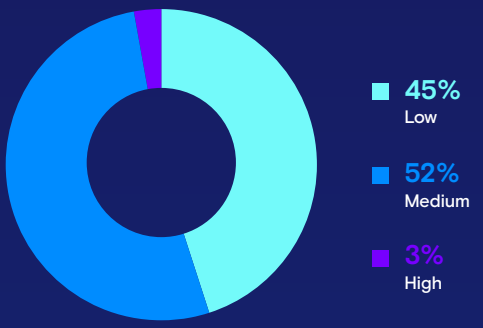
Распределение событий ИБ по кварталам



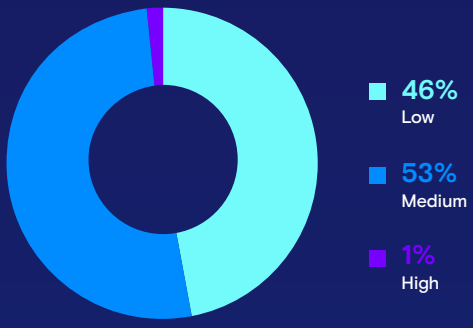
Тенденция на увеличение числа событий ИБ, сформировавшаяся еще в конце прошлого года, сохранилась и теперь, однако темпы роста снова ускорились: с **3%** в I квартале до нынешних **12%**. Количество подтвержденных инцидентов из всего объема выявленных событий ИБ – **8850**: прирост составил **24%** по сравнению с I кварталом 2023 г.
Все это напрямую указывает на то, что злоумышленники активизировались с новой силой, но изменили векторы и задачи проведения кибератак. Зафиксированная во II квартале хакерская активность в первую очередь нацелена на оказание деструктивного воздействия, а не на достижение быстрых успехов посредством взлома публичных сервисов компаний.

Распределение инцидентов по критичности

I квартал 2023



II квартал 2023

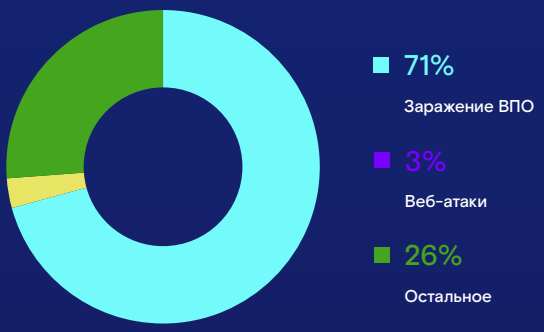


В целом удельный вес каждого типа инцидента по сравнению с предыдущим кварталом существенных изменений не претерпел. Если же оценивать абсолютные значения, то можно заметить некоторую переориентацию атак: увеличение числа инцидентов низкой и средней степени критичности говорит об изменении векторов атак и смещении фокуса внимания злоумышленников на ИТ-инфраструктуру и пользователей компаний (это выражается, в частности, в росте фишинга и атак через подрядчиков).

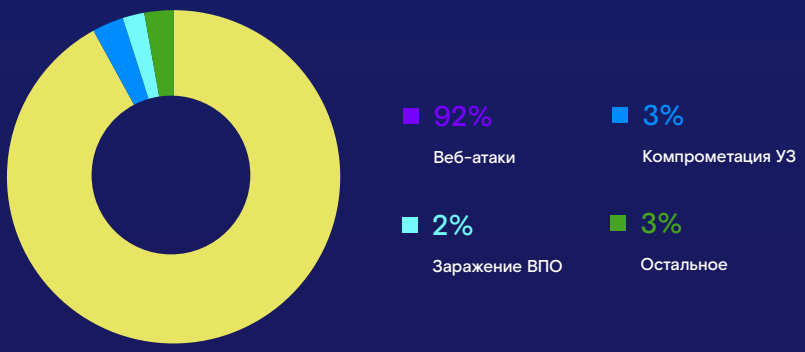
Распределение высококритических инцидентов по категориям

I квартал 2023

II квартал 2023



II квартал 2022

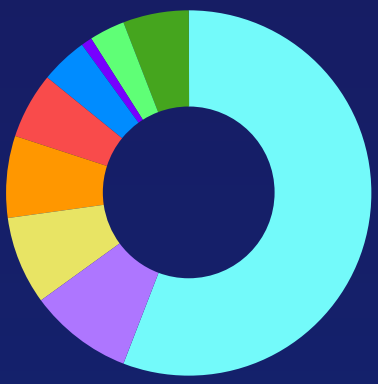


Как и в предыдущие периоды, во II квартале применение ВПО – наиболее частый инструмент в руках хакеров, который приводит к наступлению критических инцидентов. Из них **36%** были связаны с применением шифровальщиков, что на **26%** превышает аналогичный показатель I квартала текущего года. Это подтверждает предыдущие наши прогнозы о том, что атаки становятся более сложными и точечными.

