Ростелеком
Солар

# Кибербезопасность сегодня: аналитика, кейсы, прогнозы и рекомендации

**Павел Гончаров**
Заместитель директора по развитию бизнеса 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 заграничных 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**



Ростелеком Солар

# Динамика за февраль-март 2022 года

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

| +4,7% | +10,6% | +15,4% | +16,2% | +16,5% | +18,8% | +22% |
|---|---|---|---|---|---|---|
| Образование | Телеком | Здравоохранение | ТЭК | Финансы | Промышленность | Госсектор |

**+14,9%** Средний показатель роста атак



Ростелеком Солар

# 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

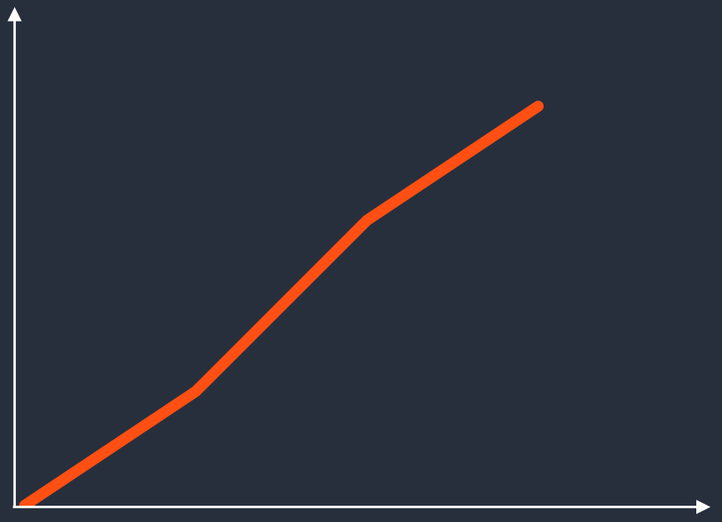


Ростелеком Солар

# Насколько реальны риски

Правда – первая жертва во время обострения международных отношений.

Информация – инструмент воздействия на сознание людей. СМИ часто манипулируют фактами.



Нам говорят, что события развиваются так

Помните, что тысячи людей зарабатывают деньги на новостях, искусственно создавая тот или иной информационный фон.

