Анализ трендов киберугроз последнего месяца глазами крупнейшего SOC России. Меры защиты.

Данные на 18.03.2022 г.

Павел Гончаров

Ситуация сегодня

90% компаний, находящихся под защитой «Ростелеком-Солар», ежедневно подвергаются нападениям **широковещательным DDoS с использованием заграничных ботнетов.** Емкость некоторых фокусированных атак превышала 750 Гбит/с

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

Рост атак через подрядчиков (дефейс через взлом счетчиков и баннеров)

Массовые атаки на веб-ресурсы со стороны иностранных злоумышленников. Bug Bounty на уровне страны

Необратимое **шифрование данных без возможности выкупа** при взломе уязвимых инфраструктур

Эксплуатация **новых критических уязвимостей**

Встраивание ВПО в Open Source

Ростелеком Солар

Ситуация сегодня

В первые дни

Со стороны профессиональных группировок:

- ориентация на госсектор и компании, попавшие в санкционные списки

Со стороны группировок низкого и среднего уровней:

- использование наиболее доступных инструментов
- быстрые удары без тяжелых длительных последствий

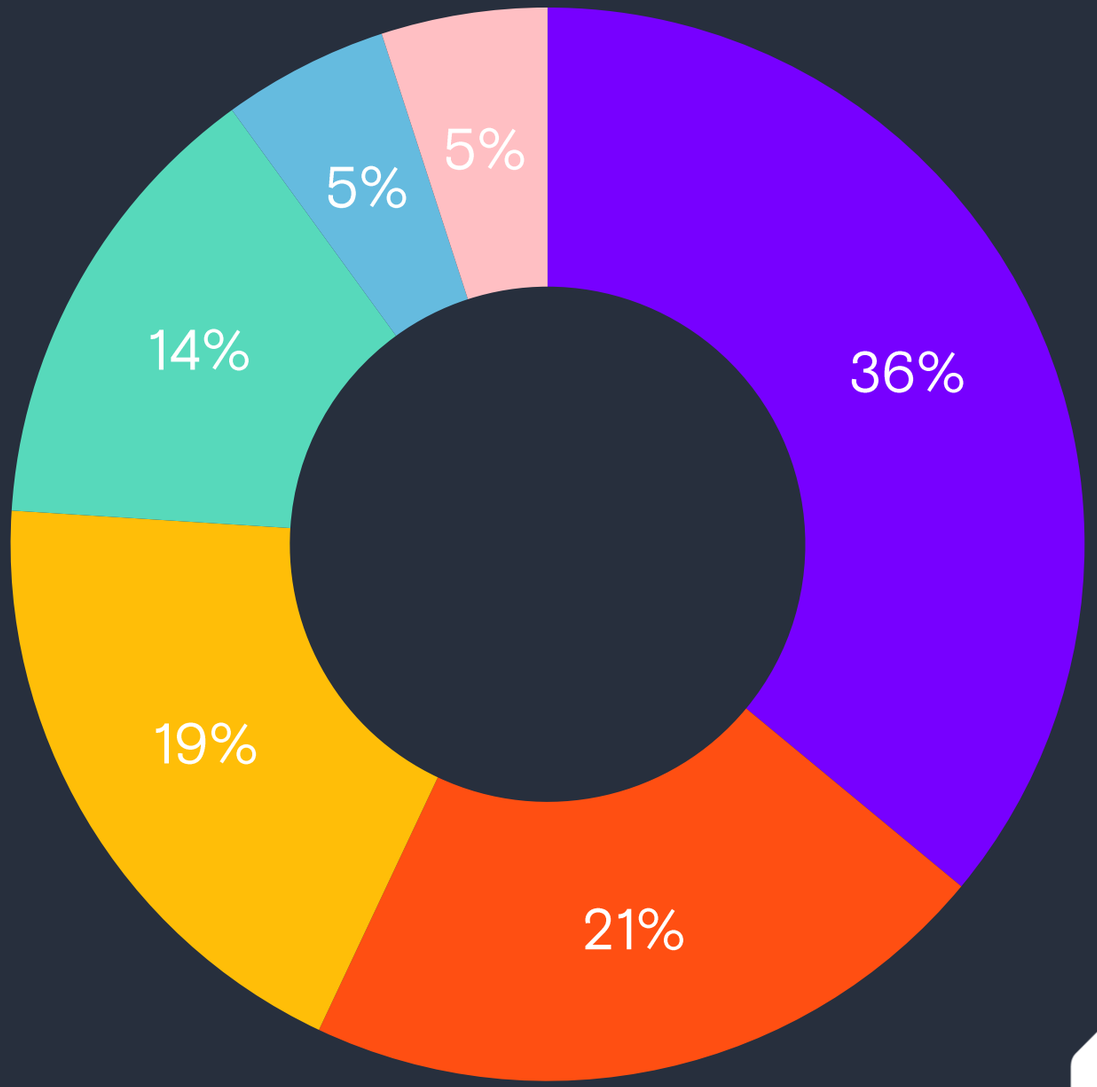
Вероятное развитие событий:

- Точечные удары по КИИ
- Усложнение атак
- Разработка нового ВПО и совершенствование существующих инструментов для повышения эффективности
- Использование зараженных хостов инфраструктур в качестве точек входа
- Использование supply chain

Ростелеком Солар

Распределение массовых атак по отраслям

Образование	36%
Госсектор	21%
Здравоохранение	19%
Промышленность	14%
Финансы	5%
ТЭК	5%



Ростелеком Солар

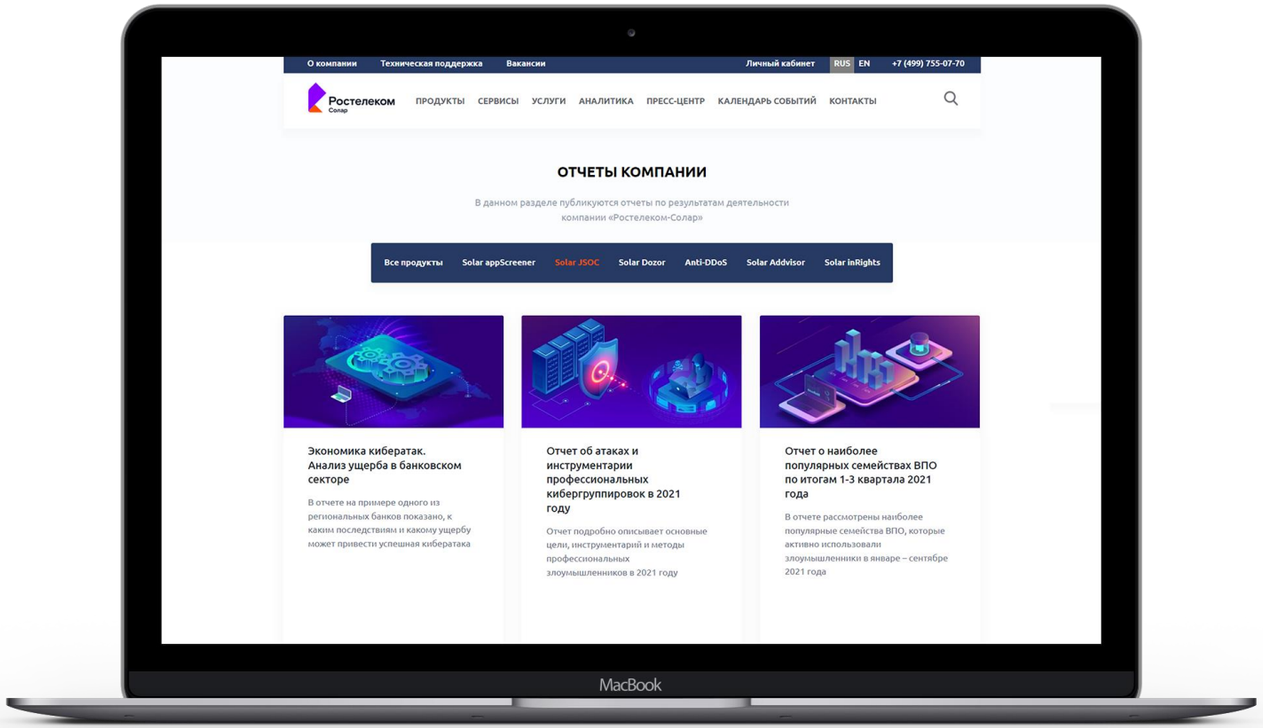
Уровни злоумышленников

УСЛОВНАЯ КАТЕГОРИЯ НАРУШИТЕЛЯ	ТИПОВЫЕ ЦЕЛИ	ВОЗМОЖНОСТИ НАРУШИТЕЛЯ
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
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

Кто ваш злоумышленник?

