СИСТЕМА СКАНИРОВАНИЯ ФАЙЛОВ МУЛЬТИСКАНЕР

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

POSITIVE / TECHNOLOGIES®

ОГЛАВЛЕНИЕ

1 Введение

Мультисканер – 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.

1.1 Принцип работы

Пользователь предоставляет файл или набор файлов. Мультисканер обрабатывает полученные файлы и собирает результаты работы всех антивирусных программ с полученным набором файлов. В отчет также включается текущая версия антивирусной программы и ее базы знаний. Для каждого файла система вычисляет хэш, который позволяет идентифицировать и получить результаты сканирования файла без пересканирования, если такие результаты уже хранятся в системе.

2 Поддерживаемые антивирусы

Система Мультисканер на момент выпуска данного руководства поддерживает следующие антивирусы.

- Avast Professional 9
- AVG AntiVirus 2013
- Avira Internet Security2014
- BitDefender for Unix
- Clam Antivirus 0.97
- Dr. Web Security Space 9
- Emsisoft Internet Security Pack
- eScan Anti-Virus 14
- ESET 7
- F-Prot Antivirus 6
- F-Secure 1.99
- Kasperky Internet Security 2014
- McAfee Total Protection 6
- Sophos Anti-Virus for Linux

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

Пользователь может выбрать антивирус (один или несколько), которым Мультисканер отсканирует его файл. Все антивирусы делятся на доверенные и недоверенные. 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.

В системе Мультисканер антивирусы можно пометить как доверенные. После этого они входят в группу доверенных антивирусов, и система использует их в каждом сканировании.

3 Работа с Мультисканером

3.1 Доступ к Мультисканеру

Для получения доступа к Мультисканеру пользователь должен пройти авторизацию.

Для авторизации используются учетные записи пользователей Мультисканера.

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.

В системы доступны два типа аутентификации — внутренняя и внешняя. Внутренняя аутентификация подразумевает ввод учетных данных, в случае внешней аутентификации используется авторизация через Полидон.

Адрес электронной почты не является обязательным полем. Его значение используется только при доставке по электронной почте автоматически сгенерированного пароля.

Роли пользователей подробно рассмотрены в соответствующем разделе.

Мультисканер позволяет автоматически генерировать пароль пользователя и присылает по указанному в свойствах учетной записи адресу электронной почты следующие сведения:

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

Если пользователь потерял пароль, администратор системы может повторно сгенерировать письмо от Мультисканера с учетными данными существующего пользователя. Это письмо будет содержать:

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

3.2 Вход в Мультисканер

Для входа в систему пользователь открывает страницу авторизации, выбирает опцию «Войтипо паролю» и вводит свои учетные данные. Мультисканер позволяет сохранить учетные данные, чтобы не вводить их заново при повторном входе в систему.

3.3 Роли пользователей

При установке системы создаются две роли — Администратор (admin) и Пользователь (user). Роль Администратор (Admin) является системным, 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) позволяет пользователю 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 для нее следующие параметры:

- Название;
- Разрешенные действия.

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

3.4 Как Мультисканер 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 Мультисканер сразу возвращает известный результат сканирования с пометкой о том, что данные получены из истории сканирования. Такой файл можно отсканировать повторно. Более того, если при проверке Мультисканер обнаружит, что файл сканировался ранее с использованием устаревшей базы данных сигнатур, то такой файл будет пересканирован автоматически.

Пользователь может выбрать один или несколько антивирусов из набора доступных в системе, которыми будет отсканирован загруженный файл. См. подробнее соответствующий раздел.

3.5 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.

Мультисканер позволяет пользователю создавать и назначать тэги для файлов. С помощью тэгов можно вести классификацию файлов, а также осуществлять поиск по тэгам.

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

3.6 Поиск файла

Мультисканер 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.

3.7 Хэш файла

Для каждого файла система вычисляет хэш (MD5, SHA1, SHA256).

Когда пользователь передает системе файл, Мультисканер вычисляет его хэш. Если в истории сканирований обнаружен файл с таким же хэшем, то система выдаст результат его сканирования. Такой файл можно отсканировать повторно. Более того, если при проверке Мультисканер обнаружит, что файл сканировался ранее с использованием устаревшей базы данных сигнатур, то такой файл будет пересканирован автоматически.

3.8 Отчет о сканировании

Результатом работы Мультисканера является отчет о сканировании файла, переданного пользователем, выбранными антивирусами. Для каждого отсканированного файла указывается различная информация:

- имя, хэш 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 Мультисканер создает архив с паролем “infected”. Пароль архива необходим, т.к. эти файлы могут быть заражены.

3.9 История сканирования

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

4 Сценарии использования Мультисканера

4.1 Как отсканировать файл или архив файлов всеми доступными антивирусами

Чтобы отсканировать файл или архив файлов всеми доступными антивирусами, выполните следующие действия.

1. Нажмите кнопку “Загрузить и сканировать файл” на главной странице Мультисканера. Выберите файлы в открывшемся меню. Также можно перетащить файл в окно Мультисканера с помощью drag&drop.
2. Сканирование запустится автоматически.
3. Мультисканер проверяет переданный файл.
4. Если пользователь выбрал архив файлов, то система Мультисканер распаковывает файлы и передает полученное дерево в интерфейс пользователя.
5. Если размер файла превышает максимальный (50Мб), то сканирование не запускается, а в отчет включается соответствующая ошибка.
6. Если такой файл был ранее отсканирован, то сканирование не запускается, а пользователь получает результаты обработки файла из истории сканирований (дата обработки, вердикт и т.д.). Если базы знаний использованных антивирусов изменились с момента проведения последнего сканирования (например, были обновлены), то Мультисканер автоматически пересканирует файл.
7. Если файл не найден в истории сканирований, то запускается сканирование.
8. После завершения сканирования результаты будут выведены на экран, а также доступны в отчете.

4.2 Как отсканировать файл или архив файлов выбранными антивирусами

Чтобы отсканировать файл или архив файлов выбранными антивирусами, выполните следующие действия.

1. Нажмите кнопку “Выбрать файлы и антивирусы для сканирования” на главной странице Мультисканера. и выберите файл. Появится окно выбора антивирусов.
2. Выберите из списка доступных антивирусов те, которые следует использовать для сканирования (доверенные антивирусы используются при каждом сканировании).
3. Затем следует запустить сканирование, нажав на кнопку “Загрузить и сканировать файл” в верхней части окна Мультисканера.

4. Если пользователь выбрал архив файлов, то система Мультисканер распаковывает файлы и передает полученное дерево в интерфейс пользователя.
5. Если размер файла превышает максимальный (50Мб), то сканирование не запускается, а в отчет включается соответствующая ошибка.
6. Если такой файл был ранее отсканирован, то сканирование не запускается, а пользователь получает результаты обработки файла из истории сканирований (дата обработки, вердикт и т.д.). Пользователь может пересканировать файл при необходимости (например, если с момента сканирования файла антивирусные базы были обновлены).
7. Если файл не найден в истории сканирований, то запускается сканирование.
8. После завершения сканирования результаты будут выведены в окне Мультисканера, а также доступны в отчете.