POSITIVE TECH PRESS CLUB

Вредоносное ПО. Топ угроз и технологии защиты

АЛЕКСЕЙ ВИШНЯКОВ,
руководитель отдела обнаружения вредоносного ПО
экспертного центра безопасности Positive Technologies
(PT Expert Security Center)

Ландшафт угроз вредоносного ПО: тренды и прогнозы

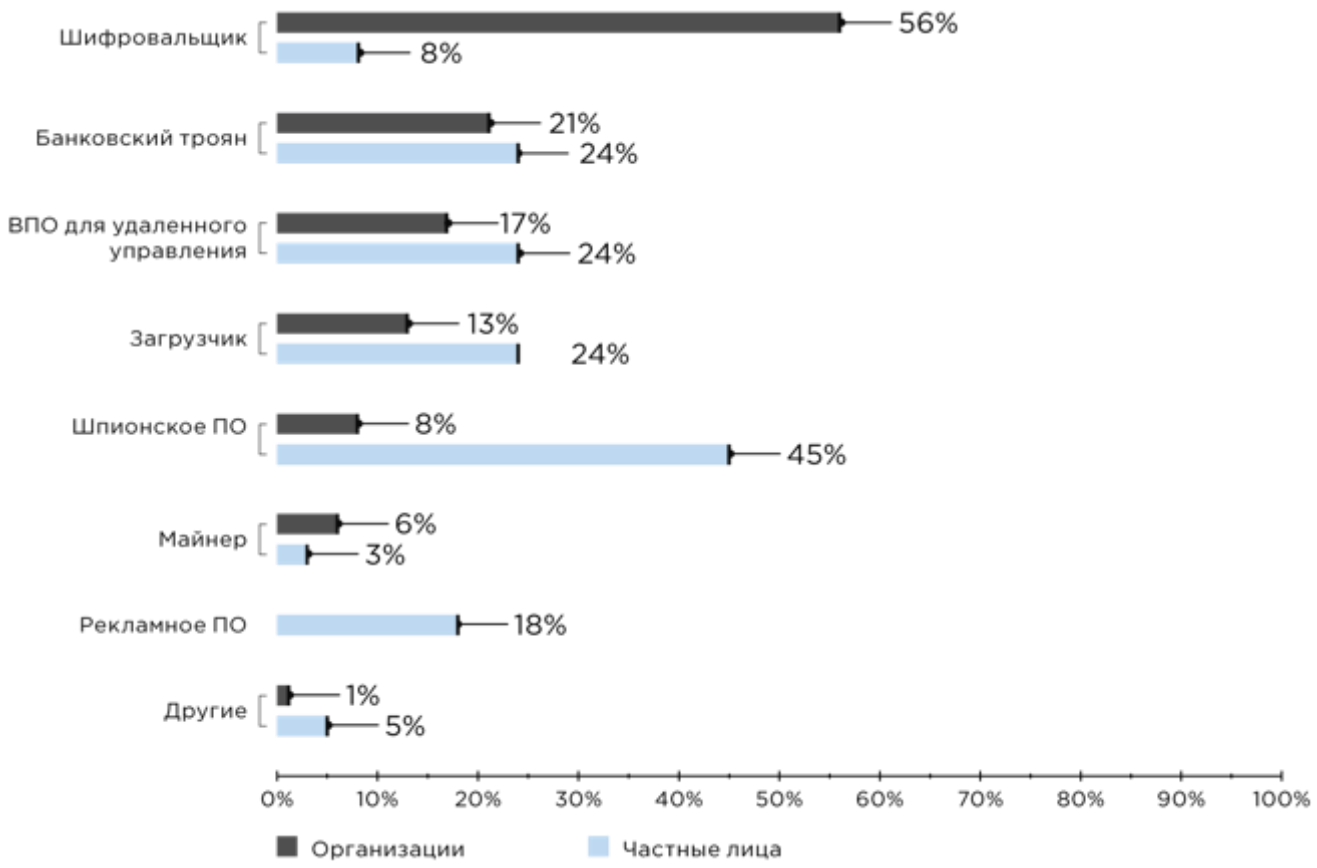
ptsecurity.com

Шифровальщики и шпионское ПО

в авангарде атак

