Positive Technologies
MultiScanner

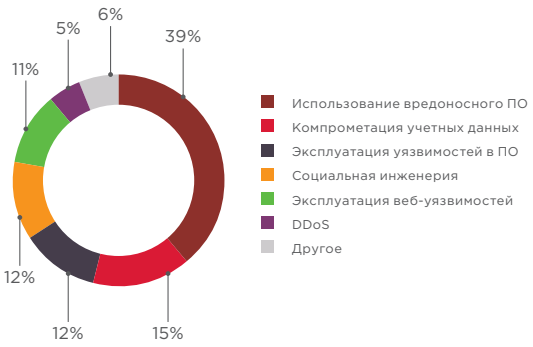
ОПИСАНИЕ ПРОДУКТА

POSITIVE TECHNOLOGIES

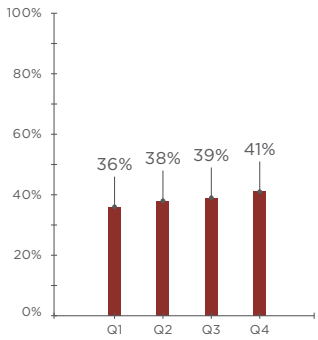
Ущерб от атак с использованием вредоносного ПО в 2017 году составил более 1,5 млрд долл. США[1].

ВРЕДОНОСНОЕ ПО: ОСНОВНЫЕ УГРОЗЫ И ВЫЗОВЫ

Атаки с использованием вредоносного ПО уверенно лидируют среди киберугроз: по итогам 2017 года их доля составила 39% всех способов атак[1].



Методы атак в 2017 году



Доля атак с использованием ВПО в 2017 году в разбивке по кварталам

Всплеск популярности переживают массовые деструктивные атаки — злоумышленники заинтересованы в масштабном охвате и причинении крупного ущерба, как в случае с нашумевшими шифровальщиками NotPetya и WannaCry. Часто логика работы подобного вредоносного ПО даже не подразумевает возможность расшифровки данных, а методы распространения так эффективны, что позволяют заражению в считанные часы распространиться по всему миру.

Также активно развивается услуга ransomware as a service, позволяющая разным лицам многократно использовать одни и те же вирусы-вымогатели. Это явление резко снизило порог входа в киберпреступный бизнес — теперь купить вредоносное ПО через интернет может любой желающий, не обладающий специальными навыками.

В чем же причины такой распространенности и разрушительности вирусных атак? Опираясь на свой многолетний опыт в расследовании инцидентов ИБ, мы выделили ряд основных факторов низкой эффективности борьбы с вредоносным ПО.

Запаздывающие обновления баз знаний антивирусных вендоров. Ежедневно в мире появляется около 250 000 образцов вредоносного ПО. В то же время промежуток между появлением новой угрозы и ее детектированием антивирусами может составлять от нескольких дней до нескольких недель, в течение которых заражение может стать катастрофическим. В этом причина низкой эффективности популярного моновендорного подхода к защите от вредоносного ПО: нельзя быть уверенным, что выбранный антивирусный продукт обнаружит угрозу быстрее, чем другие.

Неполное обеспечение корпоративных рабочих станций антивирусами. Результаты тестов на проникновение и расследований инцидентов ИБ, проведенных нашими экспертами в 2017 году, показали, что покрытие антивирусными средствами в крупных компаниях составляет в среднем 85%. Серьезное влияние на этот показатель оказывают масштаб и географическая распределенность организации: часто меры ИБ соблюдаются только в головном отделении, а в филиалах для обеспечения антивирусами всех машин не хватает бюджета или технических ресурсов. Кроме того, немногие компании проводят регулярные проверки наличия на рабочих станциях необходимого ПО — часто в организациях попросту нет систем, позволяющих автоматически проверять, установлен ли на конкретном компьютере антивирус.

1 Обзор «Актуальные киберугрозы — 2017: тренды и прогнозы», Positive Technologies.

Показательно, что неполнота антивирусного покрытия является одной из ключевых причин разрушительности массовых атак с помощью вирусов-шифровальщиков в 2017 году.

По оценкам экспертов Positive Technologies, в 2017 году каждая десятая организация столкнулась с вирусами-шифровальщиками[2].

Массовый перевод услуг в онлайн. Финансовые, страховые, телекоммуникационные компании и государственные учреждения все чаще предлагают клиентам оформлять документы и заказывать услуги через официальные сайты или по электронной почте. Такие сервисы делают инфраструктуру поставщика услуг уязвимой для атак: злоумышленники могут использовать формы приема документов для загрузки вредоносного ПО.

Рост числа целенаправленных атак с помощью вредоносного ПО, созданного для обхода конкретных антивирусов. Организация может пострадать от злоумышленников, даже если все ее рабочие станции обеспечены хорошим антивирусным решением. Например, госучреждения обязаны размещать информацию о закупках в открытом доступе, поэтому узнать о средствах защиты, которые они используют, несложно. Эти сведения злоумышленники применяют для разработки специализированного вредоносного ПО, которое гарантированно не детектируется конкретными антивирусными решениями и может оставаться незамеченным довольно долго. Угроза серьезна как никогда: по нашему опыту, в 2017 году каждая вторая крупная компания стала жертвой целенаправленной атаки[2].

