Министерство Образования, Культуры и Исследований Технический Университет Молдовы Департамент Программной Инженерии и Автоматики

**ОТЧЕТ**

Лабораторная работа №1

По предмету: **PMRI**

**Тема: Analiza unui fisier malitios**

Выполнил студент гр.SI-212: Решетников Максим

Проверил: Mitu Catalin

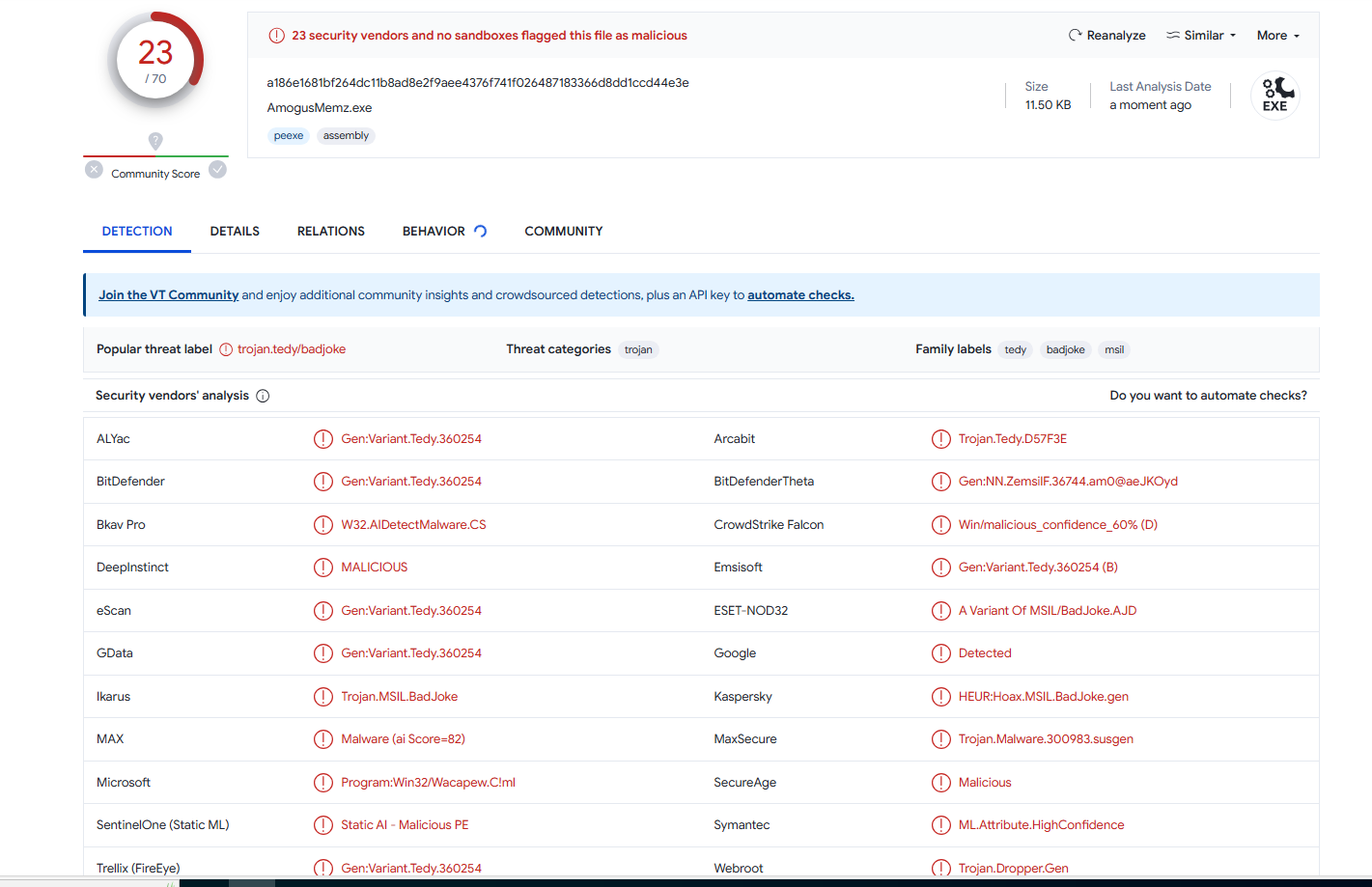
Кишинев 2024 г.

# Анализ

Анализ вируса – AmogusMemz.exe

Программа является исполняемым файлом – exe

Тип вируса – Trojan, Bad Joke.

