POSITIVE TECHNOLOGIES

ЗАО «ПОЗИТИВ ТЕКНОЛОДЖИЗ»
107061, МОСКВА, ПРЕОБРАЖЕНСКАЯ ПЛ., Д. 8
ТЕЛ. +7 495 744-01-44, ФАКС +7 495 744-01-87, PT@PTSECURITY.COM
PTSECURITY.RU, MAXPATROL.RU, SECURITYLAB.RU

СИСТЕМА СКАНИРОВАНИЯ ФАЙЛОВ MULTISCANNER

РУКОВОДСТВО ПО АДМИНИСТРАТОРА

ОГЛАВЛЕНИЕ

1. Введение

PT MultiScanner – это система, которая позволяет проводить сканирование файлов набором антивирусных программ и получать результаты сканирования в виде отчета. С помощью этого автоматизированного сервиса клиент может получить достоверную оценку опасности, исходящей от файлов, получаемых извне информационной системы.

PT MultiScanner использует несколько антивирусных программ с обновляемыми базами знаний для повышения достоверности результата.

В зависимости от варианта использования, PT MultiScanner позволяет получать файлы из корпоративного трафика, электронной почты, а также контролировать веб-порталы и файловые хранилища. Это многообразие позволяет легко интегорировать PT MUltiScanner в корпоративную сеть заказчика.

1.1. Принцип работы

PT MultiScanner функционирует следующим образом. Система получает от пользователя или извлекает из трафика, электронной почты или хранилища набор файлов или архивов файлов. Все эти файлы обрабатываются, для каждого вычисляется хеш, который используется в дальнейшем для идентификации файлов и получения результата без пересканирования для тех файлов, которые были проверены ранее. Отчет PT MultiScanner также включает в себя текущую версию антивирусной программы и ее базы знаний.

2. Поддерживаемые антивирусы

Система PT MultiScanner на момент выпуска данного руководства поддерживает следующие антивирусы.

- Avast Core Security
- AVG AntiVirus Business Edition
- AVG Server Edition for Linux
- Avira AntiVirus Pro
- BitDefender GraviteZone
- Clam AntiVirus
- Comodo Antivirus for Linux
- Dr. Web Server Security Suite
- Emsisoft Commandline Scanner
- eScan AntiVirus
- ESET Gateway Security
- F-PROT AntiVirus
- F-Secure Linxu Security
- Kasperky AniVirus for Linux Proxy Server
- McAfee VirusScan Enterprise for Storage
- +SAVDI
- Sophos Anti-Virus for Linux
- Symantec Protection Engine for Network Attached Storage

Обратите внимание, что PT MultiScanner использует только английские версии антивирусов.

Список поддерживаемых антивирусов постоянно расширяется. Обратитесь в службу технической поддержки Positive Technologies, чтобы получить актуальные данные.

В вашей системе коллекция антивирусов может отличаться, это регулируется лицензионной политикой.

Пользователь может выбрать доступный антивирус (один или несколько), которым система отсканирует его файл. Все антивирусы делятся на доверенные и недоверенные. По умолчанию, к доверенным антивирусам относятся сертифицированные версии антивируса Касперского и Dr. Web. Все остальные антивирусы считаются недоверенными.

Доверенные антивирусы используются в любом сканировании. Остальные (недоверенные) антивирусы пользователь может выбирать по своему усмотрению.

PT MultiScanner позволяет пометить антивирусы как доверенные на усмотрение пользователя. После этого они входят в группу доверенных антивирусов, и система использует их в каждом сканировании.

3. Системные требования

Для установки PT MultiScanner можно использовать как физическое, так и виртуальное оборудование. В ниже приведены аппаратные требования для физического или виртуального оборудования.

Минимальные требования к оборудованию:

- RAM: 12 Гб
- Жесткий диск: 40 Гб

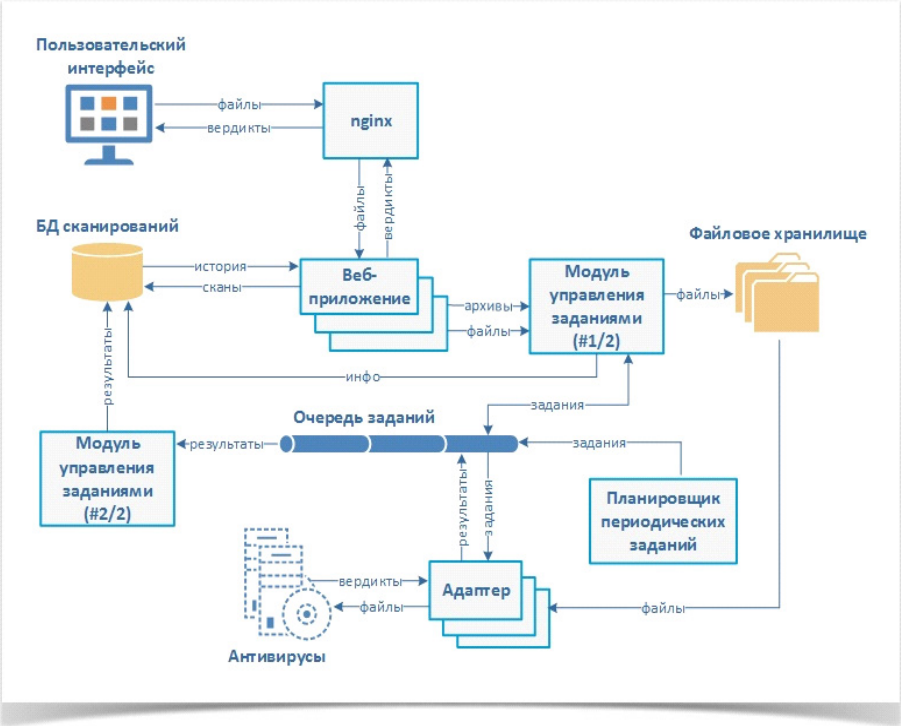
Рекомендуемые значения параметров оборудования:

- RAM: 16 Гб
- Жесткий диск: 500 Гб

Следует использовать операционную систему Ubuntu 14.04 или Windows x64 NT 6.1 и выше (только для агентов). Среда виртуализации - VMWare v.6 и старше, KVM.

4. Архитектура PT MultiScanner

Логическая архитектура системы представлена на рисунке ниже.



Пользователь взаимодействует с системой через браузер (пользовательский интерфейс). Файлы, которые пользователь загружает в систему для анализа, хранятся в базе данных (файловое хранилище). Очередь заданий управляет запуском сканирования файла разными антивирусами. Адаптеры используются для взаимодействия с антивирусами.

5. Установка PT MultiScanner

5.1. Подготовка к развертыванию системы

Для развертывания системы PT MuLtiScanner требуется следующий набор серверов (возможно объединение ролей):

- БД;
- RabbitMQ
- ;
- веб-сервер системы;
- salt-мастер;
- хранение скачанных файлов;
- агенты (адаптеры антивирусных движков);
- сервер лицензий с подключен
- ным ключем;

- дополнительные сервисы.

На сервере для развертывания должен быть развернут salt-master. На всех остальны=х серверах должен быть развернут salt-minion.

При установке системы используются следующие внешние ресурсы:

Репозитории:

- deb http://ru.archive.ubuntu.com/ubuntu/
- trusty main universe
- Если доступ осуществляется через прокси, то настройте прокси:
- Ubuntu - http://help.ubuntu.ru/wiki/%D0%BF%D1%80%D0%BE%D0%BA%D1%81%D0%B8

Если система устанавливается на сервер без доступа в интернет, то создайте локальные зеркала:

- http://help.ubuntu.ru/wiki/apt-mirror
- http://help.ubuntu.ru/wiki/%D1%81%D0%BE%D0%B7%D0%B4%D0%B0%D0%BD%D0%B8%D0%B5_%D0%B7%D0%B5%D1%80%D0%BA%D0%B0%D0%BB%D0%B0_%D1%80%D0%B5%D0%BF%D0%BE%D0%B7%D0%B8%D1%82%D0%BE%D1%80%D0%B8%D1%8F

Для скачивания зависимостей (/srv/salt/prepare.sh) требуется доступ к:

- https://pypi.python.org
- https://www.python.org

При доступ через прокси, используйте опцию help утилиты.

Если система устанавливается на сервер без доступа в интернет, то предварительно скачайте зависимости и создайте новый архив.

Для создания архива выполните:

```
cd /srv
tar -czf /tmp/multiscanner-offline-<версия>.tar.gz ./salt/ ./pillar/
```

Обратите внимание, что все узлы должны иметь уникальное имя, отличное от minion id.

