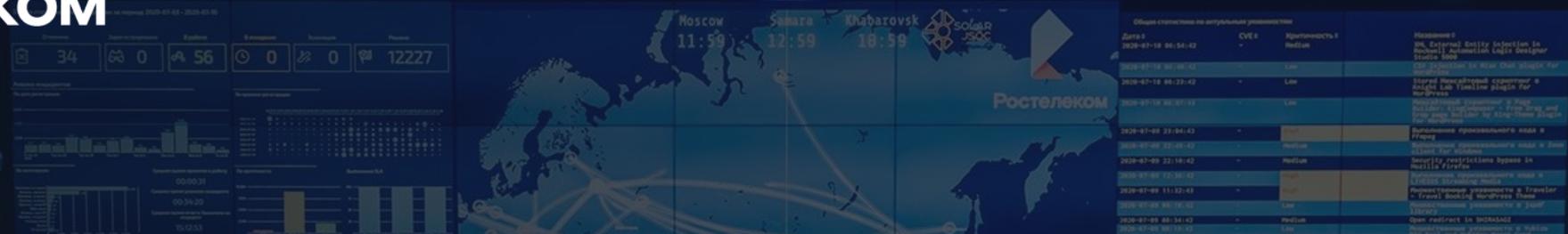


Кибербезопасность сегодня: аналитика, кейсы, прогнозы и рекомендации



Игорь Семенчев
Пресейл-аналитик Solar JSOC
компании «Ростелеком-Солар»



Ситуация сегодня

90% компаний, находящихся под защитой «Ростелеком-Солар» от DDoS-атак, ежедневно подвергаются нападениям **широковещательным DDoS с использованием преимущественно зарубежных ботнетов**

DDoS-атаки – своего рода дымовая завеса. Неприятно, но не смертельно

Массовые атаки на веб-ресурсы: **дефейс через взлом счетчиков и баннеров**. Это несет репутационный урон, но прямого взлома сайтов и утечек персональных данных с государственных ресурсов не происходит

Необратимое **шифрование** данных **без возможности выкупа**

За атаками в основном стоят **APT- и проправительственные группировки**. Но и менее квалифицированные злоумышленники не дремлют.

Проправительственные группировки повысили активность в части **проникновения и закрепления в объектах КИИ и компаниях госсектора на территории РФ**

Громкие заголовки со словом «кибератака» – в большинстве случаев лишь **манипуляция фактами и акт запугивания**

Успешных кибератак с реальным ущербом среди клиентов Solar JSOC **на текущий момент не выявлено**

Динамика за февраль-март 2022 года

Рост числа всех типов атак по отраслям (активные заражения инфраструктур)

+4,7%



Образование

+10,6%



Телеком

+15,4%



Здравоохранение

+16,2%



ТЭК

+16,5%



Финансы

+18,8%



Промышленность

+22%



Госсектор

+14,9%



Средний показатель роста атак

Ключевые факторы последних лет

01

Переход на удаленную работу в связи с пандемией стал **тренировочной площадкой для обкатки новых решений** и **стимулом для вектора на повышение защищенности** в информационном пространстве

02

Формирование **приоритета на выполнение госзаказов в России** – один из элементов **цифровизации экономики**

03

Результаты быстрого развития ИТ:

- **«сырое» ПО** на рынке
- появление **новых рисков и угроз**

04

Следствие мирового экономического кризиса:

- **стагнация рынка**
- **рост цен** на конечные продукты

В каком состоянии ИТ-рынок вошел в 2022 год

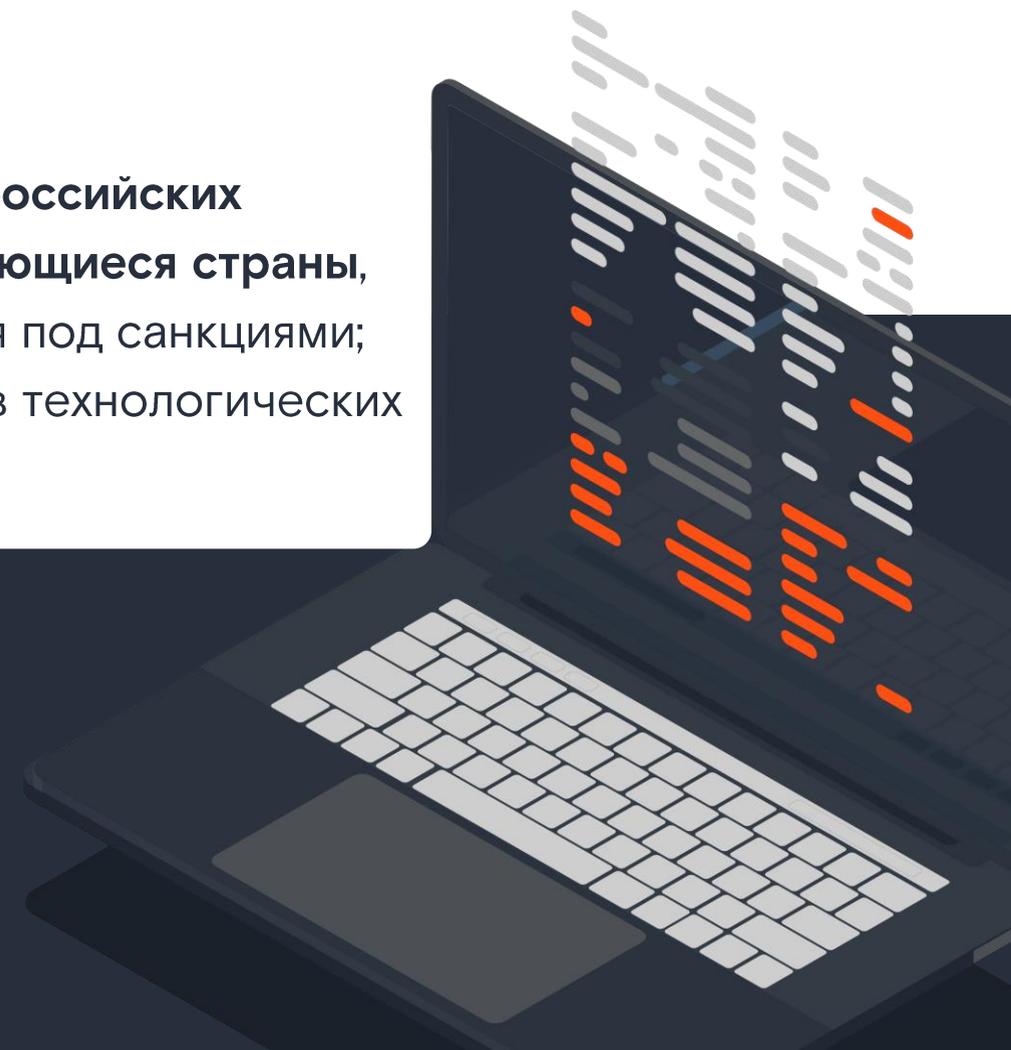
Рост российского рынка ИБ, увеличение бюджетирования данной сферы

Рост технологической защищенности различных секторов экономики, включая государственные организации

Развитие ИТ-инфраструктуры как важнейшего обеспечивающего элемента бизнеса, позволяющего сформировать целостную экосистему, способную противостоять новым угрозам

Налаживание экспорта российских ИТ-продуктов в развивающиеся страны, в том числе находящиеся под санкциями; развитие новых векторов технологических партнерств

Осознанная цифровизация бизнеса с возросшими за последние два года темпами



Уровни злоумышленников

	УСЛОВНАЯ КАТЕГОРИЯ НАРУШИТЕЛЯ	ТИПОВЫЕ ЦЕЛИ	ВОЗМОЖНОСТИ НАРУШИТЕЛЯ
Массовые атаки	Автоматизированные системы	Взлом устройств и инфраструктур с низким уровнем защиты для дальнейшей перепродажи или использования в массовых атаках	Автоматизированное сканирование
	Киберхулиган/ Энтузиаст-одиночка	Хулиганство, нарушение целостности инфраструктуры	Официальные и open-source-инструменты для анализа защищенности
	Киберкриминал/ Организованные группировки	Приоритетная монетизация атаки – шифрование, майнинг, вывод денежных средств	Кастомизированные инструменты, доступное вредоносное ПО (приобретение, обфускация или разработка), доступные уязвимости, социнжиниринг
Профессиональные атаки	Кибернаемники/ Продвинутые группировки	Нацеленность на заказные работы – сбор информации, шпионаж в интересах конкурентов, последующая крупная монетизация, хактивизм, деструктивные действия	Самостоятельно разработанные инструменты, приобретенные zero-day-уязвимости ПО
	Кибервойска/ Проправительственные группировки	Кибершпионаж, полный захват инфраструктуры для возможности контроля и применения любых действий и подходов, хактивизм	Самостоятельно найденные zero-day-уязвимости ПО и АО, разработанные и внедренные «закладки»

