АНТИВИРУС «ИММУНИТЕТ»

А. И. Бабушкин
Алтайский государственный технический университет им. И. И. Ползунова
г. Барнаул

Актуальность. В последнее время стало появляться всё больше различных вредоносных объектов, способных разрушить важные персональные данные и нанести ущерб операционной системе и информации. Данными объектами являются: вирусы, троянские программы, «черви» и «кролики». Вследствие этого возникла необходимость разработки антивирусного программного обеспечения, которое не замедляло бы работу системы, а также которое может защитить компьютер от проникновения вредоносных объектов, заражения системы и удалённого взлома хакерами.

Объектом исследований является защита данных.

Предметом исследований - антивирусное программное обеспечение.

Цель - разработка антивирусного пакета для защиты операционной системы и персональных данных.

Гипотетическая модель предполагаемого антивирусного программного обеспечения:

– занимать исключительно малые объёмы памяти;

– работать в любых режимах на любой операционной системе семейства Windows;

– включать в себя эвристический анализатор;

– контролировать интернет соединения, определяет порт, на который ведётся атака и адрес атакующего компьютера;

– удалять вирусы со съёмных носителей сразу после их определения;

– по умолчанию определять вирусы только в системных папках;

– следить за обращениями к реестру;

– иметь большую антивирусную базу, помещённую в один файл;

– проверять файлы не по всей структуре, а только по заголовку и точке входа, включая OEP;

– обновляться раз в 5 дней;

– иметь функцию ведения совершённых действий (далее логов)

– включать в себя систему активации по ключу и возможность сверки ключа с собственным сервером

– иметь наличие поддержки Proxy для возможности обновления

– хранить все настройки и конфигурацию в не компилированном проекте;

– иметь проверку состояния соединения с интернетом;

– не активировать сетевой экран, если доступ к интернету отсутствует.

Задачи:

– провести выборку и анализ существующих антивирусных программ;

– просмотреть и протестировать данные антивирусные пакеты;

– выявить сильные стороны уже существующих антивирусных пакетов;

– написать собственную антивирусную программу, соединяющую в себе все сильные стороны антивирусных пакетов;

– сравнить разработанную программу с уже существующими антивирусами.

Антивирус «Иммунитет» следит за появлением в системных папках новых файлов. Если какой-либо файл пропишется в одну из системных папок, либо в автозагрузку, то пользователь будет оповещён об этом звуковым сигналом, текстовым сигналом в виде всплывающего окна, и будет выведено соответствующее диалоговое окно (рисунок 1). За всем этим следит многокритериальный алгоритм (рисунок 2). Часть исходного кода представлена ниже:

```
…… for /f "usebackq delims== skip=8" %%a in (fsd2) do (echo %%a>>fsd)

for /f "usebackq delims== skip=7" %%a in (fsd) do (echo %%a>>fsd3)

if exist fsd set /p fsd=<fsd

if exist fsd3 set /p fsd3=<fsd3
echo %windir%\system32\drivers\%fsd2%>virlist

if exist fsd echo %win-
dir%\system32\drivers\%fsd%>>virlist

if exist fsd3 echo %win-
dir%\system32\drivers\%fsd3%>>virlist

for /f "usebackq tokens=1* delims= " %%a in (local.bin) do (

goto :movd

start /wait /realtime /abovenormal active.dll .....
```

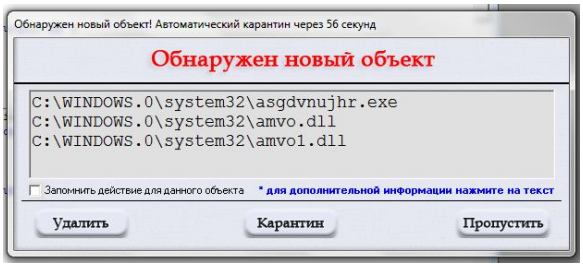

Рисунок 1 – Окно обнаружения вредоносного объекта

Антивирус является резидентным, что позволяет ему помещать ядро в систему ещё на начальном этапе загрузки и оставаться в оперативной памяти компьютера, а не в виртуальной. Запуск каждой службы производится методом вызова необходимых библиотек. Для сетевого экрана есть библиотека “NetScreen.dll”, написанная на C++, для проверки интернет соединения - “Confirm.dll”, для проверки съёмных и несъёмных носителей (флэш антивирус) - “Flash.dll”, а сама проверка файлов по внутренней структуре содержится в библиотеках “Core.dll” и “ICore.dll”. “Core.dll” отвечает за перенаправление команд и является ключевой библиотекой всей программы. Файл “Imun.exe” является стартером, для всех этих библиотек.

Все заголовки вирусов, вредоносные имена секций и точек входа, включая OEP, хранятся в файле “Base.dll”. На данный момент антивирус насчитывает приблизительно 2.610.000 вирусов, из них содержится заголовков порядка 118.000, остальное - вредоносные команды. Данные о вирусах были получены с сайта Viruslist.com, на котором любой пользователь может оставить заявку о найденном недавно вирусе и тем самым предупредить остальных, что обнаружен ручными средствами новый вирус.

Разработанное программное обеспечение может защитить от вирусной атаки из интернета, благодаря сетевому экрану и фильтру, который учится сам на действиях пользователя при тех или иных угрозах и сам отсеивает те соединения, которые известны как неблагополучные. С помощью проверки не только исходящих и входящих TCP протоколов, но и UDP пакетов, пользователь может следить за тем, чтобы никакие программы шпионы, наподобие Cain или LanSpy, не могли получить информацию о компьютере. Так же сетевой экран способствует предотвращению DDoS-атак на компьютер или на всю подсеть. Достигается это благодаря фильтру, который посылая API запросы на netstat проверяет соединение с IP адресом того компьютера, который отправляет запрос на ПК и проверяет этот IP адрес по HTTP заголовкам и по наличию такового в вирусной базе данных.

Рисунок 2. Блок-схема работы многокритериального алгоритма

В результате проделанной работы было создано программное обеспечение, предостерегающее от заражения системы вирусом, отклоняющее DDoS атаки, что является очень полезным для серверов, а так же межсетевой экран. Все задачи, поставленные перед нами - выполнены успешно. Гипотетическая модель подтверждена.

СПИСОК ЛИТЕРАТУРЫ

1. Бобровский С. Самоучитель программирования на языке C++/ О.С. Бобровский. – Из-во: ДЕСС КОМ, I-PRESS, 2001. – 322 с.
2. Герберт Шилдт. Искусство программирования на C++. – 2004. – 474 с.
3. Земсков Ю.В. Программирование на C++ с использованием библиотеки Qt4 – 2007.- 103 с.
4. Керниган Б., Ричи Д. Язык программирования Си++. – 1996. – 352 с.,
5. Павловская Т.А., Щупак Ю.А. С и C++ Структурное программирование – 240 с., 2004г
Символ-Плюс. Хакинг. Искусство эксплойта – 2009. – 512с.
6. Теренс Ч. Системное программирование на C++. – 1997. – 289 с.