Отсутствие данных о перемещении вредоносных объектов по сети. Для корректного реагирования на угрозу или эффективного расследования инцидента нужно понимать, какими путями вредоносное ПО распространялось в инфраструктуре. Частично эту информацию можно извлечь из IPS, IDS или DLP-систем, которые используются в большинстве госучреждений, банков и других крупных организаций. Однако эти системы — непрофильные средства для решения подобных задач, их эффективность для отслеживания вредоносного ПО зависит от грамотной настройки, а трудозатраты на использование их подобным образом достаточно высоки.

Бесконтрольное использование облачных сервисов кросс-проверок или необоснованный отказ от них. Облачные сервисы кросс-проверок удобны и позволяют бесплатно сканировать подозрительные файлы десятками антивирусных движков, но их бесконтрольное применение может привести к опасным последствиям. Необученные сотрудники часто загружают на внешние ресурсы конфиденциальные данные, которые могут попасть в руки злоумышленников и помочь им в подготовке атаки (в том числе с помощью вредоносного ПО).

Однако у полного отказа от подобных сервисов есть и серьезный минус: если в компании нет антивирусной защиты или используемый антивирус недостаточно эффективен, вредоносное ПО может беспрепятственно распространиться по всей инфраструктуре.

Сложность эффективного управления разрозненными защитными средствами. При наличии нескольких решений для защиты от вредоносного ПО, покрывающих разные каналы распространения данных, эффективно управлять ими часто бывает сложно. Ручная обработка множества разнородных отчетов о сканировании требует существенных трудозатрат специалистов по ИБ и не позволяет своевременно и корректно реагировать на возникающие угрозы.

Низкая осведомленность сотрудников в вопросах ИБ. Согласно нашим исследованиям[3], всего 25% компаний проводят для сотрудников тренинги по ИБ с последующей проверкой эффективности, хотя именно персонал — слабое место в защите любой организации. Всего один переход по вредоносной ссылке из

2 Обзор «Кибербезопасность (2017–2018): цифры, факты, прогнозы», Positive Technologies.
3 Исследование «Сколько стоит безопасность», Positive Technologies.

«В условиях, когда страхователи самостоятельно могут загружать документы на онлайн-сервис, риск того, что в нашу систему попадет зараженный файл, многократно вырос. Поэтому одна из задач, стоящих перед нами, — обеспечить оперативное обнаружение и своевременное блокирование вирусов. Для этого была выбрана система защиты от вредоносного контента PT MultiScanner компании Positive Technologies».

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

письма или загрузка зараженного файла могут привести к компрометации всех корпоративных ресурсов.

Успешно устранить эти негативные факторы позволяет система PT MultiScanner — решение для централизованной защиты от вредоносного ПО, обеспечивающее полное покрытие каналов распространения данных в инфраструктуре.

PT MULTISCANNER: КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

PT MultiScanner — многоуровневая система защиты от вредоносного контента, позволяющая выявлять и блокировать угрозы в различных потоках данных в инфраструктуре. В основе решения лежит уникальное сочетание дополняющих друг друга антивирусных движков, статического анализа и репутационных списков Positive Technologies.

Преимущества PT MultiScanner

Объединение ИБ-экспертизы для эффективного выявления угроз

+ PT MultiScanner использует для проверки объектов набор дополняющих друг друга антивирусных движков, обеспечивающий максимально высокий уровень детектирования вредоносного ПО.
+ Продукт также производит статический анализ объектов и проверку по репутационным спискам, которые поставляет экспертный центр PT ESC, регулярно проводящий расследования реальных инцидентов ИБ в крупных компаниях.

Защита всех возможных каналов распространения данных

+ PT MultiScanner позволяет выявлять и блокировать угрозы в различных каналах распространения данных: на веб-порталах, в почте, файловых хранилищах, сетевом и пользовательском веб-трафике.

Ретроспективный анализ

+ Благодаря ретроспективному анализу PT MultiScanner может выявлять новейшие угрозы и скрытое присутствие вредоносного ПО. Повторное сканирование уже проверенных объектов запускается автоматически после обновления баз знаний или при наличии свободных ресурсов, не влияя на производительность сканирования текущих потоков данных.

Экспертный инструмент для расследования инцидентов

+ Эксперты SOC и специалисты по ИБ могут использовать PT MultiScanner как эффективный инструмент для расследования инцидентов: система позволяет обнаружить точки входа вредоносного ПО в инфраструктуру, отследить участников и все этапы распространения угрозы.