**Российские компании не могут быть вечной мишенью для кибератак.**

Так они развиваются на самом деле



Ростелеком Солар

# 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» |



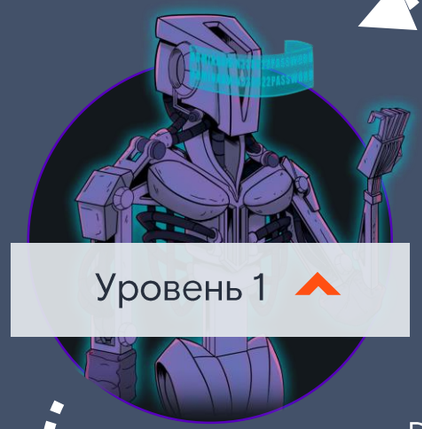
Ростелеком Солар

# Векторы атак. Уровни 1, 2, 3

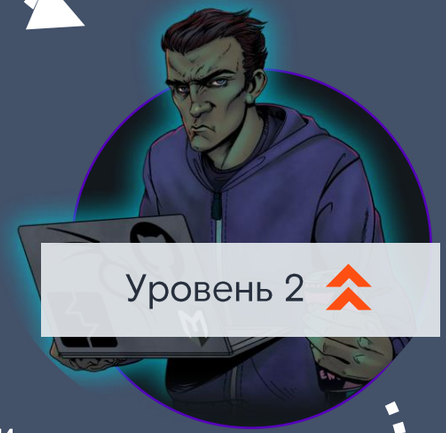
Координатор

Цели

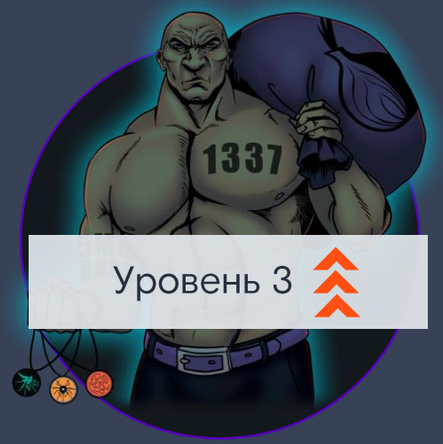
Цели, инструментарий



Уровень 1



Уровень 2




Уровень 3

DDoS-атаки,
базовые атаки на веб

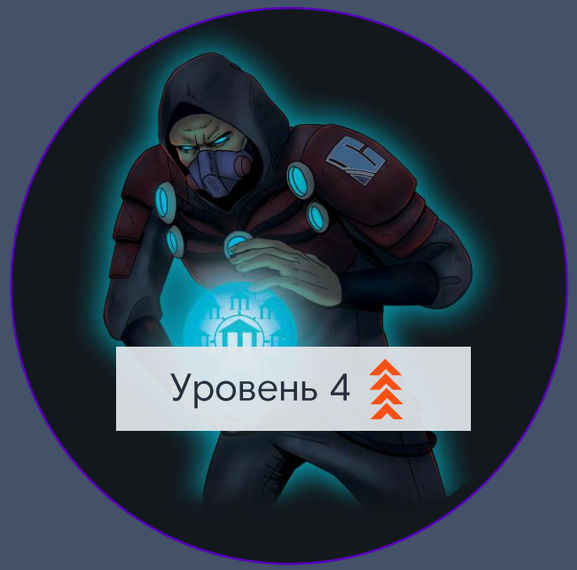
Атаки, нацеленные
на монетизацию
и шифрование данных

