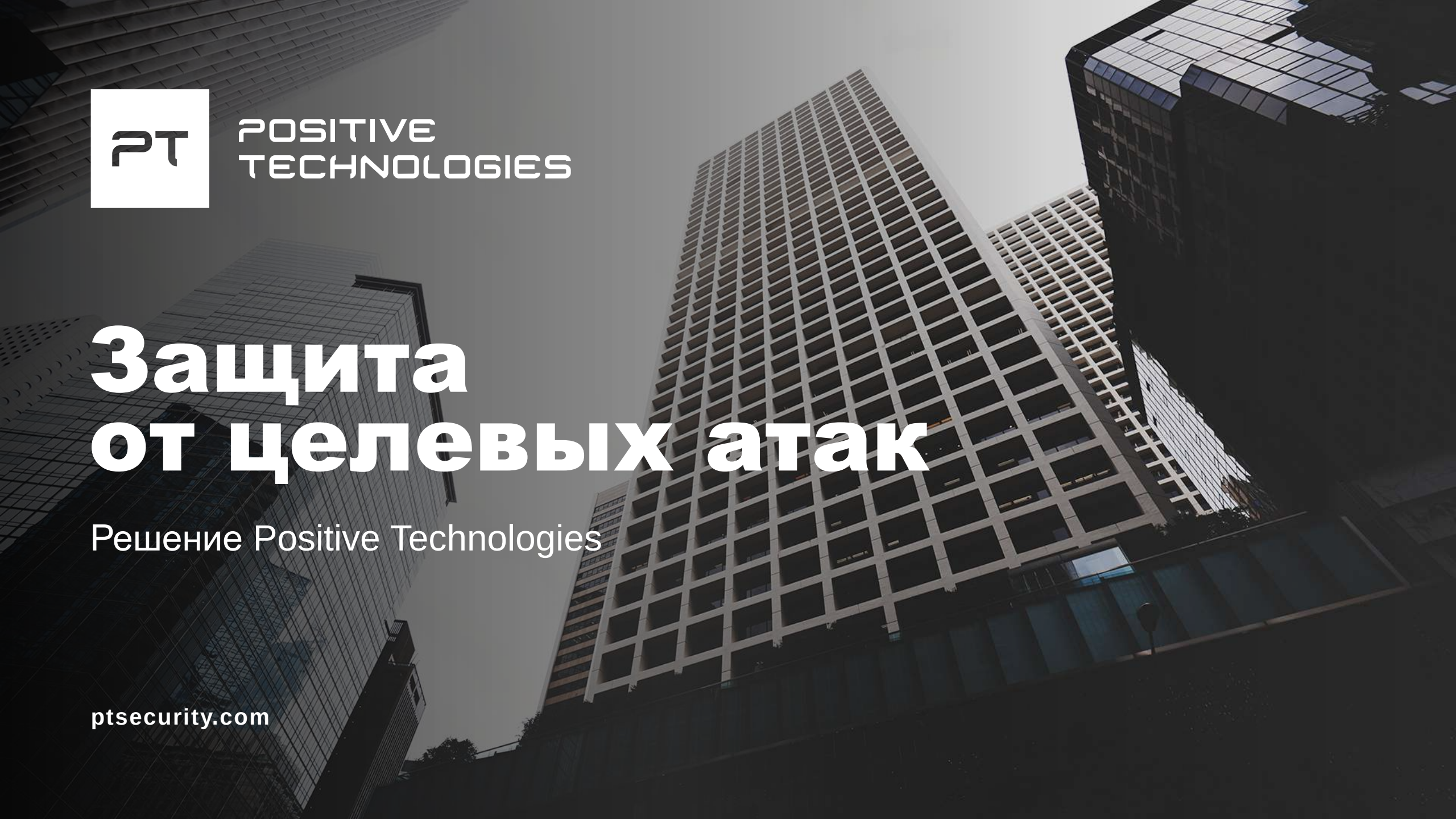


POSITIVE TECHNOLOGIES

Защита от целевых атак

Решение Positive Technologies

ptsecurity.com

О компании Positive Technologies

17 лет
опыта исследований и разработок

900 сотрудников:
инженеров по ИБ, разработчиков, аналитиков и других специалистов

250 экспертов
в нашем исследовательском центре безопасности

200+
обнаруженных уязвимостей нулевого дня в год

200+
аудитов безопасности корпоративных систем делаем ежегодно

50%
всех уязвимостей в промышленности и телекомах обнаружили наши эксперты

Защищаем крупные информационные системы от киберугроз:

- создаем продукты и решения
- проводим аудиты безопасности
- расследуем инциденты
- исследуем угрозы

Нам доверяют

Наши проекты

2018 МАРТА
ВЫБОРЫ ПРЕЗИДЕНТА РОССИИ

Задача
Усилить защищенность веб-портала ЦИК РФ во время проведения выборов.

Что сделано
Проверили защищенность веб-портала, внедрили PT Application Firewall для выявления и блокировки атак, провели мониторинг безопасности в день выборов.

Результат
Выявлены критичные уязвимости, обеспечена безопасность веб-портала и блокировка атак в режиме реального времени.

FIFA WORLD CUP
RUSSIA
2018

Задача
Обеспечить защиту сервисов, необходимых для перемещения болельщиков, регистрации компаний-перевозчиков и набора волонтеров.

Что сделано
Создали контур безопасности и проводили непрерывный мониторинг защищенности всей инфраструктуры.

Результат
Обеспечено непрерывное функционирование всех информационных систем.

ptsecurity.com

phd
Positive
Hack
Days

Ежегодный международный форум по практической безопасности, который собирает тысячи участников.

В рамках форума мы организуем 30-часовую кибербитву за контроль над эмуляцией городской инфраструктуры между командами атакующих и защитников. Формат соревнования максимально приближен к реальности.

Во время кибербитвы SOC на базе наших продуктов мониторит инфраструктуру и выявляет атаки.

phdays.com

Аналитика и расследования

ВЫПУСКАЕМ 20+ ИССЛЕДОВАНИЙ В ГОД:

- ежеквартальные отчеты об актуальных киберугрозах и трендах,
- прогнозы, расследования активности хакерских группировок,
- отраслевые исследования.

ptsecurity.com/ru-ru/research/analytics

Целевые атаки:
проблематика

ptsecurity.com

Чем опасны целевые атаки

Целевые атаки обычно хорошо спланированы и включают несколько этапов, среди которых:

- Разведка
- Внедрение, перемещение в сети и достижение цели
- Уничтожение следов присутствия

После успешного закрепления в инфраструктуре атакующие могут остаться незамеченными **в течение месяцев или даже лет**. На протяжении всего этого времени они **имеют доступ ко всей корпоративной информации**.

Действия атакующих внутри сети

Перехват учетных данных одного из сетевых узлов

Продвижение в инфраструктуре:
эксплуатация уязвимостей, применение хакерского инструментария, сокрытие своей активности от средств защиты

Охота за учетными данными администратора домена

Полная компрометация инфраструктуры:
получение доступа к контроллеру домена с максимальными привилегиями

Закрепление в инфраструктуре:
постоянный доступ к целевому хосту

Постоянный доступ к интересуемой информации

Наши пентестеры во всех исследуемых системах **получили полный контроль** над внутренней инфраструктурой.