Простота и удобство

+ Централизованный мониторинг вредоносной активности во всех потоках данных позволяет легко отслеживать и локализовать угрозу в инфраструктуре организации.
+ Объединение однотипных элементов атаки из разных потоков данных в единую угрозу помогает специалистам по ИБ быстрее и точнее реагировать на массовые заражения.
+ Система имеет интуитивно понятный интерфейс, вся необходимая специалисту по ИБ информация визуализируется на дашбордах.
+ Развертывание PT MultiScanner занимает менее часа. Источники объектов для сканирования (почтовые серверы, прокси-серверы, файловые хранилища, сетевые сенсоры) добавляются в несколько кликов.

Дополнительные преимущества

- PT MultiScanner поддерживает множество стандартных интерфейсов взаимодействия (SPAN, MTA, BCC, ICAP, REST API).
- Масштабирование системы производится путем простого наращивания компонентов.
- Все файлы сканируются внутри системы и размещаются в локальном хранилище, не покидая периметр компании (on-premise решение).
- PT MultiScanner входит в единую экосистему с другими продуктами Positive Technologies.

ВНЕДРЕНИЕ PT MULTISCANNER: ЦЕЛИ И ЗАДАЧИ

Цели внедрения

- Защита от вредоносного ПО на всех потоках данных в инфраструктуре компании.
- Повышение эффективности расследования инцидентов ИБ, связанных с вредоносным ПО.
- Общее повышение эффективности мер ИБ в компании, повышение уровня защищенности.
- Повышение осведомленности пользователей в вопросах ИБ.

Решаемые задачи

- Мониторинг вредоносной активности на сетевом уровне.
- Проверка объектов с помощью множества антивирусных решений, статического анализа и репутационных списков.
- Уведомление пользователей и специалистов по ИБ об обнаруженных угрозах.
- Блокировка обнаруженного вредоносного контента.
- Ведение базы знаний по загруженным объектам, их метаданным и вердиктам, истории перемещений внутри сети.
- Ретроспективный анализ, уведомление об обнаружении вредоносного ПО в ранее загруженных объектах.
- Анализ результатов проверок, формирование статистики и отчетов.

Возможности интеграции

Система поддерживает основные стандартные интерфейсы взаимодействия: SPAN, MTA, BCC, ICAP, REST API.

SPAN

PT MultiScanner имеет встроенные возможности для интеграции с сетевыми устройствами, поддерживающими технологию зеркалирования трафика с заданного порта (SPAN), и может анализировать объекты, передаваемые по протоколам HTTP, SMTP, POP3, IMAP, FTP, SMB.

MTA

PT MultiScanner позволяет выявлять и блокировать вредоносные объекты в почтовом трафике. Для этого на почтовом сервере компании устанавливается специальный легковесный плагин MTA (mail transfer agent), который пересылает электронные письма вместе с вложениями на проверку в PT MultiScanner. После проверки система возвращает результат и итоговое решение — пропустить письмо или блокировать его.

BCC

PT MultiScanner может проверять электронные письма и вложения путем интеграции с почтовым сервером компании через BCC. В этом случае почтовый сервер отправляет копию входящего письма на проверку в PT MultiScanner и параллельно

«Мы осознаем, насколько высока вероятность заражения вредоносным ПО в такой крупной компании, как ВГТРК. Для эффективного противостояния этой угрозе нам потребовалось одновременно надежное и максимально гибкое решение, способное легко адаптироваться под наши нужды. Именно таким решением стал PT MultiScanner — продукт, который объединил в себе глубокую экспертизу Positive Technologies и многолетний опыт AV-вендоров.

Благодаря PT MultiScanner мы решили проблему эффективной антивирусной защиты».

Дмитрий Сафронов,
начальник отдела защиты информации ВГТРК

доставляет исходное письмо получателю. Этот вариант интеграции исключает блокировку письма, в отличие от интеграции посредством MTA.

ICAP

PT MultiScanner может осуществлять проверку всех файлов, проходящих через прокси-серверы, межсетевые экраны уровня веб-приложений, системы обнаружения и предотвращения вторжений (IDS, IPS) и любые другие средства, поддерживающие ICAP.

REST API

PT MultiScanner поддерживает интеграцию с сетевыми устройствами, средствами защиты или произвольными внутренними ресурсами, используемыми в компании, посредством открытого HTTP REST API.

Возможности масштабирования

Архитектура PT MultiScanner позволяет легко производить как вертикальное, так и горизонтальное масштабирование. В последнем случае система может быть развернута в кластер, причем в режимах как active—passive, так и active—active.

КАК ЭТО РАБОТАЕТ:
ПОДСИСТЕМЫ PT MULTISCANNER И ИХ НАЗНАЧЕНИЕ

Подсистема сканирования

Подсистема сканирования производит проверку объектов, поступающих из различных источников.

Источники объектов

- Почтовые серверы.
- Прокси-серверы.
- Файловые хранилища, доступные по протоколам NFS, FTP, SMB.
- Зеркалируемый сетевой трафик.
- Сервисы ручной проверки объектов (в веб-интерфейсе и электронной почте).
- Другие источники (через API-запросы).

