Ростелеком
Солар

Отчет
Атаки на российские компании в 1-м квартале 2022 года

rt-solar.ru

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 – 1300+ 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 1-го квартала 2022 года значительно повлияли на ландшафт киберугроз. С конца февраля эксперты «РТК-Солар» начали фиксировать рост массовых атак на российские компании и многочисленные попытки взломов различных веб-ресурсов. Уровень атакующих в большинстве случаев был относительно невысоким: они использовали наиболее доступные инструменты и наносили быстрые удары без тяжелых длительных последствий.

В настоящем отчете приведены данные об инцидентах, выявленных командой Solar JSOC[1] в 1-м квартале 2022 года, и их сравнение со статистикой 4-го квартала 2021 года. Аналитика отражает приоритизацию инцидентов по степени критичности, а также процентное соотношение различных типов кибератак, которые наблюдались в отчетный 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 средним 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 заказчикам Solar JSOC обеспечивает контроль и выявление инцидентов для:

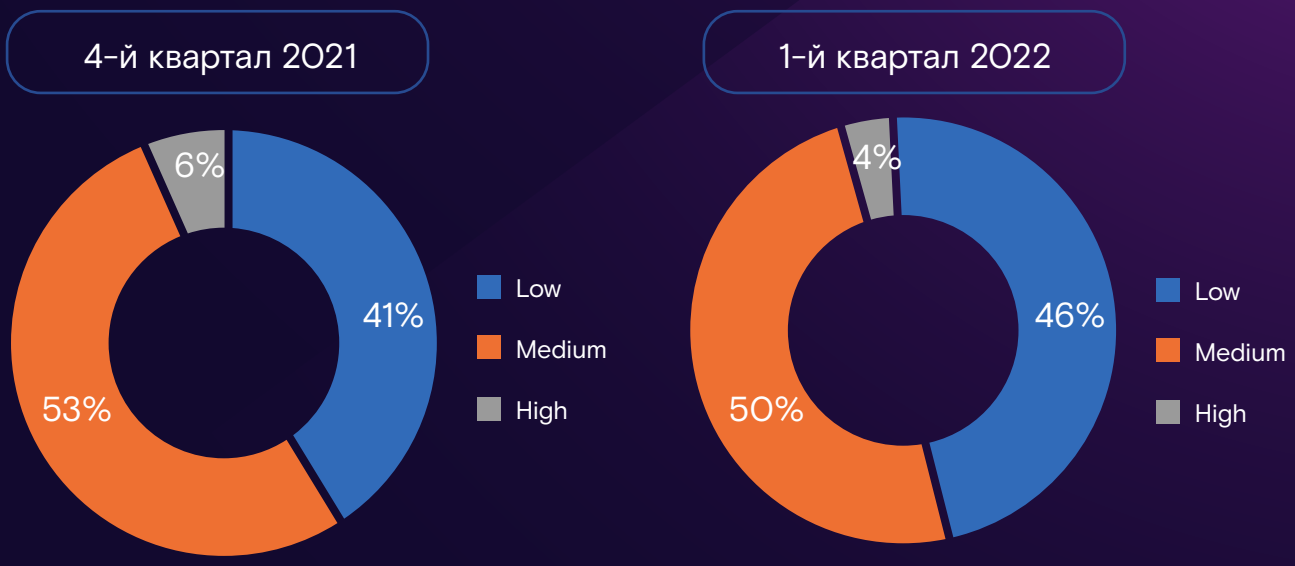
- более 2800 внешних сервисов, опубликованных в интернете;
- более 140 тыс. серверов общего, инфраструктурного и прикладного назначения.

[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 январе – марте 2022 года было зафиксировано более 184 тыс. событий ИБ – подозрений на инцидент после обработки первой линией мониторинга и фильтрации ложных срабатываний. Это на 4% превышает показатель 4-го квартала 2021 года. При этом в отчетный период отмечается рост инцидентов с низким уровнем критичности.

Распределение инцидентов по критичности:

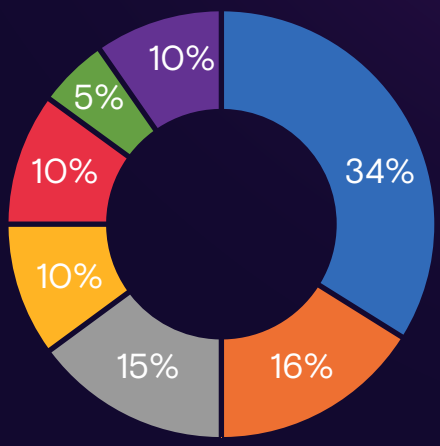


Наибольшее число инцидентов с разным уровнем критичности связано с применением хакерами вредоносного ПО, однако доля подобных инцидентов в сравнении с предыдущим кварталом сократилась.
При этом значительно выросло количество попыток несанкционированного доступа к информационным системам и серверам.