На фоне всплеска атак с шифровальщиками за анализируемый период не было зафиксировано ни одного критического инцидента, вызванного сетевой атакой или же эксплуатацией уязвимостей. Это напрямую указывает на то, что российские компании стали лучше защищать свой периметр, также это и результат закрытия «дыр» в инфраструктуре, которые появились в связи с уходом западных вендоров и невозможностью своевременных обновлений. Резко (с 24% до 3%) сократилось количество критических инцидентов, связанных с веб-атаками: они не пропали с радаров – просто за предыдущий период организации со зрелой ИБ усилили защиту онлайна, и подобные кибернападения перешли для них в разряд стандартных.

Распределение всего объема инцидентов по категориям

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
- 3% Компрометация ИС, выявленная по TI
- 6% Остальное

II квартал 2023

- 49% Заражение ВПО
- 4% Использование нелегитимного ПО
- 7% Сетевые атаки
- 15% Эксплуатация уязвимостей
- 7% НСД к ИС и сервисам
- 4% Компрометация УЗ
- 1% Веб-атаки
- 5% Компрометация ИС, выявленная по TI
- 8% Остальное

В целом анализируемый период не характеризуется какими-либо аномалиями – резкими спадами или всплесками того или иного типа атак или резкой переориентацией векторов. Количество инцидентов, вызванных заражением ВПО и сетевыми атаками, снизилось. При этом увеличилось число случаев компрометации информационных систем, выявить которые удавалось только с помощью индикаторов Threat Intelligence и процессов Threat Hunting: хакеры стали использовать вредоносное ПО (ВПО), обходящее средства антивирусной защиты, в том числе посредством фишинговых рассылок, интенсивность и опасность которых возросла.

То есть мы в очередной раз видим, что атаки становятся более точечными и высокопрофессиональными – базовые средства SOC (без использования технологий EDR, NTA и при отсутствии процессов Threat Hunting) уже не могут их предотвратить и выявить на ранних стадиях. На фоне усложнения атак хакеры стали чаще эксплуатировать уязвимости, что связано в том числе с переходом компаний на отечественное ПО: часть решений разрабатывалась и внедрялась в ускоренном режиме, что дало злоумышленникам широкое поле для выявления и использования «дыр» в безопасности.

Выводы по II кварталу

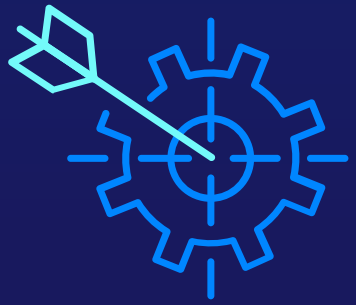
1. В отчетный период произошла очередная переориентация типов атак. Значительный рост количества инцидентов говорит о новой волне кибератак на российскую инфраструктуру. Злоумышленники стали действовать опаснее, изменив подходы и цели.

2. В комплексных атаках злоумышленники все чаще используют данные, полученные с помощью кибербразведки, что видно по характеру самих инцидентов. Поэтому наличие симметричных инструментов в руках организаций позволит не только закрыть уязвимые места ИТ-инфраструктуры, но и подготовиться к тем векторам, от которых закрытие уязвимостей не поможет.

3. Вредоносное ПО по-прежнему остается самым популярным инструментом среди хакеров. Как уже отмечалось, количество инцидентов с применением ВПО, не детектируемого средствами антивирусной защиты, увеличивается. Наличие таких вредоносов в фишинговых рассылках существенно повышает успешность проводимых атак.

4. Для проведения комплексных атак хакеры все чаще используют легитимное ПО и инструменты сокрытия своей активности в сети компаний, поэтому детектирование значительно усложняется и требует специальных решений, а также наличия продвинутых навыков у сотрудников службы ИБ.

5. Векторы эксплуатации уязвимостей иностранного ПО и оборудования, которыми активно пользовались хакеры последние полтора года, идут на спад: кто-то успел закрыть «дыры», кто-то уже, к сожалению, «погорел» на этом. Однако в целом за II квартал злоумышленники стали эксплуатировать уязвимости чаще. Безусловно, этому поспособствовал давно наметившийся тренд импортозамещения – злоумышленники начали активно эксплуатировать уязвимости в отечественном ПО, например CMS Bitrix и уязвимость CVE-2022-27228.



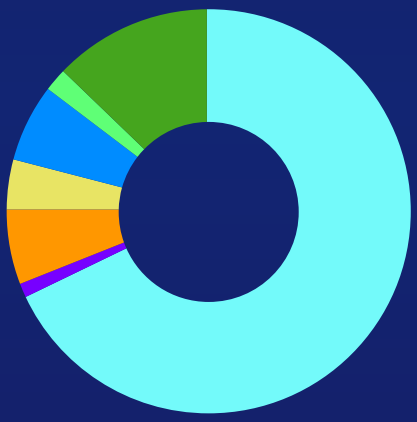
Динамика I полугодия

За I полугодие 2023 г. центр противодействия кибератакам Solar JSOC выявил **614 тысяч** событий ИБ, что практически на четверть (**24%**) превышает показатель II полугодия 2022 г. При этом доля подтвержденных инцидентов в общем объеме сократилась на 22%.