Ландшафт угроз

Число атак растет

Доля целевых атак от общего числа

+5% по сравнению с 2018 годом

в среднем проходит до обнаружения атаки**

Кого атакуют чаще всего*

20% государственный сектор

8% сфера образования

8% медицинские учреждения

5% IT-компании

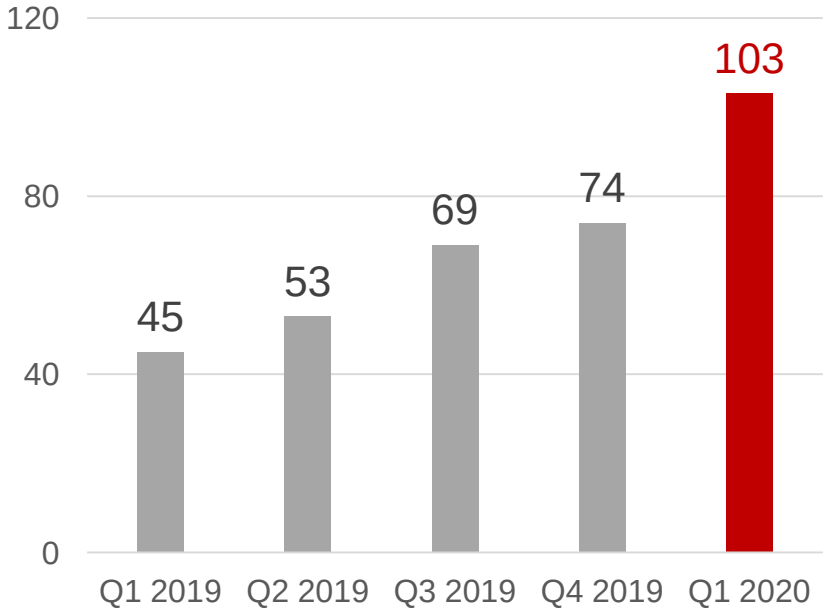
8% финансовая отрасль

10% промышленные компании

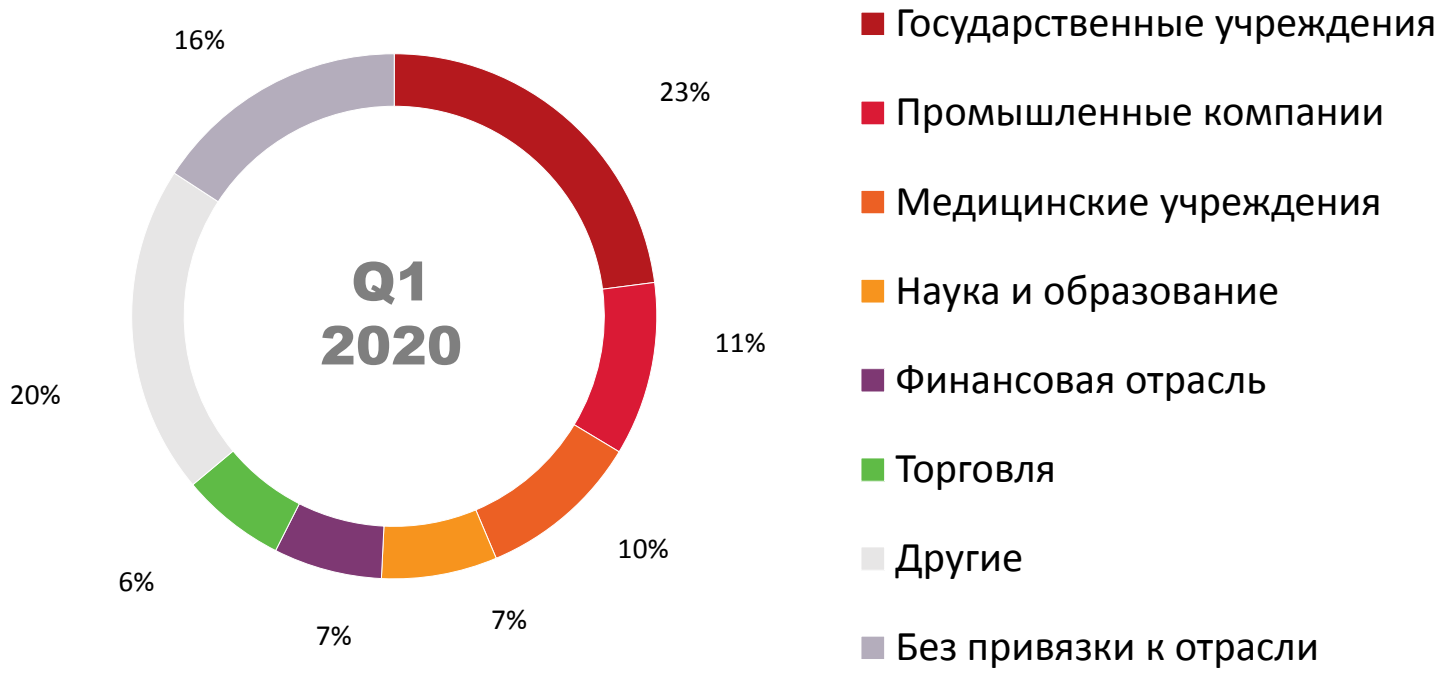
- Массовые атаки на организации уходят в прошлое, **преобладает индивидуальный подход**
- С разового взлома и кражи денежных средств фокус сместился на **долгосрочное пребывание в сети заказчика с целью похищения информации**

* «Актуальные киберугрозы: итоги 2019 года», Positive Technologies
** 2018 Cost of a Data Breach Study: Global Overview, Ponemon Institute

Атаки на госучреждения 2019-2020



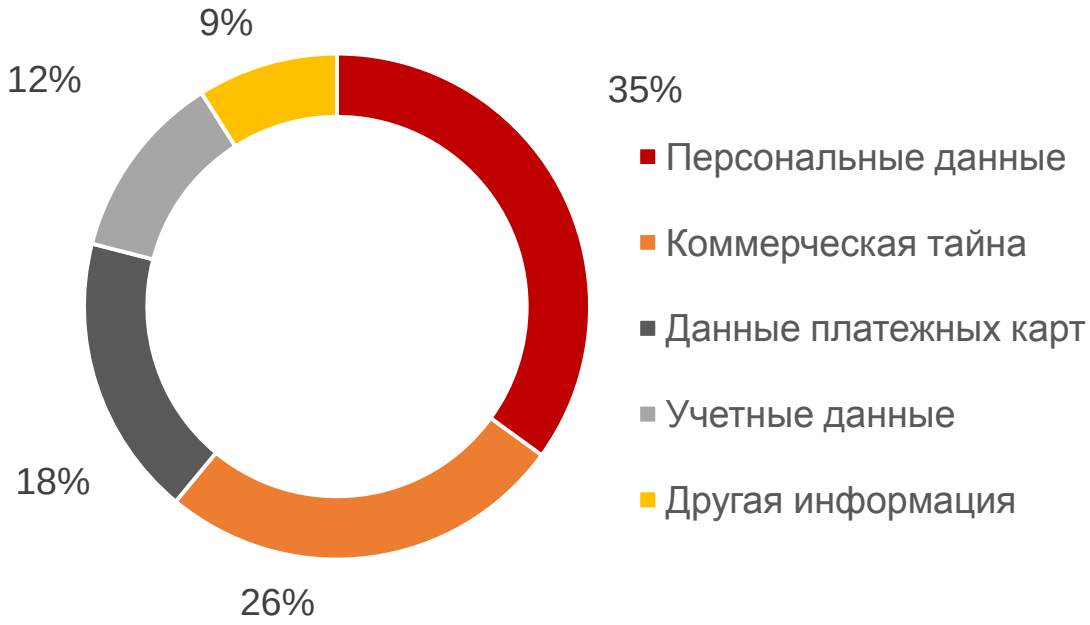
Количество атак на госучреждения по кварталам