Типы вредоносного ПО

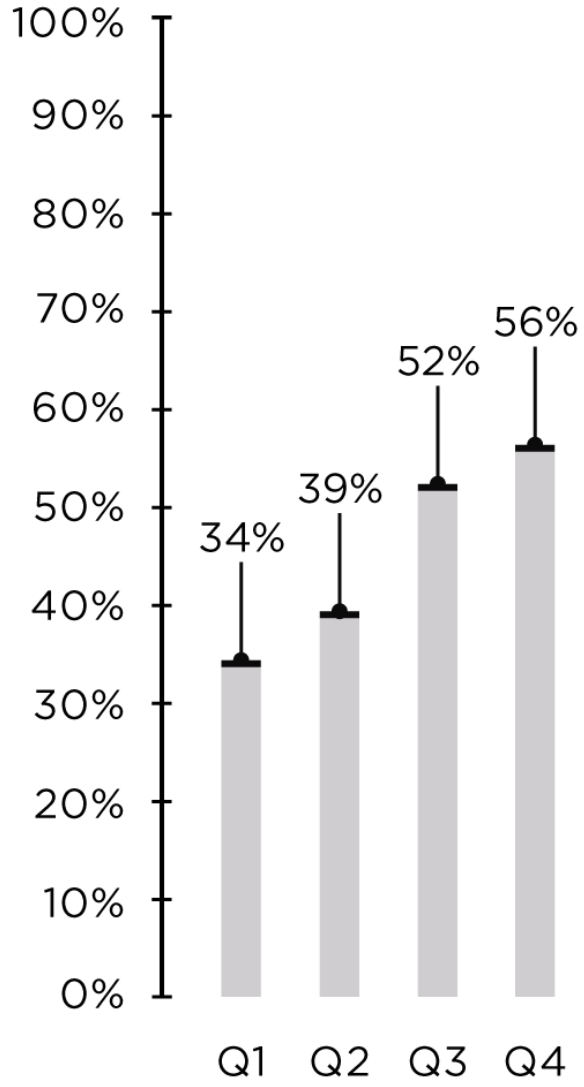
(доля атак с использованием вредоносного ПО)



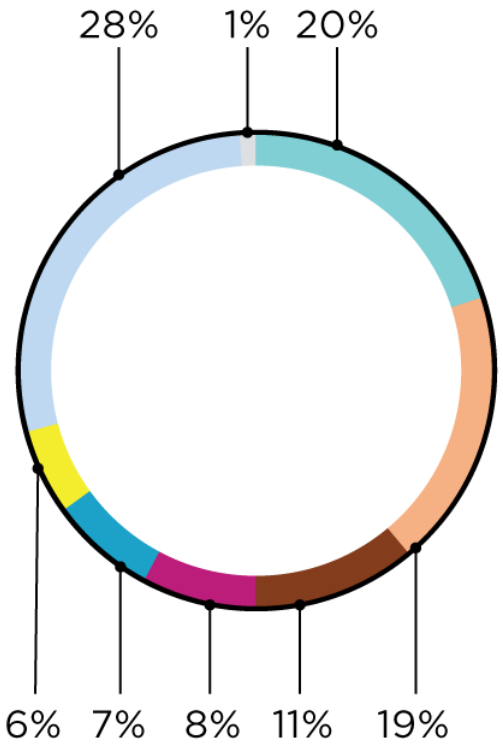
Исследование Positive Technologies
«Актуальные киберугрозы: IV квартал 2020 года»

Динамика атак шифровальщиков

Доли атак с использованием шифровальщиков среди всех атак на организации, реализованных с помощью ВПО



