УТВЕРЖДАЮ
Начальник разработки ПО

Симонова А.К

« » 20 г.

АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«DEFENDER CODE»

Описание программы

Лист утверждения
00000-00 00 01-ЛУ

Руководитель разработки

_____ **Рижская Д.А.**

“_____”_____20__

Ответственный исполнитель

_____ **Мирошникова М.А.**

“_____”_____20__

2020

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

УТВЕРЖДЕНО

00000-00 00 01-ЛУ

АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «DEFENDER CODE»

Описание программы

00000-00 00 01

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

АННОТАЦИЯ

В данном программном документе приведено описание антивирусного программного обеспечения «Defender Code» предназначенной для сканирования файлов, папок или дисков на предмет наличия вирусов и угроз безопасности. Для написания написать антивируса была предложена и реализована архитектура клиент-серверного веб-приложения.

Среда разработки, компилятор - бэкенд написан на языке Haskell с использованием библиотеки Happstack-lite. Получив файл, сервер вызывает сигнатурный анализатор Yara, отправив ему набор правил и сам файл. Вердикт анализатора собирается в формат HTML и отправляется на сторону клиента, а если предоставлен адрес электронной почты, то ещё и на почту.

Результат сканирования отображается в виде alert-полоски в верхней части экрана: зелёная - файл чист (“Everything is OK!”), красная - обнаружена угроза безопасности (“Danger found: <вид угрозы> <имя файла>”).

Сигнатурный анализатор использует версию 4.0.2, собранную с модулями crypto и androguard. Правила для анализа взяты из https://github.com/Yara-Rules/rules

Оформление программного документа «Описание программы» произведено по требованиям ЕСПД (ГОСТ 19.101-77 [1)], ГОСТ 19.103-77 [2)], ГОСТ 19.104-78* [3)], ГОСТ 19.105-78* [4)], ГОСТ 19.106-78* [5)], ГОСТ 19.402-78* [6)], ГОСТ 19.604-78* [7)]).

[1)] ГОСТ 19.101-77 ЕСПД. Виды программ и программных документов
[2)] ГОСТ 19.103-77 ЕСПД. Обозначение программ и программных документов
[3)] ГОСТ 19.104-78* ЕСПД. Основные надписи
[4)] ГОСТ 19.105-78* ЕСПД. Общие требования к программным документам
[5)] ГОСТ 19.106-78* ЕСПД. Общие требования к программным документам, выполненным печатным способом
[6)] ГОСТ 19.402-78* ЕСПД. Описание программы
[7)] ГОСТ 19.604-78* ЕСПД. Правила внесения изменений в программные документы, выполненные печатным способом

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Обозначение и наименование программы

Антивирусное программное обеспечение «Defender Code» имеет следующие атрибуты:

- Страница в сети Интернет - http://defendercode.xyz/main_page.html
- Версия продукта - 1.0.
- Название продукта - Defender Code
- Производитель - DAREMMA GROUP
- Язык - Русский (Российская Федерация)

1.2. Программное обеспечение, необходимое для функционирования программы

Для использования данной программы достаточно открыть ссылку в сети Интернет: http://defendercode.xyz/main_page.html. После этого каких-либо дополнительных настроек не требуется.

Системные программные средства, используемые программой Defender Code, должны быть представлены нелокализованной операционной системой семейства Linux, подсемейства Debian (Ubuntu, Mint, Kali, etc.) на стороне сервера и браузером на стороне клиента (пользователя).

Также для функционирования серверной части программы Defender Code необходимо предустановленное программное обеспечение стороннего разработчика: haskell-stack (версии не ниже 2.3.1), yara (версии не ниже 2.3.1). Программа может быть установлена в любую директорию, кроме /. Для установки данной программы достаточно распаковать архив с программой на компьютер, который будет использоваться как сервер, затем из директории HStackAntivirus/ запустить скрипт build.sh. При появлении сообщений об ошибках в файлах сигнатур (*.yar) вручную удалить соответсвующую строку из файла HStackAntivirus/../rules/index.yar. Затем запустить скрипт server_start.sh для запуска сервера.

