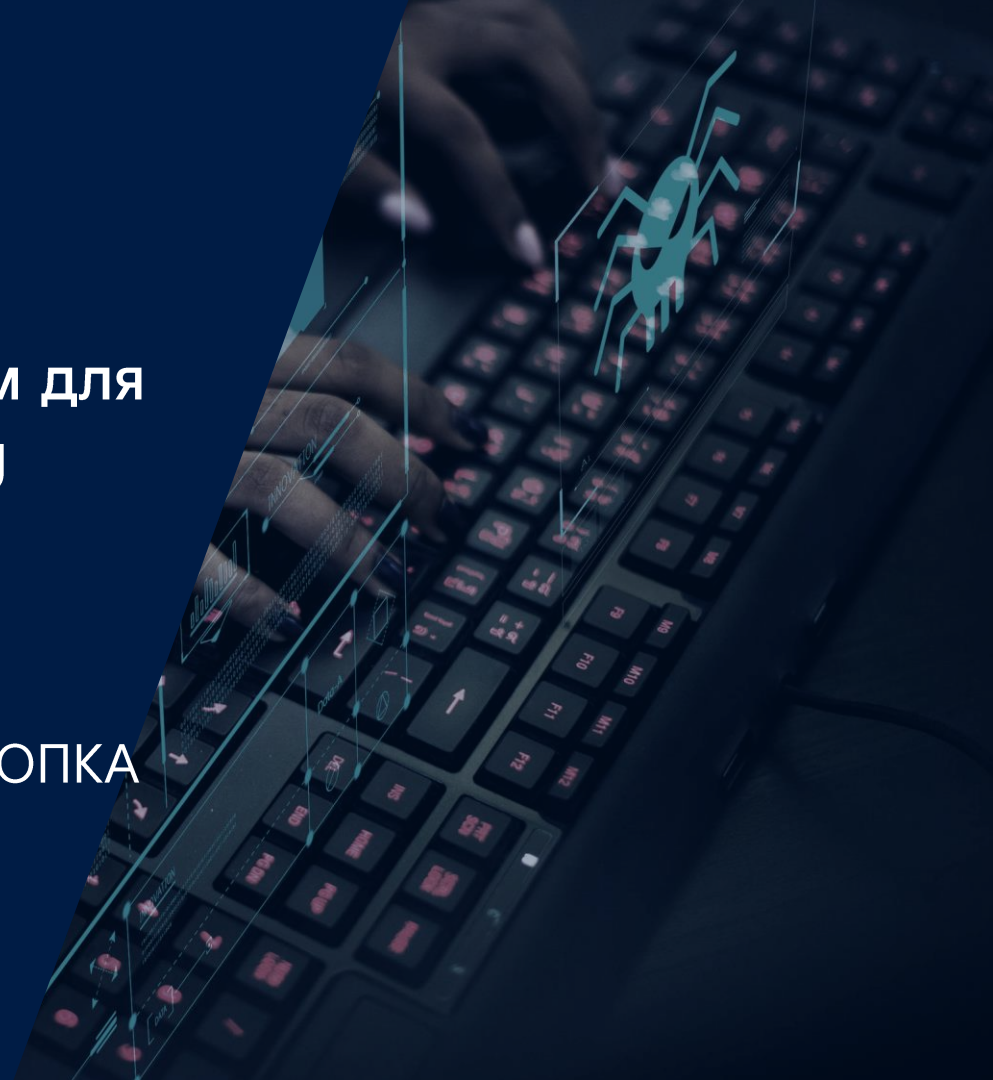
Использование NTA-систем для форензики и Threat Hunting

Павел Гончаров
Руководитель направления ГосСОПКА

Ростелеком
Солар



Тренды киберугроз

Ростелеком
Солар

Киберпреступники постоянно совершенствуются

+40%

рост атак на получение контроля над инфраструктурой организации

55,4%

событий ИБ удается выявить лишь с помощью сложных интеллектуальных средств защиты или анализа событий

По данным Solar JSOC, 2020 г.

63%

из всех атак являются целенаправленными

По данным Positive Technologies, 2020 г.