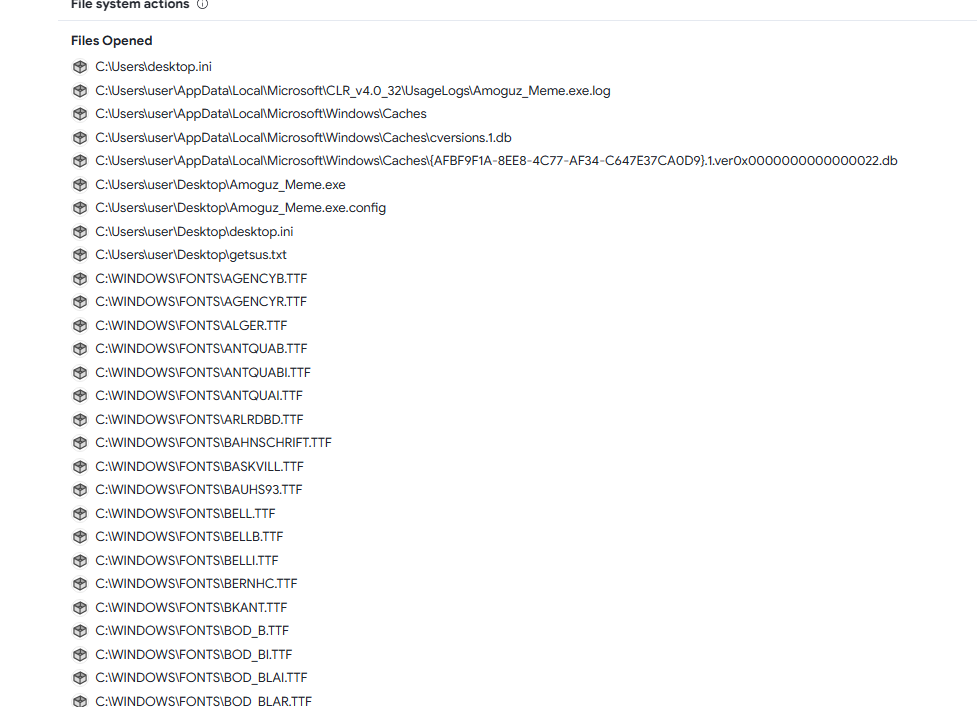


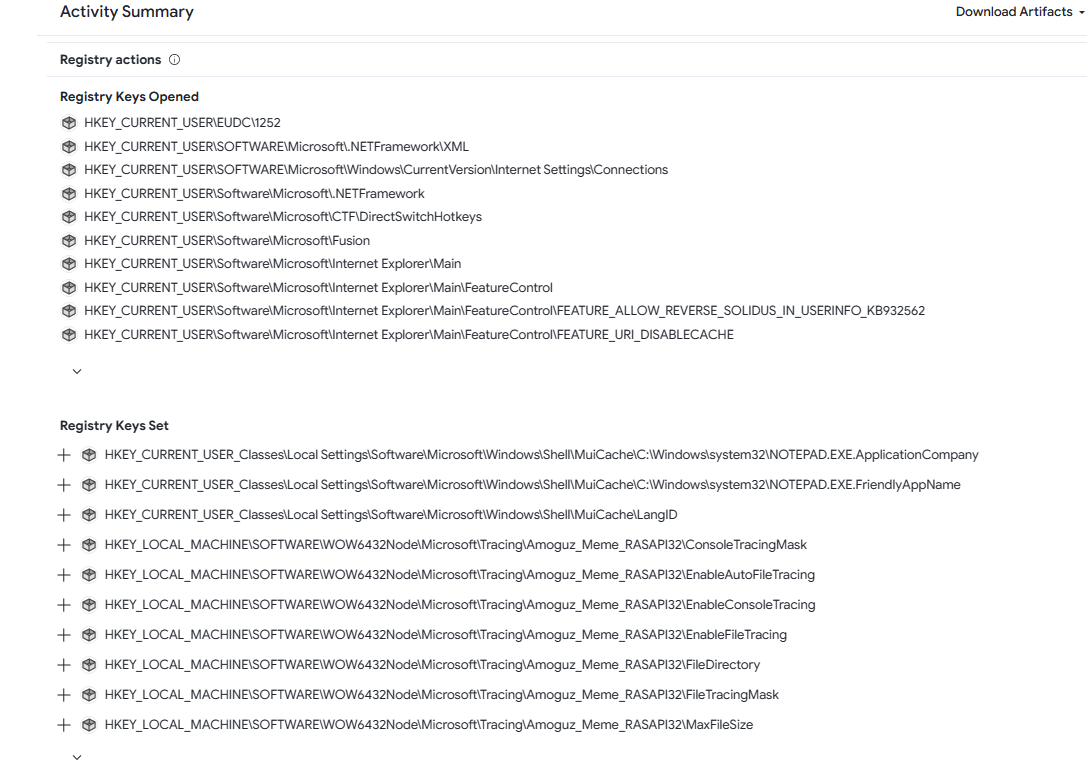
Программа написана на C# / .Net

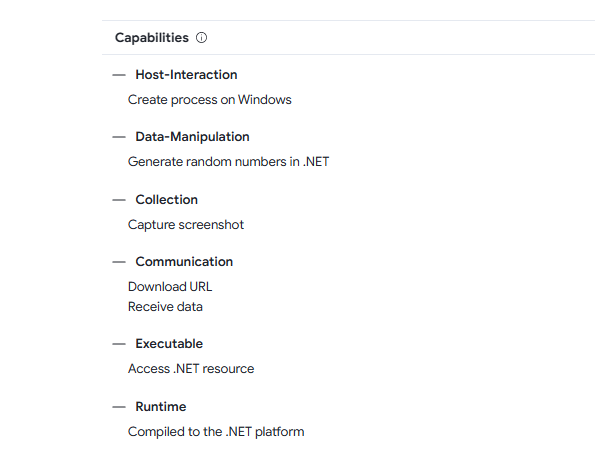
Целью заражения являются компьютеры с процессором Intel 386 и старше.

Доказательство почему Вирус именно троян:

1. Создание файлов без согласия пользователя;
2. Запуск файлов без согласия пользователя;
3. Запуск процессов без уведомления;
4. Отправка запроса в Интернет;