Проверка файла происходит с использованием нескольких антивирусных решений, каждое из которых возвращает свой вердикт. На основании этих вердиктов и данных из базы знаний Positive Technologies вычисляется общий вердикт.

После завершения проверки объект, его метаданные и данные о сканировании передаются в подсистемы управления и хранения. При обнаружении угрозы сведения также передаются в подсистему управления угрозами.

Подсистема хранения

Подсистема хранения обеспечивает хранение файлов и их метаданных. Это необходимо для повторной проверки объектов при обновлении сигнатурных баз антивирусных решений или при обновлении репутационных списков.

Все объекты размещаются в локальном хранилище с применением обратимого шифрования. Подсистема обеспечивает возможность очистки хранилища в соответствии с параметрами ротации данных.

Данные, собираемые подсистемой хранения

- Дата и время сканирования.
- Метаданные проверенного объекта (размер и имя, MIME-тип).
- Значение хеш-функций проверенного объекта.
- Информация об источнике объекта (тип, адрес источника, протокол, письма и их структура, ICAP-запрос, параметры API-запроса, сетевой узел, заголовок User-Agent/Referer и др.).
- Информация об антивирусах, которые производили проверку (имя, версия ядра, версия антивирусной базы, результат сканирования).

Подсистема хранения позволяет выполнять с отсканированными объектами следующие действия:

- искать объекты по названию, источнику или типу вредоносного ПО;
- фильтровать результаты сканирования по любому из атрибутов объекта или их комбинации;
- скачивать объекты из хранилища;
- добавлять к объектам комментарии и метки;
- просматривать общую информацию об объектах (хеш-суммы, размер, MIME-тип, источник и дату загрузки);
- добавлять объекты в черный или белый списки;
- просматривать полную историю сканирований и статистику ретроспективного анализа.

Подсистема ретроспективного анализа

Подсистема ретроспективного анализа осуществляет повторную проверку уже отсканированных объектов после обновления антивирусных сигнатур и (или) репутационных списков. Если по итогам ретроспективного анализа общий вердикт по объекту изменяется, система создает угрозу и отправляет уведомление ответственным сотрудникам служб ИБ и ИТ.

Подсистема управления угрозами

Подсистема управления угрозами осуществляет агрегацию обнаруженных угроз и позволяет управлять их жизненным циклом. С ее помощью реализуется закрытие и повторное открытие единичных угроз и групп угроз, обеспечивается навигация по угрозам и их фильтрация по различным атрибутам, связанным как с самой угрозой, так и с относящимися к ней объектами.

Подсистема мониторинга

Подсистема мониторинга следит за состоянием всех подсистем, информирует пользователя о текущей работоспособности системы через веб-интерфейс и осуществляет перезапуск проблемной подсистемы при возникновении сбоев. Также она проверяет обновления на портале Positive Technologies и, при их наличии, запускает процедуру обновления.

Подсистема управления

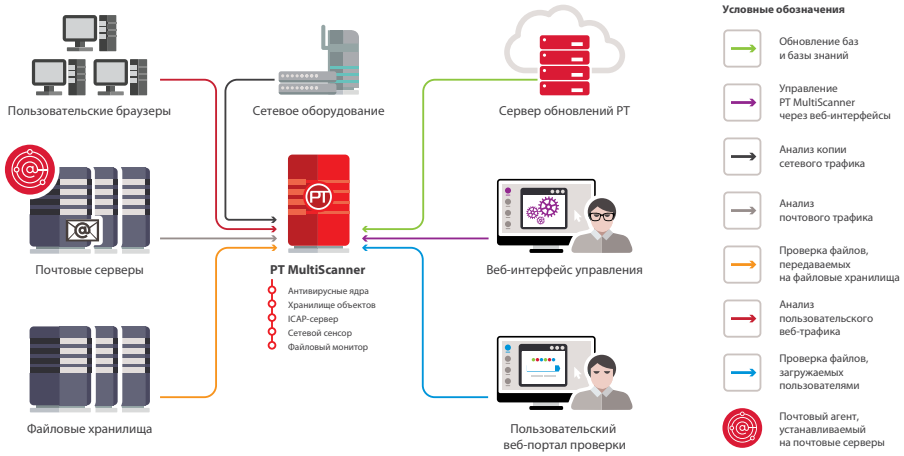
Подсистема управления осуществляет управление доступом пользователей к системе — производит идентификацию и аутентификацию по уникальному идентификатору и паролю, управляет назначением ролей.

Подсистема управления позволяет добавлять, изменять и удалять источники объектов для сканирования, просматривать и управлять угрозами, объектами, репутационными списками, настраивать параметры системы.

