Ростелеком
Солар

Отчет
Атаки на российские компании во 2-м квартале 2022 года

Москва 2022
rt-solar.ru

ОГЛАВЛЕНИЕ

О компании....3

Введение....4

Сводная статистика по инцидентам....5

Динамика 1-го полугодия в целом....9

Выводы....11

Контакты....12

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
- 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

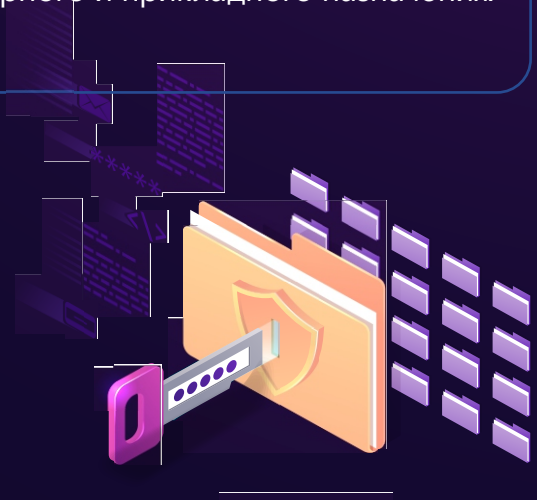
Мировые события начала 2022 года продолжают оказывать значительное влияние на ландшафт киберугроз. Драматичный рост числа инцидентов не прекращается, однако на смену массовым несложным атакам приходят более точечные удары по конкретным отраслям. На этом фоне компании начинают уделять всё больше внимания собственной кибербезопасности, а базовые средства защиты всё чаще дополняются специализированными сенсорами на сети и конечных узлах.

В настоящем отчете приведены данные об инцидентах, выявленных командой Solar JSOC[1] во 2-м квартале 2022 года, и их сравнение со статистикой 1-го квартала 2022 года. В конце также приведено сравнение ИБ-ландшавтов 1-го полугодия 2022 и 1-ого полугодия 2021 года. В исследовании отражена приоритизация инцидентов по степени критичности, а также процентное соотношение различных типов кибератак, которые наблюдались в отчётный период.

В фокус внимания экспертов попало более 250 компаний и организаций из разных отраслей экономики: госсектор, финансы, нефтегазовая отрасль, энергетика, телекоммуникации, крупный ретейл. Все компании представляют сегмент Large Enterprise и Enterprise со среднем 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 2800 внешних сервисов, опубликованных в интернете;
- более 140 тыс. серверов общего, инфраструктурного и прикладного назначения.