Жертвы шифровальщиков

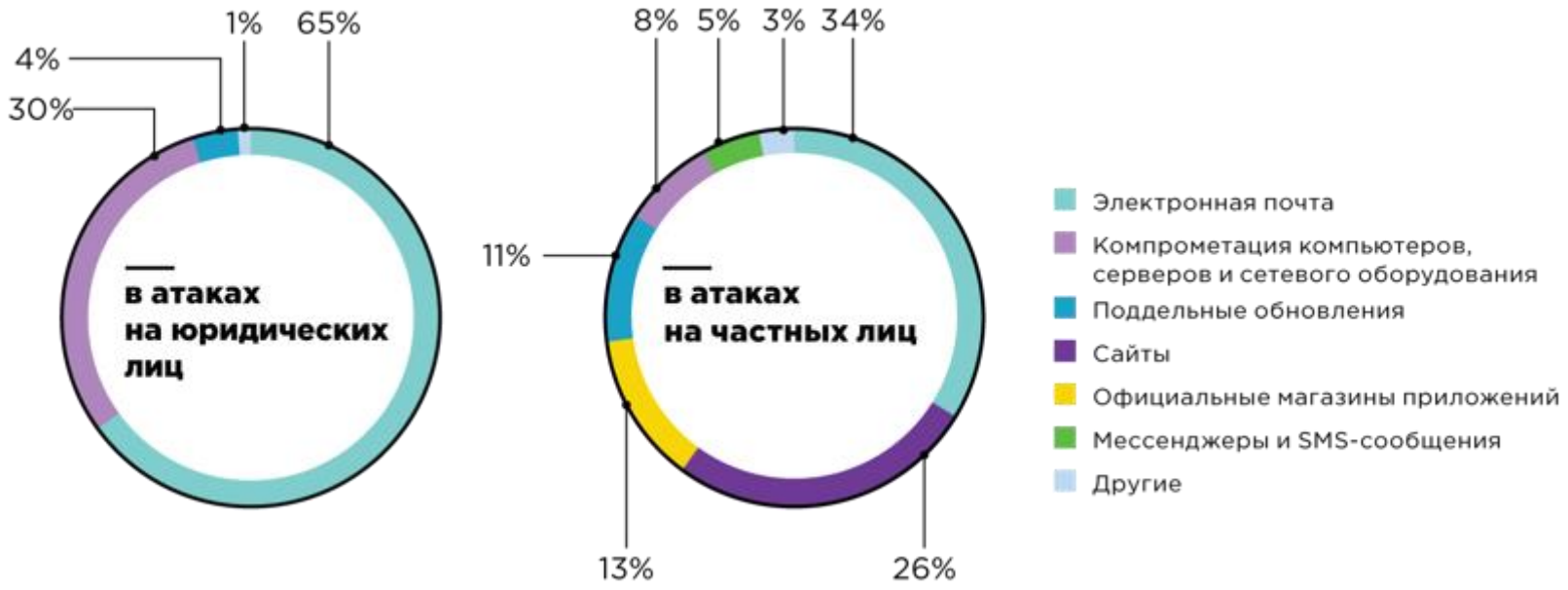


- Медицинские учреждения
- Госучреждения
- Промышленность
- Наука и образование
- IT-компании
- Торговля
- Другие
- Без привязки к отрасли

Исследование Positive Technologies
«Актуальные киберугрозы: IV квартал 2020 года»

Как вредоносы попадают в компании и на устройства пользователей

Способы распространения ВПО



Исследование Positive Technologies
«Актуальные киберугрозы: IV квартал 2020 года»

Что нужно знать о развитии ВПО: прогнозы

- Фишинг, подбор паролей на RDP-серверах и эксплуатация уязвимостей в веб-серверах будут самыми распространенными способами доставки ВПО
- Продолжится рост атак через цепочки поставок
- Спрос на доступ к взломанным компаниям будет расти
- К двойной схеме вымогательства (шифрованию файлов и шантажу публикацией украденной информации) станут прибегать все чаще
- Продолжится рост числа атак на промышленные объекты, АСУ ТП*

*Автоматизированная система управления технологическим процессом.

Что нужно знать о развитии ВПО: прогнозы

- Совершенствование операций ВПО в части закрепления в прошивках (BIOS/UEFI) и распространения внутри сети
- Появление новых техник, скрывающих присутствие ВПО и проверяющих среду запуска
- Может получить развитие использование нетрадиционных языков программирования и процессорных платформ, чтобы усложнить анализ и обнаружение, а также увеличить покрытие

Наиболее активные вредоносы

СЕМЕЙСТВО	ПРОИСХОЖДЕНИЕ	ОСОБЕННОСТЬ
NjRAT	Средний Восток	Исходный код доступен в сети
FormBook	Россия/СНГ	Инфостиллер по схеме Malware-as-a-Service
AgentTesla	Турция	Эксфильтрация данных через почтовый протокол
LokiBot	Россия/СНГ	Один из крупнейших ботнетов
NanoCore	США	Продается как легитимный инструмент для удаленного администрирования
Remcos	Россия/СНГ	Часто используется атакующими из средне-восточного региона

Наиболее активные вредоносы

СЕМЕЙСТВО	ПРОИСХОЖДЕНИЕ	ОСОБЕННОСТЬ
QuasarRAT	Н/д	Исходный код доступен в сети, используется азиатскими группировками, код сильно обфусцирован
Masslogger	Н/д	Код сильно обфусцирован, проверяет наличие антивирусов в системе
QBot	Н/д	Основные цели — компании в США, многомодульная архитектура для расширения возможностей
Minebridge	Россия/СНГ	Используется русскоязычной группировкой TA505, много-слойная упаковка исполняемого кода для усложнения анализа