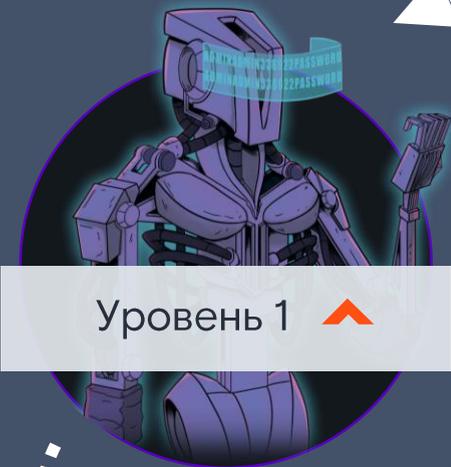
Векторы атак. Уровни 1, 2, 3

Координатор

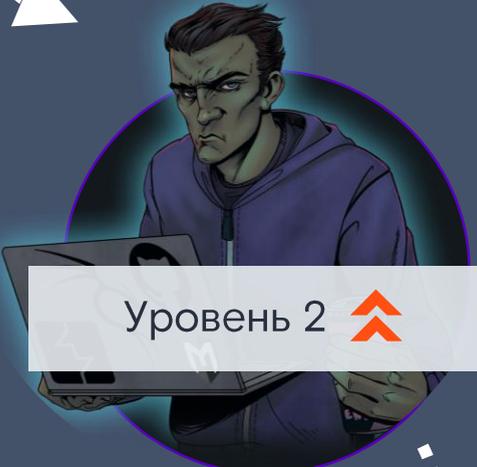


Цели

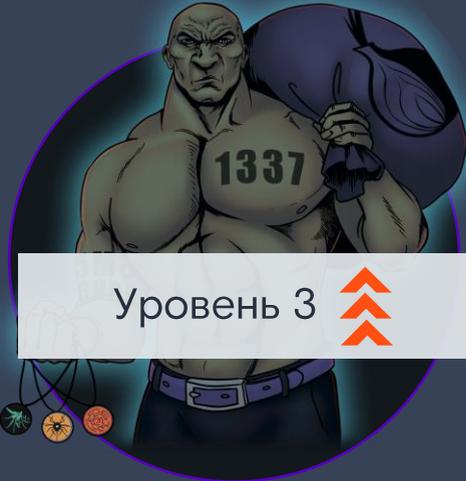
Цели, инструментарий



Уровень 1 ▲



Уровень 2 ▲▲

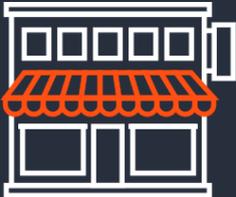


Уровень 3 ▲▲▲

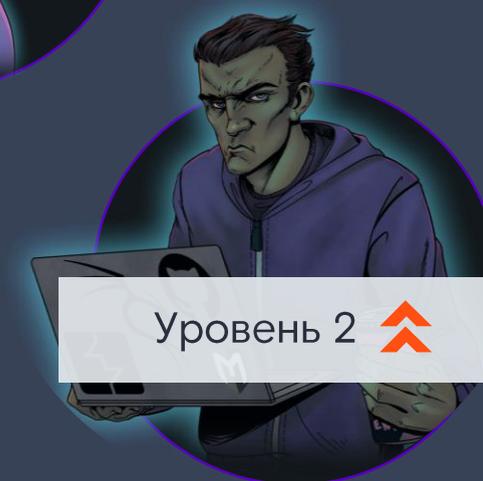
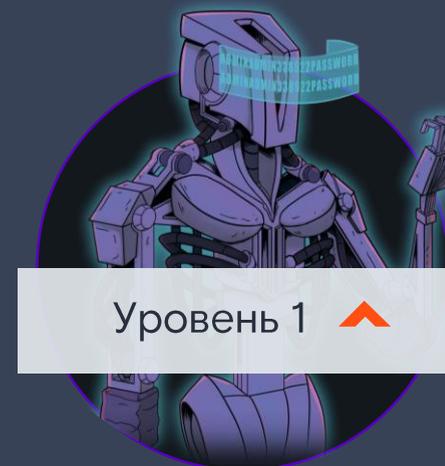
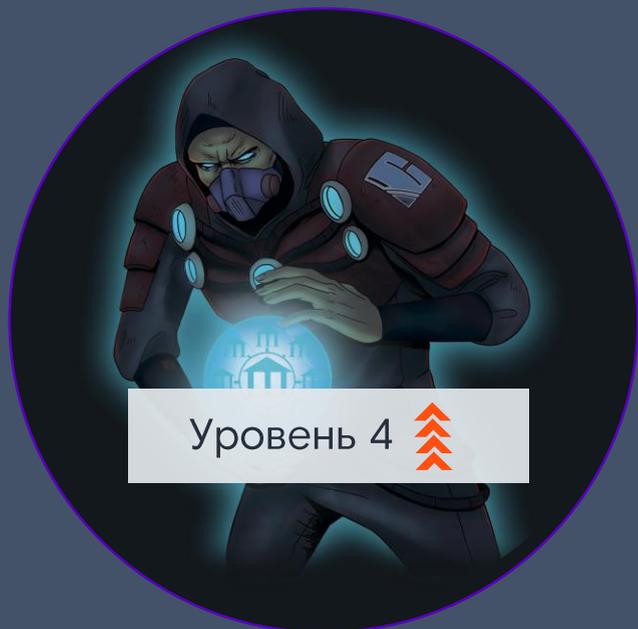
DDoS-атаки,
базовые атаки на веб

Атаки, нацеленные
на монетизацию
и шифрование данных

Компании РФ



Векторы атак. Уровни 4, 5



Продажа доступа



Шифрование данных,
кибершпионаж



Компании РФ



Чего ждать и к чему готовиться?



Атаки будут усложняться:
киберпреступники будут использовать нетипичные методы и техники



Продолжится **рост числа атак** со стороны **проправительственных группировок** на фоне «процветания» промышленного шпионажа



Под прицелом в первую очередь окажутся **государственные органы и субъекты КИИ**



Атаки **проправительственных группировок** не всегда сразу будут вести к убыткам. Основным признаком деятельности киберпреступников 5-го уровня останется длительное присутствие



SMB по-прежнему остается сферой интересов **злоумышленников 3-го уровня**, основная цель которых – **монетизация**