5.2. Лицензирование

Выберите сервер, который будет являться сервером лицензий (эта роль может быть совмещен с другими серверами), например Ubuntu 14.04 x64. Затем:

- Вставите или пробросьте ключ на этот сервер.
- Установите salt-minion.
- В файл конфигурации запишите IP-адрес сервера лицензий в license.host.

Обратите внимание, что PT MultiScanner не работает при выключенном сервере лицензий, или если к серверу лицензий не подключен ключ.

После каждого подключения (повторного подключения) ключа надо перезапускать сервер лицензий.

```
sudo service glds restart
```

5.3. Развертывание системы

- Скопировать дистрибутив на salt-мастер.
- Зайти на salt-мастер.
- Создать резервные копии файлов конфигурации.

Обратите внимание, что при обновлении версии файлы конфигурации перезаписываются.

- Изменить Salt State.

```
tar -x -f <путь до архива> --directory=/srv --recursive-unlink
```

Скачать зависимости (для варианта доступа через прокси — использовать опцию help).

```
apt-get update
apt-get upgrade
/srv/salt/multiscanner/files/prepare.sh --clean
```

Если система устанавливается на сервер без доступа в интернет, то выполнить

```
/srv/salt/multiscanner/files/prepare.sh --target /tmp/ms_req --clean
cd /tmp/ms_req
tar -czf /tmp/ms_req.tar.gz .
переносим файл ms_req.tar.gz на машину с salt-мастер и выполняем
mkdir -p /tmp/ms_req
tar -xf ms_req.tar.gz --directory=/tmp/ms_req --recursive-unlink
/srv/salt/multiscanner/files/prepare.sh --no-index --find-links /tmp/
ms_req
```

- Актуализировать Pillar.

```
vim /srv/pillar/multiscanner/config.yaml
```

Для развертывания системы на Linux:

```
salt -v -G 'kernel:Linux' pkg.refresh_db   # обновление репозиториев
salt -v -G 'kernel:Linux' pkg.upgrade      # Обновление пакетов
salt -v -G 'kernel:Linux' state.highstate --state-output=mixed
```

Для развертывания агентов на Windows:

```
salt-run winrepo.genrepo  # генерация репозитория для винды
salt -v -G 'kernel:Windows' pkg.refresh_db   # обновление репозиториев
salt -v -G 'kernel:Windows' state.highstate --state-output=mixed --
timeout=300
```

5.4. Установка master-salt

- Установите следующие пакеты

```
wget -O - https://repo.saltstack.com/apt/ubuntu/14.04/amd64/2015.8/
SALTSTACK-GPG-KEY.pub | sudo apt-key add -
add-apt-repository 'deb http://repo.saltstack.com/apt/ubuntu/14.04/amd64/
2015.8 trusty main'
```

```
apt-get update
apt-get install salt-master
```

• Запустите мастер

```
service salt-master restart
```

• Подключите minion

5.5. Установка minion-salt

Для систем на базе Windows:

• Установить Microsoft Visual C++ 2008 SP1 (x86) или Microsoft Visual C++ 2008 SP1 (x64)

• Установить salt minion версии 2015.8: https://repo.saltstack.com/windows/. При установке minion указать IP-адрес мастера.

Для систем на базе Linux:

• Установить salt-minion версии 2015.8

```
wget -O - https://repo.saltstack.com/apt/ubuntu/14.04/amd64/2015.8/SALTSTACK-GPG-KEY.pub | sudo apt-key add -
add-apt-repository 'deb http://repo.saltstack.com/apt/ubuntu/14.04/amd64/2015.8 trusty main'
apt-get update
apt-get install salt-minion
```

• Отредактировать файл настроек: sudo vim /etc/salt/minion

```
vim /etc/salt/minion
```

• Заменить master

- раскомментировать "master: salt"

- вместо "salt" указать указать IP-адрес мастера. Например: master: 10.120.4.37

• Перезапустить агента

```
service salt-minion restart
```

• Подтвердить агента на master

```
salt-key -A
```

6. Работа с PT MultiScanner

6.1. Доступ к PT MultiScanner

Пользователь может просканировать файлы без авторизации в системе. Для этого нужно окрыть окно программы и использовать кнопку «Загрузить файл». После выбора файла система запустит проверку и выдаст результат — вердикты использованных антивирусов.

Чтобы запретить анонимный доступ к системе, используйте вкладку Администрирование – Настройки. В разделе Аутентификация отключите опцию «Разрешить анонимный доступ к системе».

