УДК 681.3:553.98(574.4)

ПРОФИЛАКТИКА КИБЕРАТАК И СОЗДАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СКРЫТЫХ ФАЙЛОВЫХ УГРОЗ

А. Р. АННАЕВА, М. А. ГЕЛЬДИЕВА, Дж. Б. ГУРДОВА
(Международный университет нефти и газа имени Ягшыгелди Какаева, г. Ашхабад, Туркменистан);

Б. С. ГАФУРОВ
(Драгон Ойл Лтд, г. Ашхабад, Туркменистан)

Аннотация. *В статье рассматривается проблема разработки и применения в операционной системе Windows программного обеспечения, способного своевременно обнаружить, выявить и предупредить возникновение и распространение кибернетических угроз и атак. Авторы на основе так называемой цифровой подписи программы, создали алгоритмы выявления скрытых программ и тел вирусов, являющихся загрузчиками различных троянских и других атак.*

Ключевые слова: *кибербезопасность, скрытая угроза, цифровая подпись программы, тело вируса, скрытая программа.*

Операционная система Windows до сих пор является самой распространенной операционной системой для компьютерных систем, поэтому большинство кибернетических и других вредных атак производится именно на нее. Это еще связано со многими специфическими для данной системы особенностями ее построения и функционирования, которые могут быть применены не только для обеспечения жизнедеятельности системы и поддерживаемых ею программ и других средств, но и для нарушения этих процессов.

В данной работе мы рассмотрим такие проблемы обеспечения кибернетической безопасности, как профилактика и выявление кибернетической атаки и угрозы. С этой целью на языке системного программирования Дельфи был создан и протестирован программный комплекс, способный своевременно обнаружить скрытую потенциальную угрозу.

Основная задача программы, интерфейс которой выполнен в виде стандартного Windows приложения (рисунок 1), состоит из следующих этапов:

– проведение профилактических мер, заключающееся в выявлении неизвестных файлов, загруженных из Интернета или попавших в систему неизвестным путем;

– проверка файлов на предмет наличия среди них потенциальных загрузчиков;

– проверка файлов на предмет наличия среди них тел вирусов.

Чтобы было понятно, дадим некоторые определения.

Потенциальный загрузчик или скрытая программа – исполняемый файл, внешне не похожий на программу или на другой исполняемый машинный код, искусно замаскированный под папку или какой-нибудь документ популярного редактора, автоматически загружаемый в оперативную память при загрузке операционной системы и заражающий своим вредоносным кодом другие загружаемые файлы.