Наиболее активные APT*-группировки

ГРУППА	ПРОИСХОЖДЕНИЕ	МОТИВАЦИЯ	ЧИСЛО АТАК В Q4** 2020
Gamaredon	Украина	Шпионаж	
APT31	Китай	Шпионаж	
APT32	Вьетнам	Шпионаж	
Lazarus	Северная Корея	Финансы + Шпионаж	2 атаки
LazyScripter	Н/д	Н/д	
Sandworm	Россия	Шпионаж	
Turla	Россия	Шпионаж	
RTM	Россия	Финансы	51 атака
CloudAtlas (PowerShower)	Н/д	Шпионаж	3 атаки
Winnti (Bisonal)	Китай	Финансы + Шпионаж	2 атаки
TA428 (RoyalRoad и NccTrojan)	Китай	Шпионаж	2 атаки

*Advanced persistent threat, то есть «целевая кибератака».
** Число атак группы, зафиксированное PT Expert Security Center. Данные представлены по тем группам, которые в настоящий момент исследуются PT Expert Security Center.

Как противостоять угрозе

- Эффективный цикл обновления и патчинга ПО
- Защита сетевого периметра
- Внимание к безопасности учетных записей, применение многофакторной аутентификации
- Использование решений, способных выявлять ВПО на всех стадиях атаки: песочниц, систем обнаружения вторжений, сбора и мониторинга событий информационной безопасности, автоматизации реагирования на инциденты

АЛЕКСЕЙ ДАНИЛИН,
руководитель направления
по развитию бизнеса,
Positive Technologies

Песочницы сегодня: рынок и пользователи

ptsecurity.com

История песочниц в России

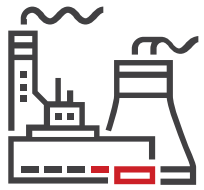
На российский рынок защиты от атак с применением ВПО
первые песочницы вышли более 8 лет назад

ЗАДАЧИ ВЕНДОРОВ ПЕСОЧНИЦ НА ТОТ МОМЕНТ:

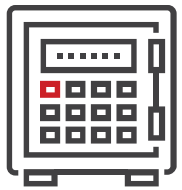
- создать эффективные техники сокрытия виртуальной среды от анализа ВПО,
- найти компромисс между производительностью и непрерывностью бизнес-процессов,
- обеспечить интеграцию с другими ИТ- и ИБ-системами.

В каких отраслях востребованы песочницы

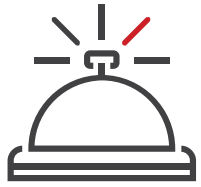
ГОССЕКТОР



ПРОМЫШЛЕННОСТЬ



ФИНАНСЫ



ЛОГИСТИКА И РИТЕЙЛ

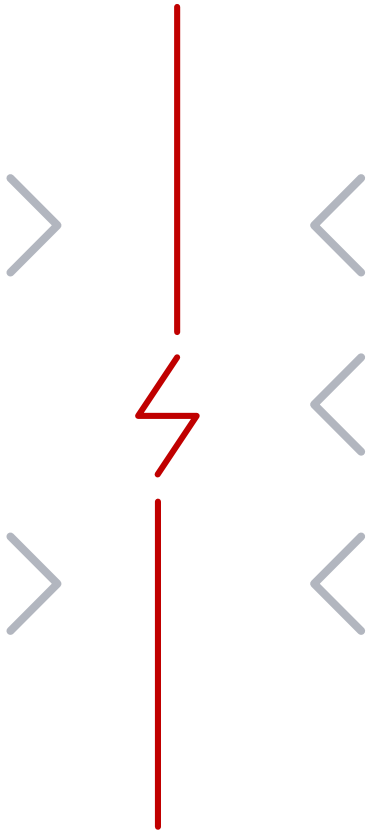
МЕДИЦИНСКИЕ УЧРЕЖДЕНИЯ

- Один из самых распространенных методов доставки ВПО — **фишинг** (65% в атаках на организации).
- Компрометация возможна в любой компании, где используется **электронная почта**.

Создатели ВПО и вендоры ИБ: кто впереди?