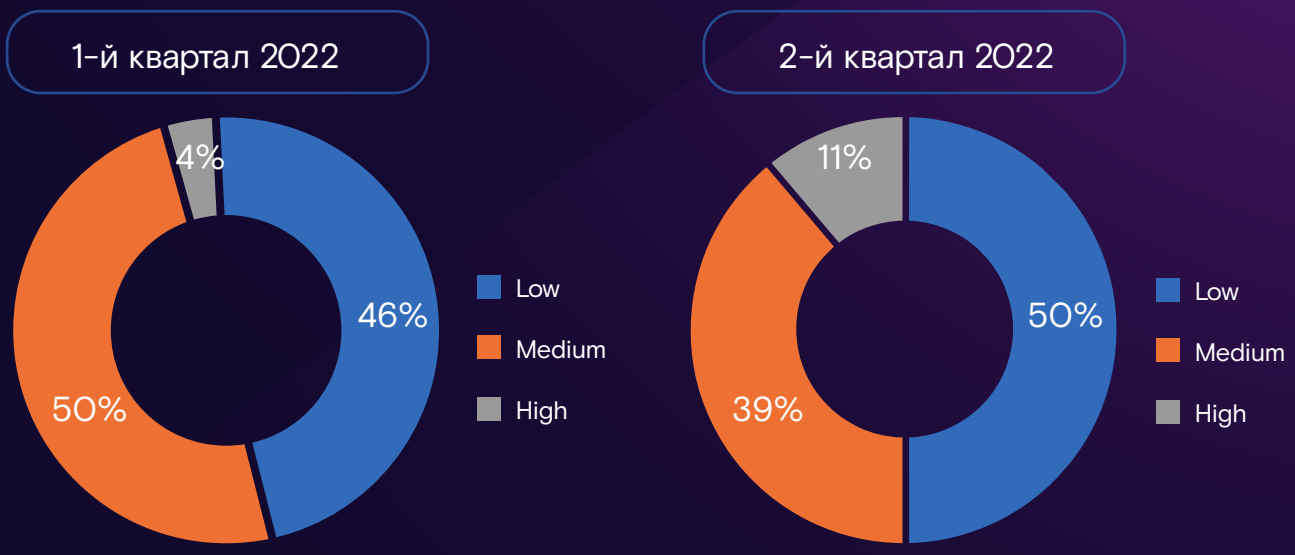


[1] В отчет вошли агрегированные данные об атаках на компании, подключенные к сервису мониторинга киберинцидентов Solar JSOC. Аналитика не учитывает информацию о клиентах управляемых сервисов кибербезопасности Solar MSS (включая магистральный Anti-DDoS), результаты услуг по расследованию киберинцидентов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

Сводная статистика по инцидентам

В апреле – июне 2022 года было зафиксировано более 236 тыс. событий ИБ – подозрений на инцидент после обработки первой линией мониторинга и фильтрации ложных срабатываний. Это практически на треть (на 31%) превышает показатель 1-го квартала 2022 года.

Распределение инцидентов по критичности:



При этом во 2-м квартале мы отмечаем почти трехкратное увеличение количества подтвержденных инцидентов высокой степени критичности. На этом фоне оперативность оповещений стала важным критерием работы SOC. Отметим, что критичность влияет на скорость оповещения, которая определяется заказчиками совместно с сервис-провайдером и может меняться в процессе оказания услуги. Время разбора подозрения на инцидент категории high составляет до 30 минут. Это подтверждает тренд на повышение внимания к ИБ со стороны всех направлений, включая бизнес.

Наибольшее число инцидентов с разным уровнем критичности связано с применением хакерами вредоносного ПО, причем во втором квартале наблюдается рост доли подобных атак: с 25% до 32%. Это объясняется несколькими трендами.

- Начиная с 24 Февраля хакеры преимущественно использовали массовые DDoS- и веб-атаки, однако со второго квартала они стали активнее применять фишинг - массовые рассылки с вредоносными вложениями и ссылками.

- Если в 1-м квартале взломы популярных веб-сайтов происходили ради дефейса и хактивизма, то сейчас также для размещения ВПО и последующего заражения хостов посетителей.

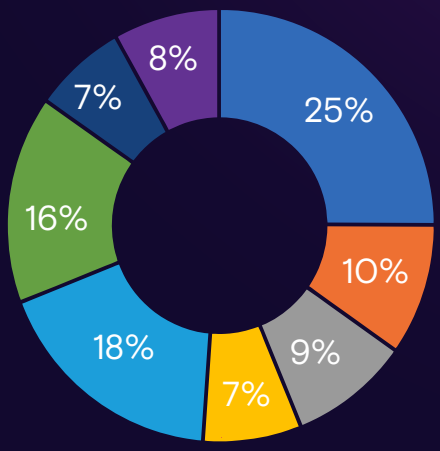
- Стали активнее распространяться сборки легитимного ПО с вредоносами на борту через файлообменники.

Также во 2-м квартале наблюдается значительный рост доли (с 9% до 15%) инцидентов, связанных с эксплуатацией уязвимостей. В то же время повышается скорость применения эксплойтов для проведения атак на ресурсы российских компаний. Это объясняется как отсутствием возможности установить обновления на уязвимый софт, так и проблемами с получением обновлений сигнатур на средствах защиты (IPS, WAF) из-за ухода зарубежных вендоров с российского рынка.

Другая проблема заключается в сроках закрытия уязвимостей. Из-за сложностей с согласованием простоя на период обновления, предварительным тестированием патчей и прочих процедур далеко не все компании готовы установить обновления на бизнес-критичные системы в течение суток. Об этом, разумеется, знают хакеры. Поэтому не стоит исключать того, что число атак, связанных с эксплуатацией уязвимостей, особенно актуальных, будет и дальше расти.

