Ростелеком
Солар

Атаки на российские компании в 3-м квартале 2022 года

Отчет

Москва
2022

Содержание

О компании

«РТК-Солар» обеспечивает и гарантирует кибербезопасность в организациях от малого бизнеса до федеральных органов власти. Ключевые направления деятельности: аутсорсинг ИБ, разработка собственных продуктов, комплексные проекты по кибербезопасности.

Компания предлагает сервисы первого и лидирующего в РФ коммерческого SOC 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, анализатор кода Solar appScreener, систему повышения эффективности труда Solar addVisor. Направление «Solar Интеграция» реализует масштабные проекты по созданию систем кибербезопасности, фокусируясь на защите территориально-распределенных объектов, центров обработки данных, а также объектов КИИ и АСУ ТП. Для повышения киберустойчивости всей России «РТК-Солар» развивает Национальный киберполигон, ключевым компонентом которого является платформа для практической отработки навыков защиты от киберугроз «Кибермир».

Штат компании 1600+ специалистов. Имеются представительства в Москве, Санкт-Петербурге, Нижнем Новгороде, Самаре, Ростове-на-Дону, Томске, Хабаровске и Ижевске. Деятельность компании лицензирована ФСБ России, ФСТЭК России и Министерством обороны России.

Список сервисов Solar JSOC:

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

Введение

Мировые события начала 2022 года продолжают оказывать значительное влияние на ландшафт киберугроз. Количество кибератак остается высоким, однако их характер меняется. Типовые инциденты и массовые сканирования сократились на порядок, а их место заняли сложные атаки. На этом фоне усложняются и контрмеры, которые применяют компании. Все чаще используются продвинутые СЗИ (NTA, EDR), растет спрос на разработку кастомизированных сценариев реагирования. В целом очевидно, что 2022 год оказал сильное влияние как на хакерские техники и тактики, так и на подход организаций к киберзащите.

В настоящем отчете приведены данные об инцидентах, выявленных командой Solar JSOC[1] в 3-м квартале 2022 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 265 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 3100 внешних сервисов, опубликованных в интернете;
- Более 158 тыс. серверов общего, инфраструктурного и прикладного назначения.

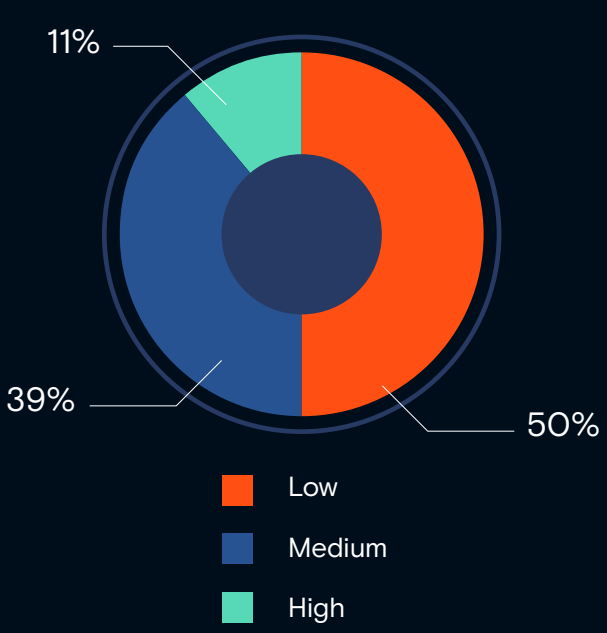
[1] В отчет вошли агрегированные данные об атаках на компании, подключенные к сервису мониторинга киберинцидентов Solar JSOC. Аналитика не учитывает информацию о клиентах управляемых сервисов кибербезопасности Solar MSS (включая магистральный Anti-DDoS и WAF), результаты услуг по расследованию киберинцидентов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

Сводная статистика по инцидентам

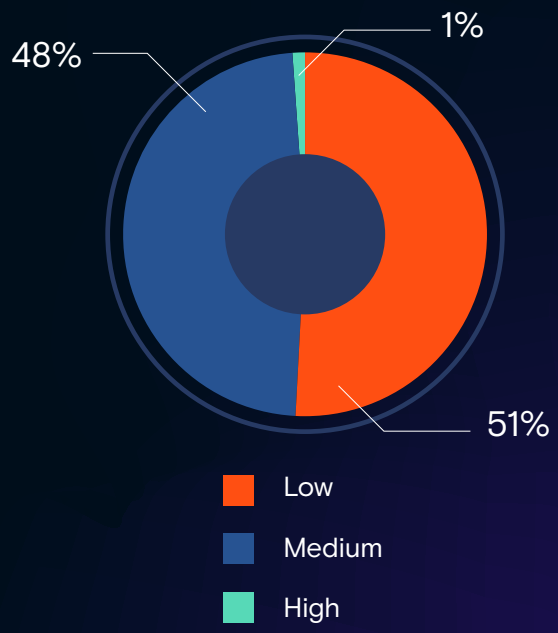
В июле – сентябре 2022 года было зафиксировано более **214 тыс.** событий ИБ – подозрений на инцидент после обработки первой линией мониторинга и фильтрации ложных срабатываний. Это немного ниже показателей 2-го квартала 2022 года (236 тыс. инцидентов), но в сравнении с началом года, когда эксперты «РТК-Солар» зафиксировали 184 тыс. инцидентов, уровень киберугрозы остается высоким. Но в то же время число подтвержденных инцидентов показало практически двукратный рост.