1.3. Языки программирования, на которых написана программа

Бэкенд написан на языке Haskell. Фронтенд написан на связке HTML-CSS-Javascript во фреймворке Vue.

2. ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ

2.1. Классы решаемых задач

Получив файл, сервер вызывает сигнатурный анализатор Yara, отправив ему набор правил и сам файл. Вердикт анализатора собирается в формат HTML и

отправляется на сторону клиента, а если предоставлен адрес электронной почты, то ещё и на почту.

Браузер отображает титульную страницу, полученную с сервера. Пользователь может выбрать его или перетащить вручную на страницу, затем отправить на проверку, приложив по желанию адрес электронной почты. В зависимости от состояния страницы - “файл не приложен”, “файл приложен или отправлен”, “файл обработан и чист” и “файл обработан, найдена угроза”, лист на странице принимает зелёный, жёлтый, зелёный и красный соответственно. Результат сканирования отображается в виде alert-полоски в верхней части экрана: зелёная - файл чист (“Everything is OK!”), красная - обнаружена угроза безопасности (“Danger found: <вид угрозы> <имя файла>”). Если указан е-мэйл, то на него отправляется сообщение с таким же текстом.

Для отправки сообщений взяты сервис smtp.gmail.com, как один из самых простых для настройки, и библиотека smtp-mail для Haskell.

2.2. Назначение программы

Программа «DefenderCode» предназначена для быстрой проверки любого вида файлов на наличие в них вредоносного кода. Вызов программы производится пользователем в произвольный момент времени, если ему необходимо что-то проверить.

Программа «DefenderCode» реализует следующие функции:

- проверка загружаемого файла на наличие вирусов
- проверка хэш-суммы загружаемого файла

Данные функции помогают повысить безопасность используемого программного обеспечения и наличествующих у пользователя файлов

2.3. Сведения о функциональных ограничениях на применение

Клиентская часть программы «DefenderCode» может использоваться при работе с любой версией браузера Mozilla Firefox и с некоторыми ограничениями - с Google Chrome. Серверная часть работает на любой ОС семейства Linux подсемейства Debian с версией ядра >= 4.18.

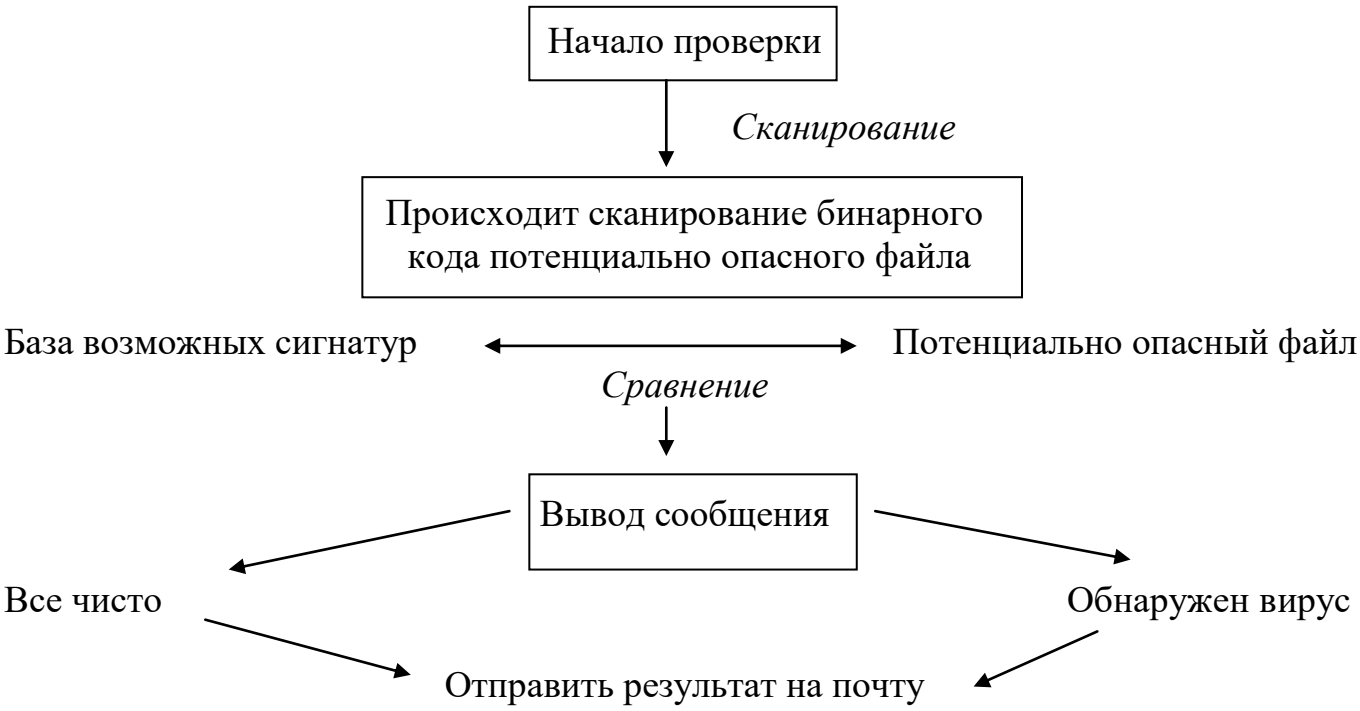
Программа «DefenderCode» не предназначена для самостоятельной проверки ПК, для её функционирования необходимо вручную переходить по указанной ранее ссылке и загружать необходимый файл для проверки.