Компании РФ

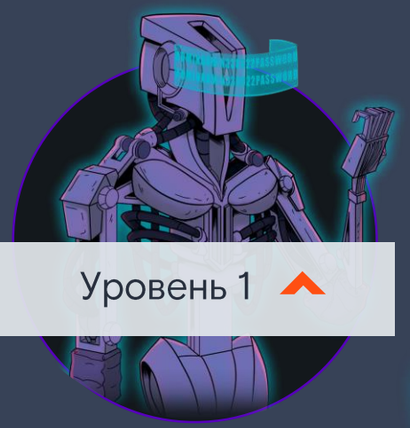


Ростелеком
Солар

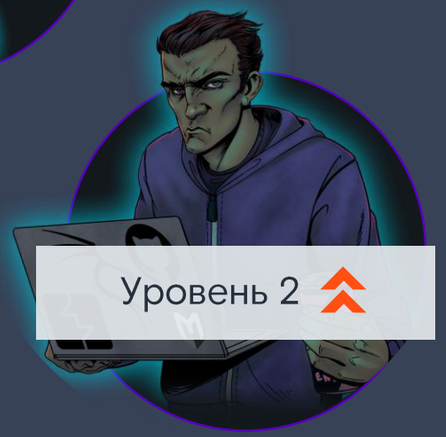
# Векторы атак. Уровни 4, 5








Продажа доступа




Шифрование данных, кибершпионаж

Компании РФ



Ростелеком Солар

# Чего ждать и к чему готовиться?

**Атаки будут усложняться**: киберпреступники будут использовать нетипичные методы и техники

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

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

Продолжится рост **атак через подрядчиков**

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

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

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



Ростелеком Солар

# 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



Ростелеком Солар

# 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

**250+**
клиентов из всех отраслей экономики

**110+**
млрд анализируемых событий в сутки

**10 минут**
на обнаружение кибератаки

**30 минут**
на реагирование и защиту

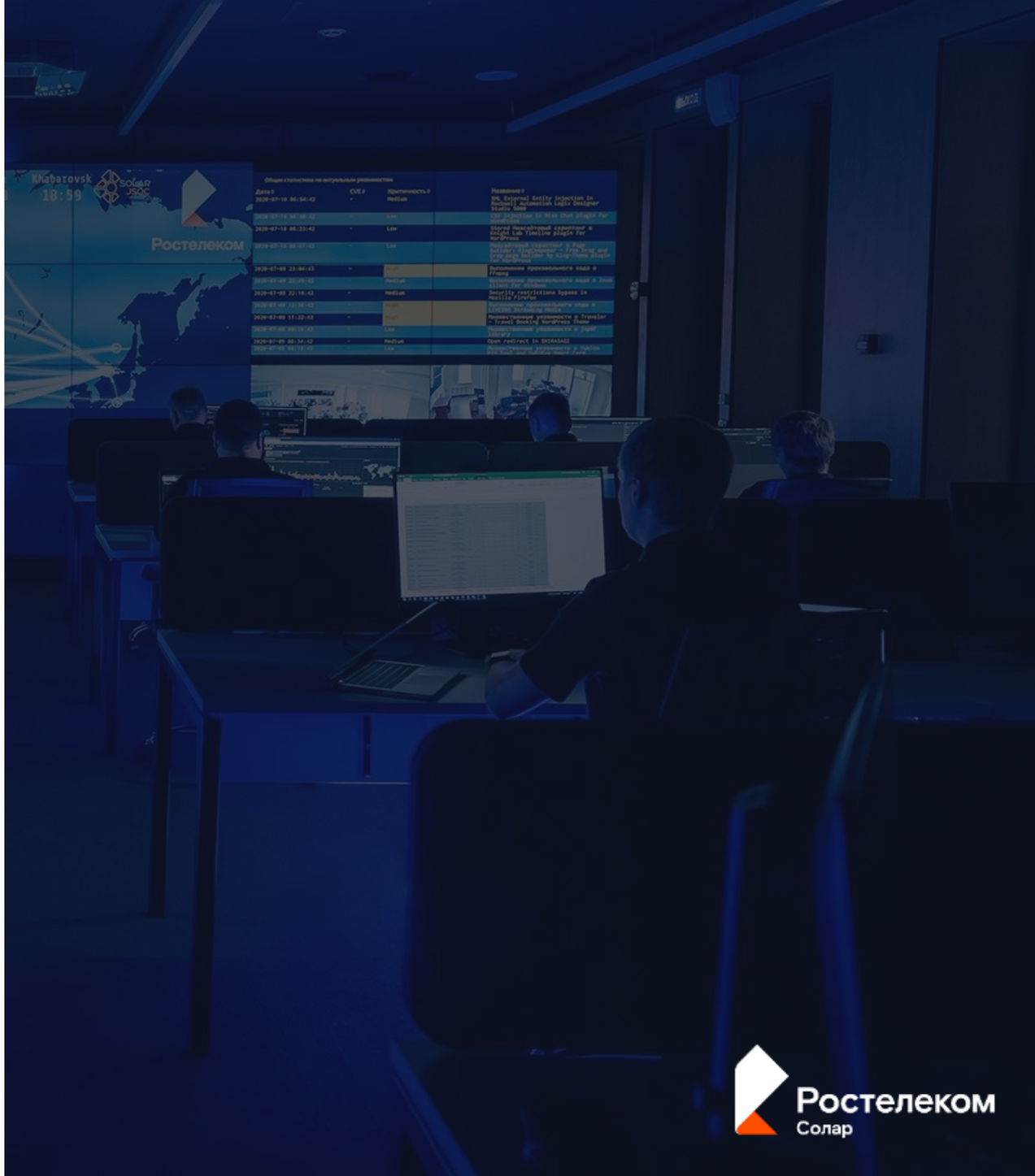


Ростелеком Солар

# Ответы на вопросы


## Павел Гончаров

Заместитель директора по развитию бизнеса Solar JSOC компании «Ростелеком-Солар»



## Контакты

+7 (499) 755-07-70

solar@rt-solar.ru