Software Requirements Specification

For

Defender

Version 1.0 approved

Prepared by Victor Babkov

DonNTU

03/09/2012

Revision History

Name	Date	Reason For Changes	Version
Victor Babkov	01/09/2012	Initial version	0.1
Victor Babkov	02/09/2012	Add requirements	0.2
Victor Babkov	03/09/2012	Add references, sketches for GUI	1.0

Table of Contents

1. Introduction

1.1 Purpose

Данный документ описывает спецификацию программного продукта Defender 1.0. Спецификация распространяется на весь программный продукт.

1.2 Document Conventions

*Далее по тексту **полужирным курсивом** будут выделены термины, определение, которых дано в Глоссарии (Appendix A).*

1.3 Project Scope

Продукт разрабатывается с целью снижения расходов на обслуживание рабочих станций на предмет выявления вредоносного ПО. Программный продукт повысит скорость реакции на появление вредонсоного ПО, автоматизирует данный процесс, упорядочит процесс проверки рабочих станций и, в итоге, снизит стоимость обслуживания за счет уменьшения количества рабочих часов администратора, затрачиваемых на осблуживание рабочих станций.

1.4 References

http://en.wikipedia.org/wiki/Computer_virus
http://www.sqlite.org/
http://www.jrsoftware.org/isinfo.php [Inno setup]
http://opensource.org/licenses/bsd-license.php

2. Overall Description

2.1 Product Perspective

Программный продукт Defender является полностью самостоятельной разработкой компании.Ранее продукт не разрабатывался. Представляет собой независмый, самодостаточный программный продукт.

2.2 Product Features

Продукт должен ручном и автоматическом режиме выявлять на накопителях рабочей станции потенциально вредоносные объекты. Под вредоносными объектами понимаются файлы произвольных типов, зараженные ***вирусом неполиморфного типа****. Работа продукта не должна снижать производительность выполнения других задач на рабочей станции. Продукт должен обеспечивать поддержку актуальной базы для идентификации угроз на каждой рабочей станции. Продукт должен иметь интуитивно понятный, удобный интерфейс. Продукт должен быть снабжен справочной документацией в формате html и равзорачиваться на целевой системе с использованием инсталляционного пакета.*

2.3 User Classes and Characteristics

Две роли пользователей:
- обычный пользователь – управляет работой программного продукта с целью выявления угроз, настройки, запуска-остановки и обновления базу угроз;
- администратор – управляет инсталляцией-деинсталляцией продукта, поддержанием базы угроз в актуальном состоянии.
- роли могут объединятся в одном лице.

2.4 Operating Environment

Продукт должен запускаться на семействе ОС Windows: Windows Vista (Windows NT 6.0), Windows 7 (Windows NT 6.1), Windows 8 (Windows NT 6.2), на архитектурах x86, x86-64

2.5 Design and Implementation Constraints

Работа приложения не должна блокировать работу других приложений и своего собственного интерфейса, продукт должен использовать протокол передачи данных TCP и адресацию типа IPv4 и IPv6 для передачи данныхпо сети, для хранения информации продукт должен использовать БД SQLite.

2.6 User Documentation

Должна быть предусмотрена справка для продукта в виде иллюстрированной html-документации. Документация устанавливается с учетом устанавливаемой версии продукта и располагается в рабочей папке программы.

2.7 Dependencies

Предположительно, внешняя библиотека для работы с SQLite БД.

3. System Features (FR)

3.1 System Feature “Structure”

3.1.1 Description and Priority

Продукт должен состоять из двух модулей. Первый – для запуска на рабочих станциях (имя DefenderWorkStation.exe). Второй – для запуска или на рабочей станции или на выделенной машине. (имя DefenderThreatsStore.exe) *Приоритет высокий.*

3.1.2 Functional Requirements

REQ-1: В задачи модуля DefenderWorkStation входит анализ объектов в файловой системе рабочей станции, уведомление пользователя о найденных угрозах, выполнение действий над найденными объектами, настройка программы, обновление локальной копии базы угроз.

REQ-2: В задачи модуля DefenderThreatsStore входит хранение базы угорз определенного формата и распространение данной базы между модулями DefenderWorkStation

REQ-3: Возможна одновременная установка двух модулей на одной машине.

3.2 System Feature “Threats Detect” (DefenderWorkStation)

3.2.1 Description and Priority

Продукт должен выявлять объекты файловой системы (файлы), зараженные ***вирусами неполиморфного типа.*** *Приоритет высокий.*

3.2.2 Functional Requirements

REQ-1: Угроза (вирус) не должен менять свою структуру и всегда имеет один и тот же вид

REQ-2: Вирус может сохраняться в любом месте любого файла в виде непрерывного блока байтов некоторой длины

REQ-3: Обнаружение вируса следует производить на основе ***сигнатуры –*** блока байтов, однозначно идентифицирующего наличие вируса в файле

3.3 System Feature “Threats Notify” (DefenderWorkStation)

3.3.1 Description and Priority

Продукт должен информировать о наличии угрозы и предоставлять возможность удаления инфицированного объекта. *Приоритет высокий.*