Создатели ВПО
развивают технологии обхода средств защиты

Антивирусы, шлюзы безопасности, IDS/IPS **злоумышленники могут обойти**



Песочницы способны выявлять неизвестные ранее угрозы — те, которые еще не «видели» классические средства защиты

Ожидания
от песочниц сегодня

САМЫЕ ПОПУЛЯРНЫЕ ЗАДАЧИ*, РЕШАЕМЫЕ С ПОМОЩЬЮ ПЕСОЧНИЦ:

- проверка файлов из сети интернет (64%),
- ручные проверки (57%),
- проверка электронной почты (54%).

ЗАПРОСЫ БИЗНЕСА К ПЕСОЧНИЦАМ:

- экспертиза из коробки,
- интеграция с другими системами,
- качество детектирования.

*По результатам опроса Positive Technologies среди представителей 100 компаний, уже использующих песочницы, из различных отраслей

Как изменятся песочницы в будущем

Постоянное усложнение угроз

Рост числа целевых атак

Реалистичная виртуальная среда

Персонализированная защита бизнеса

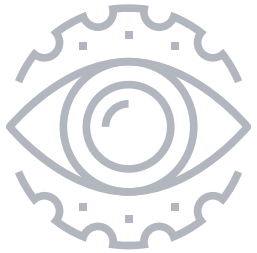
Deception-технологии

ДЕНИС КОРАБЛЕВ,
директор по продуктам,
Positive Technologies

Технологические тренды развития песочниц

ptsecurity.com

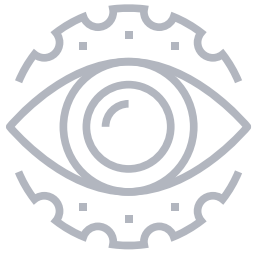
Расширение покрытия модели угроз



Анализ заголовков:
видны попытки фальсификации адресов отправителя, составление индикаторов злонамеренной рассылки (программа-почтовик, создавшая письмо, идентификаторы письма, адреса промежуточных узлов пересылки).

В 65% атак с использованием ВПО
злоумышленники используют социальную инженерию

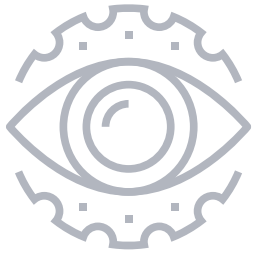
Производительность: «стеклянный потолок»



Массовая единовременная проверка больших наборов файлов по косвенным признакам: попыткам закрепиться в системе, подключиться к сети интернет и др.

Время проверки одного файла — 1–2 минуты в среднем

Реальные риски — персонализированность защиты



Кастомизация виртуальных сред: софт, процессы и файлы, свойственные реальной инфраструктуре.

80% от общего числа атак — целевые

Ксения Кириллова,
менеджер по продуктовому маркетингу
Positive Technologies

PT Sandbox 2.2: риск-ориентированный подход

ptsecurity.com

Риски целевых атак
с применением вредоносного ПО

- Остановка бизнес-процесса
- Остановка производственного процесса
- Необходимость платить вымогателю
- Утечка конфиденциальных данных, ноу-хау
- Риск разрыва деловых отношений и потеря репутации