1 из 5

ВПО, доставляемое с фишингом, имеет встроенный инструментарий обхода песочницы

По данным Solar JSOC, 2020 г.

17%

компаний способны эффективно сопротивляться кибератакам

По данным Accenture, 2020 г .

207 дней

среднее время обнаружения компанией взлома ее инфраструктуры

По данным Ponemon Institute, 2020 г.

Ростелеком
Солар

Киберландшафт-2020

Рост квалификации злоумышленников

Усложнение инструментария

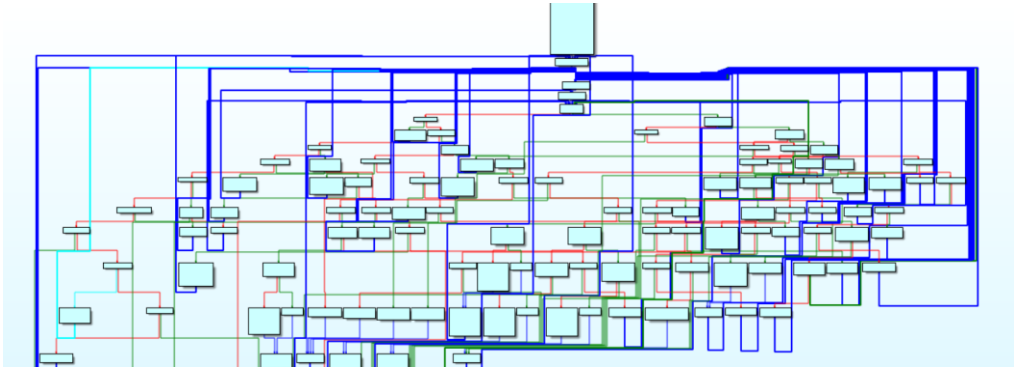
Повышение темпа использования новый уязвимостей

Длительное присутствие в инфраструктуре

Итог: расслоение подходов злоумышленников к атакам на инфраструктуру

Инструменты злоумышленников: ВПО

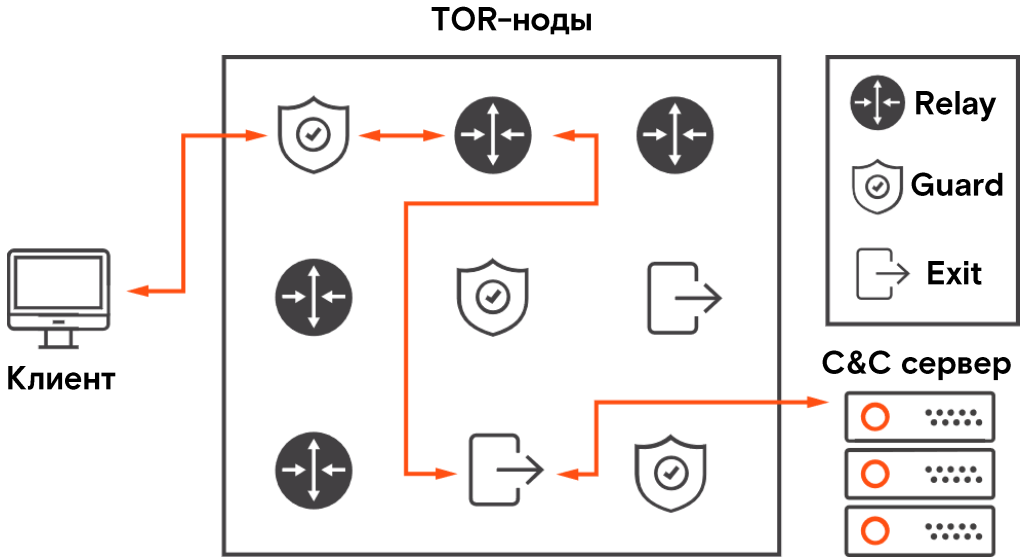
- Механизмы обфускации для гарантированной доставки и запуска ВПО
- Сокрытие C&C через TOR-ноды
- Проверки окружения
  - Виртуализация
  - Стенды