3.3.2 Functional Requirements

REQ-1: Продукт должен выдавать список потенциально опасных объектов (файлов) в окно приложения (в ручном режиме).
REQ-2: Продукт должен сигнализировать о найденной угрозе всплывающей подсказкой в системном лотке (в автоматическом режиме), а полный список раскрывать при запросе с указанием имени и размещения инфицированного объекта в файловой системе.
REQ-3: Удаление должно производится только после подтверждения пользователя для одного объекта (файла) или группы объектов (файлов)

3.4 System Feature "Defense Scope" (DefenderWorkStation)

3.4.1 Description and Priority

Продукт должен предоставлять возможность определить область для анализа в ручном и автоматическом режиме. *Приоритет высокий.*

3.4.2 Functional Requirements

REQ-1: В любом режиме работы область поиска – это указанная директория в любом месте файловой системы (включая сменные накопители и сетевые) или указанный накопитель (включая сменные и сетевые)

REQ-2: Для выбора области должен быть организован диалог, который предоставляет список накопителей системы (включая сменные и сетевые), на каждом накопителе пользователь может выбрать произвольную директорию
REQ-3: Продукт должен проверять все объекты, расположенные в указанной области для анализа.
REQ-4: Если при анализе продукт встречает директорию или накопитель, к которому нет доступа (из-за ограничений безопасности, неготовности и т.п.), то он должен проиггорировать такое местоположение.

3.5 System Feature "Work Mode" (DefenderWorkStation)

3.5.1 Description and Priority

Продукт должен работать в двух режимах работы: ручном и автоматическом. *Приоритет высокий.*

3.5.2 Functional Requirements

REQ-1: В ручном режиме пользователь указывает область анализа и действие, производимое с результатом анализа.
REQ-2: В автоматическом режиме продукт осуществляет анализ переодически, через заданный в настройках интервал времени
REQ-3: По умоляанию активирован автоматический режим
REQ-4: Интервал запуска в автоматическом режиме составляет от 10мин. до 24 часов с шагом в 10 мин.
REQ-5: По умолчанию интервал – 30 мин.

3.6 System Feature “Responsibility” (DefenderWorkStation)

3.6.1 Description and Priority

Продукт не должен снижать производительность других программ и операционной системы и блокировать свой собственный интерфейс во время работы (Многопоточность). *Приоритет высокий.*

3.6.2 Functional Requirements

REQ-1: Процесс анализа может быть прерван в любой момент. Интерфейс приложения должен реагировать на команды пользователя во время процедуры анализа.

REQ-2: Выход из приложения невозможен до завершения процедуры анализа при поптыке выйти пользователю должно выдаваться соответствующее сообщение

REQ-3: Переключение между режимами работы невозможно до завершения процедуры анализа при поптыке переключить режим пользователю должно выдаваться соответствующее сообщение

REQ-4: Изменение настроек невозможно до завершения процедуры анализа при поптыке изменить настройки пользователю должно выдаваться соответствующее сообщение

3.7 System Feature “User Interface” (DefenderWorkStation)

3.7.1 Description and Priority

Продукт должен иметь интуитивно понятный и удобный пользовательский интерфейс. Приоритет высокий.

3.7.2 Functional Requirements

REQ-1: При запуске приложение должно демонстрировать заставку (не более 10 сек.) и размещаться в системном лотке.

REQ-2: Интерфейс активируется при клике на пиктограмме приложения в системном лотке

REQ-3: В интерфейсе и контекстном меню пиктограммы должен быть предусмотрен выход из приложения.

REQ-4: В интерфейсе должен быть предусмотрен пункт редактирования настроек

REQ-5: Для ручного режима должен быть предусмотрен запуск-останов анализа.

REQ-6: Должна быть возможность свернуть интерфейс приложения в системный лоток

REQ-7: Должен быть предусмотрен пункт обновления локальной копии базы угроз.

3.8 System Feature "User Interface" (DefenderThreatsStore)

3.8.1 Description and Priority

Продукт должен иметь интуитивно понятный и удобный пользовательский интерфейс. Приоритет высокий.

3.8.2 Functional Requirements

REQ-1: При запуске приложение должно демонстрировать заставку (не более 10 сек.) и размещаться в системном лотке.

REQ-2: Интерфейс активируется при клике на пиктограмме приложения в системном лотке

REQ-3: В интерфейсе и контекстном меню пиктограммы должен быть предусмотрен выход из приложения.

REQ-4: В интерфейсе должен быть предусмотрен пункт редактирования настроек

REQ-5: Должен быть предоставлен интерфейс для навигации (просмотра) полного списка угроз, занесенных в хранилище

REQ-6: Должен быть предоставлен интерфейс для удаления, редактирования и создания записей об угрозах.

3.9 System Feature "Settings" (DefenderWorkStation)

3.9.1 Description and Priority

Продукт должен иметь блок настроек, который сохраняется между запусками программы. Приоритет высокий.