ДОСТУПНЫЕ РЕЖИМЫ РАБОТЫ

Режим работы	Назначение	Источники объектов
Ручная загрузка файлов	Средство проверки подозрительных объектов, обнаруженных пользователями	+ Пользовательский веб-портал + Выделенный почтовый ящик
Выявление вредоносного ПО в трафике	Выявление вредоносного ПО и оповещение службы ИБ об обнаруженных в трафике угрозах	+ Корпоративный трафик, зеркалируемый с сетевого оборудования (анализ протоколов SMTP, HTTP, POP3, IMAP, FTP, SMB) + Почтовый агент, который устанавливается на корпоративном почтовом сервере и отвечает за передачу сообщений на сканирование + Корпоративный почтовый сервер, отправляющий копии сообщений на сканирование + Межсетевой экран прикладного уровня, системы обнаружения и предотвращения вторжений (IDS, IPS), прокси-серверы + Файловые хранилища (NFS, FTP, SMB)
Выявление и блокировка вредоносного ПО в трафике	Выявление и предотвращение распространения вредоносного ПО в инфраструктуре, оповещение службы ИБ об обнаруженных в трафике угрозах	+ Почтовый агент, который устанавливается на корпоративном почтовом сервере и отвечает за передачу сообщений на сканирование и блокировку сообщений с угрозами + Межсетевой экран прикладного уровня, системы обнаружения и предотвращения вторжений (IDS, IPS), прокси-серверы + Файловые хранилища (NFS, FTP, SMB)

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ



Общая схема работы PT MultiScanner

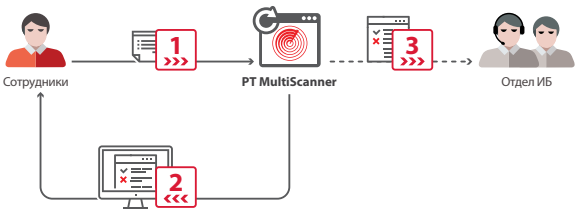
Пользовательский веб-портал (режим ручной загрузки)

На основе PT MultiScanner может быть создан локальный пользовательский сервис в виде веб-портала. Загрузка отдельных файлов для проверки на наличие вредоносного ПО и просмотр результатов сканирования производятся через веб-интерфейс.

Данный сценарий предназначен только для информирования об угрозе, без ее блокирования.

Сценарий

1. Сотрудник отправляет файл или архив, скачанный из интернета или загруженный с внешнего носителя, на проверку в PT MultiScanner через веб-портал.
2. PT MultiScanner выполняет антивирусную проверку загруженного объекта и проверку по репутационным спискам. Результат сканирования пользователь получает непосредственно в веб-интерфейсе.
3. При обнаружении вредоносного ПО PT MultiScanner автоматически отправляет уведомление об угрозе отделу ИБ.



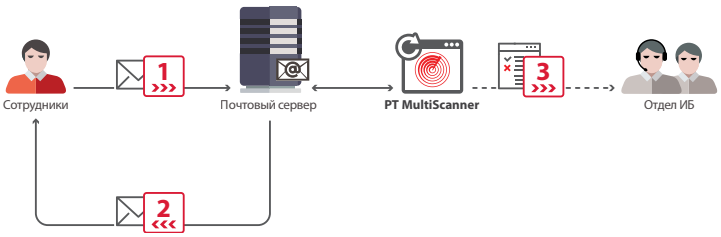
Данный сценарий предназначен только для информирования об угрозе, без ее блокирования.

Пользовательский сервис проверки через электронную почту (режим ручной загрузки)

Пользователь может отправить подозрительные файлы на проверку на специализированный почтовый адрес PT MultiScanner внутри организации.

Сценарий

1. Сотрудник отправляет файл или архив, скачанный из интернета или загруженный с внешнего носителя, на проверку в PT MultiScanner через специализированный почтовый адрес.
2. PT MultiScanner выполняет антивирусную проверку загруженного объекта и проверку по репутационным спискам. Результат сканирования пользователь получает в виде ответного электронного сообщения.
3. При обнаружении вредоносного ПО PT MultiScanner автоматически отправляет уведомление об угрозе отделу ИБ.

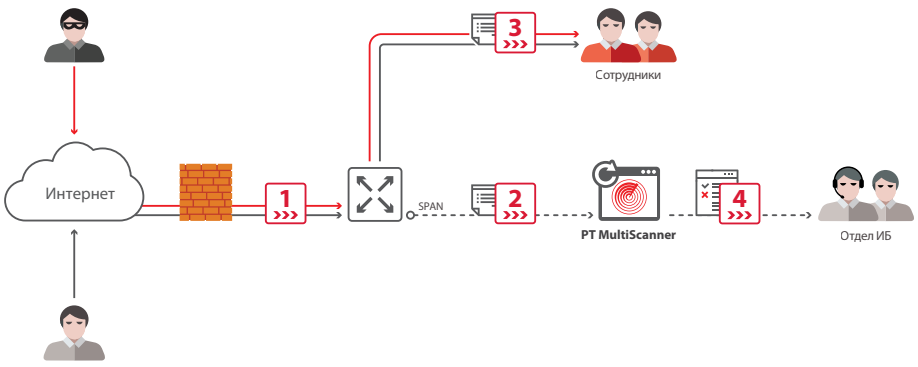


Данный сценарий предназначен только для информирования об угрозе, без ее блокирования.

