МИНИСТЕРСТВО НАУКИ и высшего образования

**РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное автономное образовательное учреждение

высшего образования

«Санкт-Петербургский политехнический университет Петра Великого»

(ФГАОУ ВО «СПбПУ»)

**Институт среднего профессионального образования**

**Отчёт по Лабораторной работе № 6**

**по учебной дисциплине «МДК: Обеспечение качества функционирования компьютерных систем»**

**Тема: «Обнаружение вируса и устранение последствий его влияния»**

Выполнил студент специальности 09.02.07

Информационные системы и программирование

Курс № 2 Группа №22919/21

*Антонов Даниил Александрович*

Преподаватель: Иванова Дарья Васильевна

Санкт-Петербург,

2025

**Цель работы:** изучить поведение различных вредоносных программ, узнать методы обнаружения и устранения последствий их воздействия на ПК.

**Задачи:** установить 3 вируса – вымогатель, блокировщик, майнер. Разобраться с принципом запуска, просмотреть типичные места запуска вирусов, проанализировать компьютер через антивирус. Попытаться удалить вирусы.

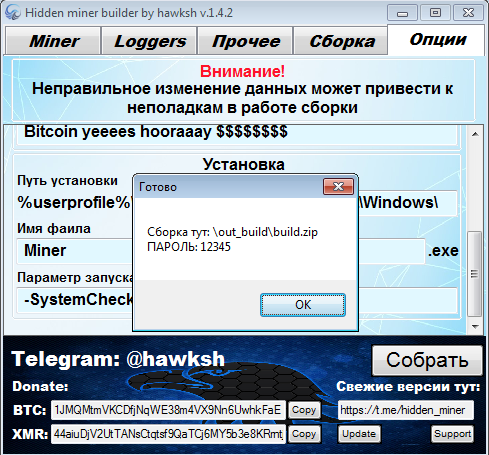


Рисунок 1 – Настройка и сборка майнера

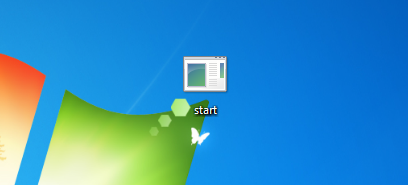


Рисунок 2 – Файл для запуска майнера

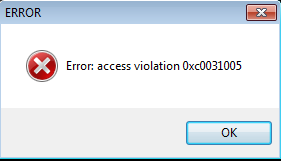


Рисунок 3 – Фейковая ошибка

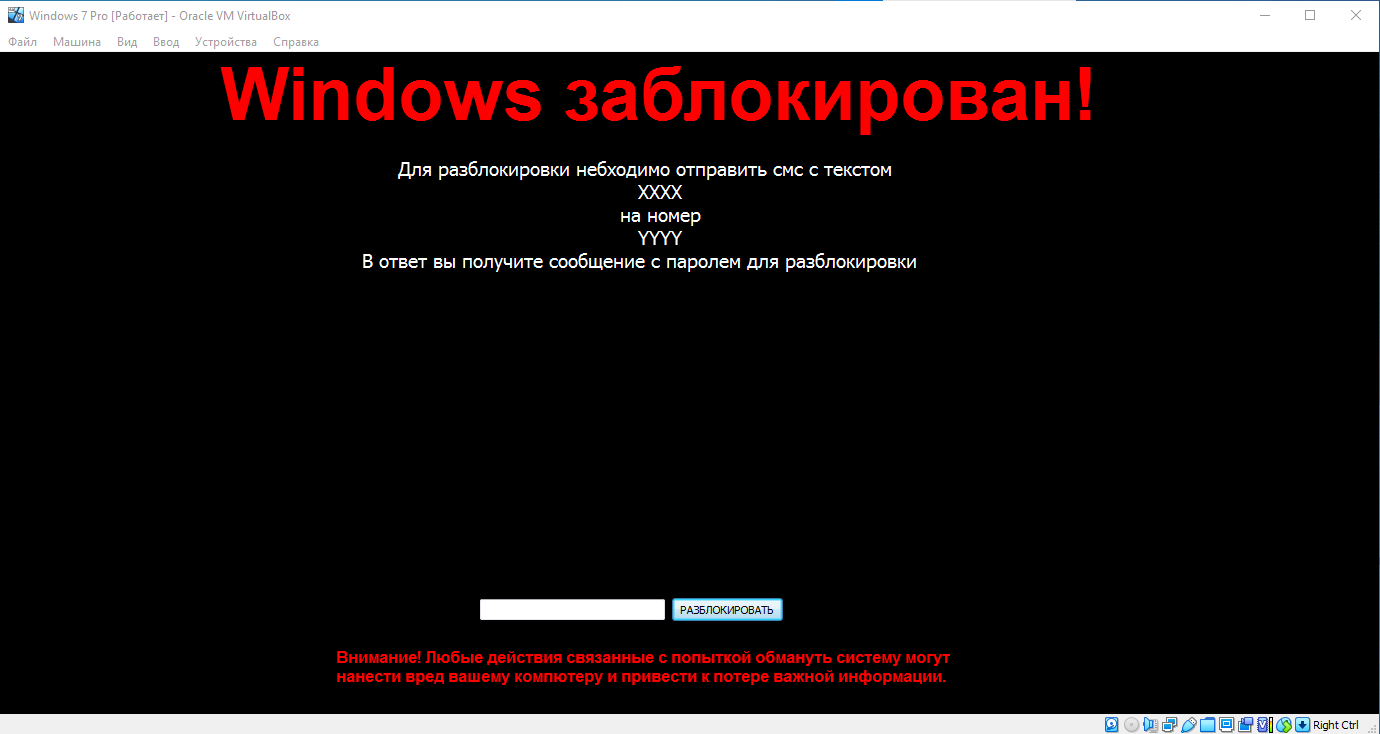


Рисунок 4 – Запуск винлокера

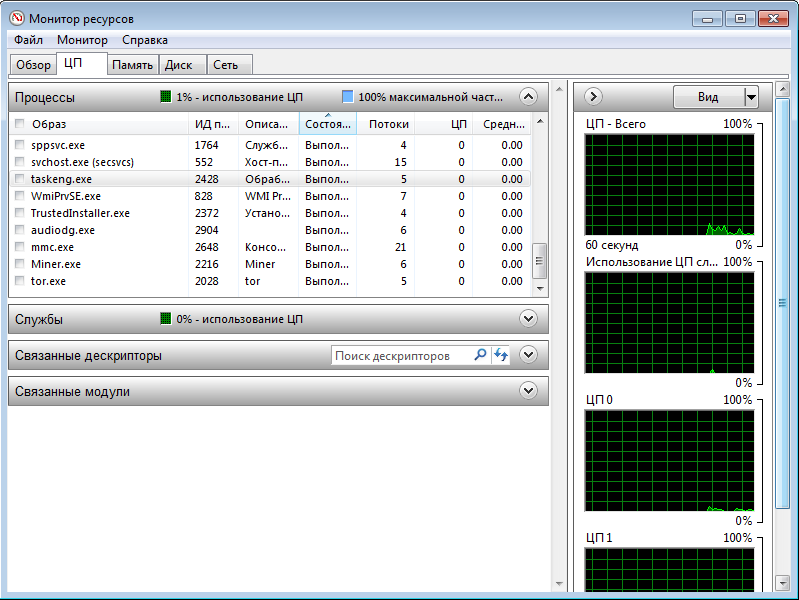