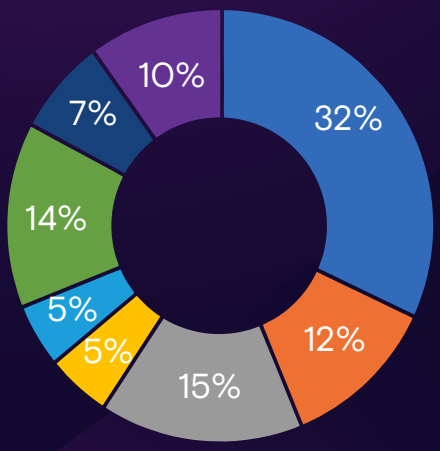
Распределение всего объема инцидентов по категориям:

1-й квартал 2022



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

2-й квартал 2022



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

В целом перечень наиболее популярных типов атак сохраняется, что объясняется дешевизной и простотой ряда техник, а также наличием стандартных слабых мест в инфраструктурах атакуемых компаний.

Набор критических инцидентов по сравнению с 1-м кварталом 2022 года немного изменился. Как и ранее, большая их часть связана с веб-атаками, доля которых за квартал выросла с 77% до 95%. Резкий всплеск веб-атак наметился в конце февраля, когда из-за стремления посеять панику злоумышленники атаковали веб-платформы, чтобы, например, залить на сайт какой-нибудь провокационный баннер.

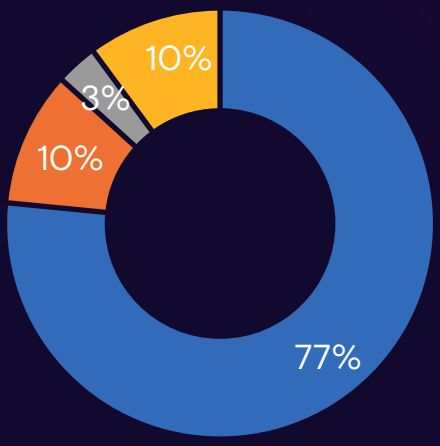
Также атаки были связаны с желанием дестабилизировать работу значимых онлайн-порталов, создав видимость того, что «хакеры без конца атакуют российские компании». При этом на фоне громких взломов и дефейсов защищать интернет-ресурсы как зеницу ока стали даже те организации, бизнес которых напрямую не зависит от онлайна.

Наша статистика показывает, что фокус был верным: основная масса злоумышленников сосредоточилась именно на атаках веб-платформ разнообразных компаний как коммерческого, так и государственного сектора. Но если анализировать сработки в пределах квартала – ближе к концу периода тренд веб-атак пошел на спад.

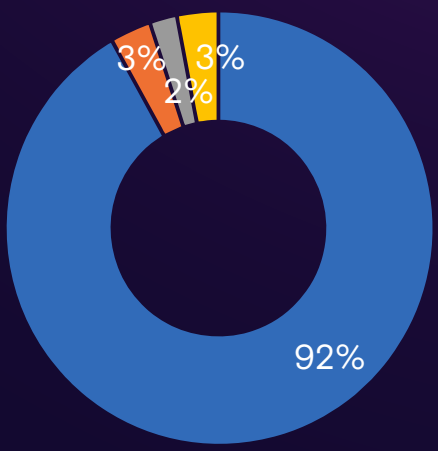
Вместе с тем в атаках на веб учитывались как широковещательные автоматизированные сканы и брутфорсы, так и целевые удары по конкретным ресурсам. Однако стоит учесть, что даже автоматизированные сканы могут привести к успешной хакерской атаке, если компании не следят за своим ИТ-периметром, актуальностью обновлений и базовой гигиеной удаленного доступа.