Для получения полного доступа к PT MultiScanner пользователь должен пройти авторизацию.

Учетные записи пользователей в системе создает администратор системы. Каждая учетная запись содержит следующие сведения о пользователе:

- Имя пользователя;
- Адрес электронной почты;
- Тип аутентификации;
- Роль пользователя;
- Логин и пароль для входа.

Для аутентификации в системе нужно ввести учетные данные.

Адрес электронной почты не является обязательным полем и используется только для доставки автоматически сгенерированного пароля при смене пароля.

Роли пользователей подробно рассмотрены в соответствующем разделе 6.3.

Для удобства работы пользователей и администратора системы PT MultiScanner позволяет автоматически генерировать пароль пользователя и присылает по указанному в свойствах учетной записи адресу электронной почты следующие сведения:

- Ссылка на страницу авторизации;
- Логин;
- Пароль.

6.2. Роли пользователей

При установке системы создаются две роли — Администратор (admin) и Пользователь (user). Роль Администратор (Admin) является системной, ее нельзя изменить или удалить. Также при установке создается пользователь admin с ролью Администратор (admin), который также является системным. Его нельзя удалить, но его пароль можно изменить. Для этого следует в настройках учетной записи admin задать электронный адрес, а затем использовать его для смены пароля.

Роль Администратор (admin) предоставляет пользователю полные права в системе: запускать сканирование файлов, получать результаты сканирования, просматривать историю запросов всех пользователей и результаты их выполнения. Учетным записям с ролью Администратор доступна статистика выполнения запросов, информация о текущем состоянии антивирусов и хранилища файлов.

Роль Пользователь позволяет пользователю запускать сканирование файлов, получать результаты сканирования, а также просматривать историю своих запросов и результаты их выполнения.

Пользователь системы при наличии соответствующих прав может создавать в системе новые роли. Для этого нужно открыть список ролей, добавить роль и указать ее название и разрешенные действия.

Все пользовательские роли (т.е. такие роли, которые создали пользователи системы), можно редактировать или удалять при необходимости.

Привилегии пользователей делятся на несколько групп, которые настраиваются отдельно.

- Доступ к результатам сканирования
- Доступные антивирусы.
- Доступ к просканированным файлам
- Доступ к статистике
- Функции администрирования.

Для создания или настройки ролей пользователей используется вкладка Администрирование – Роли и права доступа.

Для создания или настройки учетных записей пользователей используется вкладка Администрирование – Пользователи.

6.3. Как PT MultiScanner обрабатывает файлы

Пользователь может передать Мультисканеру один файл или один архив файлов. Мультисканер поддерживает следующие типы архивов:

- zip
- rar
- bzip
- tar
- gzip

Система распаковывает вложенные архивы до второго уровня. Это означает, что если в архив вложены другие архивы, то они будут также распакованы. Архивы последующих уровней вложенности обрабатываются как обычные файлы.

При распаковывании архива создается дерево файлов.

Размер каждого файла не должен превышать 50 Мб. Все файлы, размер которых превышает 50 Мб, не включаются в задачу сканирования. В результатах сканирования таких файлов содержится ошибка «Превышен максимальный размер файла».

Если пользователь пытается загрузить файл, который уже был обработан ранее, то система сразу возвращает известный результат сканирования с пометкой о том, что данные получены из истории сканирования. Такой файл можно отсканировать повторно. Если при проверке PT MultiScanner обнаружит, что файл сканировался ранее с использованием устаревшей базы данных сигнатур, то такой файл будет пересканирован автоматически.

6.4. Просмотр файлов

Пользователь может просматривать файлы в системе в соответствии с правами, определенными настройками его учетной записи. Для отсканированных файлов доступны результаты сканирования. Кроме того, пользователь может добавлять комментарии к файлам в системе.

PT MultiScanner позволяет пользователю создавать и назначать теги для файлов. С помощью тегов можно вести классификацию файлов, а также осуществлять поиск.

Пользователям с соответствующими правами доступна статистика по использованию и состоянию антивирусов. Также можно получить информацию о дате обновления антивируса и его баз знаний и его текущем состоянии (запущен, остановлен). Статистика использования включает в себя общее число запросов к антивирусу, среднее время обработки файла, объем просканированных файлов, статистику файлов по вердиктам.