Распределение инцидентов по критичности:

2-й квартал 2022



3-й квартал 2022

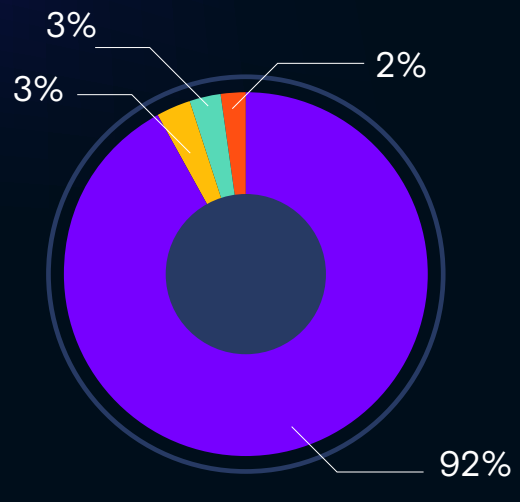


Количество инцидентов с высокой степенью критичности сократилось. Это объясняется тем, что компании выстроили эффективную защиту от ключевых угроз, которые проявились в 1-м и 2-м кварталах года. Благодаря этому «градус инцидентов» снизился.

Наша практика показывает, что норма количества инцидентов с высокой степенью критичности составляет 2-4%, а летом традиционно уровень падает до 1-2%. Поэтому скорее можно говорить о стабилизации ситуации и возвращении к норме.

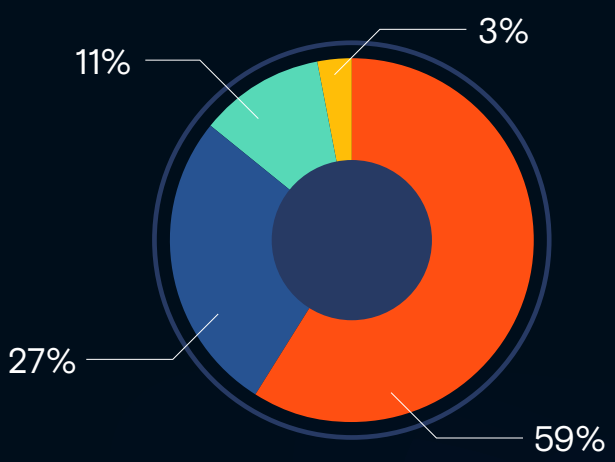
Распределение высококритичных инцидентов по категориям:

Инциденты с высокой долей критичности, 2-й квартал 2022



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

Инциденты с высокой долей критичности, 3-й квартал 2022



- Заражение ВПО
- Эксплуатация уязвимостей
- Компрометация УЗ
- Остальное

Несмотря на существенное снижение общего числа критических инцидентов, они по своему содержанию стали более серьезными. Если в 1-м и 2-м кварталах большая их часть приходилась на веб-атаки, то в 3-м квартале абсолютное большинство (**59%**) подобных атак связано **с использованием ВПО**. В частности, шифровальщики на хосте были обнаружены при разборе 20% критических инцидентов. Значительная доля вредоносов доставлялась на компьютер жертвы с помощью фишинговых рассылок. То есть мы наблюдаем поэтапное развитие общего ландшафта кибератак, когда в первом квартале года злоумышленники массово пытались проникнуть в инфраструктуру компаний, используя уязвимости и атаки на веб.

Теперь же они успешно практикуют технику проникновения, используя человеческий фактор либо реализуя шаги по закреплению в инфраструктуре.

Более активная **эксплуатация хакерами уязвимостей** также была прогнозируема и связана с уходом зарубежных вендоров с российского рынка. В таких условиях пропала возможность «пропатчить» выявленные уязвимости или обновить сигнатуры на зарубежных СЗИ. Безусловно, переход на отечественное ПО происходит, но очевидно, что это поэтапный процесс, требующий времени.

Помимо этого, компании, учитывая векторы атак 1-го и 2-го кварталов, усилили контроль за периметром, поэтому злоумышленники пытаются активнее использовать новейшие уязвимости, реализуя PoC-эксплойт в своих инструментах спустя всего несколько часов с момента публикации. Этот тренд фиксируется SOC (Security Operations Center) на уровне правил, логов и кастомных сигнатур для пограничных СЗИ (IPS, WAF), так как вендорские обновления либо запаздывают (срок появления составляет часы и дни), либо отсутствуют в силу того же ухода западных игроков.

В то же время **веб-атаки**, составлявшие ранее практически весь пул критичных инцидентов, в 3-м квартале фигурируют на уровне базовых флуктуаций. Сетевые атаки, число которых стало сокращаться еще во втором квартале, также утратили свою критичность.