5. Скачивание файлов из Интернета;
6. Изменение изображения экрана;
7. Появление сообщений на экране;
8. Включение таймеров.

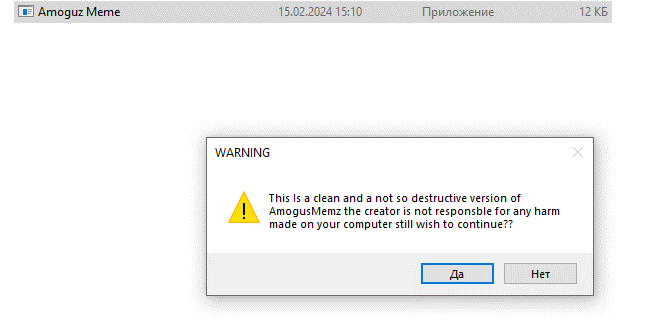
Затрагиваемые файлы

Затронутые регистры системы

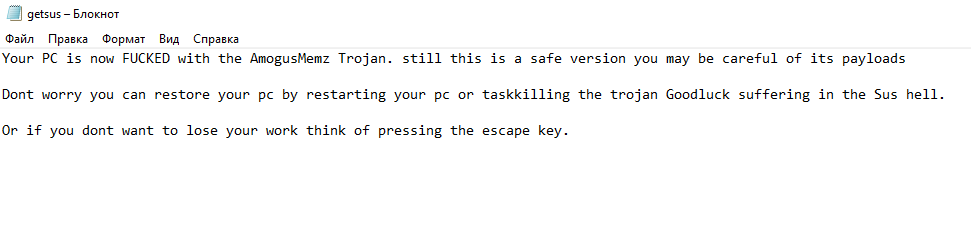
Возможности вируса`

# Действия вируса

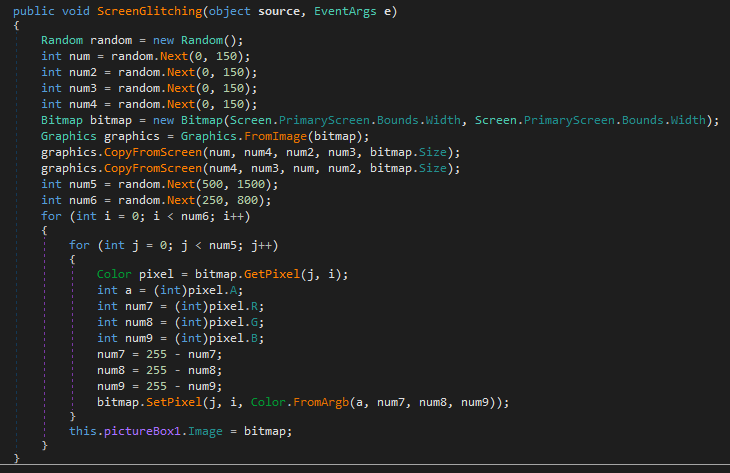
При запуске программы выдает окно WindowsForms с предупрежденем