Рисунок 5 – Майнер в Мониторе ресурсов

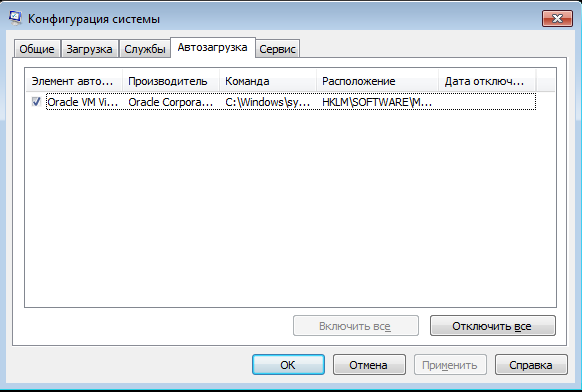


Рисунок 6 – В msconfig автозагрузке майнера и винлокера нет

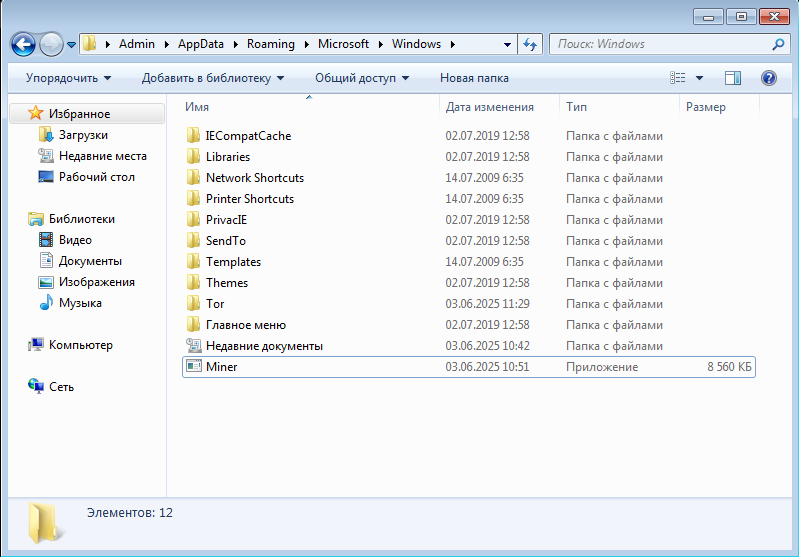


Рисунок 7 – Майнер в папке Windows

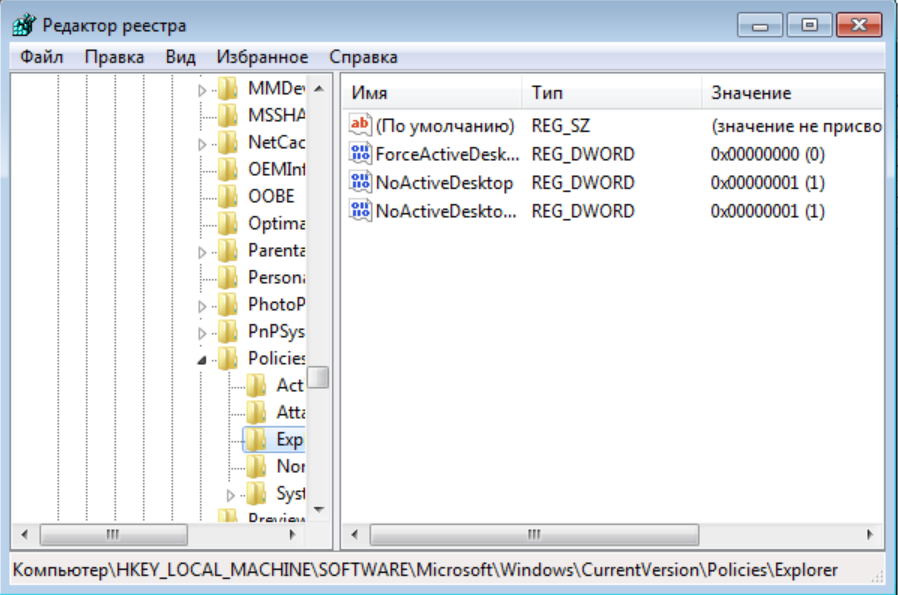


Рисунок 8 – Автозагрузка групповой политики, майнер и винлокер не обнаружены

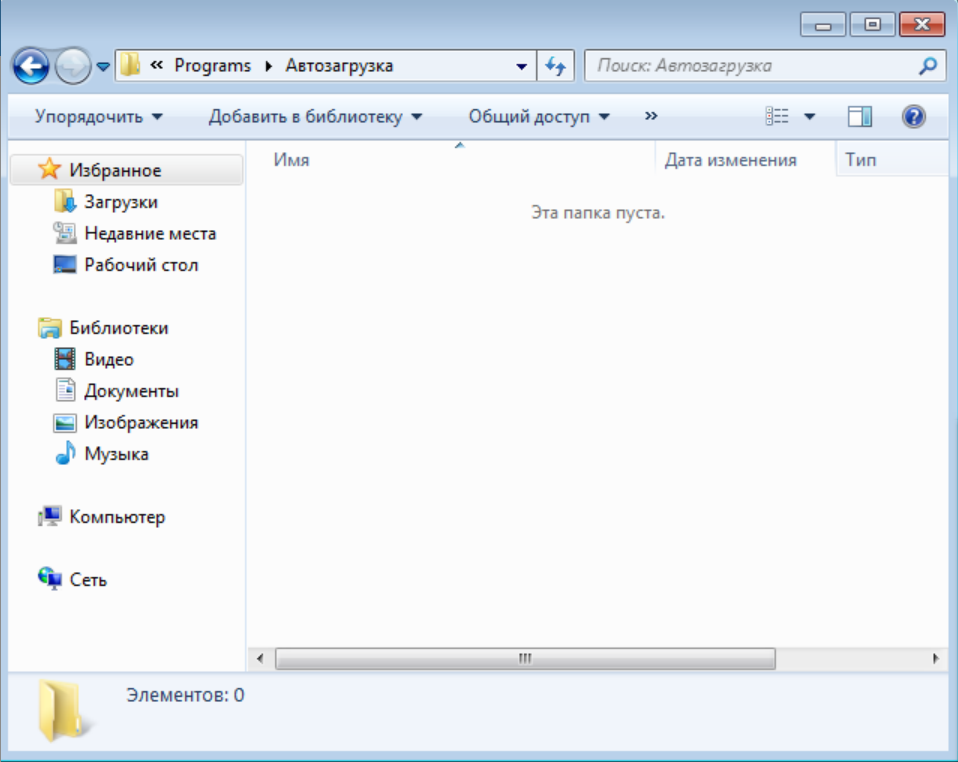


Рисунок 9 – Автозагрузка в ФС, майнер и винлокер не обнаружены