6.5. Поиск файла

PT MultiScanner позволяет проводить поиск файлов, которые загружены в систему. Результаты поиска по заданным критериям можно загрузить в отдельный архивный файл с паролем или пересканировать заданным набором антивирусов.

6.6. Хеш файла

Для каждого файла, переданного на проверку, система вычисляет хеш (MD5, SHA1, SHA256). Если в истории сканирований обнаружен файл с таким же хешем, то система выдаст результат его сканирования. Такой файл можно отсканировать повторно. Более того, если при проверке PT MultiScanner обнаружит, что файл сканировался ранее с использованием устаревшей базы данных сигнатур, то такой файл будет пересканирован автоматически.

6.7. Отчет о сканировании

Результатом работы PT MultiScanner является отчет о сканировании файла выбранными антивирусами. Для каждого отсканированного файла указывается информация:

- имя, хеш и размер отсканированного файла;
- результат: вердикт каждого антивируса;
- дата и время сканирования;
- версия и дата обновления каждого использованного антивируса;
- классификация вредоносного ПО.

Результаты незавершенного сканирования отображают прогресс обработки файла антивирусами, т.е. количество антивирусов, которые уже обработали файл. Это позволяет оценить, как долго продлится сканирование.

Система позволяет скачать ранее отсканированный файл. При скачивании файлов PT MultiScanner создает архив с паролем “infected”. Пароль архива необходим, т.к. файлы могут быть заражены.

6.8. История сканирования

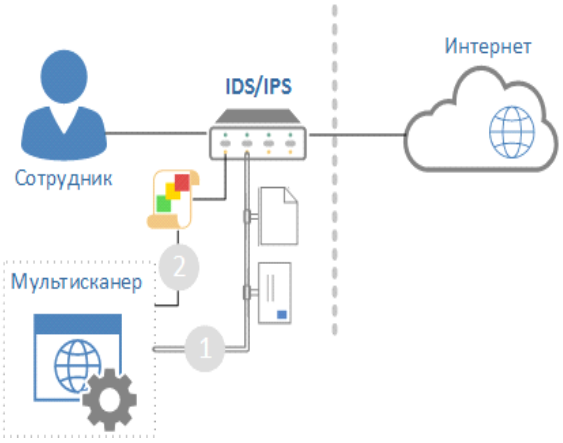
PT MultiScanner позволяет просмотреть историю сканирования файлов. Для каждой задачи сканирования в истории хранятся результаты сканирования всех файлов, включенных в эту задачу. История сканирований включает ту же информацию, что и отчет о сканировании:

- имя, хеш и размер отсканированного файла;
- результат: вердикт каждого антивируса;
- дата и время сканирования;
- версия и дата обновления каждого использованного антивируса;
- классификация вредоносного ПО.

7. Сценарии использования PT MultiScanner

7.1. Контроль корпоративного трафика

Система PT MultiScanner осуществляет проверку файлов и ссылок из захватываемого сетевого трафика в режиме реального времени, выявление ботов во внутренней сети, блокировку угрозы на лету, оперативное реагирование и расследование инцидентов, а также обогащение событий систем защиты (IPS/IDS, SIEM). Этот вариант установки огбеспечивает защиту независимо от действий пользователя, т.к. работает непосредственно с сетевым трафиком, а кроме того не требует обучения пользователей и организации работы с подразделением ИБ.



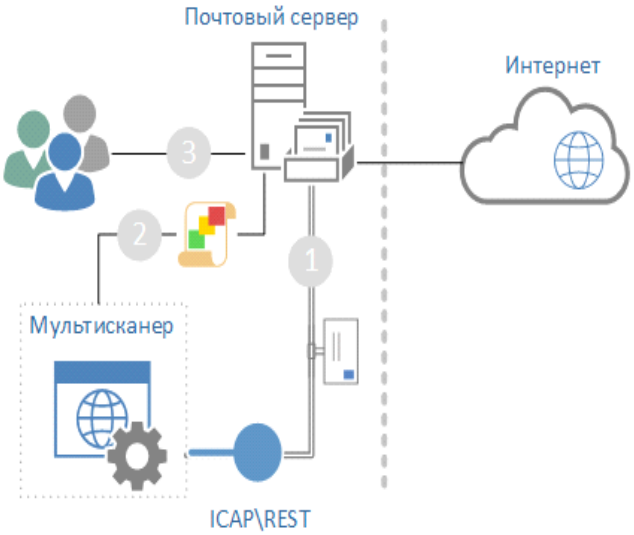
Алгоритм работы:

1. Система PT MultiScanner получает передаваемые по сети файлы и почтовые вложения.
2. Система PT MultiScanner осуществляет проверку полученных файлов.
3. Вердикт передается системе IPS/IDS.

