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 учебной дисциплине «МДК 04.02 Обеспечение качества функционирования КС»**

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

Выполнил студент

специальности 09.02.07

Информационные системы и программирование

2 курса группы №22919/21

Десятский Ян Дмитриевич

Преподаватель: Иванова Дарья Васильевна

Санкт-Петербург

2025

**ОТЧЕТ О РАБОТЕ**

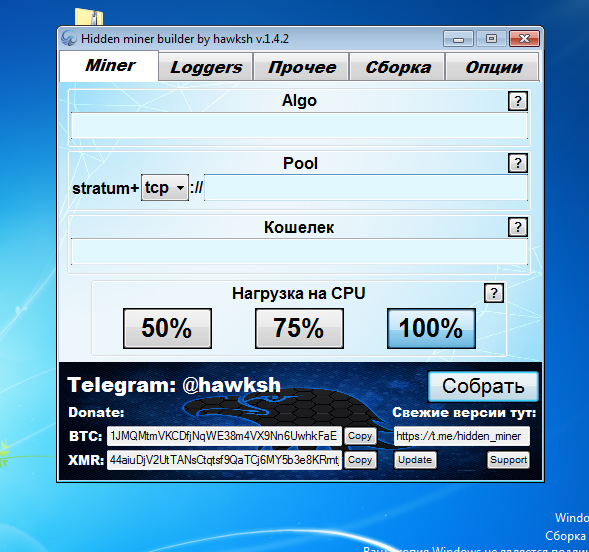
**Цель работы:** изучить поведение различных типов вредоносного ПО, а также методы их обнаружения и освоить подходы к устранению их воздействия на ОС в виртуальной среде.

**Задачи:**

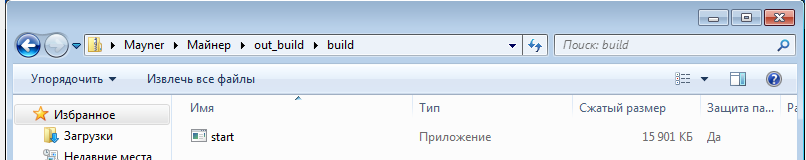
1. Запустить каждый из вирусов (WinLocker, Miner, Petya)и зафиксировать его действия в системе.
2. Определить признаки заражения, характерные для каждого вируса.
3. Применить методы обнаружения и диагностики зараженной системы.
4. Устранить последствия воздействий вирусов, восстановить работоспособность системы.