Категории жертв среди юридических лиц

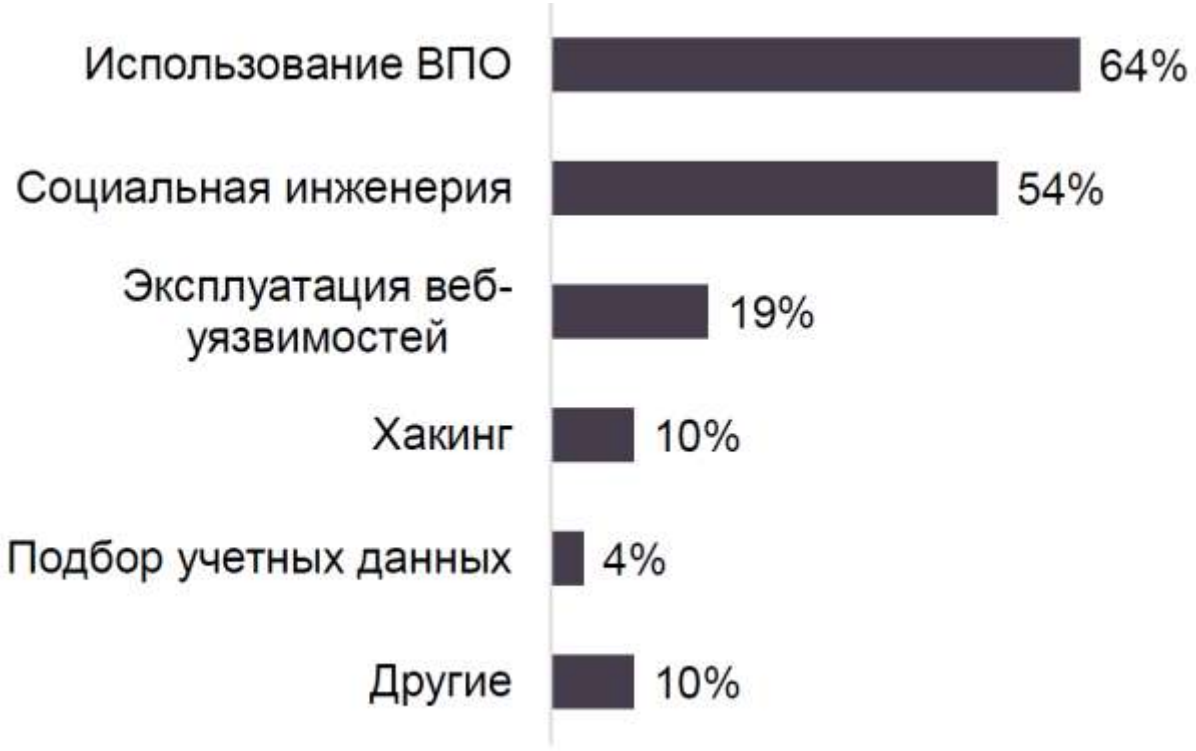
Мотивы атакующих

Мотивы атак в 2019 году

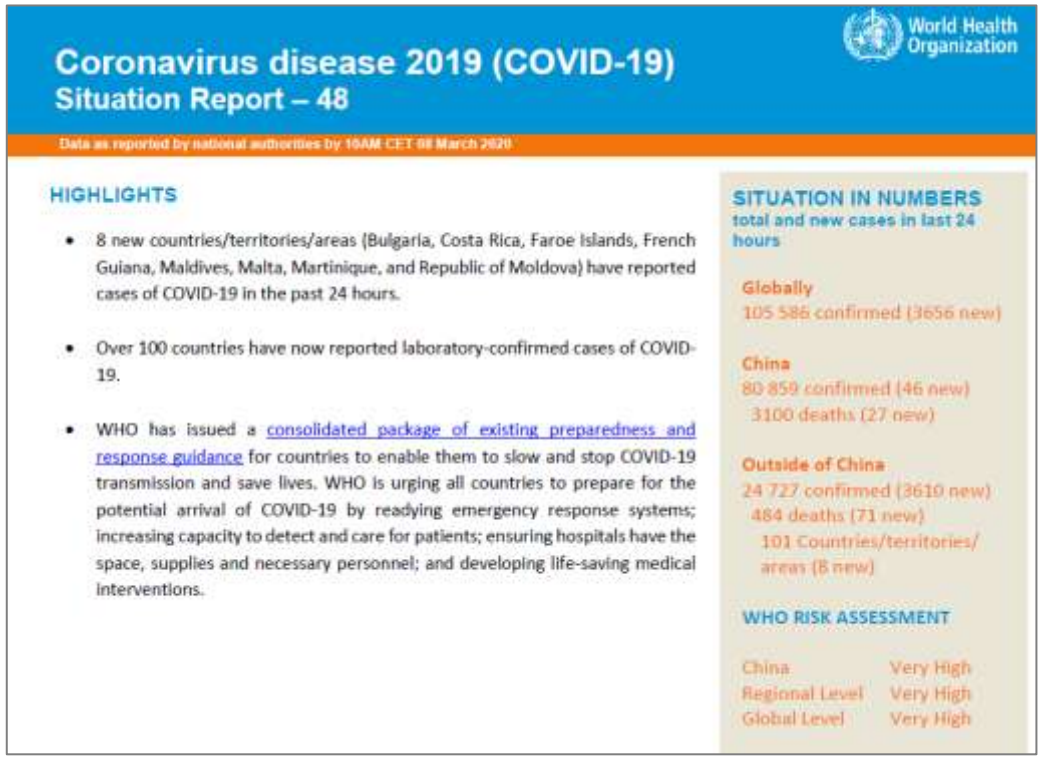


Типы украденных данных в 2019 году

Методы атак



Методы атак на госучреждения в 2019 году



World Health Organization

Coronavirus disease 2019 (COVID-19)
Situation Report – 48

Data as reported by national authorities by 10AM CET 08 March 2020

HIGHLIGHTS

- 8 new countries/territories/areas (Bulgaria, Costa Rica, Faroe Islands, French Guiana, Maldives, Malta, Martinique, and Republic of Moldova) have reported cases of COVID-19 in the past 24 hours.
- Over 100 countries have now reported laboratory-confirmed cases of COVID-19.
- WHO has issued a consolidated package of existing preparedness and response guidance for countries to enable them to slow and stop COVID-19 transmission and save lives. WHO is urging all countries to prepare for the potential arrival of COVID-19 by readying emergency response systems; increasing capacity to detect and care for patients; ensuring hospitals have the space, supplies and necessary personnel; and developing life-saving medical interventions.

SITUATION IN NUMBERS
total and new cases in last 24 hours

Globally
105 586 confirmed (3656 new)

China
80 859 confirmed (46 new)
3100 deaths (27 new)

Outside of China
24 727 confirmed (3610 new)
484 deaths (71 new)
101 Countries/territories/areas (8 new)

WHO RISK ASSESSMENT

China	Very High
Regional Level	Very High
Global Level	Very High

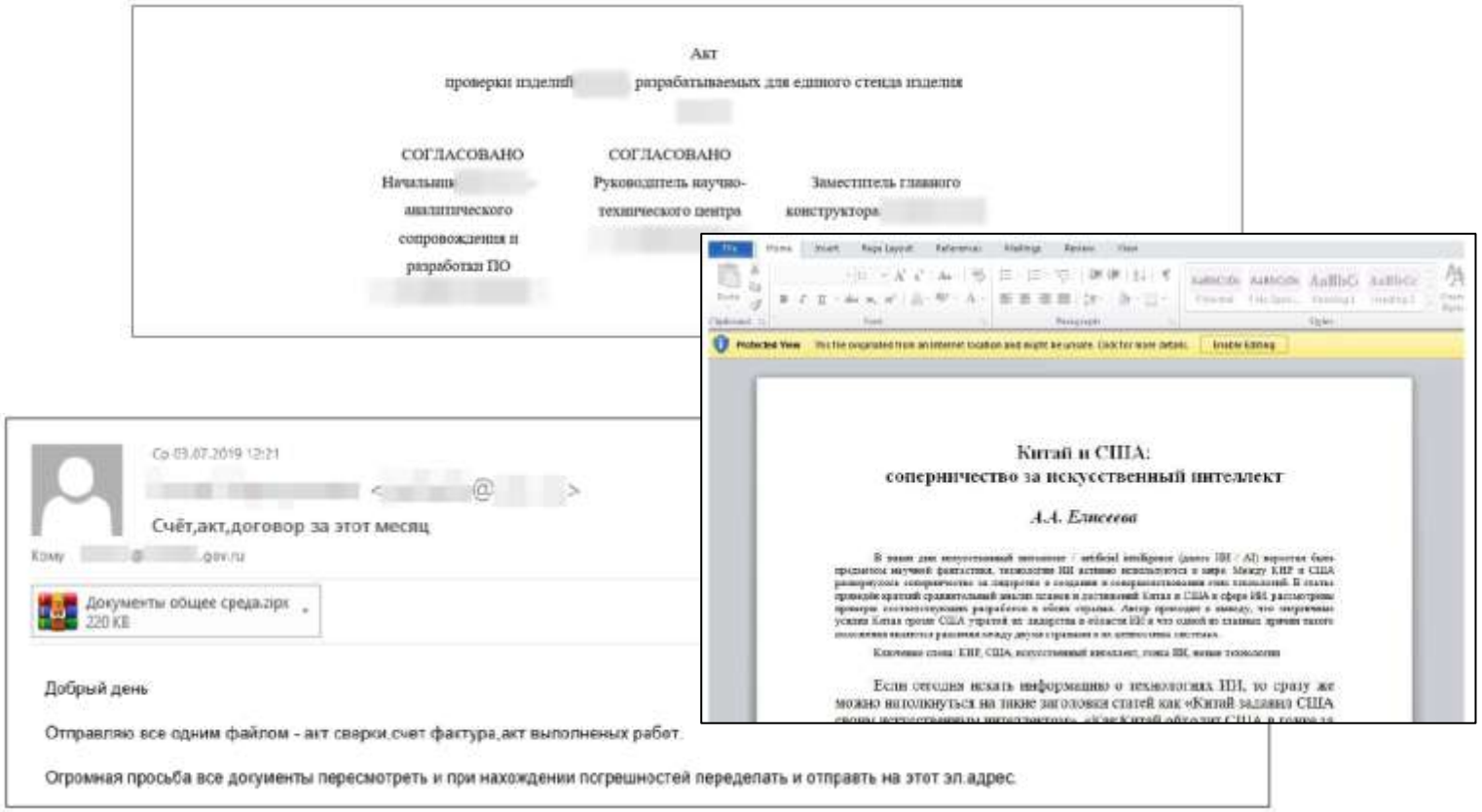
В Q1 2020 года выросла доля атак с использованием социнженерии и ВПО

APT-группировки

На государственные учреждения нацелены **высококвалифицированные APT-группировки**

Мотивы APT-атак – шпионаж, кража данных, хищение денежных средств

87% APT-группировок начинают атаки на российские госучреждения с рассылки фишинговых писем



Фишинговые письма в адрес госучреждений

Уязвимые патчи открыли хакерам доступ к контенту The Last of Us Part II

Уязвимость в патчах от разработчика игр Naughty Dog позволила хакерам получить доступ к закрытому контенту из готовящейся к выходу игры The Last of Us Part II. По словам исследователей, все конфиденциальные данные хранились в ведре Amazon S3.

Напомним, что ещё неделю назад Сеть взорвалась наполненными спойлерами роликами из ещё не вышедшей игры.

Теперь же утечка из ведра Amazon S3 — дело рук неизвестной группы киберпреступников. Ходят слухи, что за сливом также может стоять экс-сотрудник Naughty Dog, затаивший на компанию обиду.

SCADA-системы израильской сферы водоснабжения подверглись целевым атакам

Власти Израиля предупредили организации, снабжающие население очищенной питьевой водой, о серии целевых кибератак, основной целью которых являются объекты водоснабжения.

Согласно официальному уведомлению, опубликованному Управлением по кибербезопасности Израиля, злоумышленники атакуют SCADA-системы насосных станций и канализаций.

«Всем организациям сферы водоснабжения и энергообеспечения рекомендуется срочно поменять пароли от систем, имеющих доступ в Сеть. Также необходимо обновить используемое программное обеспечение», — пишет регулятор.

NCSC: Хакеры России и КНР пытаются выкрасть данные о вакцине от COVID-19

Национальный центр кибербезопасности Великобритании (NCSC) предупредил исследовательские центры страны о волне кибератак, исходящих от правительственных хакеров. В рамках этих операций страны-оппоненты якобы пытаются завладеть данными, полученными в ходе изучения нового коронавируса SARS-CoV-2.

По словам представителей NCSC, зарубежные киберпреступники уделяют особое внимание информации о разработке вакцины против коронавирусной инфекции COVID-19.

Звучит логично, поскольку для многих стран важно быть первыми в этой гонке. Создав по-настоящему рабочую и безопасную вакцину, та или иная страна сможет получить внушительные геополитические козыри.

Данные оформивших в 2017-2019 годах микрозаймы россиян продаются в Сети

На сайте хакерской тематики злоумышленники выставили на продажу данные россиян, которые имели неосторожность оформить микрозаймы в период между 2017 и 2019 годом. Продавцы утверждают, что в соответствующей базе находится 12 миллионов записей.

В итоге за определённую сумму любой может купить полные имена, номера паспортов, телефонные номера и информацию об электронных кошельках граждан России. Эксперты предполагают, что утечку могла допустить одна из МФО.

Продающие данные киберпреступники предоставили бесплатный «пробник» базы данных, в котором, как

Трамп объявил чрезвычайное положение из-за атак на энергосистемы США

Нынешний президент США Дональд Трамп подписал указ, согласно которому в стране вводится чрезвычайное положение из-за кибератак правительственных группировок на энергетические системы Америки.

По словам Трампа, нанятые странами-оппонентами хакеры «всё больше создают и эксплуатируют уязвимости».

В указе президента США о чрезвычайном положении говорится, что Западу угрожают «хакерские операции». В качестве контрмер Трамп решил запретить компаниям, находящимся под контролем недружественных стран «приобретение, импорт, перенос и инсталляцию оборудования для энергосистем».