3.9.2 Functional Requirements

REQ-1: Перечень настроек:
Режим работы: ручной, автоматический
Область поиска:
Интервал запуска в автоматическом режиме: 10мин .. 24 часа с шагом 10 мин.
Адрес: доменное имя, IPv4, IPv6 узла с базой угроз
Порт: 0..65535

REQ-2: Перечень настроек по умолчанию:
Режим работы: автоматический
Область поиска: рабочая директория приложения
Интервал запуска в автоматическом режиме: 30 мин.
Адрес: localhost
Порт: 5555

REQ-3: Настройки должны сохраняться в системном реестре (значения по умолчанию записываются при первом запуске программы) в ветке HKEY_LOCAL_MACHINE\SOFTWARE\DONNTU\DEFENDER

3.10 System Feature "Settings" (DefenderThreatsStore)

3.10.1 Description and Priority

Продукт должен иметь блок настроек, который сохраняется между запусками программы. Приоритет высокий.

3.10.2 Functional Requirements

REQ-1: Перечень настроек:
Расположение файла БД с угрозами:
Порт: 0..65535

REQ-2: Перечень настроек по умолчанию:
Расположение файла БД с угрозами: рабочая папка приложения\Threats.db
Порт: 5555

REQ-3: Настройки должны сохраняться в системном реестре (значения по умолчанию записываются при первом запуске программы) в ветке HKEY_LOCAL_MACHINE\SOFTWARE\DONNTU\DEFENDER

3.11 System Feature "Database" (DefenderWorkStation)

3.11.1 Description and Priority

Продукт должен обеспечивать хранение информации об актуальных угрозах в виде файла БД. Приоритет высокий.

3.11.2 Functional Requirements

REQ-1: Имя файла Threats.db

REQ-2: Расположение файла в рабочей директории приложения

REQ-3: Файл имеет формат БД SQLlite

REQ-4: Внутрення структура файла – линейный список (таблица) записей об угрозах

REQ-5: Формат записи об одной угрозе:

THREATS_ID	UINT (4)	PK	NOT NULL	UNIQUE
THREATS_NAME	CHAR (256)	-	NOT NULL	-
THREATS_LEN	UCHAR (2)	-	NOT NULL	-
THREATS_SIGN	BLOB (1..65535)	-	NOT NULL	-

REQ-6: Для получения файла базы модуль DefenderWorkStation должен установить сетевое соединение с модулем DefenderThreatsStore и скопировать файл на локальную машину

3.12 System Feature "Network" (DefenderWorkStation, DefenderThreatsStore)

3.12.1 Description and Priority

Продукт должен обеспечивать получение актуальной базы с помощью сетевого соединения Приоритет высокий.

3.12.2 Functional Requirements

REQ-1: Модуль DefenderWorkStation выполняет роль клиента, а модуль DefenderThreatsStore выполняет роль сервера.
REQ-2: Протокол передачи данных - TCP
REQ-3: Порт сервера 5555 (может меняться), порт клиента – произвольный пользовательский порт

4. External Interface Requirements (NFR)

4.1 User Interfaces

Смотри документы:
Defender_Screens_Logo.pdf
Defender_ThreatsStore_Screens_ContextTrayMenu.pdf
Defender_ThreatsStore_Screens_MainWindow.pdf
Defender_ThreatsStore_Screens_SettingsWindow.pdf
Defender_Workstation_Screens_ContextTrayMenu.pdf
Defender_Workstation_Screens_MainWindow.pdf
Defender_Workstation_Screens_SettingsWindow.pdf

4.2 Hardware Interfaces

Not applicable

4.3 Software Interfaces

Продукт должен использовать API взаимодействия с файлами БД SQLite.

5. Other Nonfunctional Requirements (NFR)

5.1 Performance Requirements

Not applicable

5.2 Security Requirements

Not applicable

5.3 Installation Requirements

Продукт должен устанавливаться с помощью инсталлятора на основе Inno Setup. При установке должен обеспечиваться выбор версии продукта (для рабочей станции, для хранилища угроз – одна из них или обе), место установки, создание ярлыка на рабочем столе. При установке путь по умолчанию %Program files%\DonNTU\Defender
Внутрення структура рабочей папки:

- *DefenderWorkStation.exe (файл программы)*
- *DefenderThreatsStore.exe (файл программы)*
- *Threats.db (файл базы с угрозами)*
- *HelpDefenderWorkStation\ (папка помощи)*
- *HelpDefenderThreatsStore\ (папка помощи)*

Возможно наличие других компонентов при необходимости использовать компоненты третьих лиц.

5.4 Licensing Requirements

Продукт должен использовать BSD License

Appendix A: Glossary

Вирус неполиморфного типа

Блок вредоносного кода, который не обладает свойством изменяться в процессе работы. После создания данный тип вирусов имеет неизменную байтовую структуру.

Сигнатура

Блок бинарных данных, наличие которого в анализируемом объекте дает основание подозревать наличие в объекте вируса определенного типа. Является индиктором зараженности.