Также растет число скомпрометированных учетных записей, что дает основания говорить о том, что не все компании озаботились внутренней политикой безопасности на фоне обострения международной обстановки.
В то же время на теневом рынке все чаще появляются заказы на получение доступа к учетным записям различных компаний.

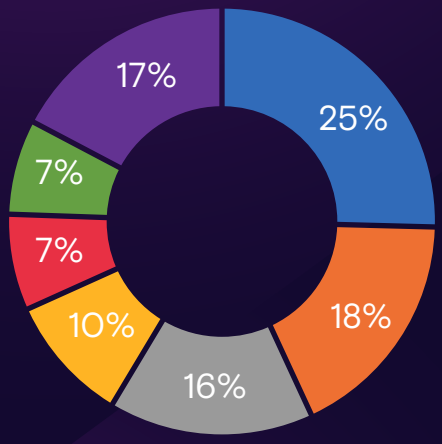
Распределение всего объема инцидентов по категориям:

4-й квартал 2021



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

1-й квартал 2022



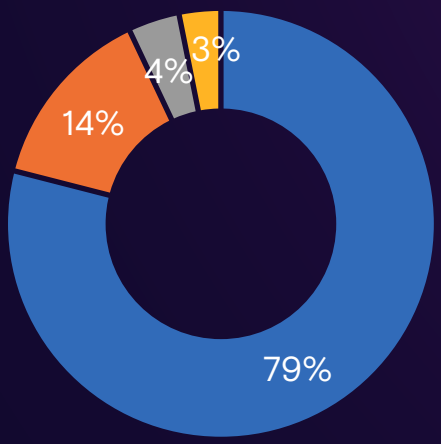
- Заражение ВПО
- Компрометация УЗ
- НДС к ИС и сервисам
- Веб-атаки
- Использование нелегитимного ПО
- Сетевые атаки
- Остальное

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

Однако набор критических инцидентов по сравнению с последним кварталом 2021 года существенно изменился. Так, в предыдущем периоде наибольшая доля (79%) пришлась на сетевые атаки (как правило, это сканирование внешнего периметра общедоступными средствами) и заражение вредоносным ПО (14%), при этом критических веб-атак зафиксировано не было, в то время как в 1-м квартале 2022 года их доля составила 77%.

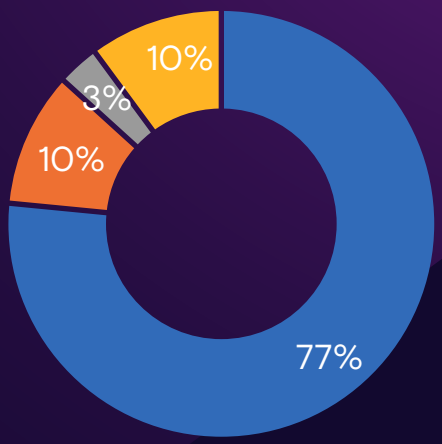
Распределение высококритичных инцидентов по категориям:

Инциденты с высокой долей критичности, 4-й квартал 2021



- Сетевые атаки
- Заражение ВПО
- Использование нелегитимного ПО
- Остальное

Инциденты с высокой долей критичности, 1-й квартал 2022



- Веб-атаки
- Сетевые атаки
- Заражение ВПО
- Остальное

Резкий всплеск веб-атак можно объяснить общей тенденцией, которая наметилась с конца февраля, когда из-за стремления посеять панику злоумышленники атаковали веб-платформы, чтобы, например, залить на сайт какой-нибудь провокационный баннер. При этом фактического взлома сайта не происходило (в случае с баннерами затронута была только подсистема рекламных модулей). Также это может быть связано с желанием дестабилизировать работу онлайн-портала, создав видимость того, что «хакеры без конца атакуют российские компании», хотя в большинстве случаев подобные инциденты не влекут за собой каких-либо серьезных последствий и могут быть вызваны множественными неверными попытками входа, сканированием сайтов, блокировками запросов ДБО и т. п. Фактически речь идет о неоднократных попытках прорваться сквозь внешний периметр с применением простейших автоматизированных систем.

Выводы

Каких-либо аномалий за анализируемый период не выявлено, однако общее количество зафиксированных Solar JSOC событий ИБ выросло. В то же время увеличилось число инцидентов с низкой степенью критичности. Это говорит о том, что атаки стали более простыми и массовыми. За большинством из них, скорее всего, стояли злоумышленники с низкой квалификацией.

Несколько изменился общий ландшафт киберугроз, тем не менее заражение ВПО по-прежнему остается самым популярным типом атаки, хотя его доля в первом квартале 2022 года несколько сократилась. Также возросло количество скомпрометированных учетных записей, что напрямую связано с попытками взлома инфраструктур атакуемых компаний.

Абсолютное большинство критических инцидентов связано с атаками на веб-приложения. Резкий всплеск подобных инцидентов начался с конца февраля. При этом целью хакеров был скорее не взлом веб-приложений для хищения ценных данных, а дестабилизация работы сайтов или дефейс.

Ростелеком
Солар

rt.ru
rt-solar.ru

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