7.2. Защита почты

Система PT MUltiScanner выполняет онлайн-проверку почтовых сообщений, выявление вредоносных вложений, ссылок и источников рассылки, проверку почтовых архивов (в

том числе и разделенных на части и защищенных паролем), осуществляет защиту против атак средствами социальной инженерии с использованием вредоносного ПО.

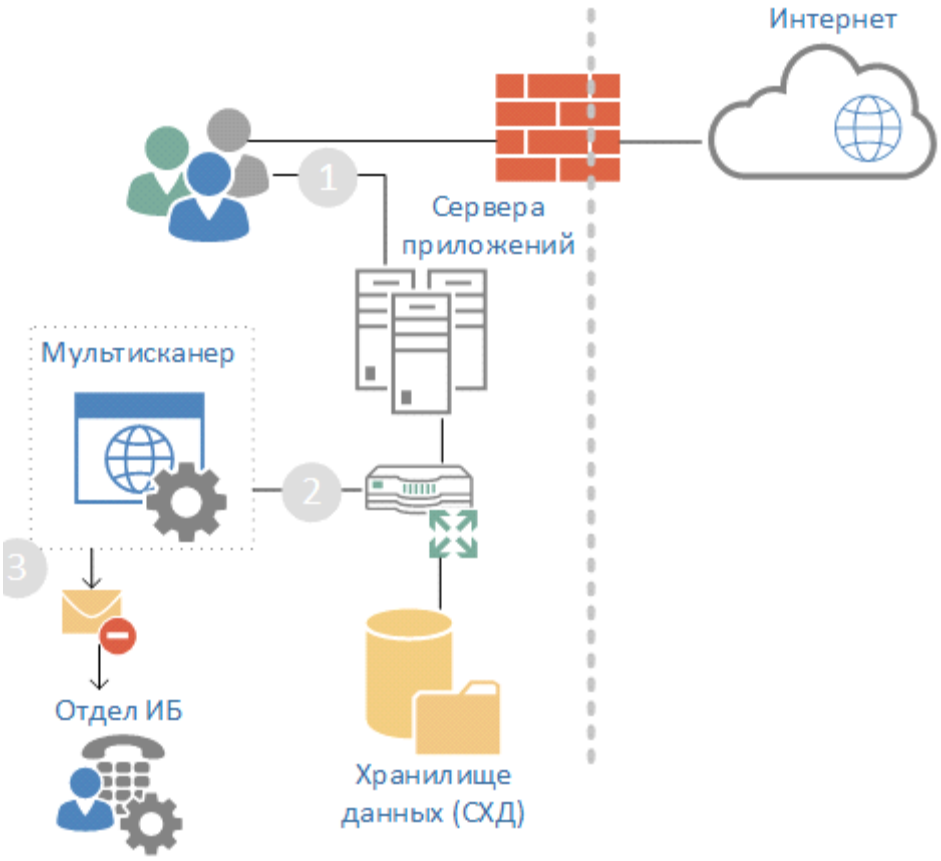


Алгоритм работы:

1. Система PT MultiScanner получает почтовые вложения от почтового сервера.
2. Система PT MultiScanner осуществляет проверку полученных файлов и передает вердикт почтовому серверу.
3. Сервер блокирует вредоносное ПО.

7.3. Контроль файловых хранилищ

Для файловых хранилищ система PT MultiScanner позволяет выявлять вредоносное ПО, зараженные дистрибутивы и документы, а также своевременно блокировать распространение вредоносного ПО и проводить ретроспективу и выявление угроз без пересканирования исходного файла. Этот вариант установки предотвращает долговременное хранение вредоносного ПО в файловых хранилищах и обеспечивает полноценное удаление последствий заражения.