Мониторинг корпоративного трафика

Сценарий

1. PT MultiScanner анализирует зеркалированный трафик, маршрутизируемый через сетевое оборудование, поддерживающее технологию SPAN. Не влияя на производительность сети, система выполняет антивирусную проверку и проверку по репутационным спискам объектов, передаваемых в трафике по протоколам SMTP, HTTP, POP3, IMAP, FTP, SMB.
2. При обнаружении вредоносного ПО PT MultiScanner автоматически отправляет уведомление об угрозе отделу ИБ.



Защита веб-приложений и порталов

PT MultiScanner можно использовать для защиты веб-приложений и порталов от атак с помощью вредоносного ПО — совместно с межсетевым экраном уровня веб-приложений (web application firewall, WAF). В этом случае система интегрируется с WAF посредством протокола ICAP.

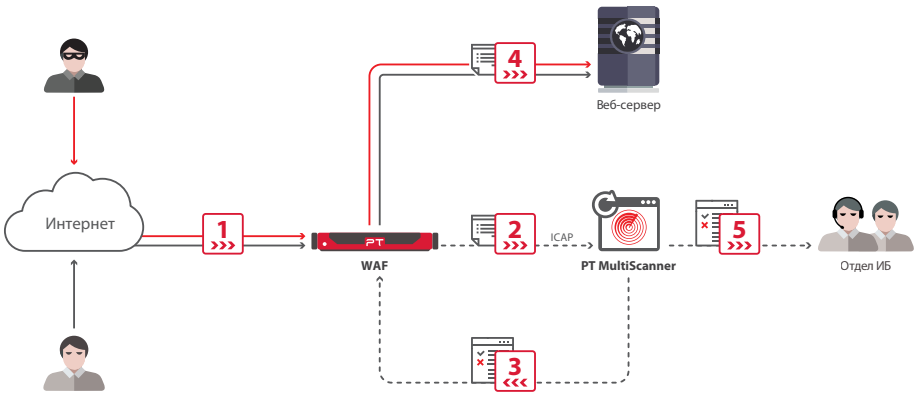
Данный сценарий поддерживает два варианта реализации — без блокировки и с блокировкой вредоносного ПО.

В сценарии рассматривается интеграция с продуктом Positive Technologies — PT Application Firewall.

Сценарий

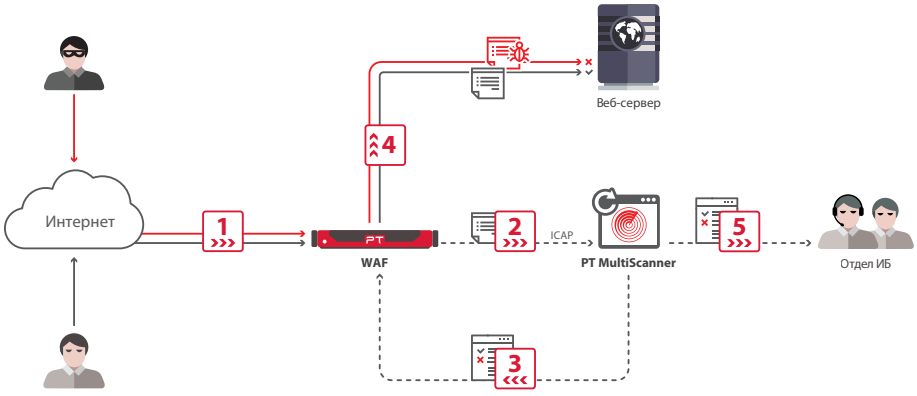
1. Весь трафик, направленный на веб-сервер, контролируется межсетевым экраном уровня веб-приложений.
2. Вложения из трафика вместе с дополнительной информацией об источнике загрузки межсетевой экран направляет для проверки в систему PT MultiScanner.
3. После сканирования объекта PT MultiScanner возвращает межсетевому экрану вердикт проверки.
4. Дальнейшие действия PT MultiScanner зависят от выбранного варианта реализации: без блокировки или с блокировкой вредоносного ПО.

Без блокировки



+ Трафик, прошедший через межсетевой экран, попадает на веб-сервер.
+ При обнаружении вредоносного ПО PT MultiScanner автоматически отправляет уведомление об угрозе отделу ИБ.

С блокировкой



+ При отсутствии угрозы трафик, прошедший через межсетевой экран, попадает на веб-сервер. В противном случае вредоносное ПО блокируется, а PT MultiScanner автоматически отправляет уведомление об угрозе отделу ИБ.

Данный сценарий поддерживает два варианта реализации — без блокировки и с блокировкой вредоносного ПО.