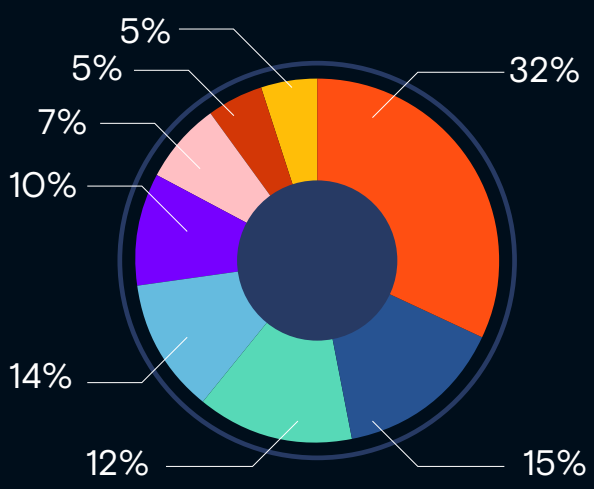
Можно предположить, что тенденция, связанная с дальнейшим дифференцированием подходов к проникновению и закреплению в инфраструктуре, будет нарастать, как и использование тактик не «в лоб», а, например, атак через подрядчиков.

В целом круг инцидентов с разным уровнем критичности уже на протяжении длительного периода остается неизменным. Однако за минувший квартал можно говорить о ряде изменений, связанных в первую очередь с уменьшением числа веб-атак после резкого роста в начале года. В первом квартале взломы сайтов во многом осуществлялись ради мгновенной реакции со стороны общественности, появления резонансных инфоповодов и создания паники среди населения. Очевидно, что такой подход в принципе не мог существовать долго, поэтому уже летом злоумышленники начали

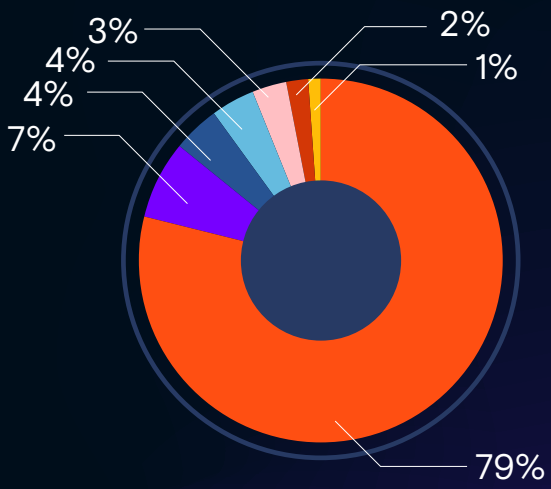
перестраивать тактики, а сейчас их фокус сместился окончательно. Текущие цели во многом определяют позиционный характер этих тактик, направленный на проникновение, закрепление и нанесение ущерба. Наметившиеся во втором квартале тенденции к снижению количества сетевых атак, случаев компрометации УЗ и совершения НСД к ИС и сервисам сохранились, в остальном же существенных изменений киберландшафт не претерпел.

Распределение инцидентов с разным уровнем критичности по категориям:

2-й квартал 2022



3-й квартал 2022



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

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

Выводы

Можно предположить, что до конца года эксплуатация уязвимостей и применение ВПО будут формировать киберландшафт на ближайшую перспективу. Успешность же атак во многом будет зависеть от своевременности принимаемых компаниями мер в части ИБ и скорости импортозамещения. При этом SOC (неважно – внешний или внутренний) в текущей ситуации должен являться ядром кибербезопасности компаний, так как он позволяет контролировать состояние ИТ-инфраструктуры в конкретный момент времени (в отличие от аудита) и оперативно выявлять возникающие внешние угрозы.

Вторым вектором, как и прогнозировалось, стали атаки, связанные с эксплуатацией уязвимостей. Этот тренд сохранится, так как отечественные компании имеют ряд проблем, которые не получится оперативно решить. В частности, это долгий переход на отечественное ПО и сложности с обновлением сигнатур и модулей безопасности западных СЗИ. Кроме того, хакеры атакуют компании любых масштабов из разных отраслей, и далеко не все организации скорректировали свой подход к ИБ на фоне нарастающей угрозы.

Снижение числа критичных инцидентов едва ли говорит о стабилизации ситуации и скорее указывает на то, что злоумышленники концентрируются на определенных целях и более сложных подходах к атакам. Однако при этом существенный рост удельного веса инцидентов со средней и низкой степенью критичности указывает на определенное повышение уровня защищенности российских компаний.

DDoS- и веб-атаки сделали свое дело, и теперь злоумышленники активно применяют различное ВПО. Фишинг будет одним из двух основных векторов проникновения в инфраструктуру компаний в ближайшие месяцы.

В третьем квартале сформировался четкий тренд на переход от массовых атак к более точечным.

Контакты

rt.ru

rt-solar.ru

solar@rt-solar.ru

+7 (499) 755-07-70