Распределение высококритичных инцидентов по категориям:

Инциденты с высокой долей критичности, 1-й квартал 2022



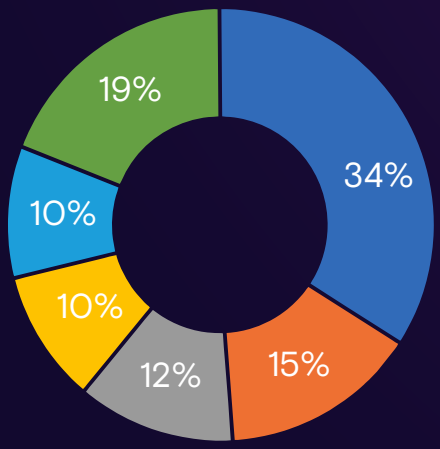
Инциденты с высокой долей критичности, 2-й квартал 2022



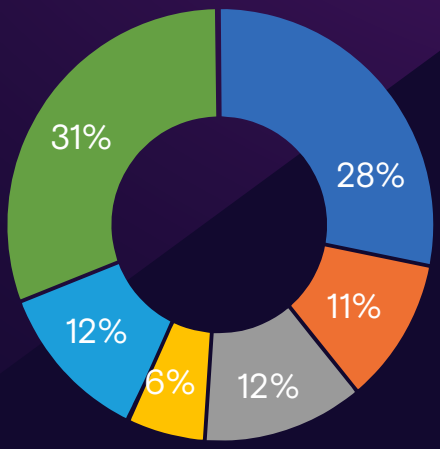
Динамика 1-го полугодия в целом

С динамикой кибератак в 1-м квартале 2022 года можно ознакомиться по ссылке. В целом в 1-м полугодии 2022 года количество ИБ-инцидентов выросло практически на четверть в сравнении со 2-м полугодием 2021 года.

2-ое полугодие 2021



1-ое полугодие 2022



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

Если в части высококрических инцидентов в 2021 году в топе были сетевые атаки (65%) и заражение ВПО (11%), то спустя год подавляющее большинство (85%) атак было связано с вебом. В основном же веб-атаки связаны с дефейсом и фактически большой угрозы не представляют. Отдельно стоит отметить, существенное снижение числа сетевых атак, что в очередной раз указывает на переориентацию злоумышленников на веб. Подтверждением того, что данная «массовость» спланированная, является то обстоятельство, что большинство таких атак организуется из-за рубежа, то есть налицо определённая консолидация, направленная на то, чтобы посеять панику как среди простых граждан, так и среди представителей российского бизнеса.

При этом с начала года мы наблюдаем значительное повышение интереса со стороны различных организаций к add-on базовой услуги мониторинга в виде компонентов (EDR, NTA). С их помощью организации хотят повысить общую эффективность мониторинга, улучшить возможности детекта продвинутых злоумышленников, а также снизить количество оповещений, отправляемых первой линией мониторинга, и повысить информативность таких оповещений.

Тренд на снижение инцидентов, фиксируемых базовой инфраструктурой (FW, хостовые логи, AD) наблюдается последние два года и, по нашим оценкам, продолжится и дальше.