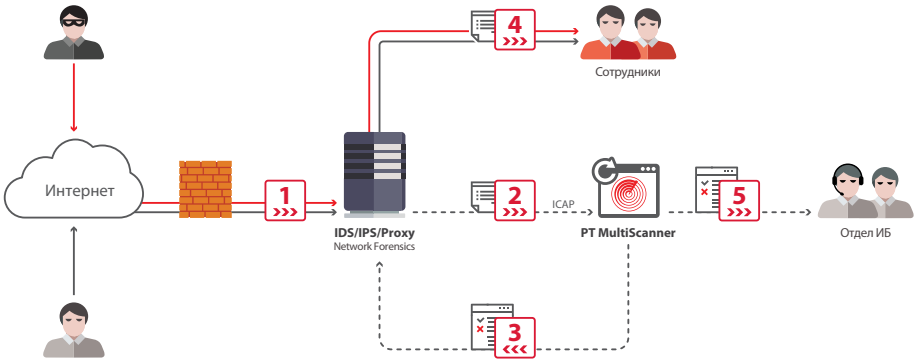
Контроль пользовательского веб-трафика

PT MultiScanner можно использовать для повышения уровня защищенности на границе контролируемого периметра, интегрируя систему со средствами контроля и анализа трафика. В качестве таких средств могут выступать системы обнаружения и предотвращения вторжений (IDS, IPS), прокси-серверы и другие средства, поддерживающие протокол ICAP.

Сценарий (с прокси-сервером)

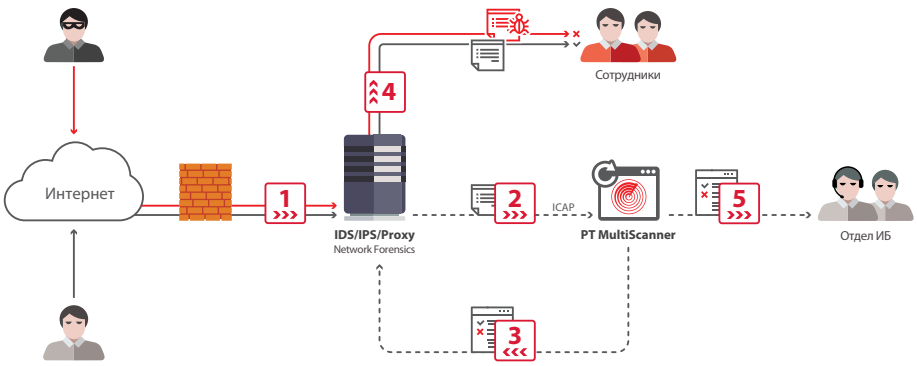
1. Пользователь, скачивая объект из интернета, инициирует процесс его загрузки через прокси-сервер.
2. После загрузки объекта прокси-сервер отправляет его копию для проверки в систему PT MultiScanner вместе с дополнительной информацией о пользователе и источнике загрузки.
3. Дальнейшие действия PT MultiScanner зависят от выбранного варианта реализации: без блокировки или с блокировкой вредоносного ПО.

Без блокировки



+ После сканирования объекта вердикт возвращается прокси-серверу, который передает объект пользователю.
+ При обнаружении вредоносного ПО PT MultiScanner автоматически отправляет уведомление об угрозе отделу ИБ.

С блокировкой



+ При отсутствии угрозы объект перенаправляется пользователю. В противном случае вредоносное ПО блокируется, а PT MultiScanner автоматически отправляет уведомление об угрозе отделу ИБ.

Контроль почтовых вложений

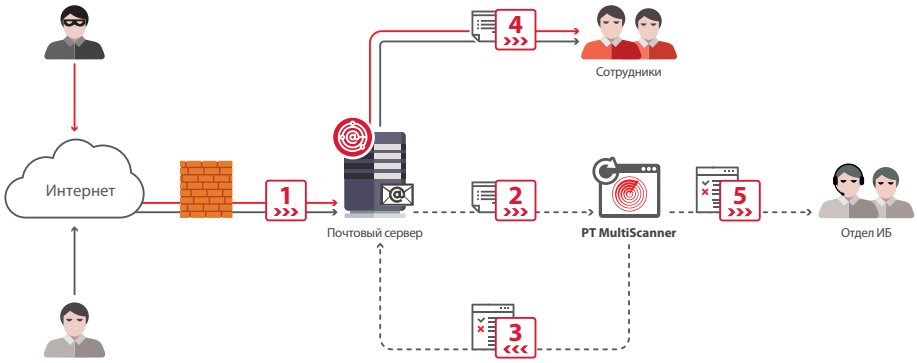
PT MultiScanner можно использовать для выявления и блокировки вредоносного ПО в почтовых вложениях, интегрируя его с почтовыми серверами.

Данный сценарий поддерживает два варианта реализации — без блокировки и с блокировкой вредоносного ПО.