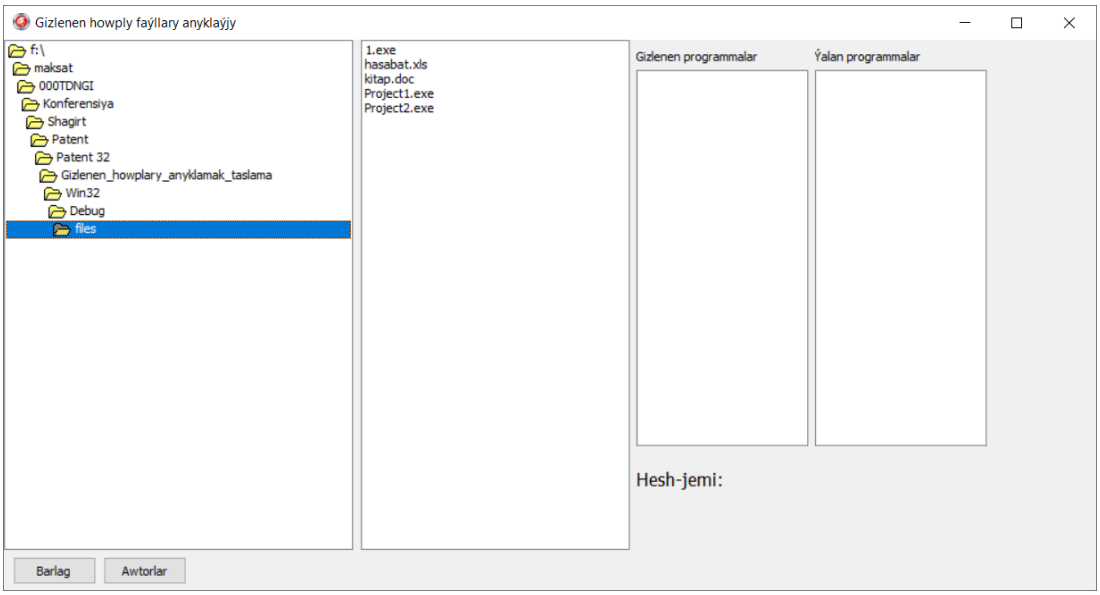

Рисунок 1. – Интерфейс программы

Тело вируса или псевдопрограмма – неисполняемый файл, имеющий внешние признаки программы или другого исполняемого машинного кода (например расширения *.exe, *com, *.bat, *.cmd и т.д.), в котором при запуске компилируется его вредоносная часть кода, формирующаяся как отдельный программный модуль. В повседневной жизни каждый пользователь в глобальной паутине или на локальной станции сталкивается с сотнями и тысячами подобного рода файлов. Быстрота их появления и распространения настолько велика, что современные антивирусные программы не успевают их вовремя обнаруживать и уничтожать.

Однако самостоятельно выявлять данные файлы не очень сложно, просто это рутинная работа и она занимает много времени. Как известно у каждого исполняемого файла есть цифровой код, состоящий из двух байтов (MZ), расположенных в самом начале машинного кода программы.

Достаточно открыть данный файл в обычном текстовом редакторе (в таком как «Блокнот») и данные байты (если это программа) появятся в самом начале машинного кода открытого в редакторе файла.

Таких файлов может быть сотни, а то и тысячи. Открывать их вручную – это слишком длительный процесс.

Разработанное программное обеспечение открывает каждый файл размещенный в указанной директории, считывает с помощью системных WinAPI функций цифровую подпись файлов (первые два байта машинного кода), и при обнаружении цифровой подписи исполняющего файла, проверяет его расширение. Если расширение файла отлично от расширений присущих программам и другим исполняемым файлам, то она размещает его в списке скрытых программ (потенциальных вирусов и их загрузчиков), если же файл не являясь исполняемым, имеет расширение программы, то он размещается в списке псевдопрограмм (потенциальных тел вируса) (рисунок 2). Программа способна за 5–10 секунд проанализировать папку содержащую около 100 файлов. Помимо этого программа способна определить Hash сумму указанного файла с помощью специального алгоритма [4].

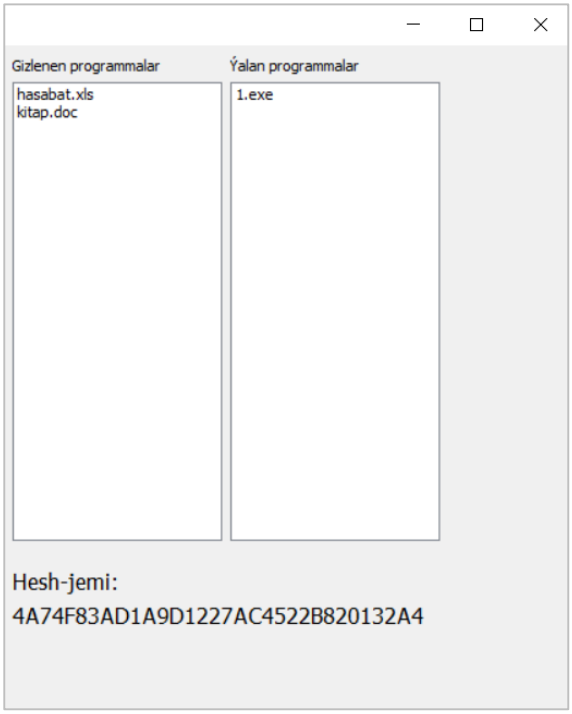

Рисунок 2. – Процесс обнаружения потенциальных загрузчиков и псевдопрограмм

Данная программа очень хорошо себя зарекомендовала, позволив автоматизировать процесс домашнего «аудита» пользовательских папок и файлов, в соответствующем порядке на нее был получен патент (№ 206).

ЛИТЕРАТУРА

1. Сикорски М., Хониг Э. Вскрытие покажет! Практический анализ вредоносного ПО. – СПб.: Питер, 2018. – 768 с.: ил. – (Серия «Для профессионалов»).
2. Монаппа К.А. Анализ вредоносных программ / пер. с анг. Д.А. Беликова. – М.: ДМК Пресс, 2019. – 452 с.: ил.
3. M. Çuriýew. Maglumatlaryň gory we banklary. Ýokary okuw mekdepleri üçin okuw kitaby. – A.: „Ylym“ neşirýaty, 2015.
4. Архангельский А.Я. Программирование в Delphi. – М.: БИНОМ, 2008.