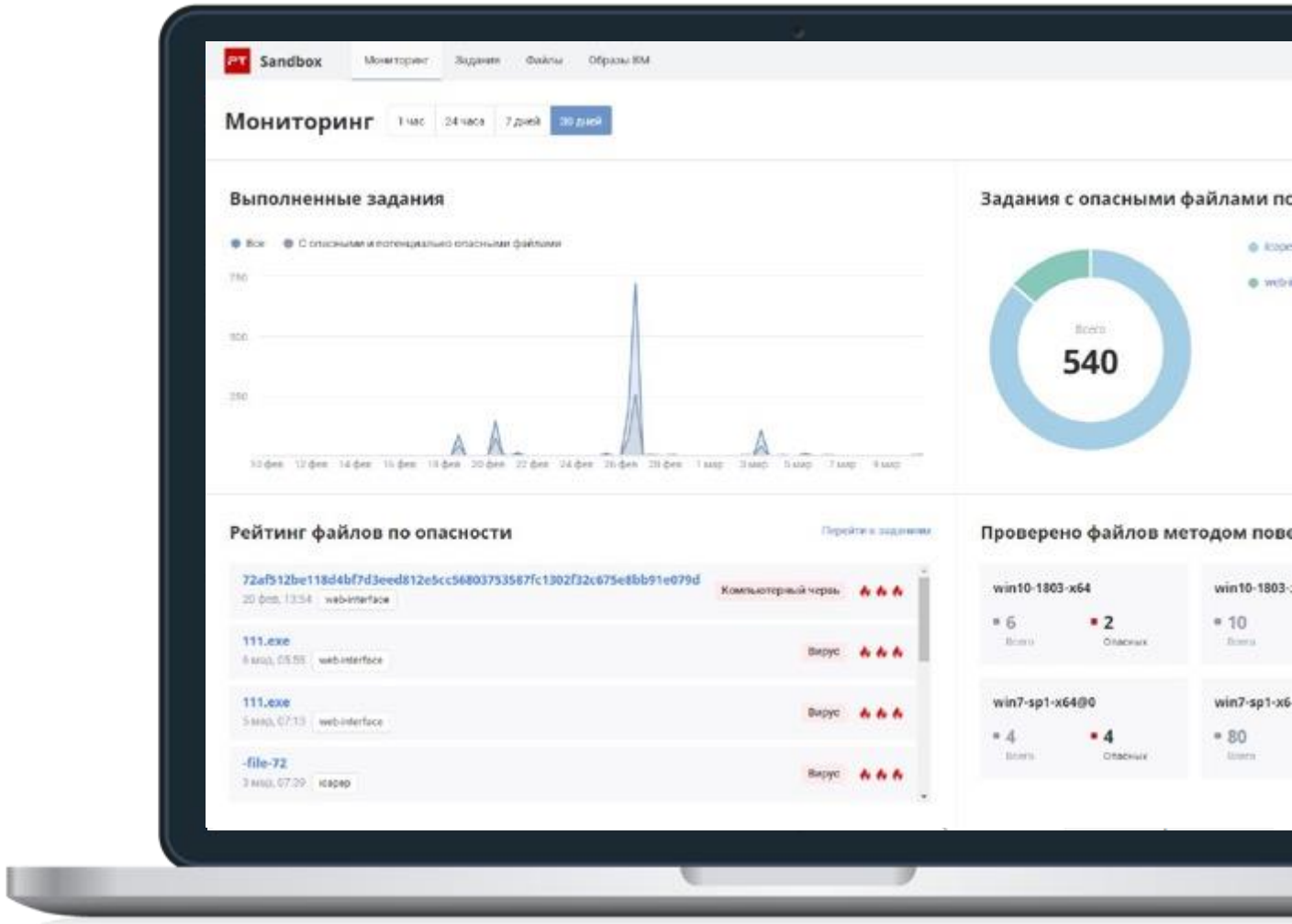
Как действуют атакующие

Применяют разные способы доставки ВПО	Нужно закрывать все основные источники поступления угроз
Обманывают базовые средства защиты	Нужны продвинутые технологии обнаружения
Обходят обычные песочницы	Нужны механизмы защиты от обхода песочниц и проверки окружения
Быстро развивают и меняют инструментарий	Нужно постоянно исследовать угрозы и улучшать защиту

Наше решение

PT Sandbox

Песочница
с возможностью
кастомизации
виртуальных сред



Покрытие основных источников угроз

Защищает
электронную почту

Контролирует
веб-трафик

Ищет угрозы
в корпоративных системах

Защищает
файловые хранилища

Обеспечивает возможность
ручных проверок

Продвинутые технологии обнаружения

Комплексный глубокий анализ файлов

Статический и динамический анализ с помощью правил PT Expert Security Center, дополнительная проверка антивирусами

Обнаружение угроз в сетевом трафике

Проверка генерируемого трафика, в том числе шифрованного, с помощью правил PT Expert Security Center

Выявление атак, которые не были обнаружены ранее

Автоматический ретроспективный анализ после обновлений баз знаний продукта

Уникальные знания для выявления угроз

Правила PT Expert Security Center создаются по итогам реагирования, расследований инцидентов в крупных компаниях, а также исследований деятельности хакерских группировок