Пройдите тест на сайте «Ростелеком-Солар» и узнайте, кто угрожает вашей инфраструктуре

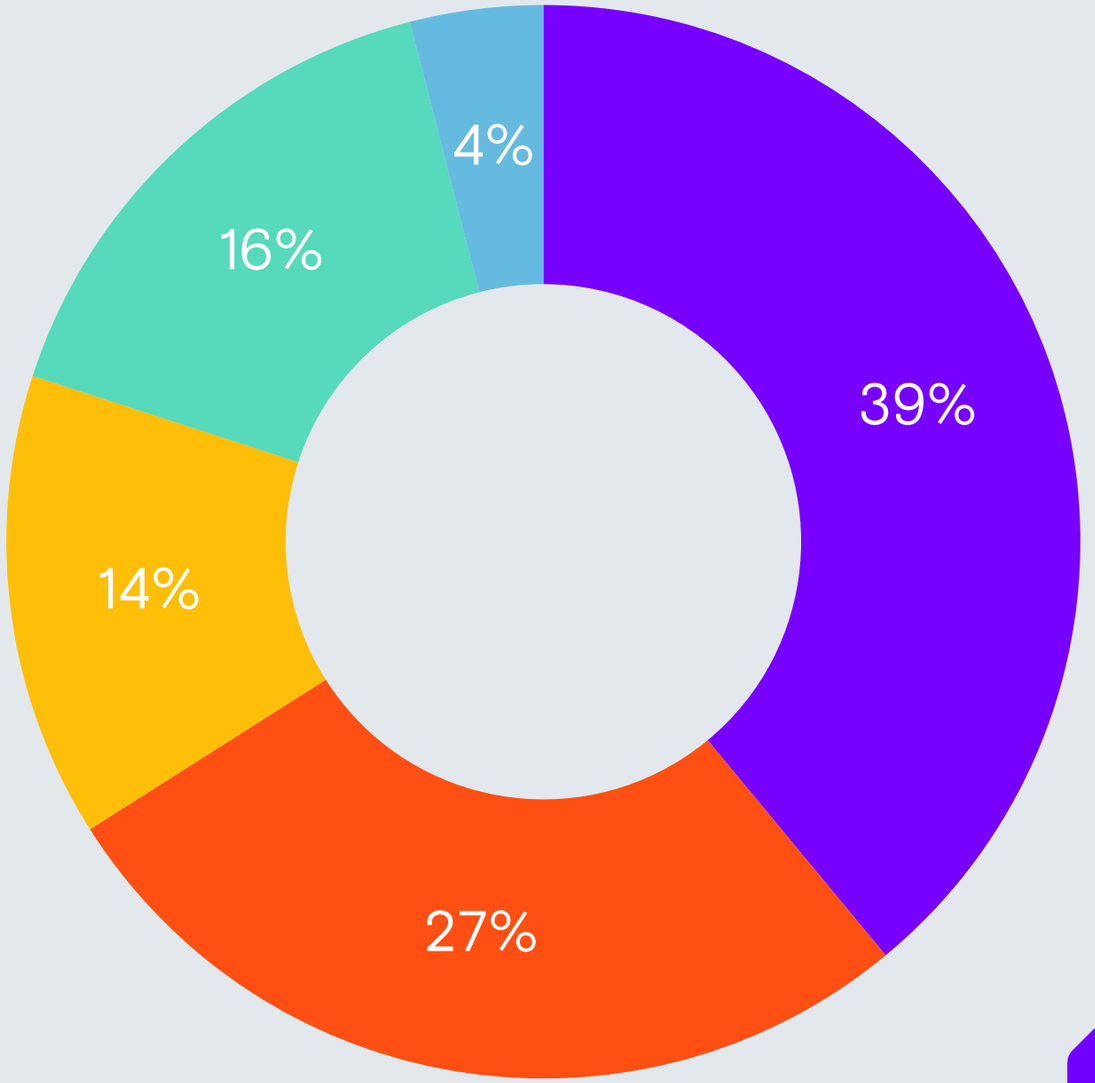


https://rt-solar.ru/profiles/

Ростелеком Солар

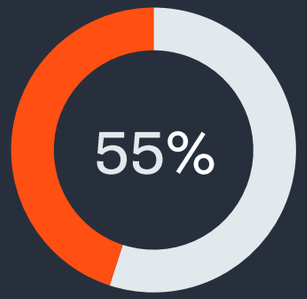
Распределение APT-атак по отраслям

Госсектор	39%
ТЭК	27%
Финансы	14%
Промышленность	16%
Другое	4%



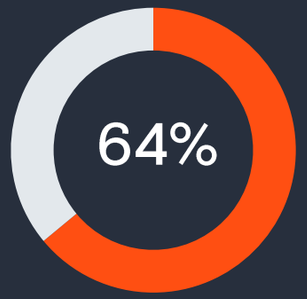
Ростелеком Солар

Многие компании уязвимы перед злоумышленниками



крупных компаний неспособны эффективно противодействовать кибератакам

Accenture, 2021 г.



уязвимостей, выявленных по результатам **внутренних пентестов**, характеризуются **высоким уровнем критичности**

уязвимостей, выявленных по результатам **внешних пентестов**, характеризуются **средним или высоким уровнем критичности**

проектов по внутреннему пентесту были завершены полной компрометацией инфраструктуры и захватом доменов

Solar JSOC, 2021 г.

Ростелеком Солар

Прогнозы

Повышенный уровень DDoS-атак в течение длительного времени

Рост числа атак со стороны проправительственных группировок

Увеличение числа массовых сканирований внешней инфраструктуры на предмет наличия уязвимостей и недостатков

Сохранение вектора атак для распространения паники среди населения и бизнеса

Использование скомпрометированных учетных записей для проникновения во внутреннюю сеть

Увеличение числа атак со стороны профессиональных группировок с целью монетизации. Вектор – фишинг

Ростелеком Солар

Рекомендации

Регулярное проведение инвентаризации внешнего периметра

Проведение работ по повышению осведомленности сотрудников в вопросах ИБ

Резервное копирование и инвентаризация иностранного ПО

Отключение неиспользуемых сервисов

Использование решений для мониторинга внутреннего и внешнего периметра и открытых источников

Настройка расширенного аудита

Аккуратный патч-менеджмент. Проверка обновлений в тестовой среде

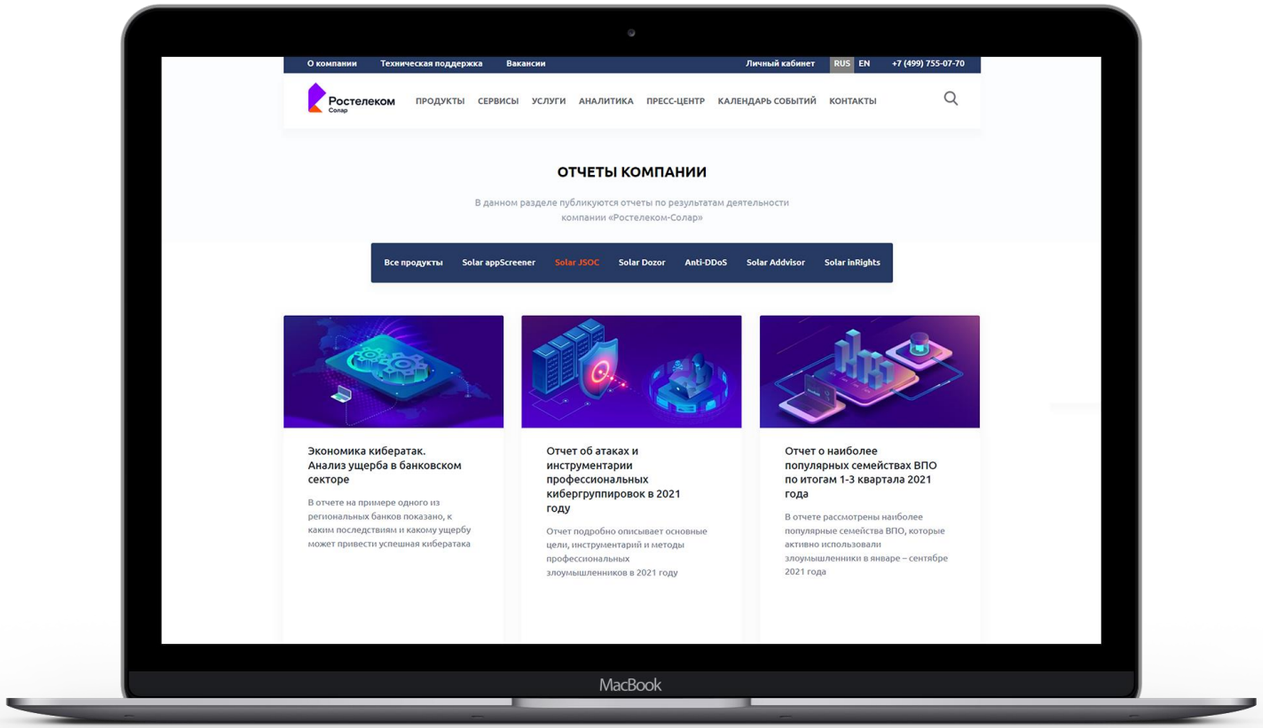
Усиленный контроль подрядчиков

Оперативная организация выявления и реагирования на инциденты ИБ (например, по сервисной модели)

Ростелеком Солар

Аналитика от экспертов Solar JSOC

Следите за обновлениями на сайте или подпишитесь на рассылку,
чтобы первыми получать новые аналитические обзоры



https://rt-solar.ru/analytics/reports/

Ростелеком Солар

Ростелеком
Солар

Центральный офис

125009, г. Москва,
Никитский переулок, 7с1

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