Почему сложно
обеспечить защиту от целевых атак

1

Обычно защищают только периметр

В большинстве случаев компании фокусируются только на защите периметра, хотя в 9 из 10 случаев злоумышленник преодолевает периметр. После этого его действия можно обнаружить только по последствиям на поздних стадиях атаки или после ее завершения

2

Угрозы постоянно развиваются

Распространяются бесфайловые атаки, сокрытие за commodity malware, злоумышленники используют шифрованные каналы, продолжаются атаки с эксплуатацией уязвимостей нулевого дня

3

Фокусировка на выявлении атак в реальном времени

Целевые атаки могут длиться долго: от нескольких дней до нескольких лет. Для их выявления недостаточно мониторинга в реальном времени: также необходимо понимать, с чего началась атака, на каком этапе развития она находится в данный момент, что произошло в сети

4

У компаний не хватает экспертизы и ресурсов

Так как целевые атаки постоянно усложняются, одних только технологий для их выявления и расследования недостаточно. Часто в компаниях не хватает необходимых экспертных знаний и ресурсов

Как преодолеть эти сложности

1

Отслеживать всю потенциально опасную активность одновременно на периметре и внутри сети, в том числе на критически важных активах

2

Сочетать глубокий анализ сетевого трафика и проверку файлов, передаваемых в сетевом трафике, на предмет наличия угроз

3

Выявлять атаки в режиме реального времени и искать их признаки в прошлом, чтобы даже длительные атаки не остались незамеченными

4

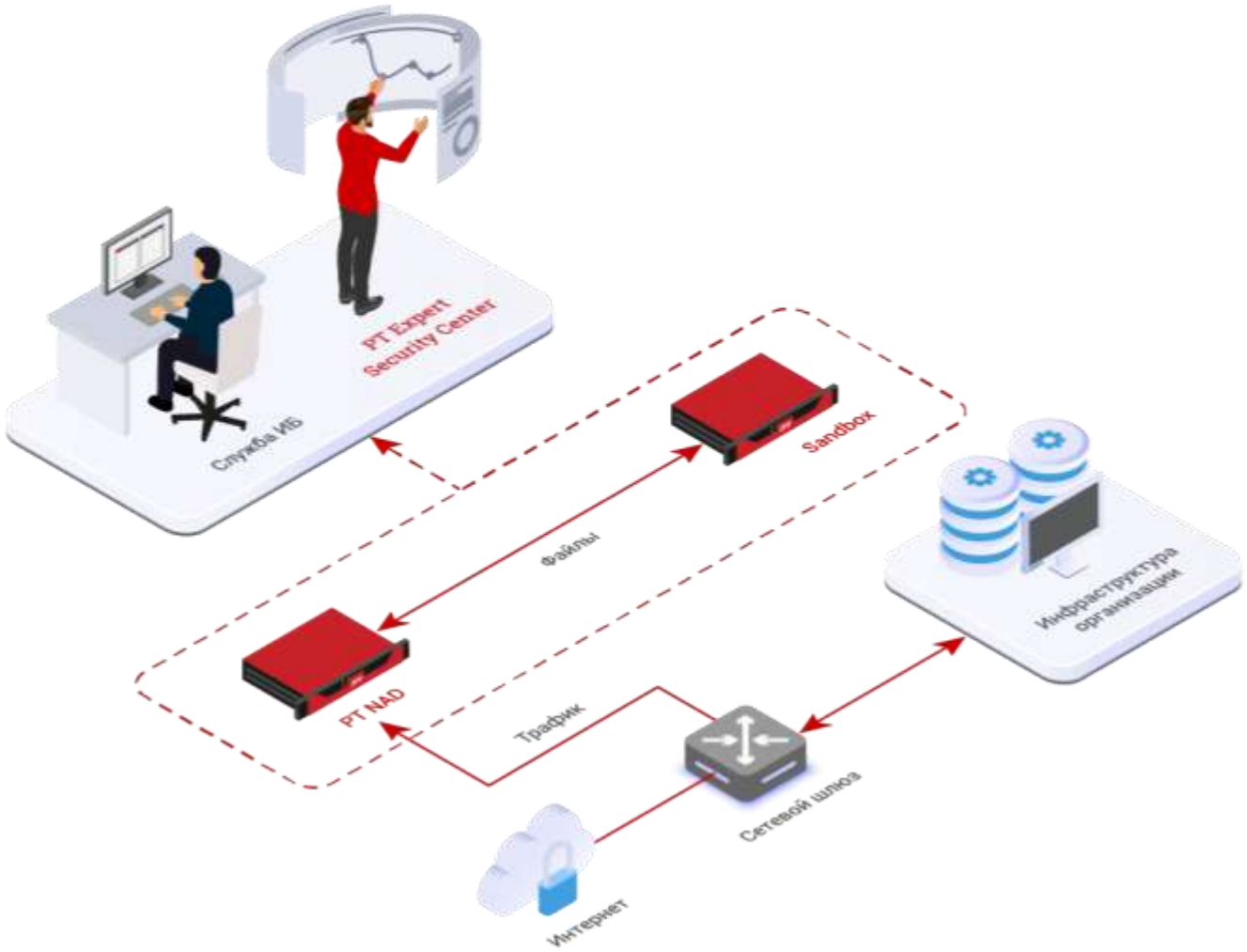
Использовать решения с регулярно обновляемой собственной экспертизой и привлекать внешних экспертов для сокращения времени реагирования и расследования

PT Anti-APT

Компоненты Anti-APT	Решаемые задачи
PT Network Attack Discovery	Выявляет признаки атак в сетевом трафике на периметре и в инфраструктуре
PT Sandbox	Производит анализ файлов, передаваемых из PT NAD, а также в почтовом, сетевом и веб-трафике, на предмет угроз
PT Expert Security Center	Дополняют команду ИБ при недостатке экспертизы или полностью берут на себя задачи по мониторингу и расследованиям

Как это работает:
long story short

- PT NAD анализирует на наличие угроз копию трафика, перенаправленную с соответствующего сетевого устройства
- Передаваемые в трафике файлы PT NAD отправляет на анализ в PT Sandbox. Вердикт возвращается в PT NAD
- В зависимости от сценария PT Sandbox также осуществляет мониторинг или блокировку писем, файлов в хранилище, пользовательских файлов из сети Интернет
- Специалисты PT ESC дополняют команду ИБ при недостатке экспертизы или полностью берут на себя задачи по мониторингу и расследованию



PT Network Attack Discovery

Глубокий анализ сетевого трафика для выявления атак (NTA)

Проводит глубокий анализ трафика: определяет 50 протоколов и разбирает 30 наиболее распространенных протоколов до уровня L7

Обнаруживает попытки кражи данных и сокрытия активности от средств защиты, признаки взлома и другие подозрительные активности в трафике

Извлекает файлы, передаваемые в сетевом трафике, и отдает их на анализ в PT Sandbox

Проводит ретроспективный анализ трафика для обнаружения атак, не выявленных ранее

Ключевые задачи:

Дает понимание, что происходит в сети

PT NAD определяет более 70 протоколов, разбирает до уровня L7 включительно 30 наиболее распространенных из них. Это позволяет получить подробную картину активности в инфраструктуре и выявить проблемы в ИБ, которые снижают эффективность системы безопасности и способствуют развитию атак.

Обнаруживает скрытые угрозы

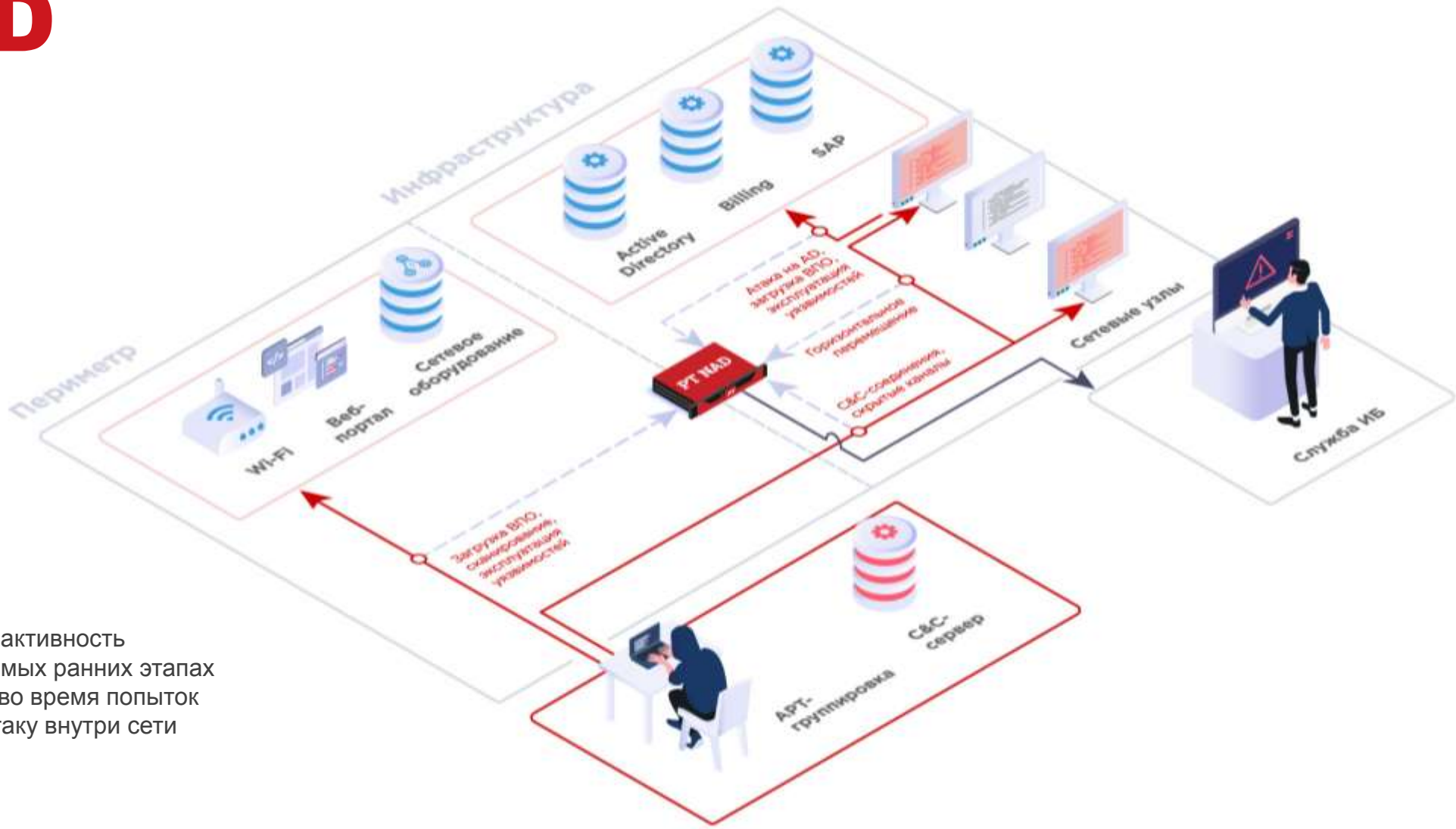
Система автоматически обнаруживает попытки злоумышленников проникнуть в сеть и их присутствие в инфраструктуре по большому количеству признаков: от применения хакерского инструментария до передачи данных на сервера атакующих.