**Miner и WinLocker**

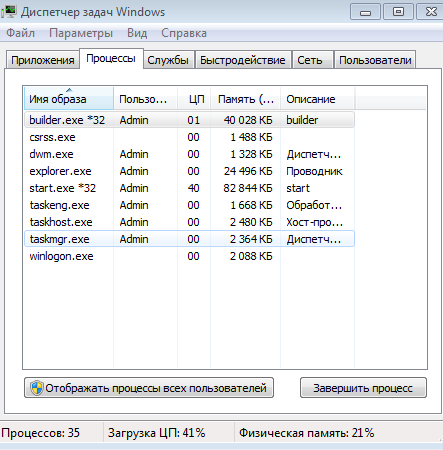
Сборка miner



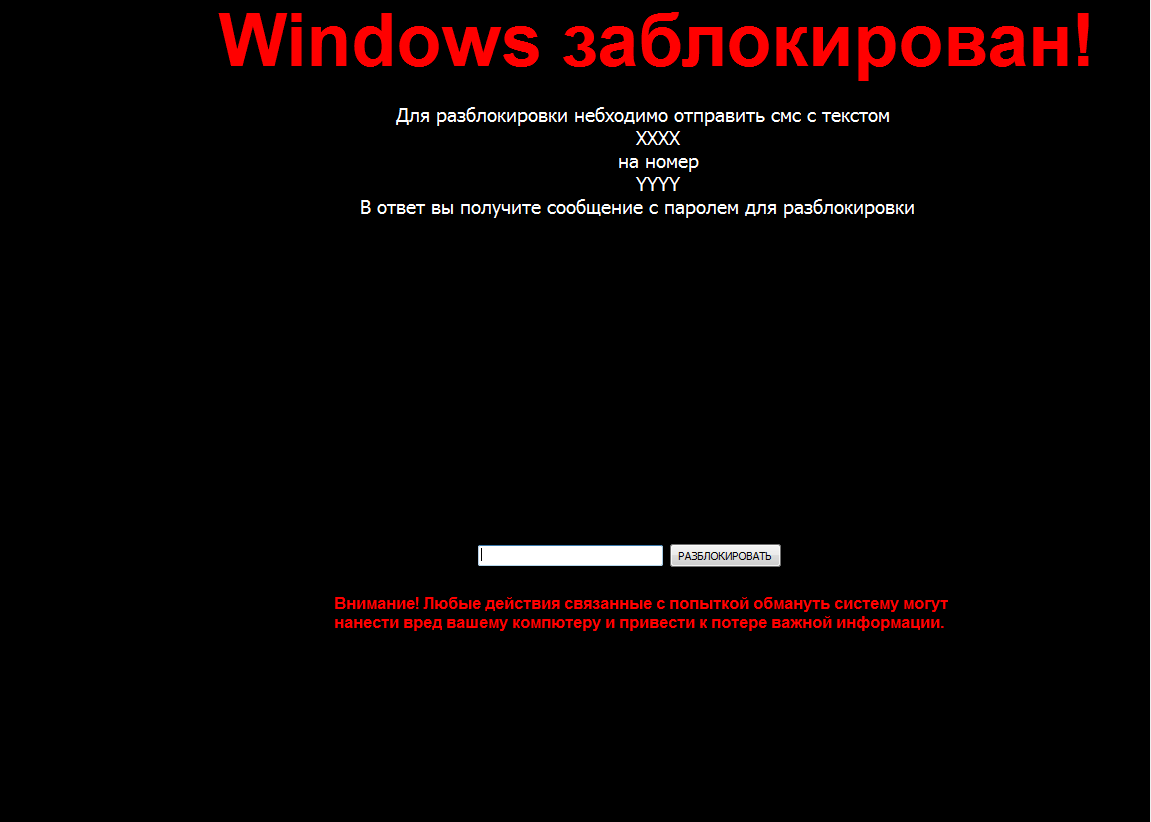
Собранный файл Miner



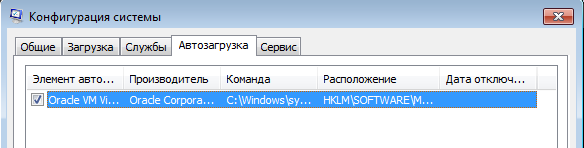
Запущенный файл Miner, отображающийся в диспетчере задач

****

Запуск WinLocker и дальнейшая разблокировка (с помощью пароля: 1)

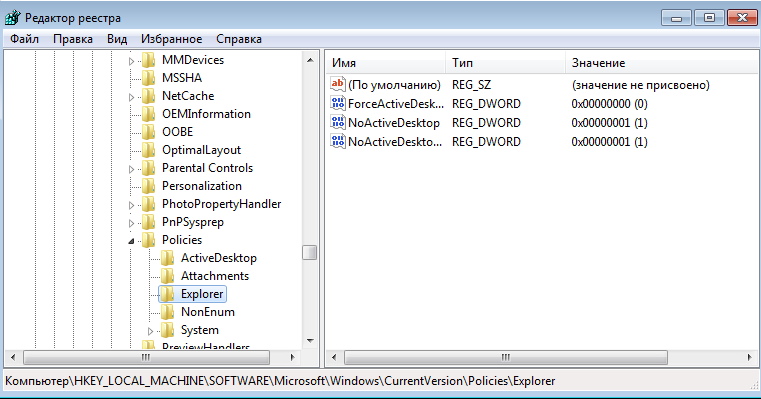


В автозагрузке (через диспетчер задач) файлов вирусов нет

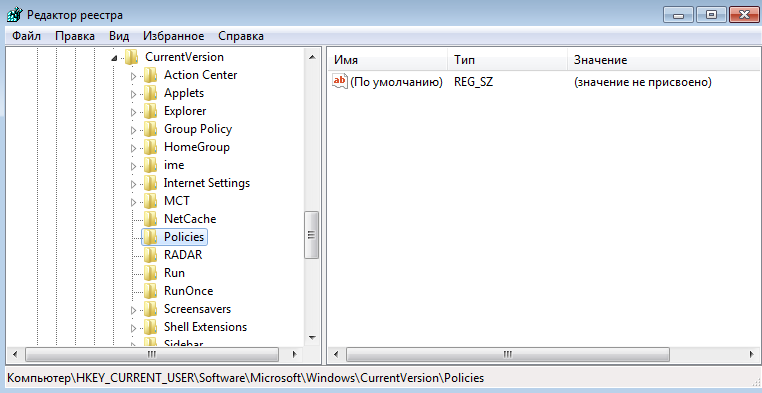


В автозагрузке (через реестр) файлов нет:

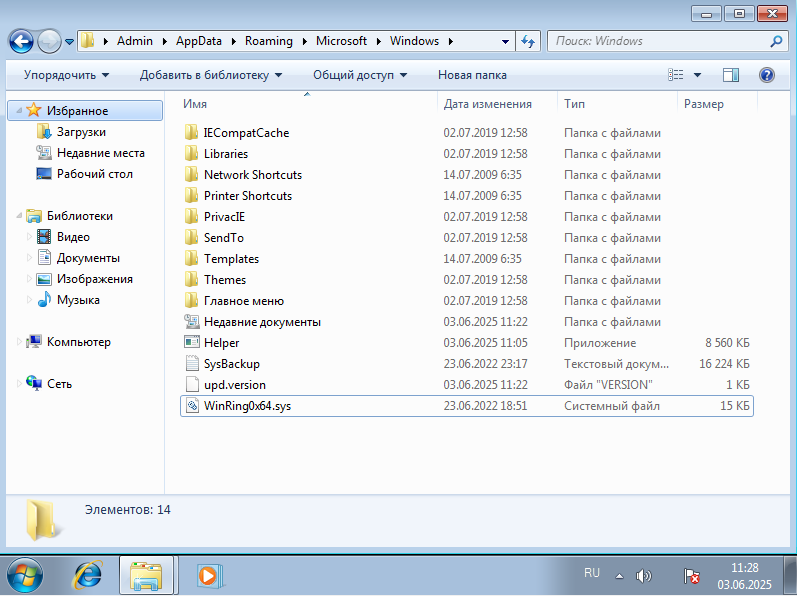
1. По пути: HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run файлов нет



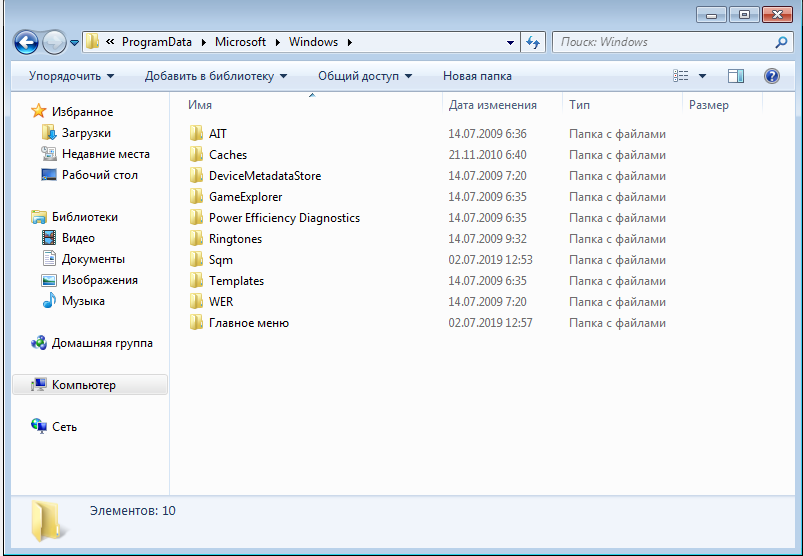
1. По пути HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run файлов нет



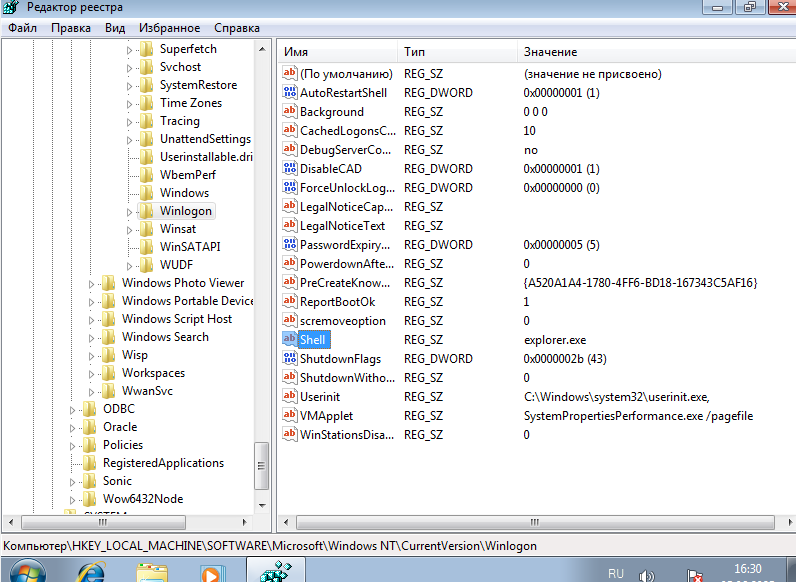
В папке %appdata% найдены следы Miner, файл Helper является частью Miner



