



POSITIVE
TECHNOLOGIES

PT MultiScanner

Многоуровневая защита
от вирусных угроз

ptsecurity.com

О компании

Positive Technologies



19 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

РТ



Задача

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

Что сделано

Проверили защищенность веб-портала, внедрились RT 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



Ежегодный международный форум по практической безопасности, который собирает более 6000 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

Наши исследования

**Выпускаем более
20 исследований в год**

Ежеквартальные отчеты об актуальных киберугрозах и трендах, прогнозы, расследования активности хакерских группировок, отраслевые исследования

ptsecurity.com/ru-ru/research/analytics

PT





Вредоносное ПО: самый популярный метод атак

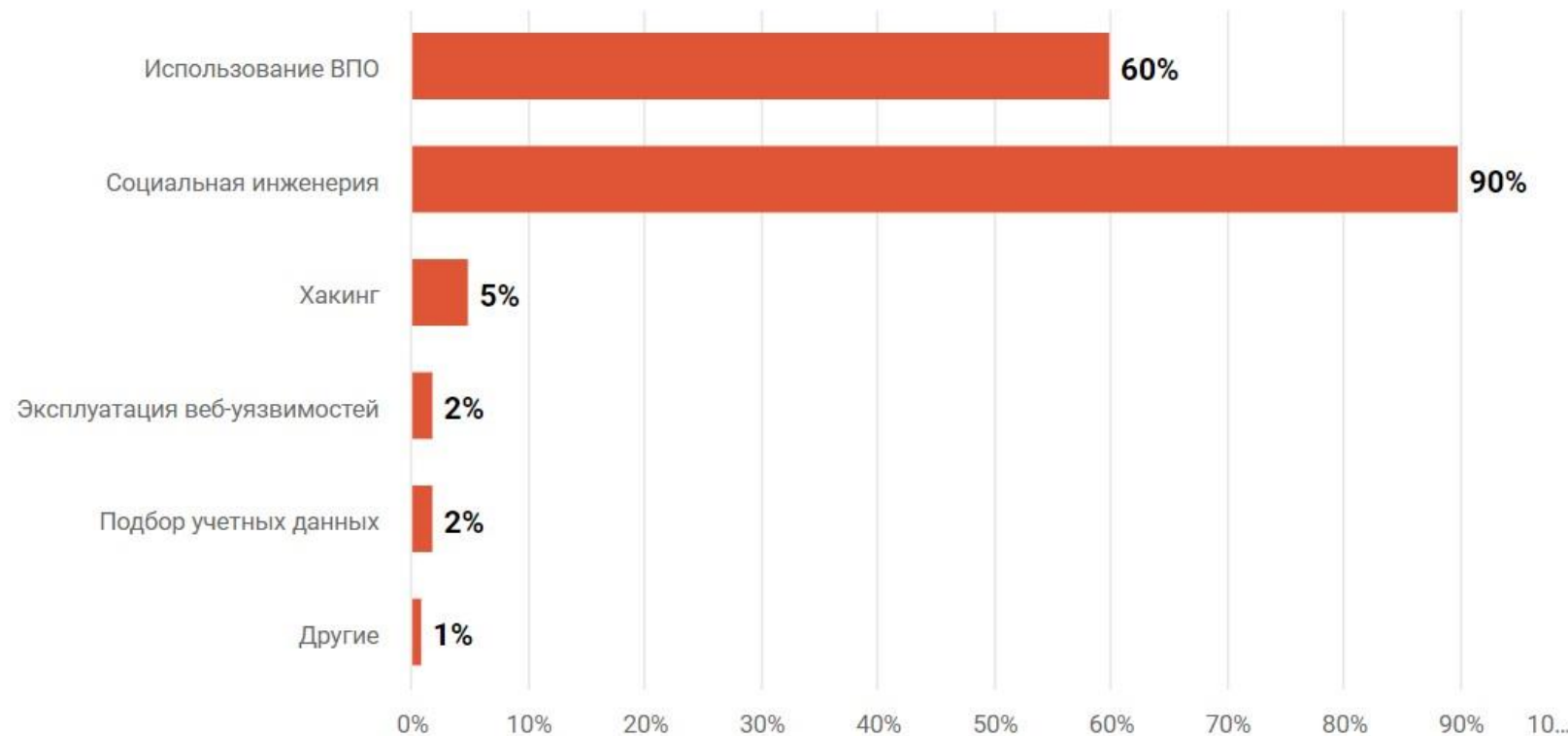
ptsecurity.com

Вредоносное ПО сегодня

РТ

Применение вредоносного ПО:
самый популярный метод атак на компании уже много лет

450 000 образцов вредоносных программ
появляется в мире ежедневно



Методы атак на компании

* Актуальные киберугрозы: II квартал 2021 года, Positive Technologies

* Данные AV-TEST, 2021

Почему от него все еще сложно защититься

РТ

Экспертизы одного вендора не хватает

Антивирусные вендоры с разной скоростью добавляют в свои базы знаний новые угрозы, которые появляются ежедневно

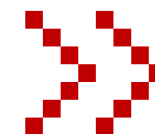
Нет единого решения для покрытия всех источников угроз

Для разных источников поступления файлов в инфраструктуру (почта, веб, файлообменники) приходится использовать «зоопарк» разных продуктов – антивирусы, шлюзы и т. д. – не взаимосвязанных между собой

Угрозу сложно локализовать в инфраструктуре

Нужно обработать данные из множества систем ИБ, чтобы понять, откуда пришла угроза, как она распространялась по сети и на каком этапе развития находится атака – и результат не гарантирован

Что
делать?