Повышает эффективность работы SOC

PT NAD дает SOC полную видимость сети, упрощает проверку успешности атаки, помогает восстановить ее хронологию и собрать доказательную базу. Для этого он хранит метаданные и сырой трафик, позволяет оперативно находить сессии и фильтровать подозрительные, экспортировать и импортировать трафик.

Как работает PT NAD

PT NAD захватывает и разбирает трафик на периметре и в инфраструктуре.



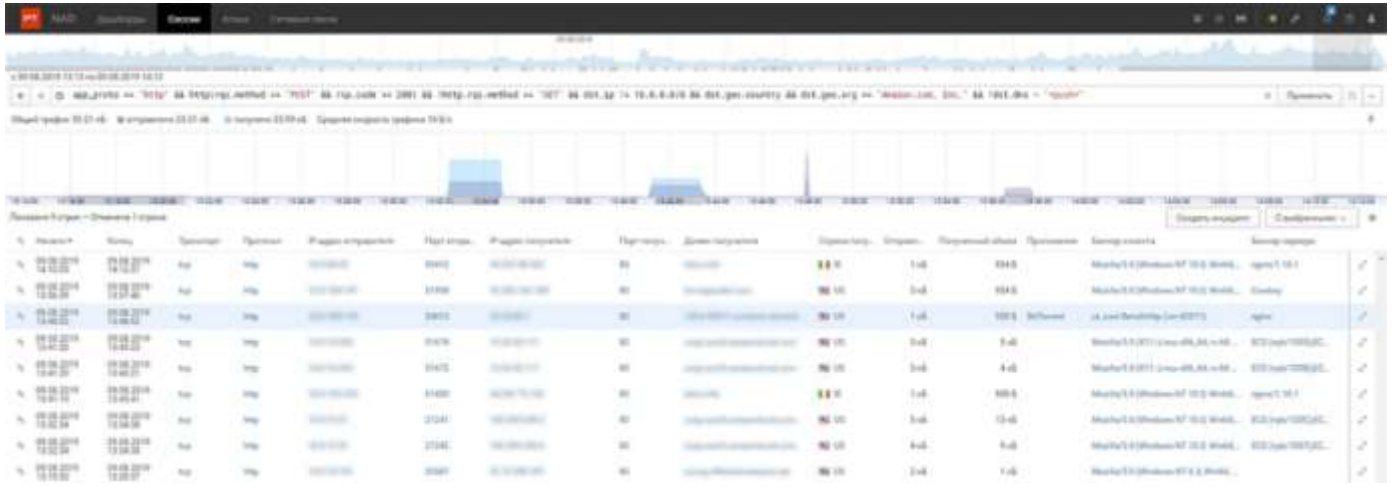
Это позволяет выявлять активность злоумышленника и на самых ранних этапах проникновения в сеть, и во время попыток закрепиться и развить атаку внутри сети

Сценарии использования

Контроль соблюдения регламентов ИБ

PT NAD помогает обнаружить ошибки в конфигурациях информационных систем и нарушения регламентов ИБ, которые снижают эффективность системы безопасности и способствуют развитию атак.

С помощью фильтров пользователи PT NAD могут оперативно обнаружить учетные записи в открытом виде, нешифрованные почтовые сообщения, использование утилит для удаленного доступа и инструментов сокрытия активности в сети.



Анализ трафика крупных компаний в 2019 году показал, что в **94%** компаний нарушаются политики ИБ. Почитайте отчет, чтобы узнать, какие ошибки – самые популярные и чем они опасны: ptsecurity.com/ru-ru/research/analytics/network-traffic-analysis-2020/

Пример

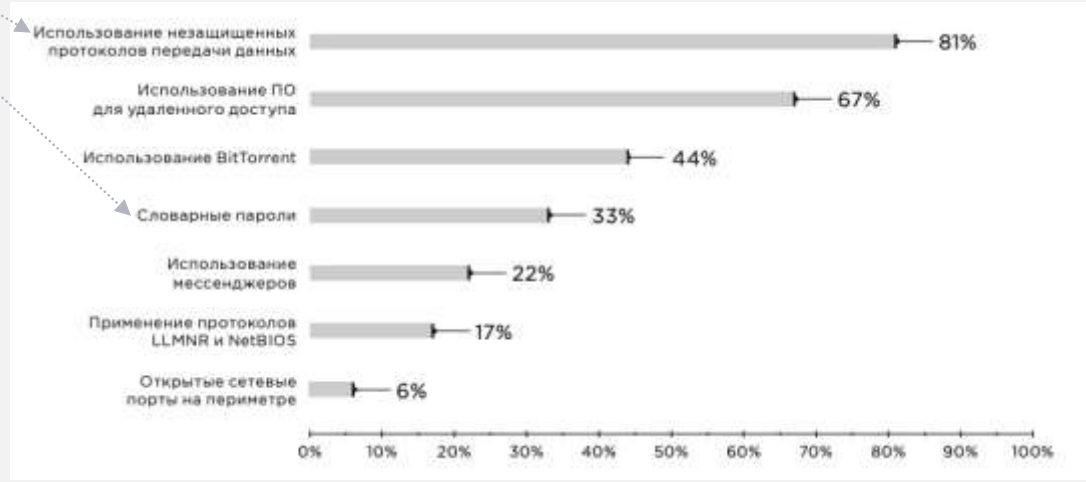
В сети летают учетные данные в открытом доступе. Они могут быть легко перехвачены в случае компрометации сети.

С помощью фильтра в PT NAD можно настроить виджет, где будут отображаться все открытые пароли:

Пары "логин — пароль" по числу сессий

Логин	Пароль	Количество се...
admin	Password	14642
admin	admin	514
Bob	alice	393
Alice	bob	204
proxy	secret123!	129

Можно увидеть конкретные сессии, где передавались открытые данные, адреса узлов отправителей и получателей.



Топ-7 нарушений регламентов ИБ (доли компаний)

*Распространенные угрозы ИБ в корпоративных сетях, 2019, Positive Technologies

Выявление
атак на периметре и в сети

Набор индикаторов компрометации и правил еженедельно пополняется экспертами PT Expert Security Center.

Встроенные технологии машинного обучения, глубокая аналитика, собственные правила детектирования угроз, индикаторы компрометации и ретроспективный анализ позволяют детектировать атаки как на самых ранних стадиях, так и когда злоумышленник уже проник в инфраструктуру.

Пример

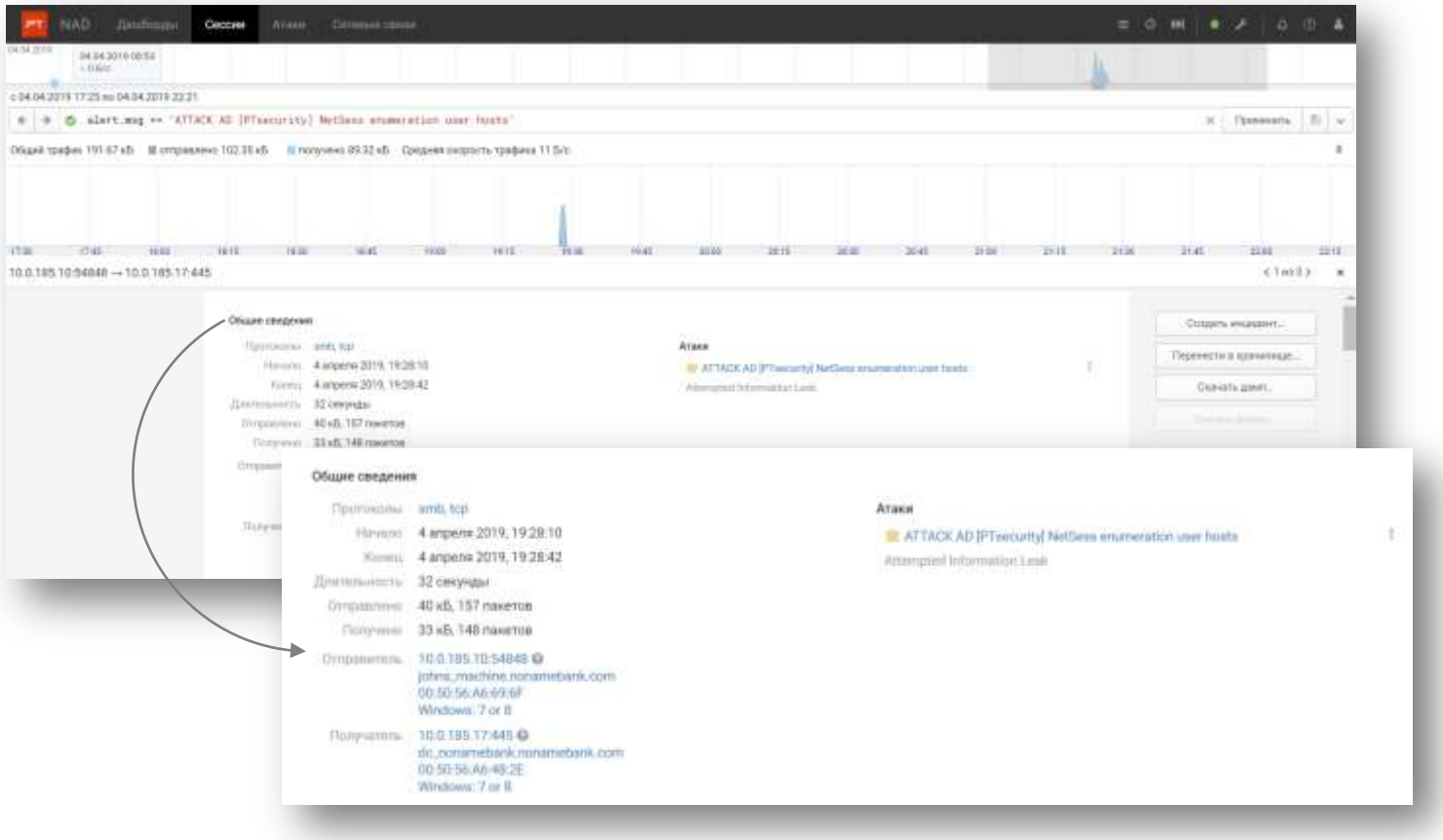
Цель атакующих — захват контроллера домена головной организации.