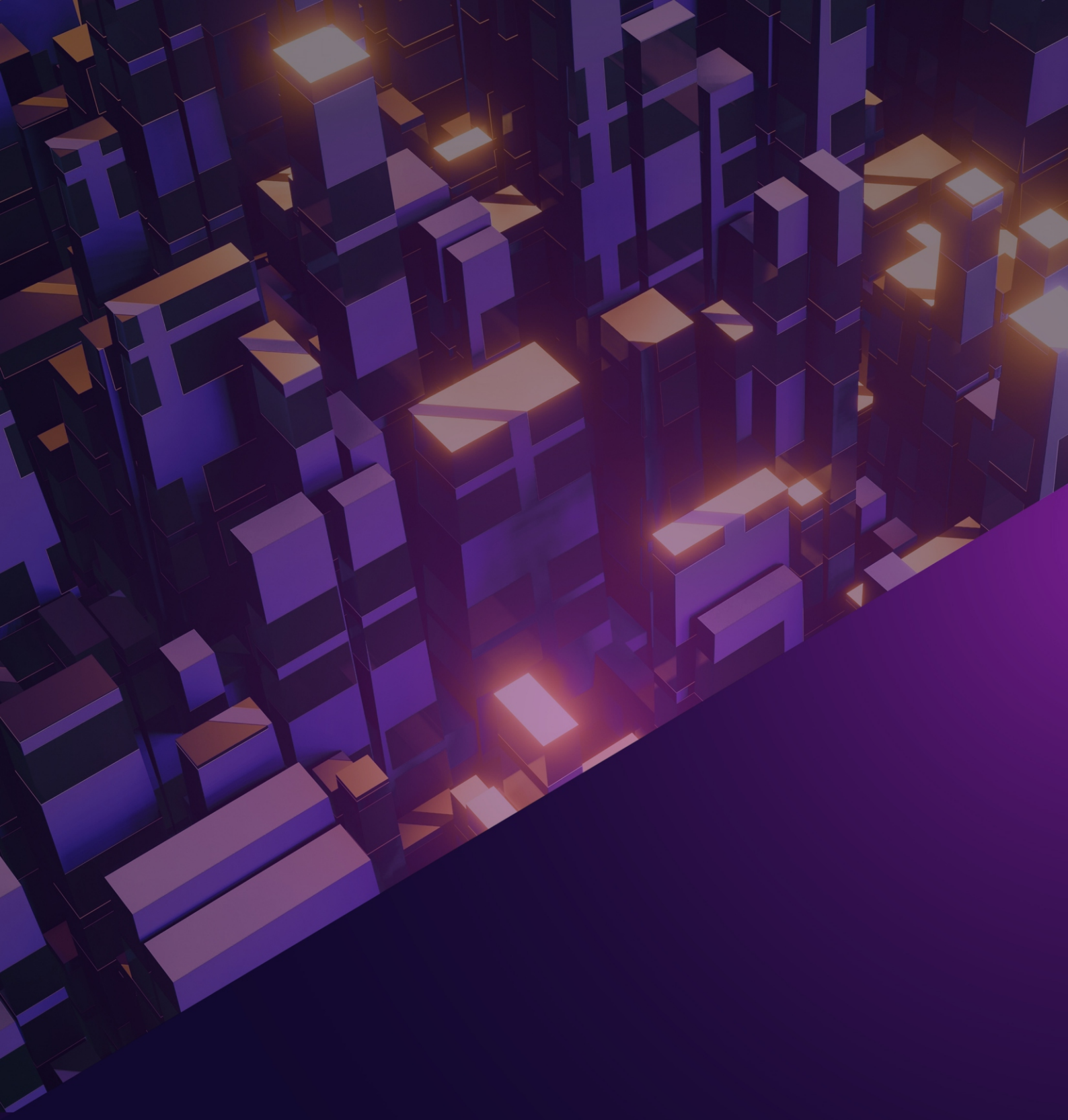
Компании в целом начали проявлять больше внимания к информационной безопасности. Интересным трендом стало значительное увеличение количества кастомных сценариев выявления инцидентов, создаваемых по запросам заказчиков. Также, стремясь закрыть слабые места собственных специфических бизнес-процессов, они всё чаще просят сервис-провайдера разработать индивидуальные сценарии реагирования.

Выводы

Во втором квартале 2022 года количество событий ИБ выросло почти на треть. Однако тренд на массовые атаки постепенно идёт на спад, уступая место точечным, более опасным взломам.

Почти треть всех атак в отчетном периоде связана с применением хакерами вредоносного ПО. А среди критических инцидентов абсолютное большинство (95%) занимают веб-атаки. Также растёт доля инцидентов, связанных с эксплуатацией уязвимостей. Этот тренд сохранится и в будущем, так как многие компании не могут установить обновления на уязвимый софт из-за ухода зарубежных вендоров с российского рынка, а злоумышленники наращивают темпы использования новых уязвимостей. Однако импортозамещение способно изменить эту опасную тенденцию, но пока темпы перехода на отечественное ПО невысоки.

На этом фоне наблюдается явное повышение значимости кибербезопасности для обеспечения непрерывности бизнес-процессов. Организации стремятся повысить эффективность мониторинга, улучшить возможности детекта продвинутых злоумышленников, а также повысить информативность оповещений.



Ростелеком
Солар

rt.ru
rt-solar.ru

solar@rt-solar.ru
+7 (499) 755-07-70