Ростелеком
Солар

Инструменты злоумышленников: ВПО

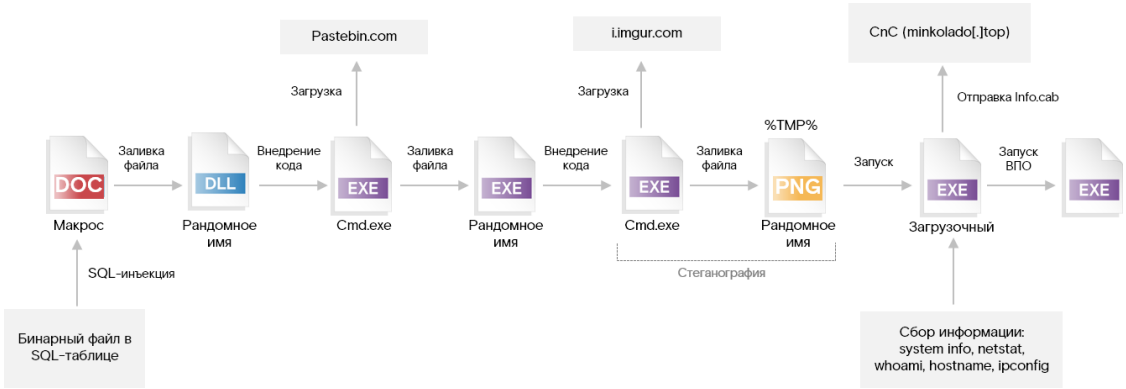
- Механизмы обфускации для гарантированной доставки и запуска ВПО
- Сокрытие C&C через TOR-ноды
- Проверки окружения
  - Виртуализация
  - Стенды



Ростелеком
Солар

Инструменты злоумышленников: ВПО

- Механизмы обфускации для гарантированной доставки и запуска ВПО
- Сокрытие C&C через TOR-ноды
- Проверки окружения
  - Виртуализация
  - Стенды



Ростелеком
Солар

Что изменилось в уровнях злоумышленников

Ростелеком
Солар

Эволюция злоумышленников

Было:

Базовые атаки

Хакеры

Кибервойска

Стало:

Автоматизированные системы

Киберхулиган/ энтузиаст-одиночка

Киберкриминал/ организованные группировки

Кибернаемники/ продвинутые группировки

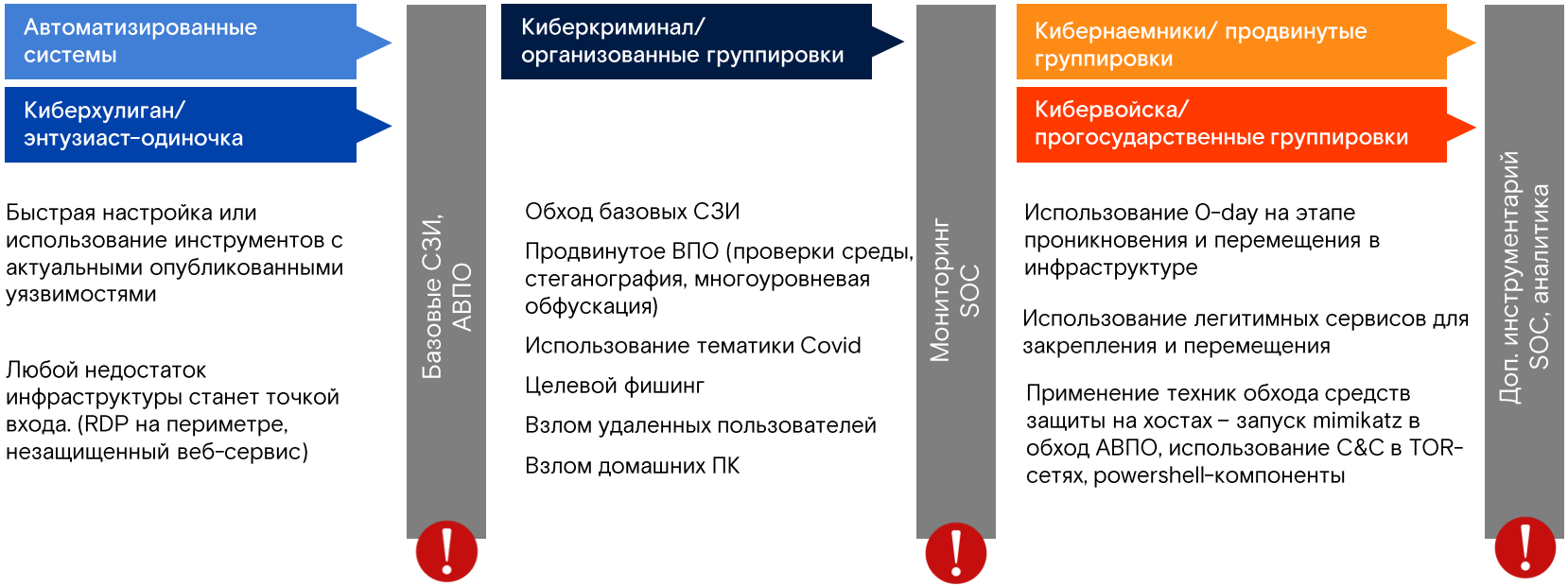
Кибервойска/ прогосударственные группировки