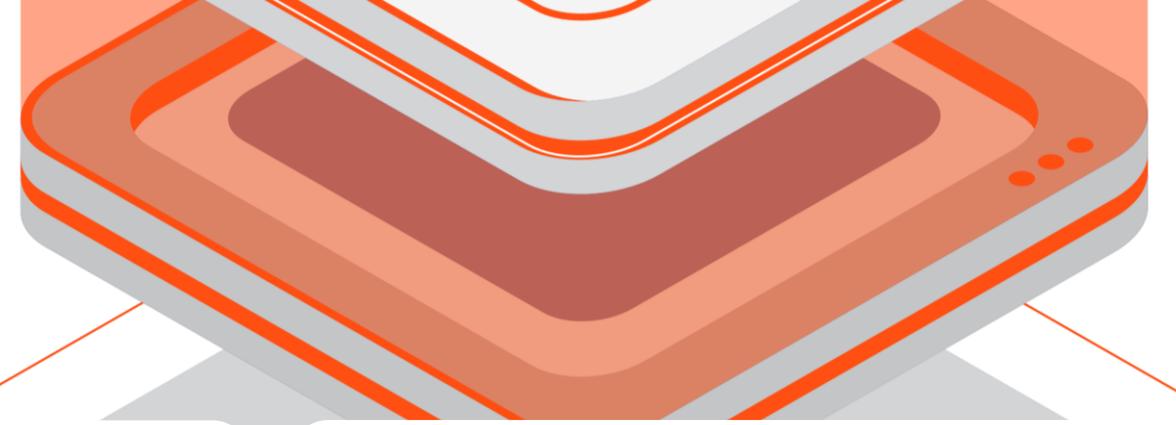


Продолжатся **атаки с использованием шифровальщиков** для распространения паники



Продолжится **рост атак через подрядчиков**

Рекомендации



Контроль периметра

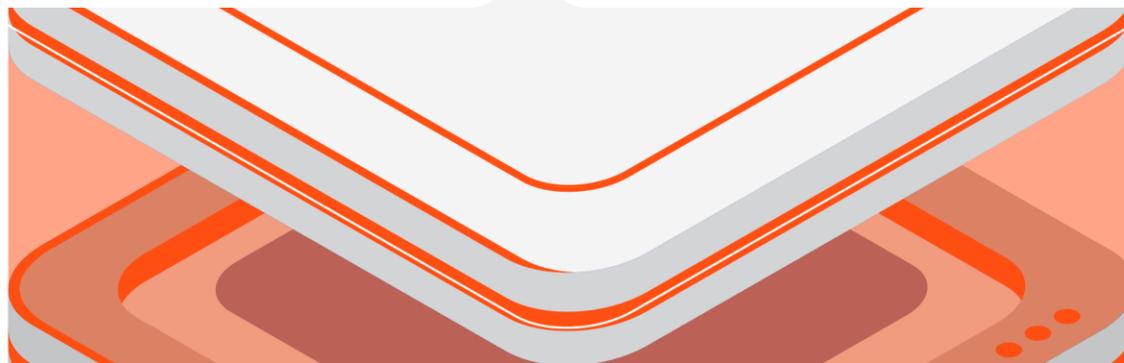
- 1 Регулярное проведение инвентаризации внешнего периметра
- 2 Отключение неиспользуемых сервисов
- 3 Использование решений для мониторинга внутреннего и внешнего периметра и открытых источников

Контроль внутренней инфраструктуры

- 1 Аккуратный патч-менеджмент. Проверка обновлений в тестовой среде
- 2 Настройка расширенного аудита
- 3 Организация регулярного аудита доменных групп

Веб-приложения

- 1 Введение белых списков для API-приложений
- 2 Защита приложений с помощью WAF и Anti-DDoS
- 3 Проверка веб-приложений на предмет наличия компонентов, загружаемых с внешних ресурсов



Экосистема сервисов Solar JSOC



Мониторинг инцидентов

- Мониторинг и анализ инцидентов
- Анализ сетевого трафика (NTA)
- Защита конечных точек (EDR)
- Мониторинг бизнес-систем
- Мониторинг АСУ ТП
- Сервисы ГосСОПКА



Расследование и реагирование на инциденты

- Управление процессами реагирования на киберинциденты (IRP)
- Разработка плейбуков
- Incident Response
- Техническое расследование инцидентов



Комплексный контроль защищенности

- Тестирование на проникновение
- Анализ защищенности
- Социотехническое исследование
- Assumed Breach
- Red Teaming
- Анализ рисков и обследование инфраструктуры
- Оценка зрелости технической защиты



Анализ угроз и внешней обстановки

- Киберразведка



Построение SOC и его частных процессов

- Построение SOC
- Консалтинг

Solar JSOC

Первый и крупнейший в России коммерческий **центр противодействия кибератакам**, действующий по модели MDR (Managed Detection and Response). Обеспечивает защиту крупных государственных и коммерческих организаций от киберугроз и оказывает помощь другим корпоративным SOC.

Предотвращение

Разведка и раннее предупреждение об угрозах, оценка рисков и управление уязвимостями

Выявление

Расширенные возможности мониторинга и анализа событий кибербезопасности 24/7, противодействие атакам на ранней стадии

Реагирование

Оперативное техническое расследование, ликвидация последствий и устранение причин возникновения инцидентов

Построение SOC и консалтинг

Помощь в создании и совершенствовании центров управления кибербезопасностью

№1

на рынке SOC
в России

400+

экспертов по
кибербезопасности

200+

клиентов из всех
отраслей экономики

110+

млрд анализируемых
событий в сутки

10 минут

на обнаружение
кибератаки

30 минут

на реагирование
и защиту

Ответы на вопросы



Игорь Семенчев,
Пресейл-аналитик Solar JSOC
компании «Ростелеком-Солар»



Контакты

+7 (499) 755-07-70

solar@rt-solar.ru