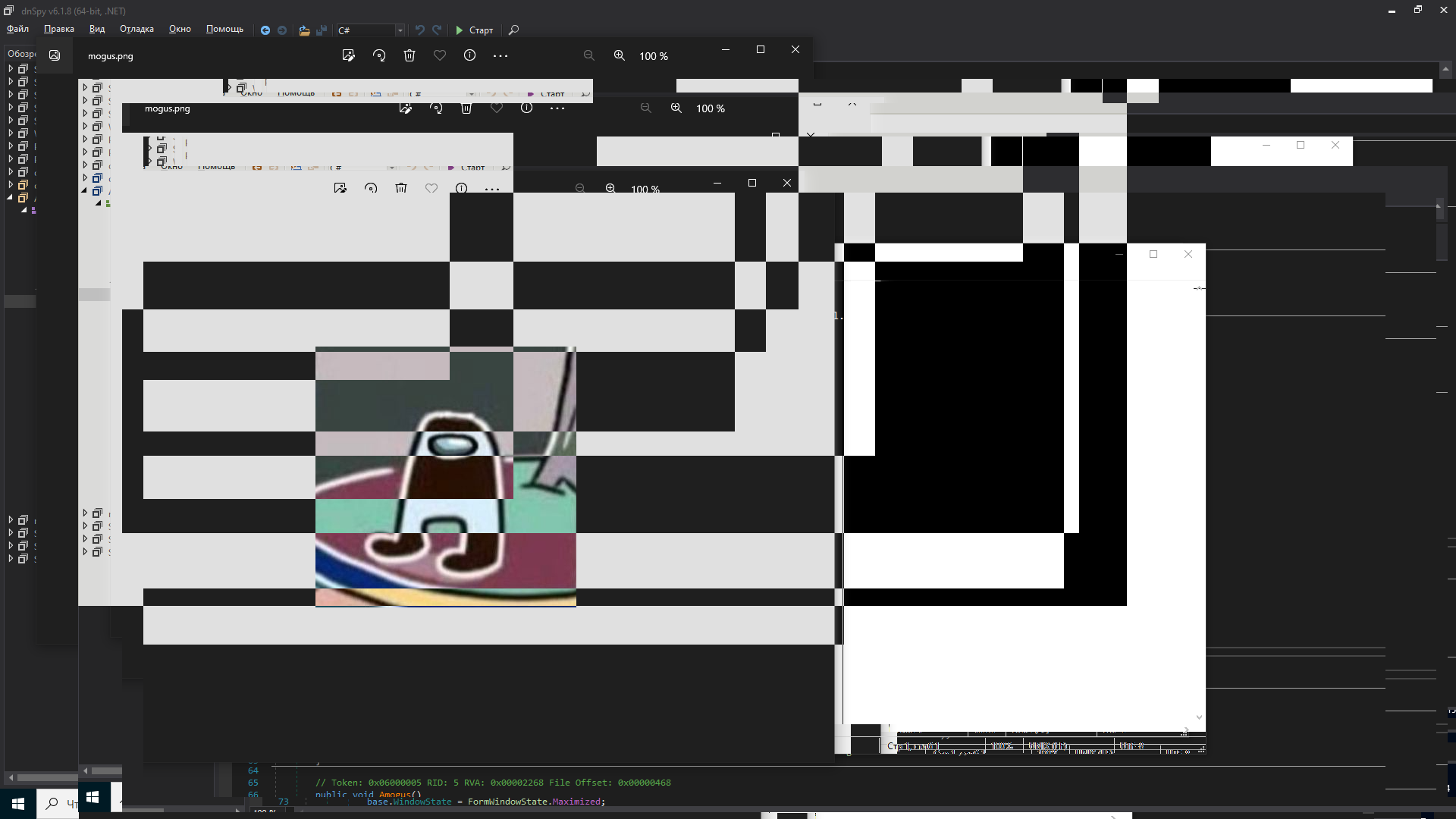


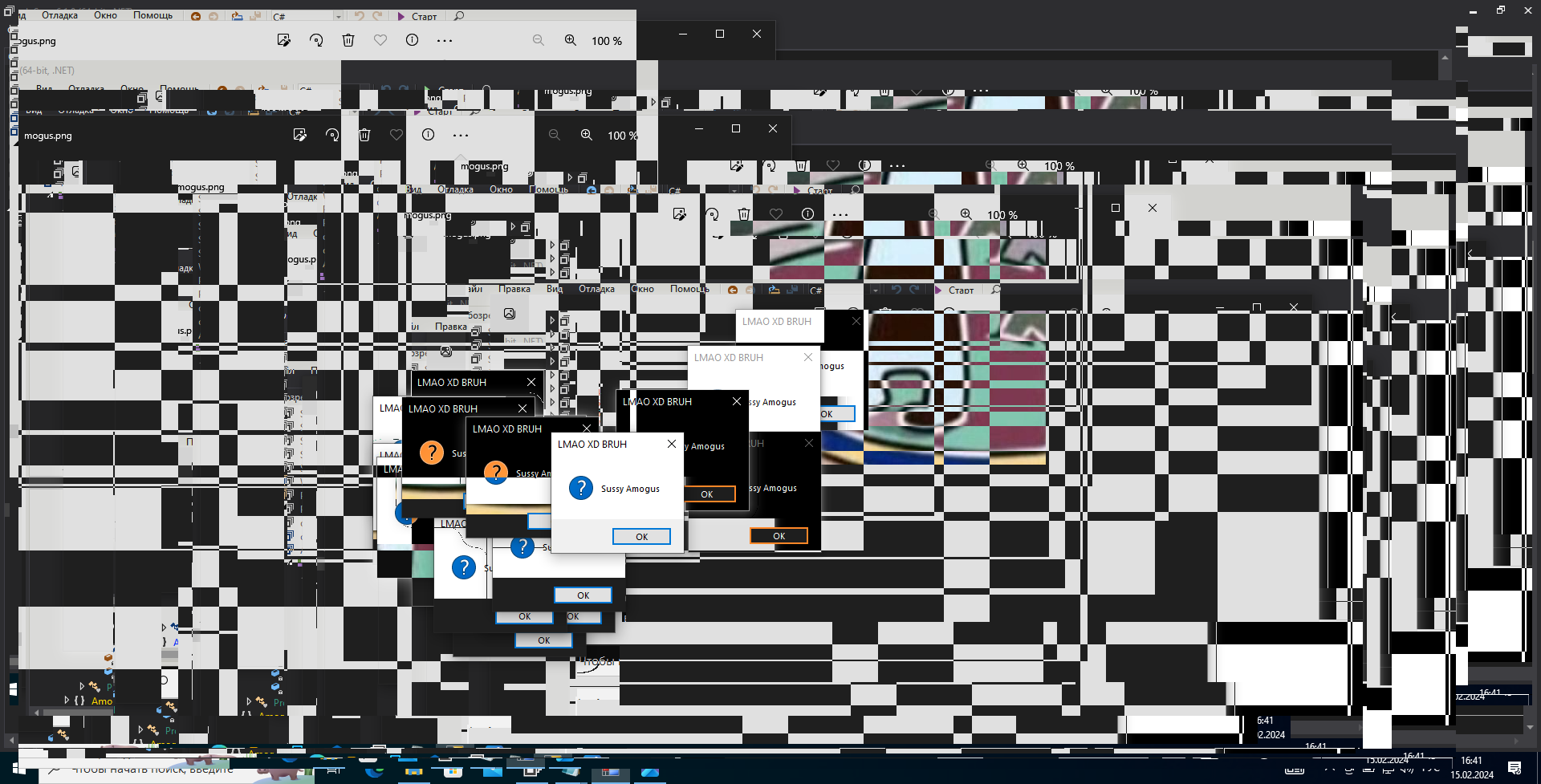
После подтверждения создает текстовый файл с пояснением как отключить вирус.



И с сайта скачивает в папку с нахождением .exe файла скачивает каритнку 



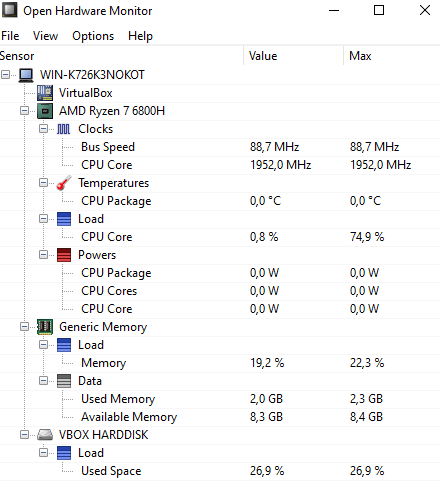
Создает 4 точки в поле экрана и с экрана копируются изображения с определенной части экрана и вставляются на другую случайно выбранную часть. Делает это дважды. Потом в цикле создает 2 точки и инвентирует в них цвета и обновляет экран.

При дальнейшем запуске программы выдается текст и глюки усиливаются

При запуске процесса создается 3 таймера для показа сообщений, глюков экрана и повторных запусках картинки каждые 60 секунд.

Вирус не имеет таймера на повторный запуск, не вписывает себя в autorun, и не вредит системе кроме как создавая визуальные глюки.

Статистика устройства до включения вируса



Статистика после