Алгоритм работы:

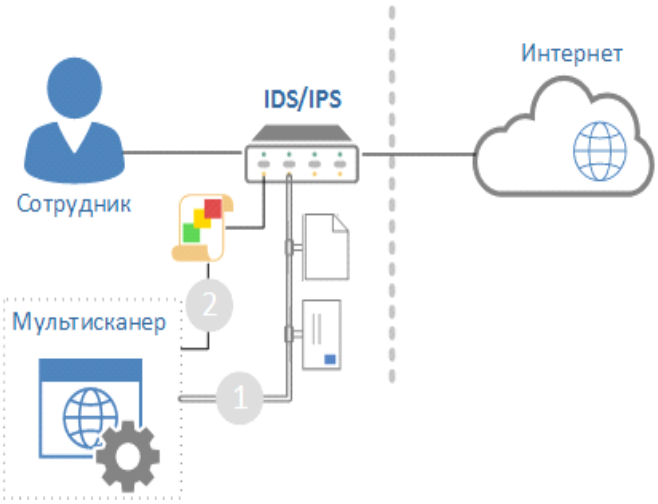
1. Система PT MultiScanner получает файлы из трафика, который направлен к хранилищу.
2. Система PT MultiScanner осуществляет проверку полученных файлов.
3. Вердикты передаются в отдел ИБ для разбора и принятия мер.

7.4. Внутренний сервис выборочной проверки

Система PT MultiScanner устанавливается как отдельный сервис внутри корпоративной сети и позволяет анализировать загружаемые вручную файлы или веб-ссылки, а также вести базу знаний и статистики по загруженным объектам и вердиктам и уведомлять пользователей об обнаруженном вредоносном ПО в ранее загруженных файлах. Проверка происходит через простой веб-интерфейс либо через корпоративный почтовый ящик, куда любой сотрудник может отправить письмо с подозрительными вложениями.

Сотрудники отдела ИБ могут оперативно узнавать о появившемся вредоносном ПО и принимать необходимые меры противодействия.

PT MultiScanner может периодически пересканировать уже проверенные файлы, используя обновленные базы знаний антивирусов, для уточнения вердиктов.



Алгоритм работы пользователя:

1. Пользователь получает файл, который считает подозрительным.
2. Пользователь отправляет этот файл на сканирование в PT MultiScanner.
3. Пользователь получает вердикт и действует далее в зависимости от полученных сведений.

Positive Technologies — лидер европейского рынка систем анализа защищенности и соответствия стандартам. Компания входит в число наиболее динамично развивающихся участников российской IT-отрасли, демонстрируя ежегодный рост более 50%. Офисы и представительства Positive Technologies расположены в Москве, Лондоне, Риме, Сеуле и Тунисе.

Разработанные экспертами компании программные продукты заслужили международное признание в сфере практической информационной безопасности.

Продукты

Система контроля защищенности и соответствия стандартам MaxPatrol помогает обеспечивать безопасность корпоративных информационных систем и формировать комплексное представление о реальном уровне защищенности IT-инфраструктуры организации. Система позволяет контролировать выполнение требований государственных, отраслевых и международных стандартов, таких как Федеральный закон № 152-ФЗ «О персональных данных», СТО БР ИББС, ISO 27001/27002, SOX 404, PCI DSS. В MaxPatrol объединены активные механизмы оценки защищенности, включая функции системных проверок, тестирования на проникновение, контроля соответствия стандартам — в сочетании с поддержкой анализа различных операционных систем, СУБД и веб-приложений.

Система анализа защищенности XSpider более 10 лет является признанным лидером среди средств сетевого аудита ИБ. На сегодняшний день это один из лучших интеллектуальных сканеров безопасности в мире. Более 1000 международных компаний успешно используют XSpider для анализа и контроля защищенности корпоративных ресурсов.

Услуги

Компания Positive Technologies специализируется на проведении комплексного аудита информационной безопасности, на оценке защищенности прикладных систем и веб-приложений, тестировании на проникновение и внедрении процессов мониторинга информационной безопасности. Статус PCI DSS Approved Scanning Vendor позволяет проводить работы по проверке соответствия данному стандарту.

Клиенты

В числе заказчиков Positive Technologies — более 1000 государственных учреждений, финансовых организаций, телекоммуникационных и розничных компаний, промышленных предприятий России, стран СНГ и Балтии, а также Великобритании, Германии, Голландии, Израиля, Ирана, Китая, Мексики, США, Таиланда, Турции, Эквадора, ЮАР и Японии.

Вклад в индустрию

Принимая активное участие в развитии IT-отрасли, Positive Technologies выступает организатором международного форума по информационной безопасности Positive Hack Days и развивает SecurityLab.ru — самый популярный ИБ-портал на русском языке.

Более подробную информацию можно получить на сайте www.ptsecurity.ru