Сценарий

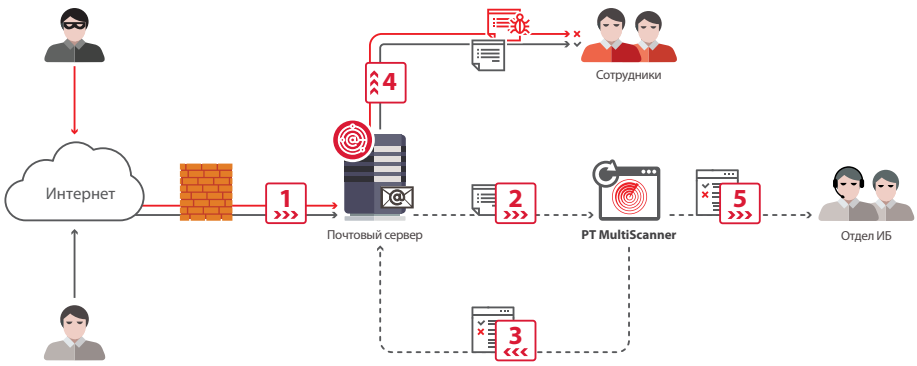
1. На почтовый сервер поступает электронное письмо с вложениями.
2. PT MultiScanner получает файл вложения, а также дополнительную информацию, содержащуюся в полях электронного письма («От кого», «Кому», «Копия», «Тема»).
3. PT MultiScanner производит сканирование объекта и возвращает вердикт проверки.
4. Дальнейшие действия PT MultiScanner зависят от выбранного варианта реализации: без блокировки или с блокировкой вредоносного ПО.

Без блокировки



+ Почтовый сервер передает электронное письмо с вложением получателю.
+ При обнаружении вредоносного ПО PT MultiScanner автоматически отправляет уведомление об угрозе отделу ИБ.

С блокировкой



+ При отсутствии угрозы электронное сообщение передается получателю. В противном случае вредоносное ПО блокируется, а PT MultiScanner автоматически отправляет уведомление об угрозе отделу ИБ.

Данный сценарий поддерживает два варианта реализации — без блокировки и с блокировкой вредоносного ПО.

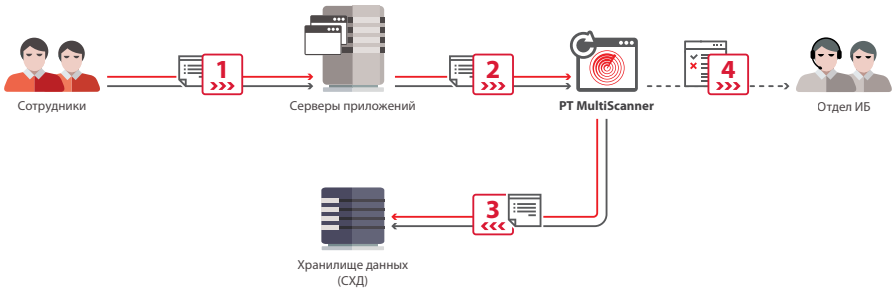
Контроль файловых хранилищ

PT MultiScanner может использоваться для выявления и блокировки вредоносного ПО в корпоративных файловых хранилищах.

Сценарий

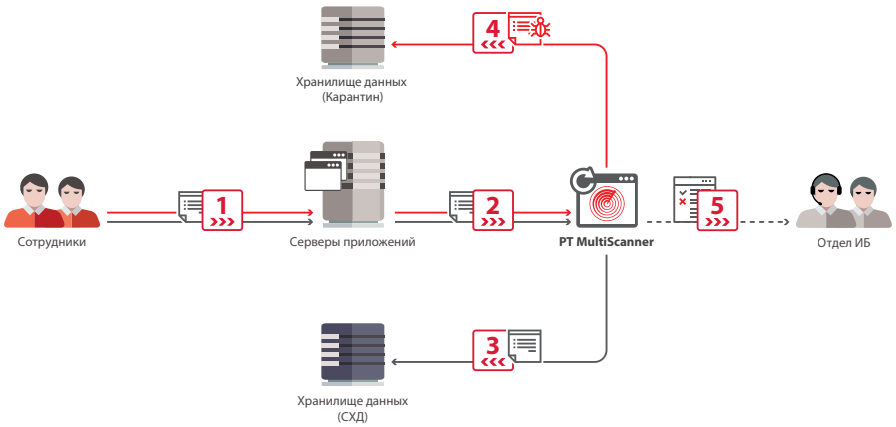
1. Пользователь загружает объект на корпоративный сетевой ресурс.
2. PT MultiScanner, осуществляющий мониторинг данного сетевого ресурса, инициирует процесс проверки нового объекта на наличие вредоносного ПО.
3. Дальнейшие действия PT MultiScanner зависят от выбранного варианта реализации: без блокировки или с блокировкой вредоносного ПО.

Без блокировки



+ Объект, загружаемый пользователем, сохраняется на корпоративном сетевом ресурсе.
+ При обнаружении вредоносного ПО PT MultiScanner автоматически отправляет уведомление об угрозе отделу ИБ.

С блокировкой



+ При отсутствии угрозы объект будет размещен в заданной папке. В противном случае объект перемещается в папку карантина, а PT MultiScanner автоматически отправляет уведомление об угрозе отделу ИБ.

ВАРИАНТЫ ПОСТАВКИ

PT MultiScanner может быть установлен как на физическом сервере, так и на виртуальной машине.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

POSITIVE TECHNOLOGIES

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays