Лабораторная работа №1
«Исследование bat-вирусов»
1 балл

Ход работы.

1. Представить схему алгоритма работы заданного эмулятора.
2. Типы заражаемых файлов.
3. Определить возможность повторного заражения.
4. Оценить степень опасности.
5. Предложить 3 сигнатуры для обнаружения (от 6 до 8 байт). Написать YARA-правила и продемонстрировать успешность обнаружения.
6. Предложить варианты защиты (при отсутствии AV).
7. Написать программу, которая в заданной директории ищет данные сигнатуры в файлах с различными расширениями. Указать - сколько сигнатур обнаружено в файле.
8. (*) Описать функциональные возможности и принцип работы антивируса ClamAV, развернуть ClamAV (https://github.com/Cisco-Talos/clamav) и интегрировать необходимые сигнатуры для поиска по ним.

Выполнение пункта (*) не является обязательным и позволяет заработать дополнительный балл.