Министерство цифрового развития,
Связи и массовых коммуникаций

Ордена Трудового Красного Знамени
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Московский технический университет связи и информатики»

Кафедра информационной безопасности

Самостоятельная работа

по предмету «ЗИ от ВПО»

на тему:

«Разработка антивирусного ПО»

Выполнил студент группы БВТ1802
Басов Александр Владимирович
github.com/maloslov/antiv

Проверил:
Барков Вячеслав Валерьевич

Москва 2021

1 Цель работы

Освоить методы проектирования антивирусного программного обеспечения и вспомогательного обеспечения.

2 Задание

Антивирусный комплекс для ОС Windows 10 x64 должен включать в себя компоненты:

1) вирусная база,
2) редактор вирусной базы,
3) пользовательское приложение
4) сервисное приложение.

3 Выполнение

Для разработки комплекса выбран язык c# (MS.Net Framework 4.5). Взаимодействие пользовательского и сервисного приложений ведется через именованный канал (named pipe). Рабочий каталог комплекса находится по пути «C:\AntiV».

3.1 Вирусная база и её редактор

Вирусная база представляет собой бинарный файл с заголовком «basov». Одна запись состоит из полей:

– Название вируса,
– Тип файла,
– Префикс вирусной сигнатуры (первые 8 байт),
– Хэш от всей сигнатуры,
– Длина сигнатуры,
– Смещение от начала,
– Смещение до конца.

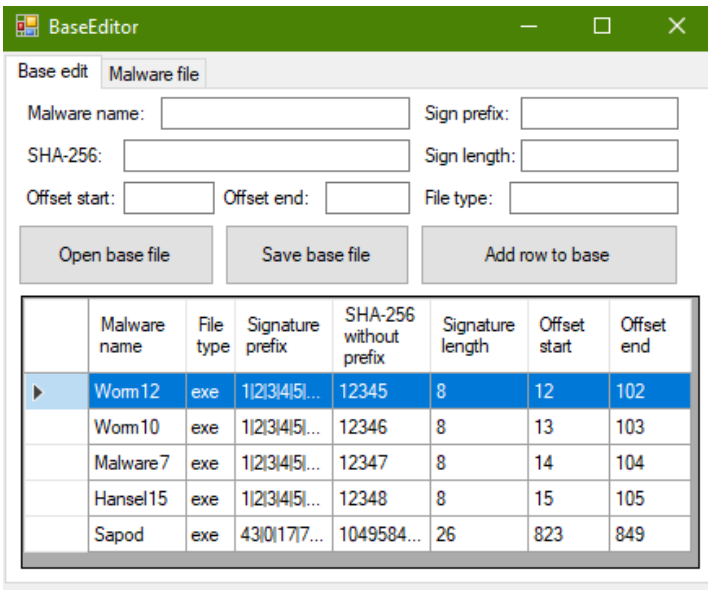

Рисунок 1 – Редактирование вирусной базы.

Редактор баз позволяет добавлять сигнатуру из читаемого файла.

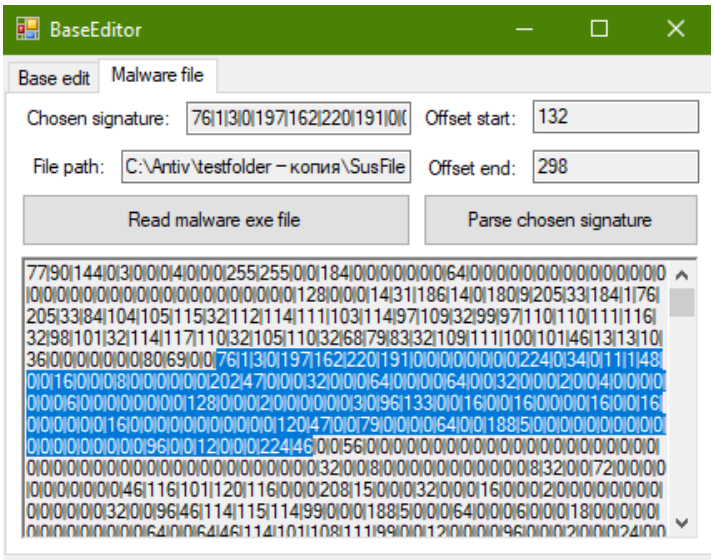

Рисунок 2 – Выделение сигнатуры из вредоносного файла.

3.2 Пользовательское приложение

Пользовательское приложение позволяет:
– Выбирать каталог или файл для сканирования,
– Запускать и завершать сканирование сразу или в назначенное время,
– Мониторить новые файлы в каталоге,
– Удалять и восстанавливать подозрительные файлы из карантина.

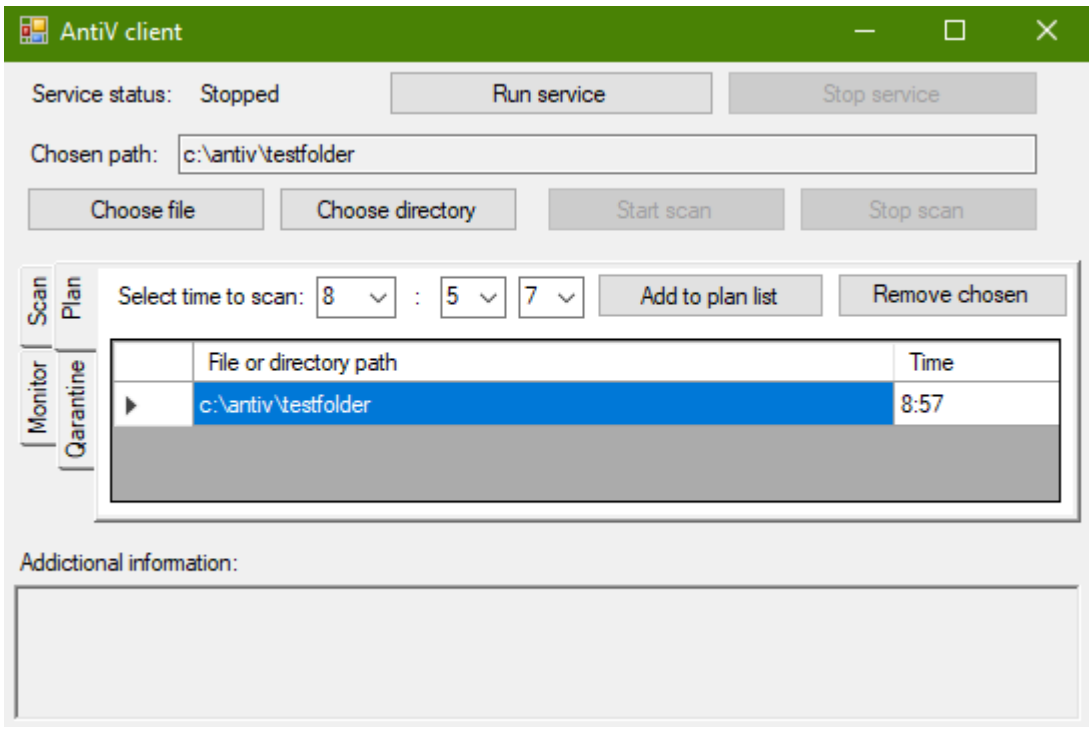

Рисунок 3 – Пользовательское приложение.

3.2 Сервисное приложение

Сервисное приложение является фоновой службой Windows, которая ожидает команд пользователя. Для большей производительности эта служба использует потоки (thread) и задачи (task). Приложение помещает найденный вредоносный файл в каталог карантина и изменяет его заголовок.

Вывод

Была приобретены навыки разработки антивирусного программного комплекса, организации межпроцессного взаимодействия, распараллеливания работы приложения, работы с файловой системой.