Ростелеком
Солар

Категории 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, соц. инжиниринг
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/ прогосударственные 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»

Чем опасны, как защититься



Отсутствие настроенных и обновляемых базовых средств защиты – 100-процентный шанс быть атакованным

Невозможность детектирования без мониторинга

Скрытое присутствие, не детектируемое базовым мониторингом

Ростелеком Солар

Ответ на современные киберугрозы

Ростелеком
Солар

Защита конечных точек от сложных угроз (EDR)

Выявляет признаки сложных атак на рабочих станциях и серверах, осуществляет сбор, запись и централизованное хранение информации о событиях безопасности на всех рабочих местах

Решаемые задачи

- Выявление и локализация целевых атак продвинутых злоумышленников
- Повышение эффективности анализа угроз и реагирования на инциденты
- Выявление атак на ранней стадии и ускорение принятия ответных мер
- Устранение брешей в системе безопасности и выявление сложных угроз, невидимых для базовых СЗИ

Ключевые преимущества

- Обнаружение невидимых для базовых СЗИ угроз
- Сокращение времени реагирования за счет автоматизации
- Больше информации об инциденте благодаря глубокой детализации журналов событий

Анализ сетевого трафика (NTA)

Network traffic analysis (NTA) позволяет выявлять сложные кибератаки и осуществлять сбор и хранение данных для расследования инцидентов.

Решаемые задачи

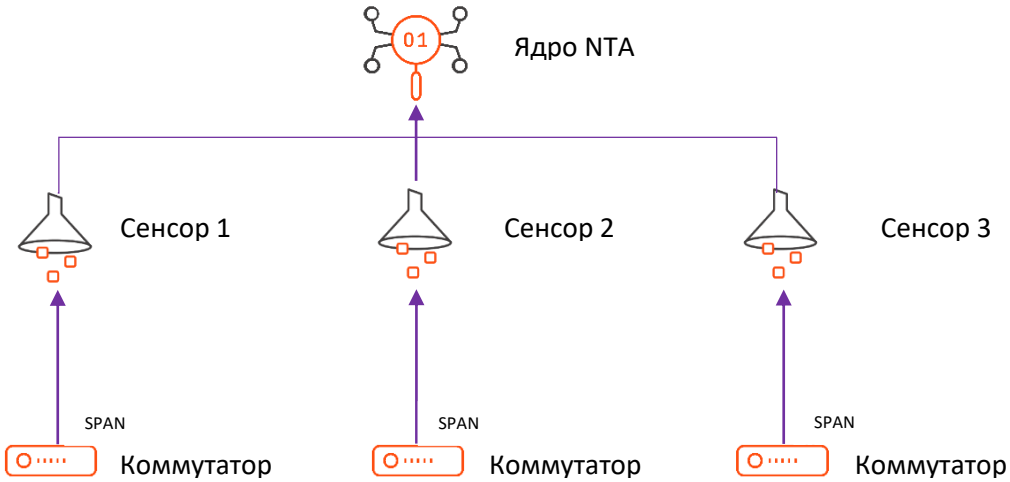
- Выявление угроз в периметровом и внутреннем сетевом трафике
- Устранение слепых зон в защите и выявление угроз, не детектируемых СЗИ уровня ОС
- Помощь в расследовании атак и восстановлении их хронологии
- Обнаружение утечек данных и нарушения политик безопасности

