Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Тульский государственный университет»

Институт прикладной математики и компьютерных наук

Кафедра информационной безопасности

**СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ**

Отчет по выполнению лабораторной работы №2

Выполнил

ст. гр. 230781 А. Р. Ивлев

Проверил

Асс. Чаговец Сергей Николаевич

Тула 2022

**Лабораторная работа №2**

**ЗАПУСК ПРОГРАММ В ИЗОЛИРОВАННОЙ СРЕДЕ («ПЕСОЧНИЦЕ»)**

**Цель работы**

Научиться использовать изолированную среду для запуска неизвестной программы или после запуска браузера посетить потенциально опасный сайт, с меньшим риском для своего компьютера.

**Задание на работу**

1. Скачать программу Sandboxie и установить её на компьютер. В современных ОС можно использовать встроенную в ОС (например, Windows 10) песочницу.
2. Настроить программу Sandboxie так, чтобы использовать её для выполнения следующих лабораторных работ.
3. Освоить способы использования Sandboxie и восстановления файлов в «песочнице».
4. Проверить работоспособность (запуск, основные операции, сохранение файлов и т.д.) следующих приложений в программе Sandboxie:
   1. Process Explorer
   2. Autoruns
   3. File and Archive (FAR) manager
   4. Редактор реестра ОС
   5. Браузер FireFox
   6. Браузер Chrome
   7. Модель саморегистрирующегося в автозапуске ОС вредоносного файла
5. Разобрать и подготовить ответ на контрольные вопросы.

**Ход работы**

Для проведения данной лабораторной работы была установлена программа Sandboxie на ОС Windows 7.

1. Process Explorer.

Программа Process Explorer работает корректно, однако нет возможности проверить системные процессы на сайте VirusTotal. Так же Process Explorer не загружает описание системных процессов.

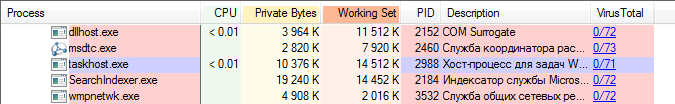


Рисунок 1 - Проверка процессов через Virus Total без Sandboxie

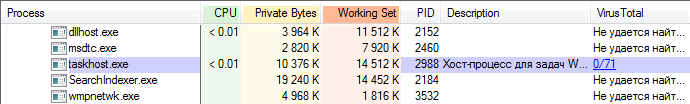


Рисунок 2 - Проверка процессов через Virus Total через Sandboxie

Завершение процесса в песочнице невозможно из-за отказа в доступе.

2. Autoruns

Песочница никак не влияет на работу программы Autoruns, в том числе и на проверку процессов через Virus Total.

3. FAR

Программа FAR в песочнице работает корректно, все команды, такие как просмотр папок и файлов, поиск файлов и другие, доступны, однако созданные и перемещенные файлы сохраняются внутри песочницы.

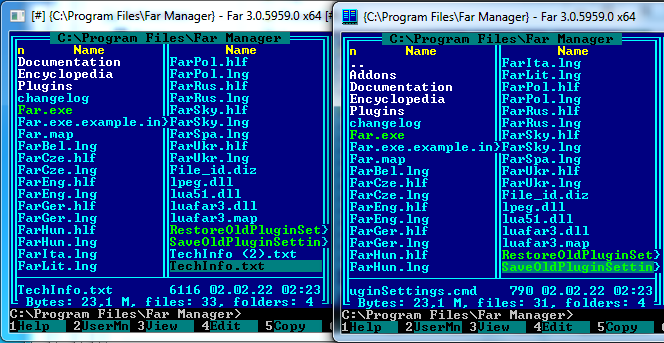


Рисунок 3 – Скопированные файлы в FAR

4. Редактор реестра ОС

Песочница позволяет менять копию реестра, все сделанные изменения не влияют на реальный реестр ОС.

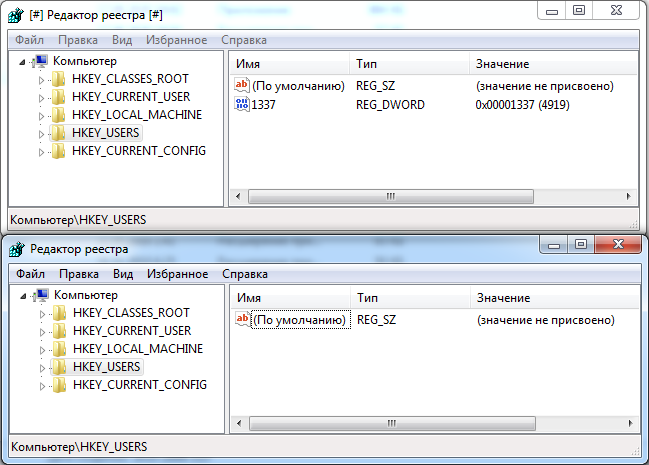


Рисунок 4 - Редактор реестра ОС в песочнице (сверху) и без нее (снизу)

5. Браузер Firefox

Браузер Firefox, запущенный в песочнице, позволяет просматривать страницы и загружать файлы из Интернета. Все скачанные файлы остаются в пределах песочницы. Загрузка файлов в Интернет происходит без ограничений. Также был замечен спад производительности браузера, что, однако, может быть списано на погрешность и субъективность оценивания.

6. Браузер Chrome

Браузер Chrome обладает схожим поведением, что и браузер Firefox, без ярко выраженных отличий.

7. Модель самогенерирующегося в автозапуске ОС вредоносного файла

Вредоносный скрипт был запущен и загружен в автозапуск только в пределах песочницы, в основной системе изменений не обнаружено.

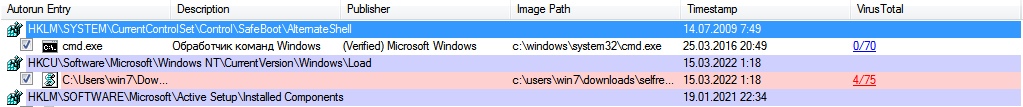


Рисунок 5 - Вредоносный файл в автозапуске (песочница).

**Вывод**

Были изучены методы использования изолированной среды для запуска неизвестных программ и проведено сравнение работы некоторых функций программ при работе в песочнице и вне нее.