Шаг №1. Проникновение в головную организацию через менее защищенный периметр одного из филиалов.

Шаг №2. Атака на контроллер домена из единой сети организации.

Шаг №3. PT NAD обнаружил угрозу за счет разбора протокола SMB и выявления нелегитимных запросов списка пользователей в домене.

В интерфейсе PT NAD пользователь видит сработку правила на выявление запросов SMB из нелегитимного сегмента



Расследование атак

Гибкая система хранения данных
Пользователь может выбрать нужные параметры для хранения метаданных и сырого трафика и таким образом оптимизировать объем хранилищ

С помощью PT NAD специалист по расследованию:

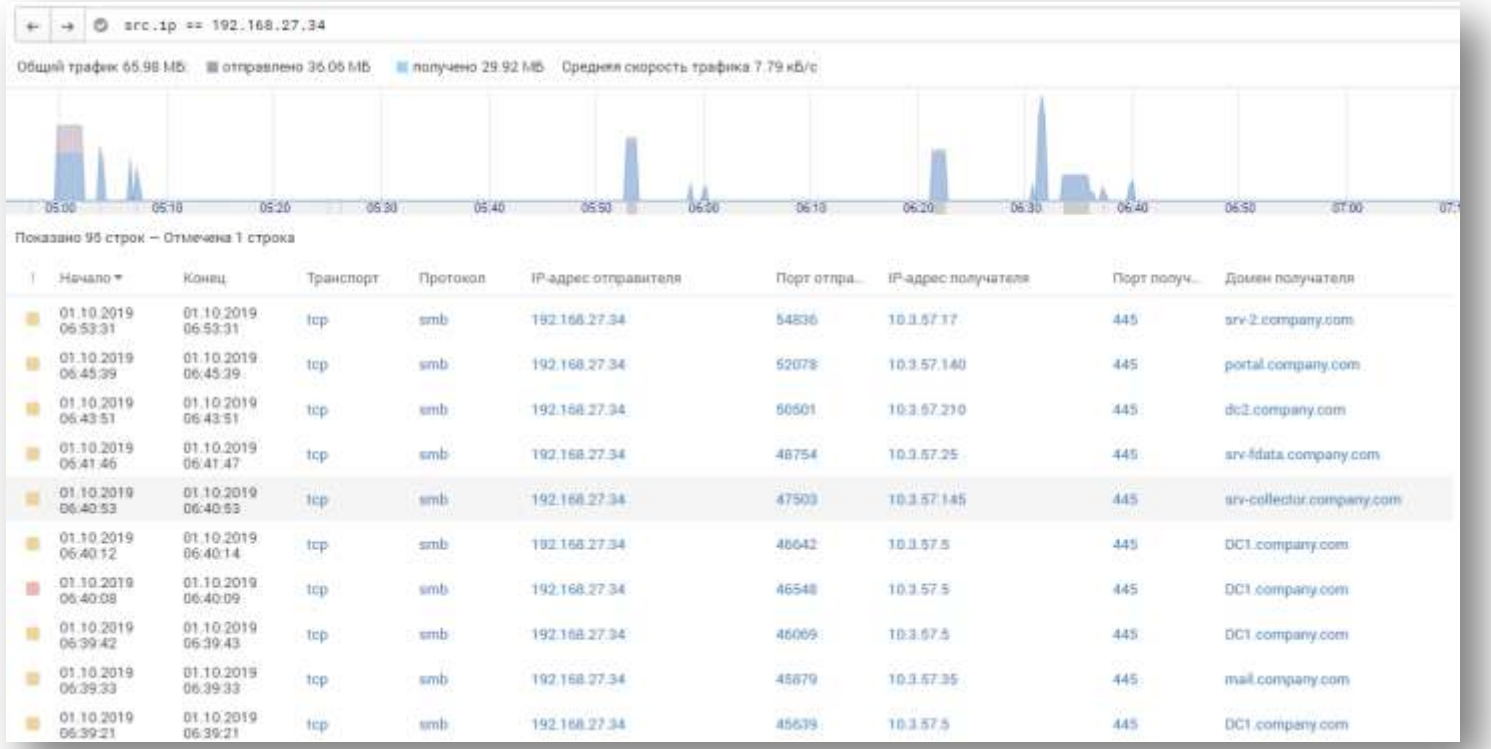
- локализует атаку,
- восстанавливает хронологию атаки,
- выявляет уязвимые места в инфраструктуре,
- вырабатывает компенсирующие меры для предотвращения аналогичных атак,
- собирает доказательную базу.

Пример

1. PT NAD уведомил о неуспешной попытке авторизации в контроллере домена с учетной записи с недостаточным объемом прав.
2. Проверив сетевую активность узла, пользователь увидел, что ранее с него было несколько попыток подключений на другие хосты во внерабочее время.
3. С помощью IT-службы пользователь заблокировал учетку и начал детальное расследование с командой PT ESC.

Пример

1. PT NAD уведомил о неуспешной попытке авторизации в контроллере домена с учетной записи с недостаточным объемом прав.
2. Проверив сетевую активность узла, пользователь увидел, что ранее с него было несколько попыток подключений на другие хосты во внерабочее время.
3. С помощью IT-службы пользователь заблокировал учетку и начал детальное расследование с командой PT ESC.



Threat hunting

PT NAD помогает выстроить процесс threat hunting в организации и выявлять скрытые угрозы, которые не обнаруживаются стандартными средствами кибербезопасности.

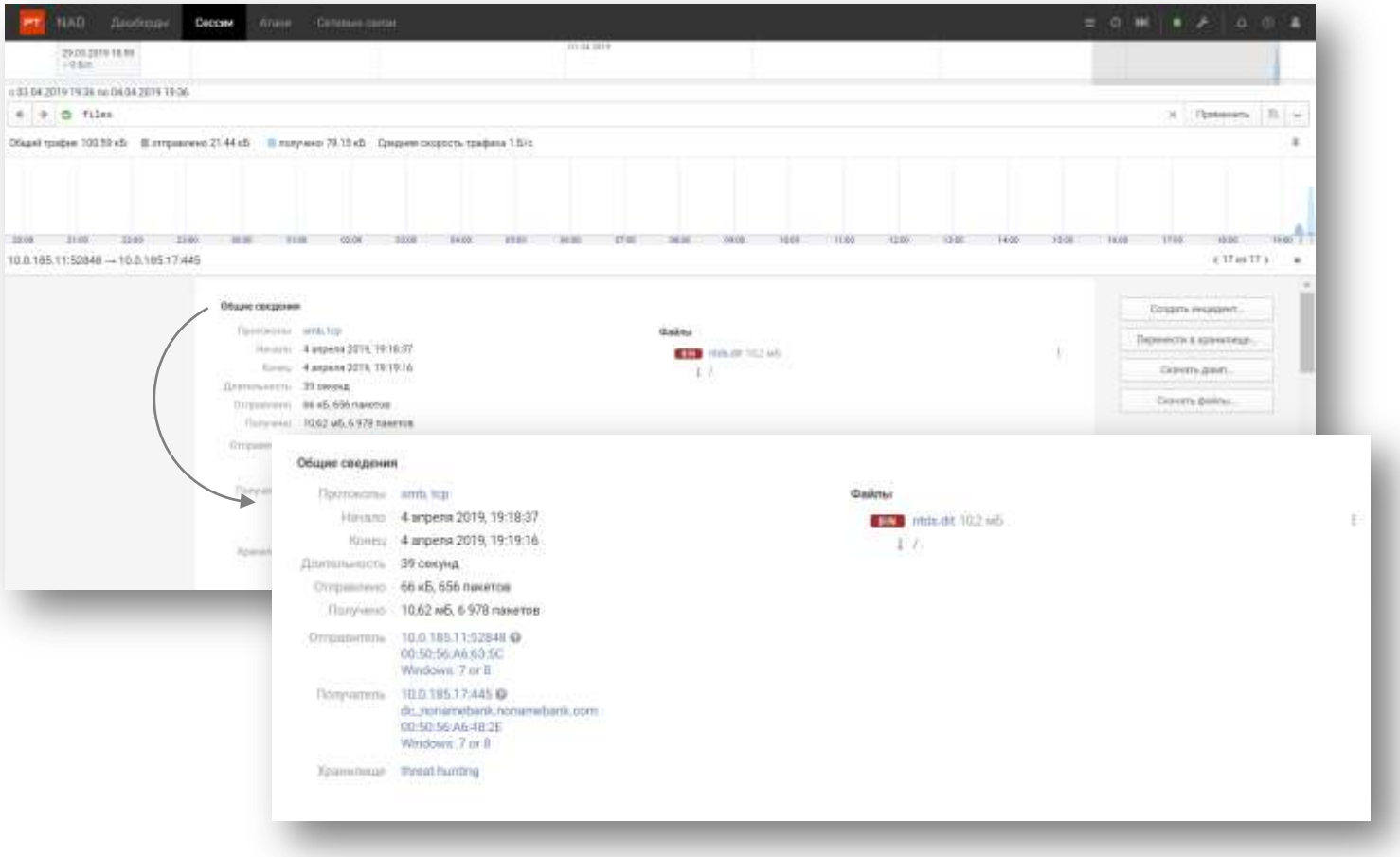
Пример

В системе нет формальных признаков компрометации. Оператор решил проверить гипотезу, что контроллер домена взломан.