Свежие правила еженедельно попадают в базы знаний продукта

Возможности интеграции

MaxPatrol SIEM

Система выявления инцидентов ИБ

PT Application Firewall

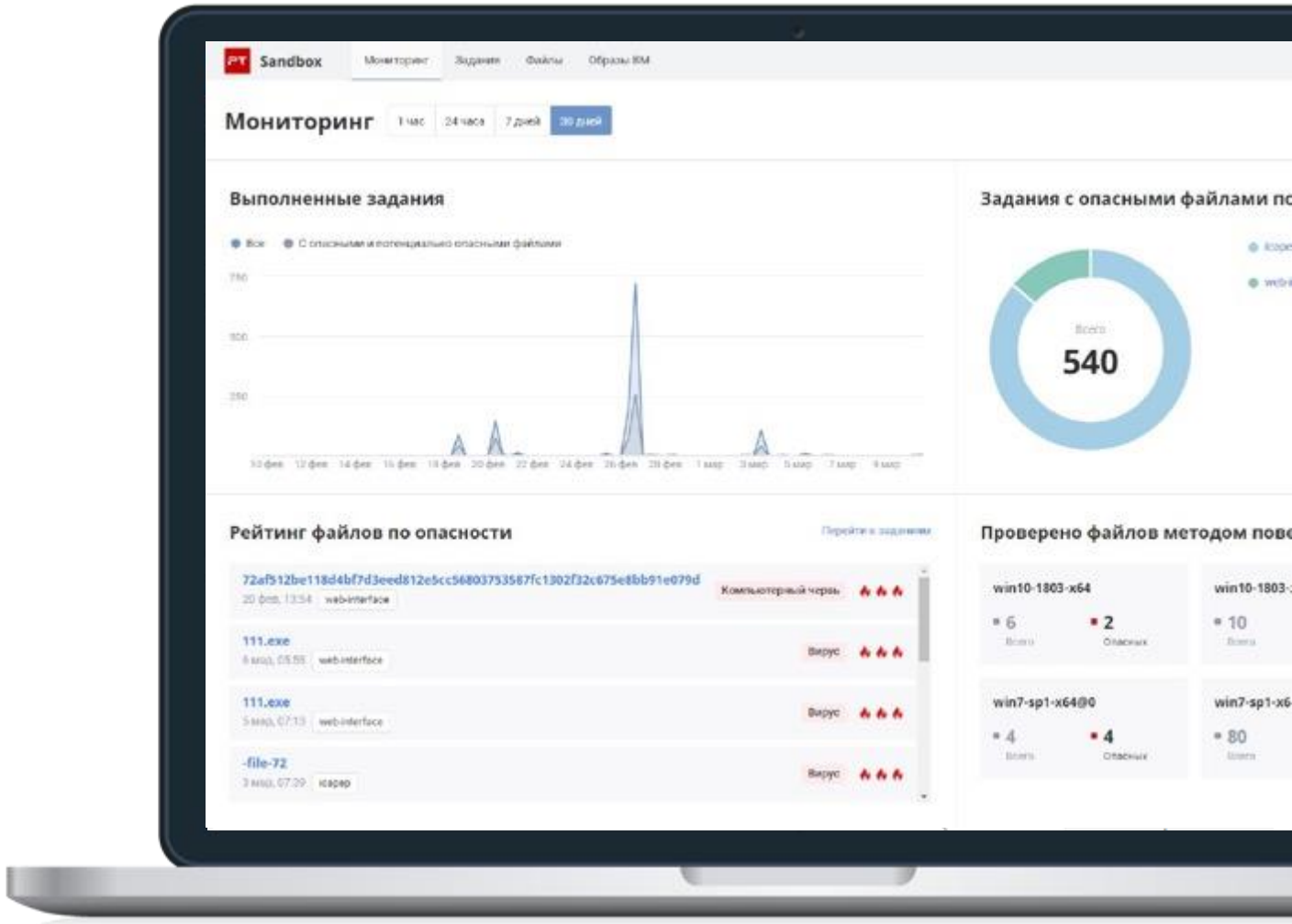
Межсетевой экран уровня веб-приложений

PT Network Attack Discovery

Система глубокого анализа сетевого трафика (**NTA**)

PT Sandbox 2.2:
коротко о главном

- Точная имитация реальной инфраструктуры «из коробки»
- «Приманки» для хакеров
- Персонализированная защита компании