Программа «DefenderCode» обладает видимым графическим интерфейсом и предоставляет пользователю возможности своего выключения путем закрытия данной вкладки браузера.

Для остановки серверной части нужно остановить процесс, связанный с запущенным сервером.

3. ОПИСАНИЕ ЛОГИЧЕСКОЙ СТРУКТУРЫ

3.1. Алгоритм программы



3.2. Используемые методы

Антивирусное программное обеспечение «Defender Code» использует следующие методы:

1. Реакция веб-сервера на HTTP-запросы:
   - GET - выдаёт титульную страницу,
   - POST - ищет в принимаемых данных файл(ы) для проверки и текст - адрес электронной почты
2. Библиотеки Happstack-lite.
3. Подгружены наборы стилей Bootstrap.
4. Сигнатурный анализатор - используется версия 4.0.2, собранная с модулями crypto и androguard
5. Vue.js, позволяющий прикрепить файлы методом drag-n-drop.
6. Для отправки сообщений взяты сервис smtp.gmail.com, как один из самых простых для настройки, и библиотека smtp-mail для Haskell

3.3. Структура программы с описанием функций составных частей и связи между ними

Антивирусное программное обеспечение «Defender Code» состоит из одной запускаемой формы и не имеет других составных частей.

3.4. Связи программы с другими программами

Программа DefenderCode в ходе своей работы запускает детектор сигнатур yara и использует средства mailutils для отправки сообщений на электронную почту. Для сборки и запуска самой программы DefenderCode необходима система сборки Haskell-stack.\

4. ИСПОЛЬЗУЕМЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА

В состав используемых технических средств входит: 1 ГБ свободного места на жёстком диске, 512 МБ ОЗУ, 64-разрядный процессор. Сервер запущен на хостинге, предоставленном платформой Digital Ocean.

5. ВЫЗОВ И ЗАГРУЗКА

Запуск программы производится через браузер путем перехода на сайт по ссылке http://defendercode.xyz/main_page.html.

6. ВХОДНЫЕ ДАННЫЕ

Серверная часть «DefenderCode» в ходе своей работы получает на вход файл, который необходимо проверить.

7. ВЫХОДНЫЕ ДАННЫЕ

Клиентская часть «DefenderCode» в ходе своей работы выводит строку, содержащую вердикт проверки: «Everything is okey!», в случае успешной проверки, и «Danger found: ...», в случае, если с проверяемым файлом есть проблемы. Результат проверки может быть отправлен по желанию пользователя ему на электронную почту.

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум	№ документа	Входящий № сопроводительного документа и дата	Подп.	Дата
Изм	измененных	замененных	новых	анулированных					