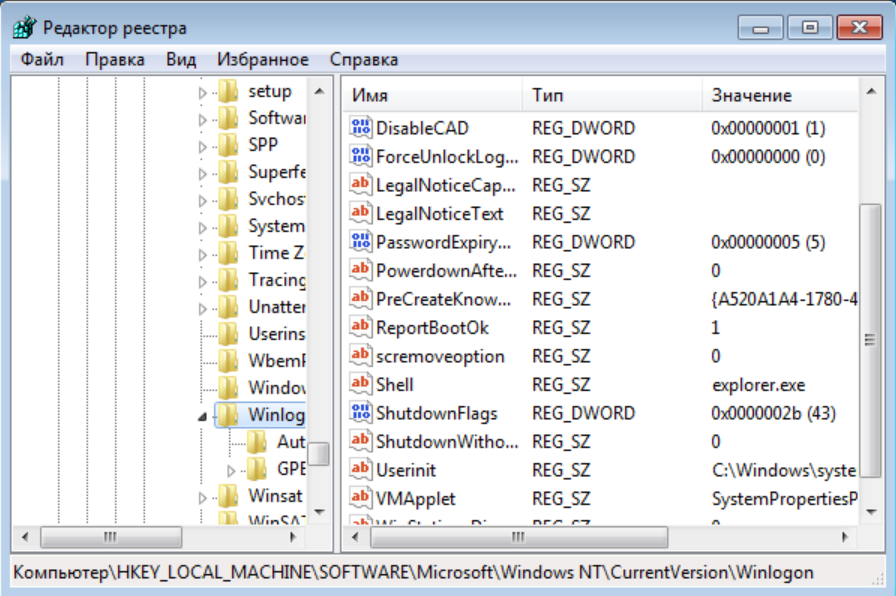


Рисунок 10 – вместо проводника и Userinit, майнер и винлокер не обнаружены

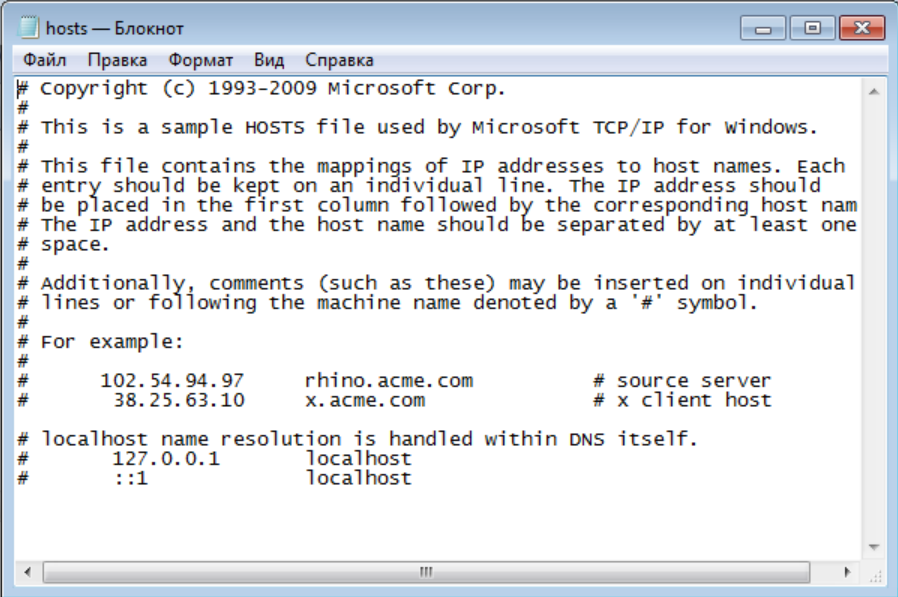
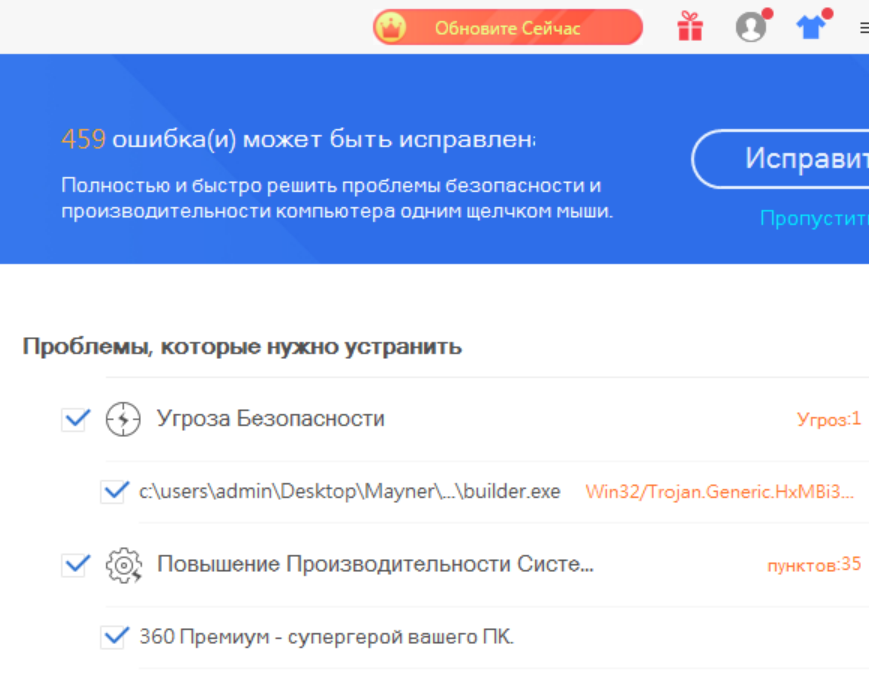


Рисунок 11 – запрета сайтов антивирусных программ нет



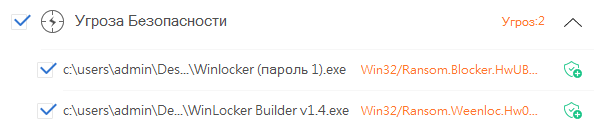
Ф

Рисунок 12 – Антивирус нашел винлокер и билдер

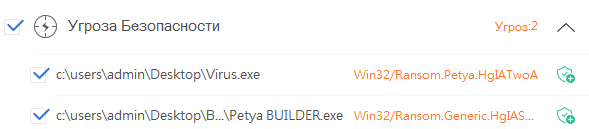


Рисунок 13 – Антивирус нашёл ещё и Петю но в текущий момент нас это не интересует