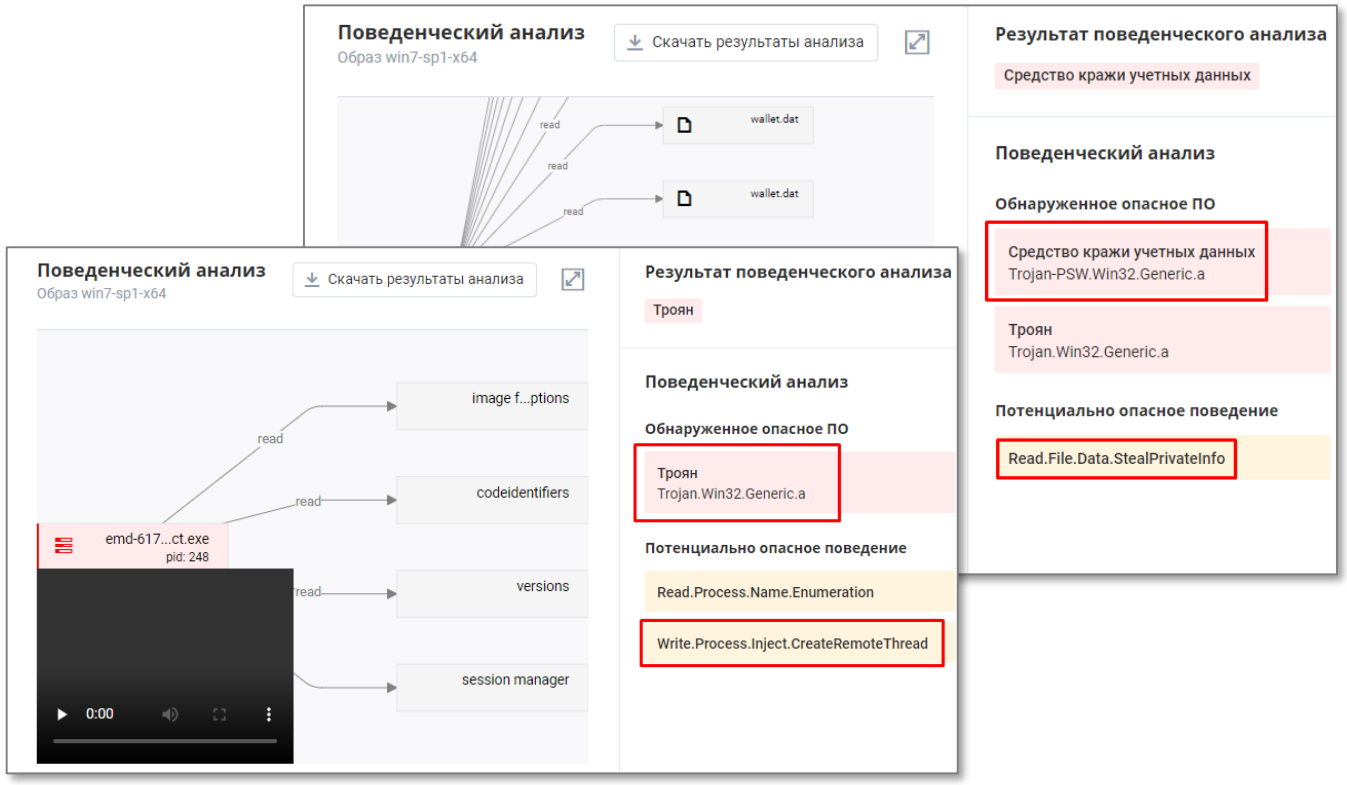
Имитирует
реальную инфраструктуру

В ходе атаки злоумышленники часто используют продвинутые вредоносные программы, которые проверяют, не виртуальная ли вокруг них среда.

PT Sandbox реалистично имитирует рабочую станцию сотрудника, не позволяет вредоносному ПО распознать, что оно в песочнице, и покрывает больше уязвимостей:

- «Из коробки» в базовых образах доступен офисный пакет, PDF-ридер, видеоплеер, оптимизатор системы, платформа для видеосвязи, эмуляторы промежуточного кода.

Провоцирует
атакующих выдать себя



PT Sandbox детектирует похищение данных-приманок в файловой системе, а также выявляет попытки внедриться в процесс-приманку

PT Sandbox оснащена приманками, которые провоцируют атакующих совершить активные действия и выдать себя.

Файлы и данные-приманки:

- в файловой системе – фейковые учетные записи, файлы конфигурации и др.;
- в буфере обмена – фейковые пароли, номера карт, номера телефонов, криптокошельки.

Процессы-приманки:

- имитация работы банковских приложений;
- имитация работы софта разработчиков;
- пользовательская активность.

Позволяет **заточить защиту под риски компании**

Настройка виртуальных сред в соответствии с реальными рабочими станциями

PT Sandbox поддерживает **гибкую кастомизацию виртуальных сред** и позволяет загрузить в них тот специфический софт и его версии, которым пользуются сотрудники и в который будут целиться злоумышленники.

Уникальные приманки по запросу

PT Sandbox позволяет **добавить дополнительные приманки**, имитирующие ценные данные из наиболее важных для бизнеса систем.