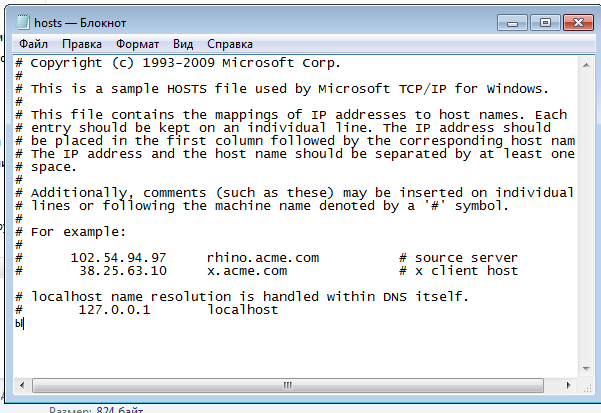
В паке ProgramData отсутствует автозагрузка



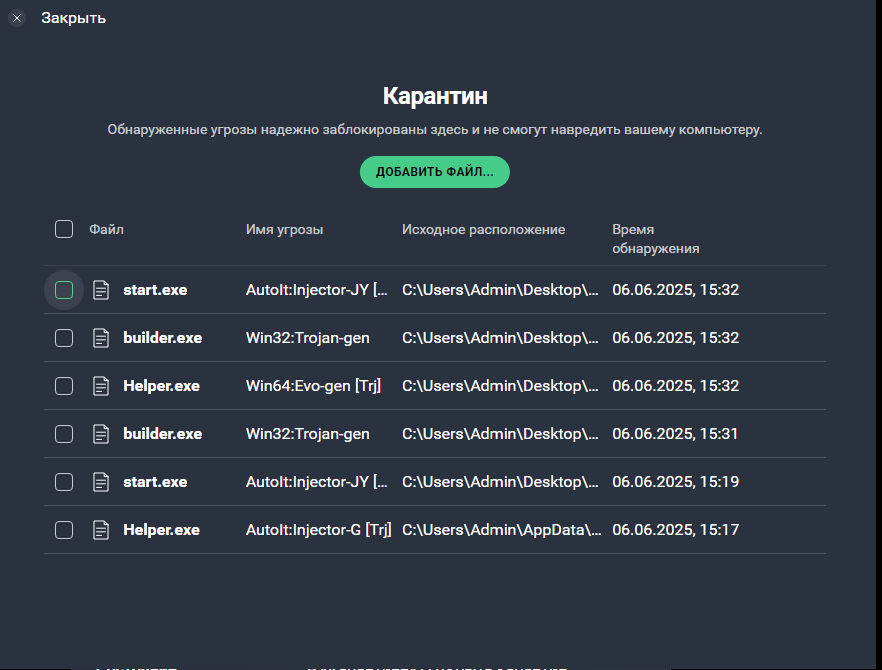
В параметре Shell значение «explorer.exe» ни на что не заменено, а также в параметре Userinit все осталось без изменений



По пути: C:\windows\system32\drivers\etc\hosts никаких следов не обнаружено

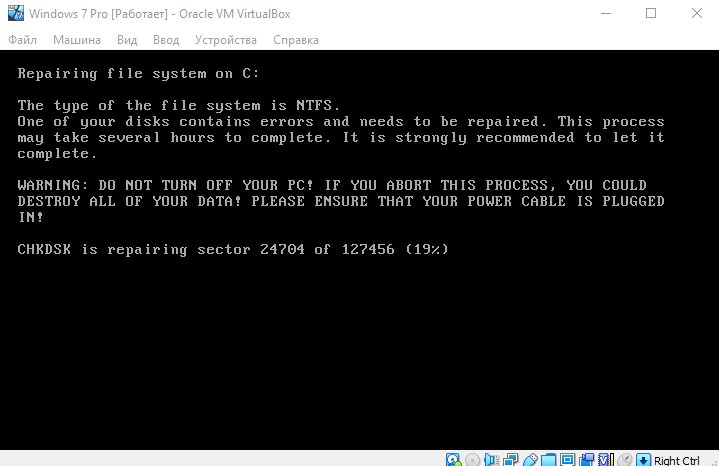


Антивирус обнаружил все файлы вирусов и переместил их в карантин:

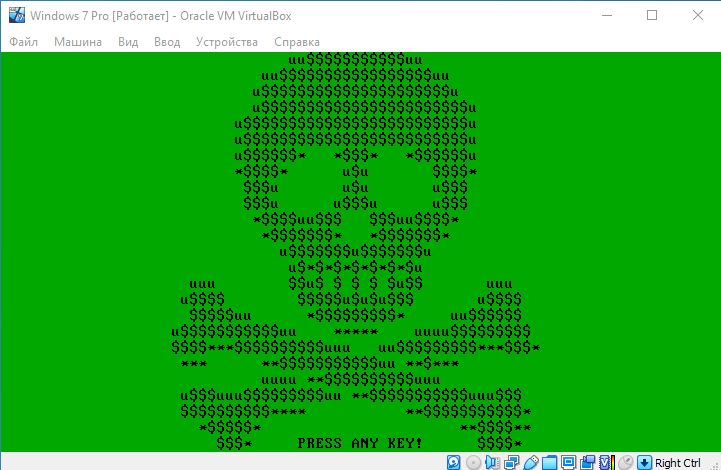


**Petya**

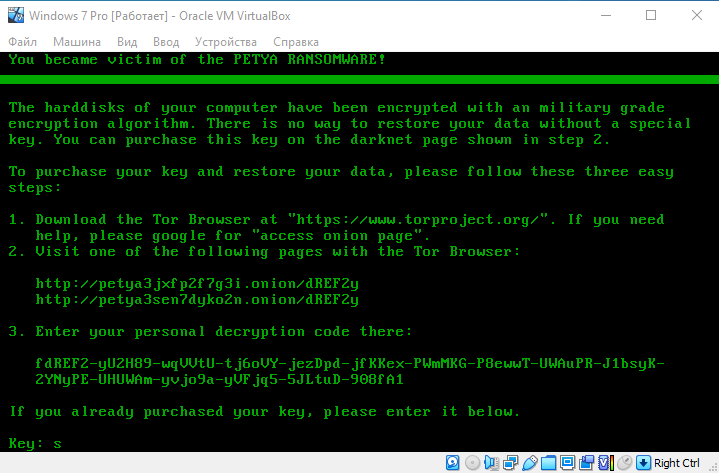
Атака от Petya:

****

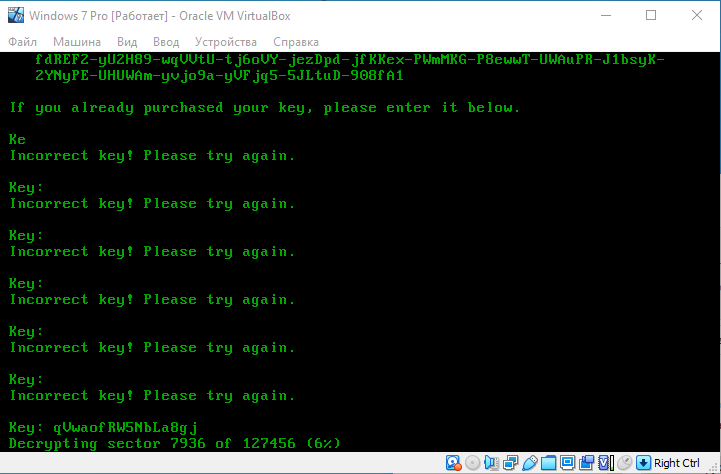
Petya завершил шифрование всех файлов:



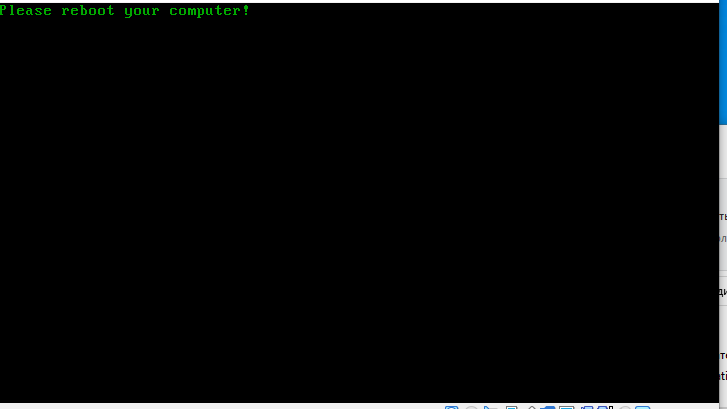
Petya вывел экран с инструкцией для расшифровки данных:



Petya начал расшифровку файлов (после ввода ключа):

****

Petya сломал загрузчик

****

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

**Вывод:** в результате работы были выявлены особенности поведения вирусов WinLocker, Petya и Miner, зафиксированы их воздействия на систему и опробованы способы обнаружения и устранения последствий.