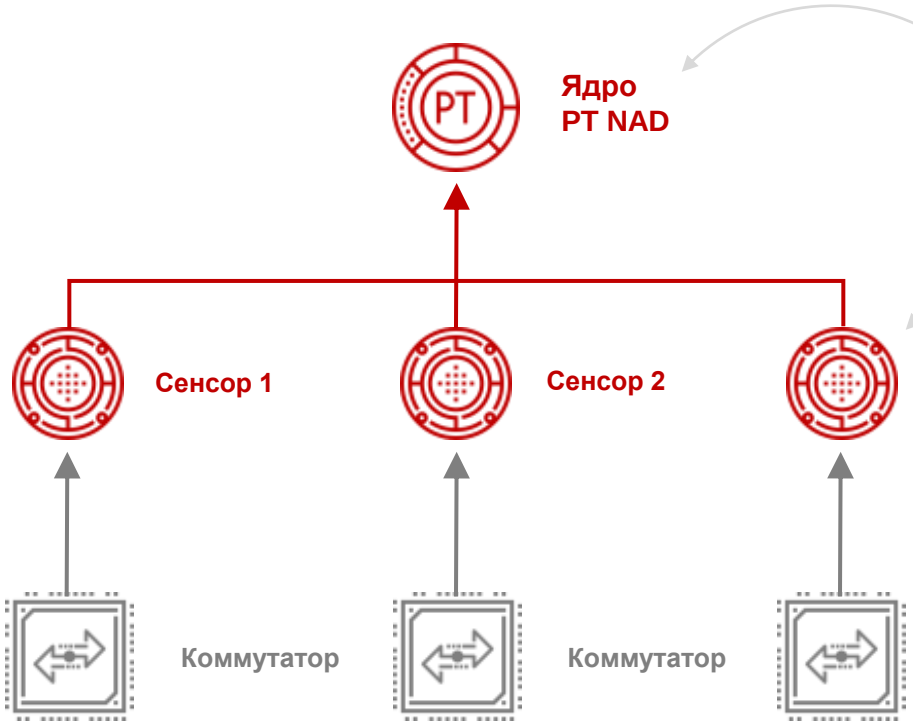
1. С помощью фильтров оператор проанализировал сетевую активность в адрес контроллера домена.
2. С внутреннего адреса был запрос на получение списка пользователей домена и несколько запросов на авторизацию в домен-контроллере. Последний из них оказался удачным.
3. Обнаружено скачивание по протоколу SMB файла ntds.dit*. Гипотеза подтверждена — домен скомпрометирован, нужно провести расследование.

*файл, содержащий все данные каталога Active Directory

Карточка сессии, в которой был скачан файл с данными каталога Active Directory



Логическая архитектура



- Машинное обучение
- Ретроспективный анализ
- Индикаторы компрометации
- Глубокая аналитика
- Хранилище метаданных

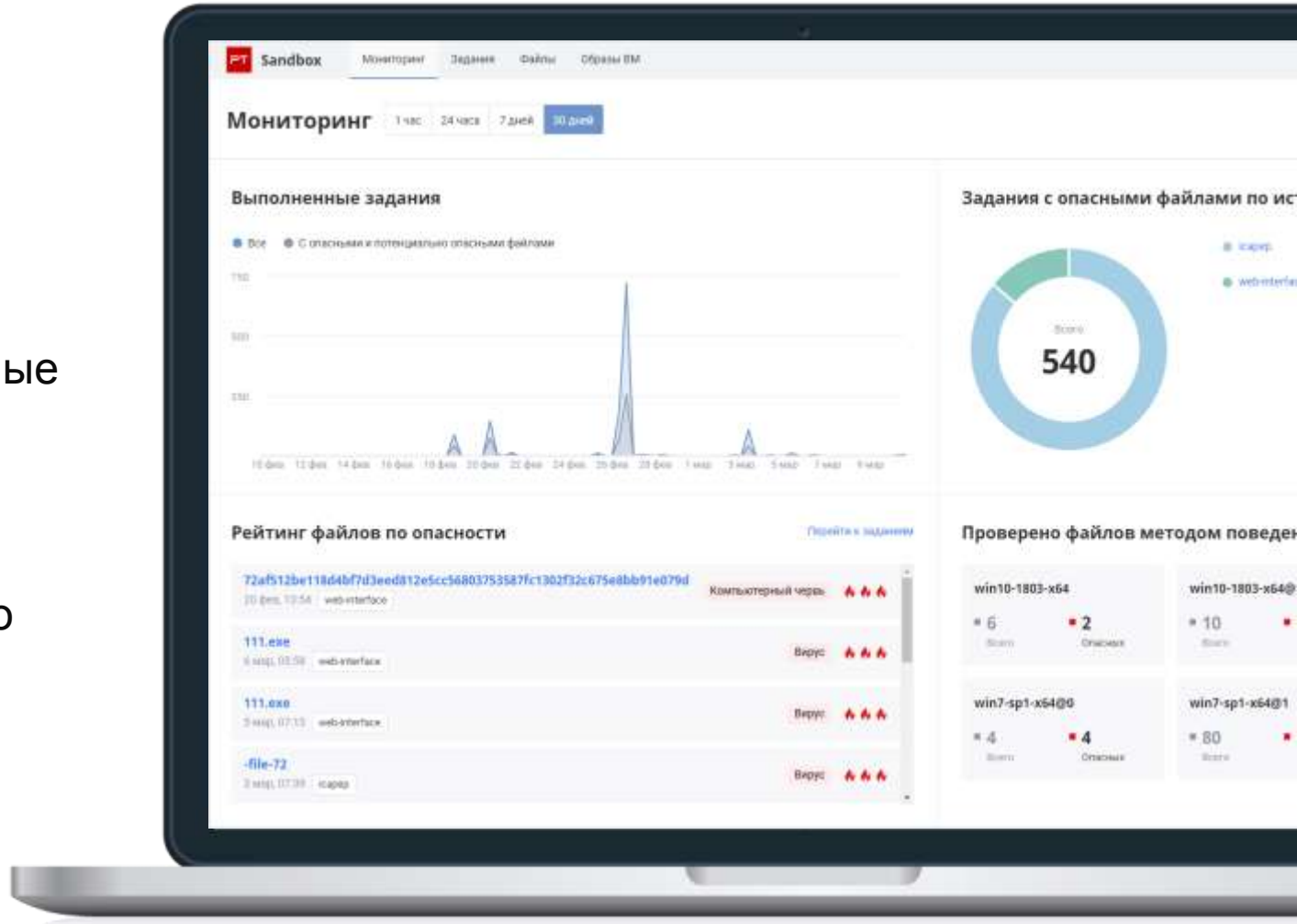
- Глубокий разбор протоколов
- Анализ правилами Positive Technologies
- Хранилище сырого трафика

Ядро поддерживает горизонтальное масштабирование

PT Sandbox

Передовая песочница с возможностью кастомизации виртуальных сред

- В PT Sandbox можно настроить виртуальные среды для в соответствии с реальными рабочими станциями
- Так продукт выявляет сложные атаки, даже если зловреды заточены специально под инфраструктуру заказчика



Возможности PT Sandbox

Выявляет атаки, которые не были обнаружены ранее

После обновления баз знаний PT Sandbox автоматически перепроверяет уже проанализированные файлы, обнаруживая скрытые угрозы.

Обнаруживает угрозы не только в файлах, но и в трафике

PT Sandbox проверяет трафик, который генерируется в процессе анализа файла, и расшифровывает TLS-трафик, выявляя вредоносную активность.

Выявляет известное вредоносное ПО и массовые атаки

PT Sandbox осуществляет префильтеринг файлов с помощью 7 антивирусов, выявляя известные угрозы и сокращая число объектов для проверки в песочнице.

Дополнительные возможности

Механизм Anti-evasion, защита от 20+ техник обхода песочниц

Доступны режимы мониторинга и блокировки

Раскрытие архивов с паролями

Интеграция: почта, веб, файловые хранилища, API

Поддержка ОС: Win10_x64, Win7_x64/x86, Win8.1_x64

Возможность работы on premise

Производительность: от 10 000 файлов в сутки

Virtual / hardware

Сценарии использования

Защита корпоративной почты

Интеграция продукта с почтовыми серверами дает возможность выявлять и блокировать вредоносное ПО в почтовых вложениях.

Выборочная проверка

PT Sandbox позволяет вручную загрузить подозрительный объект на проверку и получить вердикт о его безопасности.

Защита пользовательского веб-трафика

Интеграция продукта со средствами контроля и анализа трафика позволяет выявлять и блокировать вредоносное ПО в веб-трафике пользователей.

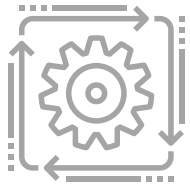
Защита файловых хранилищ

PT Sandbox позволяет проверять файлы на наличие угроз перед загрузкой на корпоративный сетевой ресурс.

Дополнительные сценарии

Выявление и предотвращение целевых атак и сложных угроз

PT Sandbox входит в комплекс защиты от целевых атак вместе с PT Network Attack Discovery и услугами экспертного центра PT Expert Security Center.



Ручной анализ вредоносных программ при расследовании

PT Sandbox сохраняет трассы событий и дампы трафика. Они могут использоваться экспертами при изучении поведения вредоносной программы.

Повышение эффективности продуктов Positive Technologies

PT Sandbox поддерживает интеграцию с другими продуктами Positive Technologies и обогащает их знаниями об угрозах, связанных с вредоносным ПО.