PT MultiScanner

Многоуровневая защита от вирусных атак

ptsecurity.com

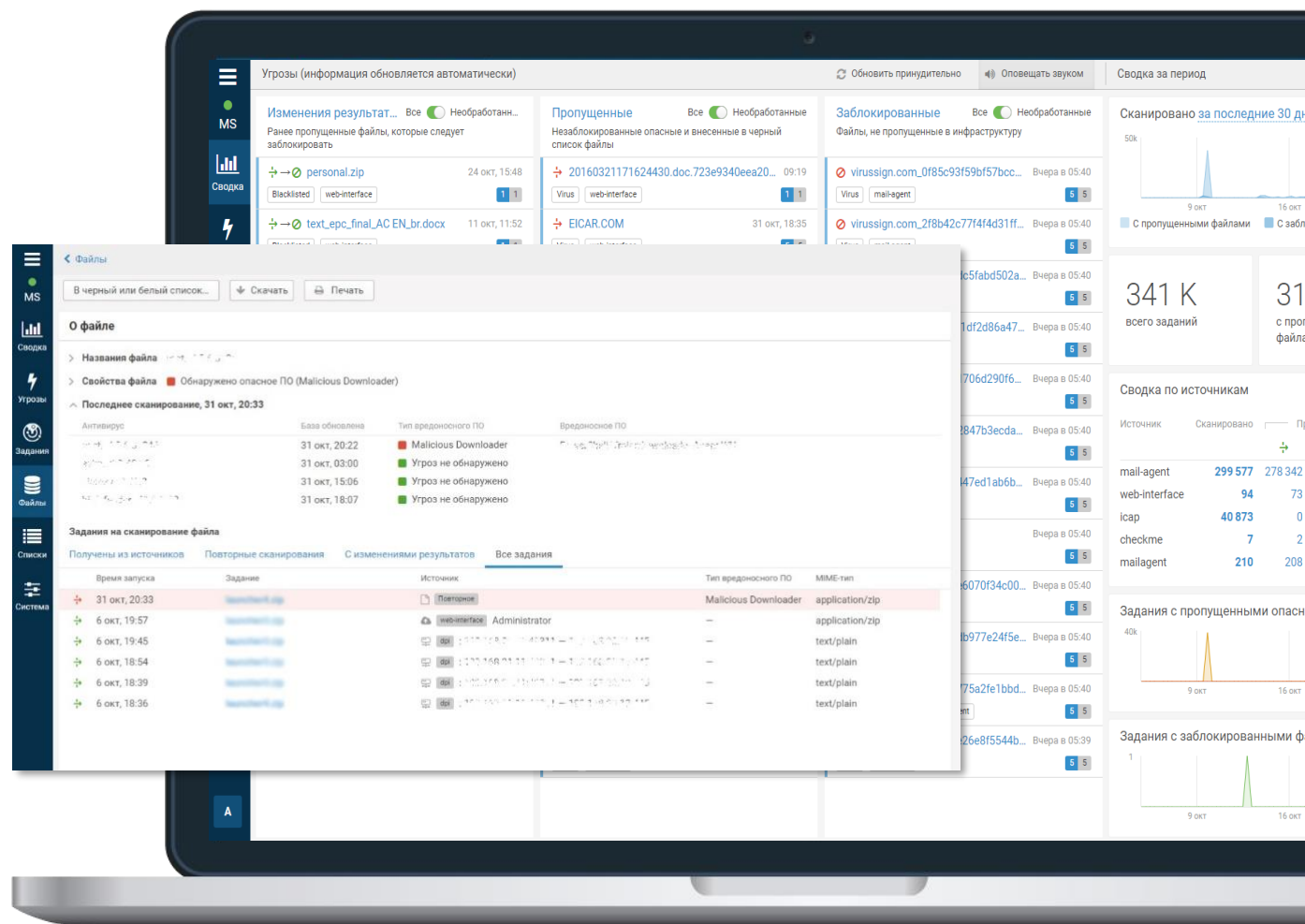
Наше решение

РТ

РТ MultiScanner

Система многоуровневой защиты от вредоносных программ

- Защищает от атак с применением вредоносного ПО: шифровальщиков, троянов, вирусов
- Универсальное решение для централизованной защиты от вредоносных программ



Возможности PT MultiScanner



Надежно защищает от массовых угроз и хакерских атак

Каждый файл проходит проверку несколькими антивирусами, проверку по репутационным спискам, а также статический анализ с помощью правил PT Expert Security Center. Это позволяет защититься как от массовых угроз, так и от атак хакерских группировок



Позволяет точно локализовать угрозу

Предоставляет точную информацию обо всех пораженных узлах сети и позволяет локализовать угрозу: найти ее источник, отследить всех участников и этапы распространения угрозы, а следовательно – оперативно принять необходимые меры



Выявляет атаки, не обнаруженные в прошлом

Благодаря ретроспективному анализу PT MultiScanner находит вредоносное ПО, которое не было обнаружено ранее. Автоматическая перепроверка файлов запускается после обновления баз знаний продукта

Возможности PT MultiScanner



Следит за всеми потоками данных

Анализирует файлы, которые попадают в корпоративную сеть в сетевом и почтовом трафике, загружаются в веб-приложения и файловые хранилища компании



Дополнительно



В продукте доступны режимы мониторинга и блокировки: отслеживайте угрозы или блокируйте их сразу



Возможность работы on premise: ваши файлы и конфиденциальные данные не покидают пределы компании



Высокая производительность: продукт способен анализировать десятки тысяч файлов в час и поддерживает масштабирование



Легкое и быстрое встраивание в существующую инфраструктуру благодаря поддержке SPAN, MTA, ICAP, REST API



Быстрый старт: весь процесс установки продукта занимает не более часа



Единая экосистема Positive Technologies: продукт бесшовно интегрируется со всеми решениями компании



Сценарии использования

ptsecurity.com

Сценарии использования



Защита почты

Интеграция с почтовыми серверами позволяет выявлять и блокировать вредоносное ПО в почтовых вложениях



Анализ веб-трафика

Интеграция со средствами контроля и анализа трафика позволяет выявлять угрозы в веб-трафике сотрудников



Ручная проверка

Продукт позволяет загрузить объект на проверку через UI или настроить специализированный электронный адрес для отправки объектов на проверку по почте



Защита хранилищ и общих папок

Продукт позволяет проверять файлы на наличие угроз перед загрузкой на корпоративный сетевой ресурс – напрямую или через папку-шлюз



Интеграция **с продуктами Positive Technologies**

ptsecurity.com

Возможности интеграции



MaxPatrol SIEM

Система выявления
инцидентов ИБ

Позволяет построить более полную картину состояния ИТ-инфраструктуры и точнее выявлять инциденты

PT Application Firewall

Межсетевой экран уровня
веб-приложений

Позволяет защитить веб-приложения компании от атак с помощью вредоносного программного обеспечения

PT Network Attack Discovery

Система глубокого анализа
сетевого трафика (NTA)

Позволяет выявлять угрозы, связанные с вредоносными программами, во внутреннем сетевом трафике



Истории успеха

ptsecurity.com

История успеха: ВГТРК



Дмитрий Сафронов,
начальник отдела защиты
информации ВГТРК

«PT MultiScanner — очень гибкая система. Она легко адаптируется к любым нашим нуждам, а поддержка разных интерфейсов взаимодействия заметно упрощает интеграцию с существующими системами. Благодаря PT MultiScanner мы решили проблему эффективной антивирусной защиты»

Подробнее на сайте ptsecurity.com

История успеха: Ингосстрах

PT



Андрей Поломошнов,
заведующий сектором эксплуатации средств
защиты информации СПАО «Ингосстрах»

«Одна из задач, стоящих перед нами, — обеспечить оперативное обнаружение и своевременное блокирование вирусов. Для этого была выбрана система выявления вредоносного контента PT MultiScanner компании Positive Technologies. Интеграция системы с нашим онлайн-сервисом и другими системами защиты позволила повысить безопасность наших корпоративных ресурсов».

Подробнее на сайте ptsecurity.com

История успеха: Абсолют Банк

PT

Руслан Ложкин,
руководитель службы
информационной безопасности
Абсолют Банка

«Внедрение PT MultiScanner было логичным этапом в процессе выстраивания комплексной защиты банка от киберугроз. Тесная интеграция с межсетевым экраном PT Application Firewall и подтвержденная эффективность продукта стали ключевыми факторами выбора PT MultiScanner, который позволил нам решить задачу по защите банковских веб-ресурсов от вредоносного ПО».

Подробнее на сайте ptsecurity.com



Как начать работу с PT MultiScanner

ptsecurity.com

Как пропилотировать PT MultiScanner



Заявка

Свяжитесь с вашим менеджером в Positive Technologies



Подписание NDA, заполнение анкеты



Разворачивание PT MultiScanner: установка, настройка, подключение источников



Пилотирование, мониторинг специалистами Positive Technologies



Отчет об обнаруженных угрозах

≈ 4 недели