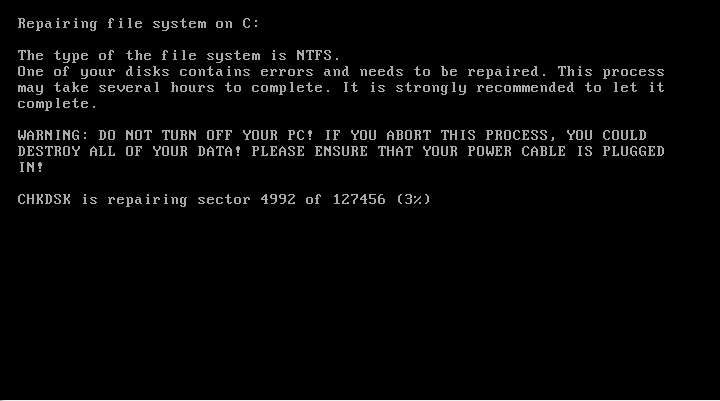


Рисунок 14 – Петя шифрует файлы



Рисунок 15 – Петя все сломал

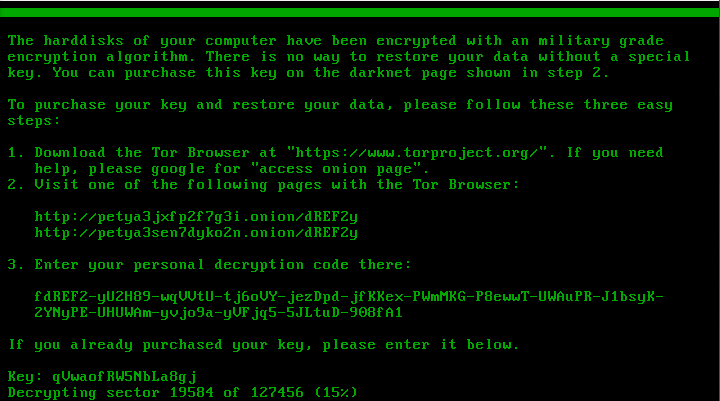


Рисунок 16 – После введения ключа Петя начинает расшифровывать файлы



Рисунок 17 – Просит перезагрузить ПК

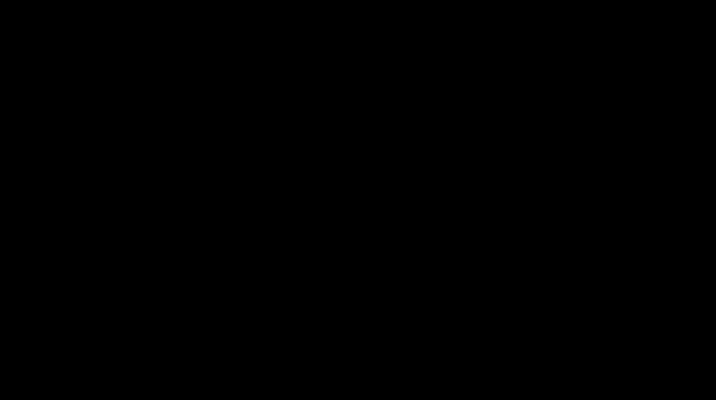


Рисунок 18 – Все сломалось

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Классификация Вирусы | По среде обитания | По способу заражения | По деструктивным возможностям | По особенность алгоритма вируса |
| Miner | Файловый | Резидентный | Опасный | Стелс-вирус |
| Winlocker | Системный | Резидентный | Очень опасный | Простейший |
| Petya | Файлово-системный | Резидентный | Очень опасный | Червь |

**Вывод:** в результате проделанной лабораторной работы, были установлены, рассмотрены и изучены методы поведения 3-ёх типов вирусов – вымогатель, майнер, блокировщик. Вирусы получилось частично выявить в расположениях в реестре и системных файлах – майнер было найти проще всего. После распаковки архивов с вирусами, антивирус почти сразу выявлял угрозу и предлагал поместить программы в карантин. Вирусы, поддающиеся удалению – Winlocker и майнер, Петю удалить не получится, снова запустить работу виртуальной машины можно только путём восстановления VM.

В ходе работы я изучил поведение различных типов вирусов, а также методы их обнаружения и устранения последствий их воздействия. Была составлена таблица с классификацией рассмотренных вирусов.