PT Expert Security Center

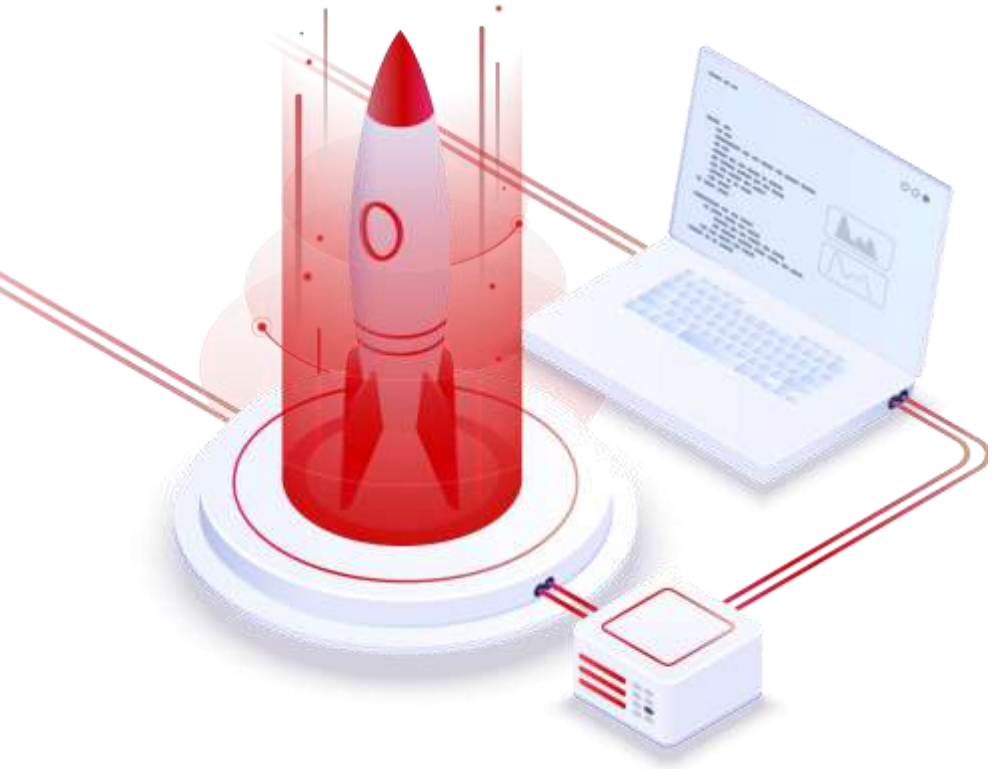
Экспертное сопровождение и расследование

Оказывают помощь в расследовании выявленных инцидентов:

- Проводят анализ хронологии инцидента
- Выявляют все затронутые инцидентом системы
- Помогают в выработке плана по устранению последствий
- Осуществляют сбор доказательной базы
- Помогают в разработке компенсирующих мер

Осуществляют экспертный мониторинг и дополнительный ручной анализ результатов работы комплекса

Преимущества решения



Выявление атак и на периметре, и внутри сети

Система может быть развернута как на периметре, так и перед критически важными активами в инфраструктуре. Это позволяет выявлять активность злоумышленников, даже если они уже проникли в сеть.

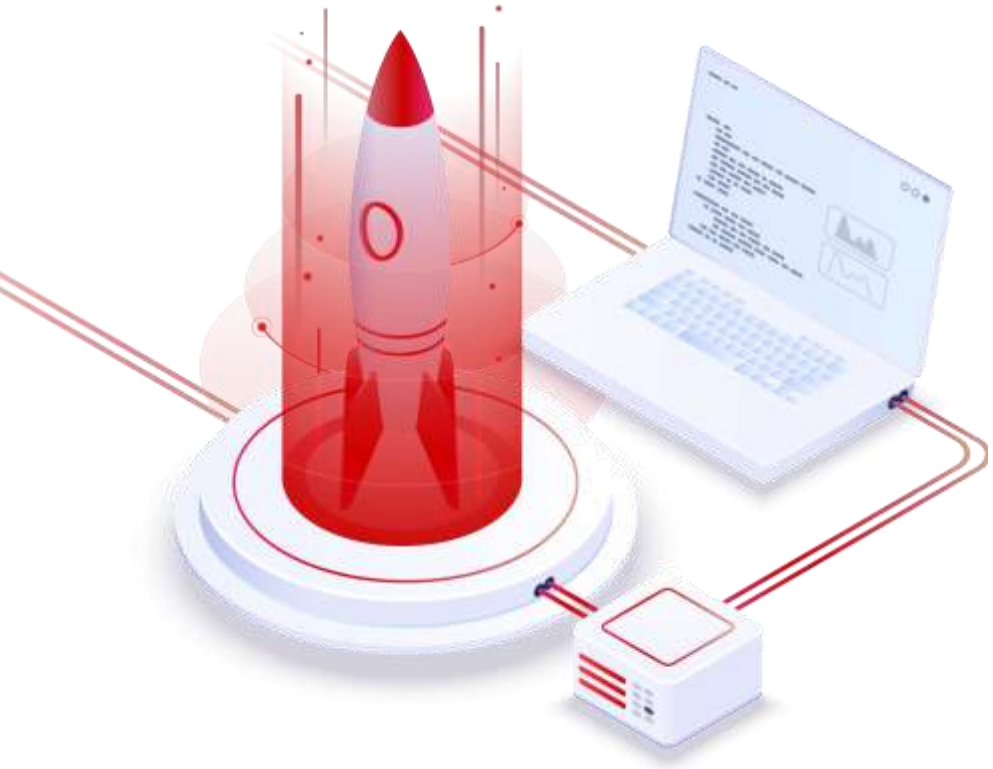
Передовой динамический анализ

Наша песочница знает и блокирует более 20 техник обхода песочниц, которые использует современное вредоносное ПО. Позволяет настроить среды для анализа так, чтобы они максимально соответствовали реальным рабочим станциям в компании. Отслеживает все создаваемые анализируемым объектом процессы, проверяет на наличие угроз генерируемые файлы.

Экспертные технологии распознавания атак в трафике

Решение выявляет угрозы в зашифрованном трафике, горизонтальное перемещение злоумышленника, скрытые каналы (туннелирование), автоматически сгенерированные домены, эксплуатацию уязвимостей, использование хакерского инструментария

Преимущества решения



Регулярный ретроспективный анализ

Ретроспектива помогает обнаруживать атаки, которые не были выявлены ранее, понимать, с чего они начались и что успело произойти с момента взлома. Перепроверка файлов и трафика запускается после обновления баз знаний решения и репутационных списков

Самые актуальные знания для выявления атак

В базу знаний решения постоянно добавляются знания, поставляемые PT ESC по итогам расследований реальных инцидентов в крупных компаниях (включая специфические для России): методы атак, индикаторы компрометации, репутационные списки IP-адресов, доменных имен, файлов и т. п.

Результат использования решения

Сокращение времени скрытого присутствия угрозы

Решение позволяет максимально **сократить время присутствия злоумышленника в сети**:

- выявляет целевые атаки на периметре и внутри сети на самых ранних этапах благодаря глубокому анализу сетевого трафика и файлов;
- обнаруживает атаки, которые не были выявлены в прошлом, благодаря регулярному ретроспективному анализу.

Результат использования решения

Эффективное расследование инцидентов ИБ

Решение дает **всю необходимую для эффективного расследования информацию**:

- Дает глубокое понимание контекста атаки благодаря тому, что может хранить 1200 параметров сессий без ограничений по времени
- Позволяет обнаружить точки входа вредоносных файлов в инфраструктуру, отследить участников и все этапы распространения угрозы

Благодаря этому использование нашего решения **гарантирует успешность расследования, обеспечивает его быстроту и, как следствие, низкую стоимость**.

Покрытие требований 187-ФЗ

Приказ ФСТЭК России от 25.12.2017 № 239, меры защиты:

АУД.5. Контроль и анализ сетевого трафика

СОВ.1. Обнаружение и предотвращение компьютерных атак

СОВ.2. Обновление базы решающих правил

Приказ ФСТЭК России от 25.12.2017 № 235:

Пункт 18. Сертифицированные средства защиты информации применяются в случаях, установленных законодательством Российской Федерации, а также в случае принятия решения субъектом КИИ.

PT NAD также позволяет выполнить требования по защите персональных данных (приказ ФСТЭК № 21), информации в ГИС, в АСУ ТП и в информационных системах общего пользования (приказы ФСТЭК № 19, 31 и 489).

Сертификаты

PT NAD входит в **реестр Российского ПО**,
рег. номер ПО № 4710 от 19 сентября 2018

Сертификат ФСТЭК России №4042
от 30 ноября 2018 позволяет применять PT NAD в качестве системы обнаружения вторжений уровня сети 4 класса защиты в ГИС и в ИСПДн

New

Комплекс раннего выявления сложных угроз PT Anti-APT входит в **реестр Российского ПО**,
рег. номер ПО № 6284 от 7 апреля 2020

reestr.minsvyaz.ru

ptsecurity.com

Варианты внедрения

Если нет компонентов anti-APT

- Возможно единовременное внедрение всего комплекса – PT NAD и PT Sandbox
- Возможно поэтапное внедрение каждого компонента в любом удобном порядке

Если есть компоненты anti-APT...

...Positive Technologies

- При наличии PT NAD возможен апгрейд до полноценного решения: дополнительно внедряется PT Sandbox
- При наличии PT Sandbox также возможен апгрейд: внедряется PT NAD

...другого вендора

- Можно исключить сходный компонент из нашего решения: например, если у вас уже есть песочница, вы можете приобрести PT NAD
- Можно внедрить решение в полном составе в параллель с существующими системами для повышения защищенности (замена текущих систем не требуется)

Попробуйте решение

ЗАЯВКА

Запросите пилот на сайте: ptsecurity.com/ru-ru/solutions/anti-apt/ или свяжитесь напрямую с вашим менеджером в Positive Technologies

ОТЧЕТ

Подписание NDA, заполнение анкеты об инфраструктуре

Разворачивание компонентов, подключение источников

Пилотирование, мониторинг специалистами PT Expert Security Center

≈ 4 недели

В ХОДЕ ПИЛОТА:

- Мы предоставим вам оборудование для пилотирования
- Произведем развертывание и конфигурирование решения, подключим источники
- В ходе пилота специалисты PT ESC будут осуществлять экспертный мониторинг
- По итогам пилота вы получите отчет об обнаруженных угрозах

Мы обнаруживаем APT-атаки
в каждом пятом пилотном проекте

Спасибо за внимание!

ptsecurity.com