В среднем на одного клиента во II полугодии 2022 г. приходилось 1813 событий ИБ, тогда как в I полугодии 2023 – уже **2112**, то есть рост составил **17%**. Среднее количество подтвержденных инцидентов, напротив, снизилось на **38%** (с 76 до 55 на клиента). Доля критических инцидентов, приходящихся на одного заказчика, осталась неизменной, тогда как во II полугодии 2022 г. мы наблюдали ее снижение на 71%.

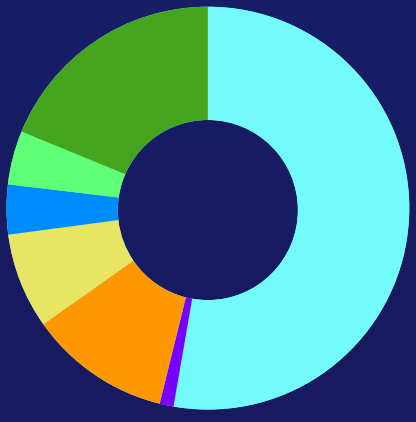
Распределение всего объема инцидентов по категориям

II полугодие 2022



- 68% Заражение ВПО
- 1% Веб-атаки
- 6% Эксплуатация уязвимостей
- 4% Сетевые атаки
- 6% Компрометация УЗ
- 2% Компрометация ИС, выявленная по TI
- 13% Остальное

I полугодие 2023



- 53% Заражение ВПО
- 1% Веб-атаки
- 11% Эксплуатация уязвимостей
- 8% Сетевые атаки
- 4% Компрометация УЗ
- 4% Компрометация ИС, выявленная по TI
- 19% Остальное

Наиболее популярным инцидентом во II полугодии 2022 года стало заражение ВПО (68%), в I полугодии текущего года доля инцидентов данного типа снизилась (53%), однако он все еще в топе. Примерно в 2 раза увеличились доли сетевых атак, эксплуатации уязвимостей и сложных компрометаций ИС, выявляемых только с помощью индикаторов Threat Intelligence и процессов Threat Hunting. Последнее говорит о том, что количество продвинутых и наиболее опасных атак растет и мы наблюдаем новую волну киберпротивостояния. С предыдущим ее вариантом компании более-менее научились справляться – в части своевременного детектирования инцидентов и обеспечения ИБ в целом. Однако и злоумышленники все это время не стояли на месте: большое количество утечек и взломов, появление в открытом доступе более продвинутого хакерского инструментария сформировали обширные возможности для целевых атак.

Вместе с тем рост сетевых атак подтверждает сформированный ранее тезис о том, что в 2023 году злоумышленники будут активно использовать кибербразведку для поиска уязвимостей в инфраструктуре компаний. Однако сетевые атаки, являясь, с одной стороны, довольно простым и не требующим высокой квалификации типом инцидентов, могут указывать на то, что компания попала в поле зрения хакеров. Не исключено, что в будущем она столкнется с более серьезной кибератакой.

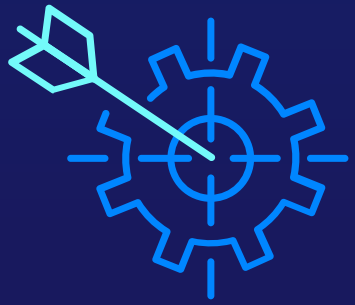
Выводы по I полугодию

1 За прошедшее полугодие векторы кибератак существенно изменились: все больше наблюдается расслоение подходов. Злоумышленники низкой квалификации генерируют большое количество «фонового шума», но для большинства компаний такие атаки не являются критичными и не влекут за собой последствий, однако при этом явно выделяются группы, координируемые централизованно. Функционал, оснащенность и квалификация последних значительно выросла за последний год, а в качестве целей они выбирают нанесение серьезного ущерба компаниям, а не простую организацию DDoS-атак и взломов веб-сайтов.

2 Аналогичная ситуация и по веб-атакам. Они были очень популярны в 2022 году, сейчас же крайне малая их доля наносит существенный ущерб российским компаниям: усиление защиты онлайна снизило эффективность DDoS-атак уровня приложений (L7). Тем не менее периодически возникают всплески активности, направленной на эксплуатацию очередных критических уязвимостей сайтов, использующих популярные движки и компоненты.

3 Число событий ИБ продолжает расти. Вместе с тем мы видим, что российские компании научились справляться с ситуацией предыдущего года и обеспечивать защищенность. Но не стоит расслабляться – атаки усложняются, квалификация злоумышленников повышается, и этот тренд явно получит дальнейшее развитие в будущем. В том числе и поэтому мы продолжаем наблюдать рост спроса на сервисы SOC с расширениями в части хостового и сетевого детекта (EDR и NTA), с расширением на АСУ ТП, а также на решения для работы с инцидентами (системы класса SOAR/IRP).

4 Злоумышленники ежедневно сканируют инфраструктуры в поисках уязвимых сервисов с целью развития вектора проникновения. Существенное увеличение числа сетевых атак во многом спровоцировано активным распространением инструментария для разведки поверхности атаки – в том числе самописных сборок новых инструментов.



Ростелеком
Солар

rt.ru
rt-solar.ru

Email:
solar@rt-solar.ru

Телефон:
+7 (499) 755-07-70