Ключевые преимущества

- Охват всей инфраструктуры комплексным мониторингом
- Определение модифицированного или бесфайлового вредоносного ПО
- Выявление угроз в зашифрованном трафике
- Проверка гипотез Threat Hunting и выявление скрытых угроз
- Поиск скрытых каналов взаимодействия с управляющими серверами злоумышленников

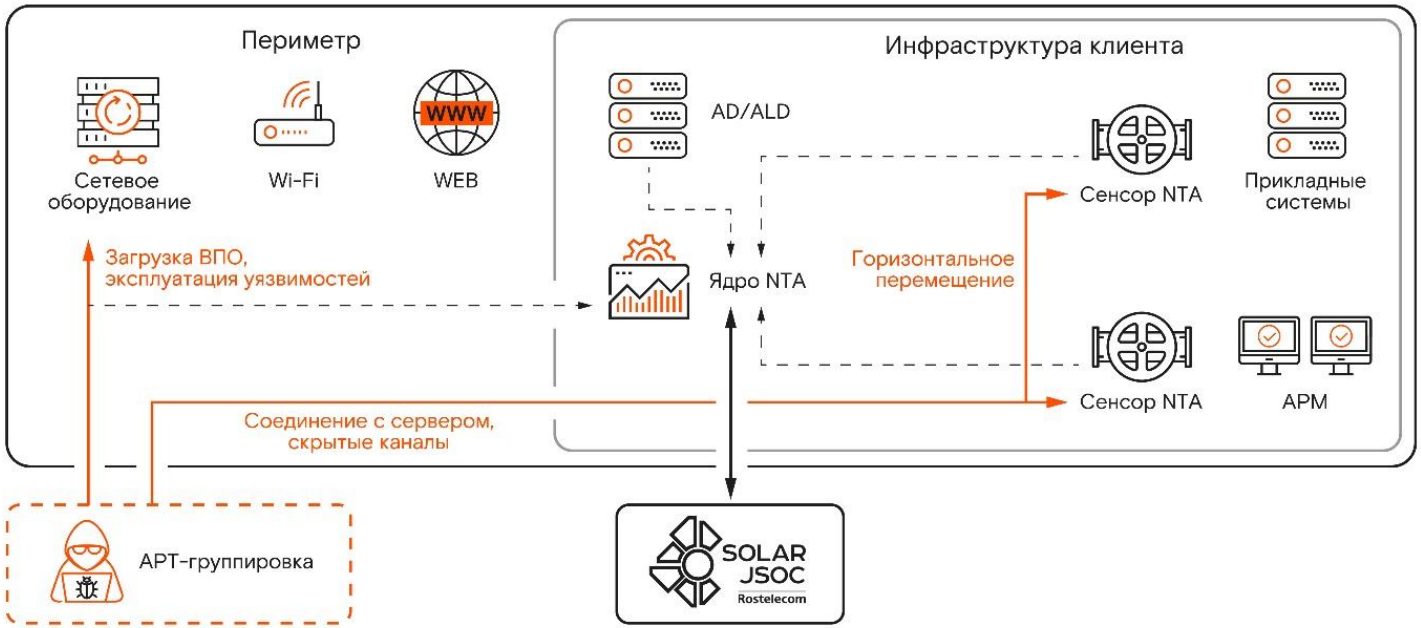
Ростелеком
Солар

NTA – покрытие всей инфраструктуры



Ростелеком
Солар

Технологическое решение: NTA



Возможности NTA

Хранение трафика для последующего анализа

Выявление атак

Ретроспективная проверка по индикаторам компрометации

Контакты

Центральный офис

125009 г. Москва,
Никитский переулок, 7с1

+7 (499) 755-07-70

info@rt-solar.ru

Узнать подробнее или заказать сервис

presale@rt-solar.ru

Ростелеком
Солар