**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное бюджетное образовательное**

**учреждение высшего образования**

**«Санкт-Петербургский государственный университет телекоммуникаций**

**им. проф. М. А. Бонч-Бруевича»**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Кафедра «Защищенные системы связи»

Дисциплина «Компьютерные вирусы»

# Лабораторная работа № 1

**«Malware Detection and Removal»**

Выполнил: Громов А.А.

Миколаени М.С.

ИКТЗ-83

Проверил: Косов Н. А.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Санкт-Петербург

2021

**Пункт 1. Yara**

Первым делом с помощью документации yara. Мы написали правило для отлова eicar.



Рис.1 - Правило для yara

Вот что нашлось:

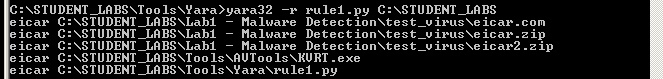


Рис.2 - Найденные текстовые файлы

На выше представленном выводе было несколько false positive. По этой причине сузили поиск.

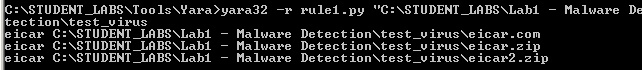


Рис. 3 - Сузили поиск

**Пункт 2. Криптолокер X.exe.**

В папке cryptors были найдены 2 вируса. По заданию необходимо поменять расширение у файла X.ex\_ на X.exe. Это было выполнено с помощью Total commander.



Рис. 4 - Поменяли расширение

После запуска X.exe все файлы были зашифрованы



Рис. 5 - Файлы зашифрованы

Для расшифрования требовался пароль

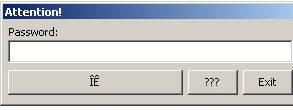


Рис.6 - Пароль

Было загуглено расширение enciphered. Таким образом мы начали догадываться, что это xorist.



Рис. 7 - Расширения

Закинув на сайт virustotal файл x.exe мы подтвердили наши догадки.

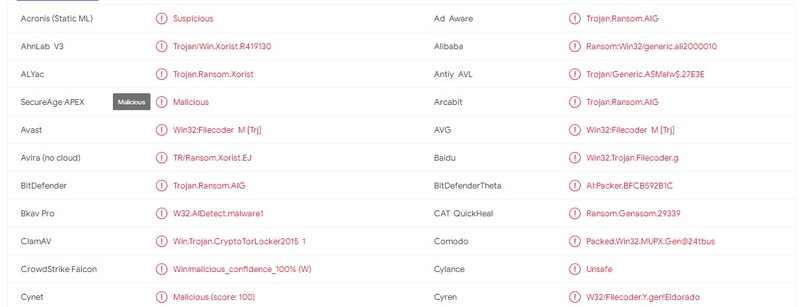


Рис. 8 – Virustotal считает, что это вирус

В папке decruptors был найден необходимый декриптор от Касперского.



Рис. 9 - Отработал декриптор

**Пункт. 3. Поиска ключа для дешифрования.**

С гугл-диска были скачены файлы. Открыв текстовый файл, мы решили загуглить текст, появившийся после шифрования диска. После чего мы пришли к выводу, что это nemucod.

В папке decryptors есть программа для расшифровки nemucod. Так как файлы у нас зашифрованы RSA 1024, для расшифровки необходимо знать ключ. Для расшифровки 2222.jpg сначала надо перетащить 2 файла: 1111.jpg и зашифрованный 1111.jpg. Программа вычислит ключ и после предложит выбрать наш зашифрованный файл 2222.jpg



Рис. 10 - Ключ

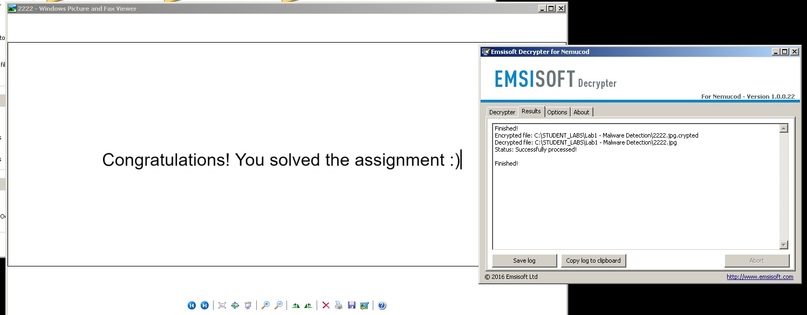


Рис. 11 - Расшифрованый 2222

**Пункт 4. ILSpy.**

В данном пункте нам требовалось декомпилировать вирус D.exe.

С помощью программы ILSpy мы восстановили код программы, после чего начали поиск. Решили поискать по ключевым словам – key, sha, md5, crypto. Первоначально была найдена функция createKey и рядом с ней createIV. Перешли на уровень выше и нашли пароли. По программе было ясно, что этот пароль хэшируется с помощью sha-512. При помощи питона был найден хэш. Зная ключ и инициализирующий вектор, появилась возможность расшифровать файл. Файл был зашифрован алгоритмам aes256-cbc.

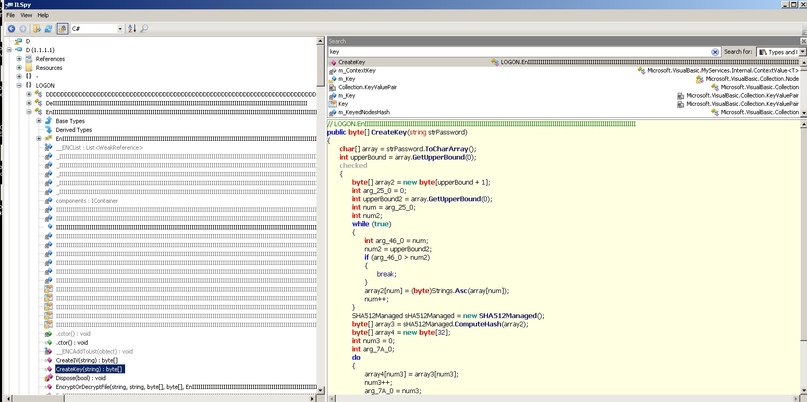


Рис. 12 - ILSpy



Рис. 13 - createIV



Рис. 14 - createKey



Рис. 15 - Найденные ключи

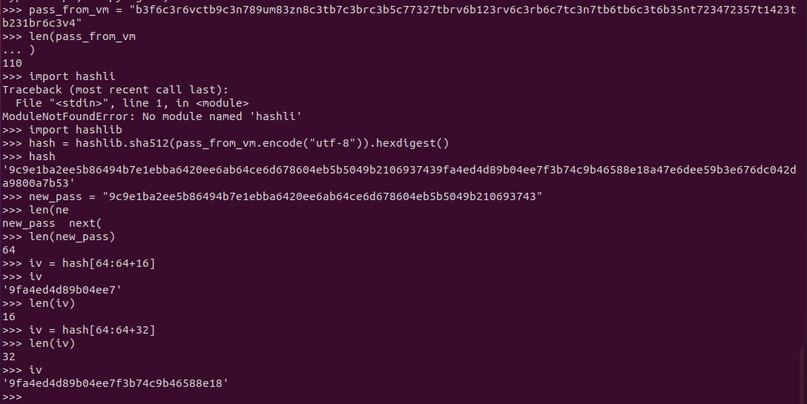


Рис. 16 - Хэш

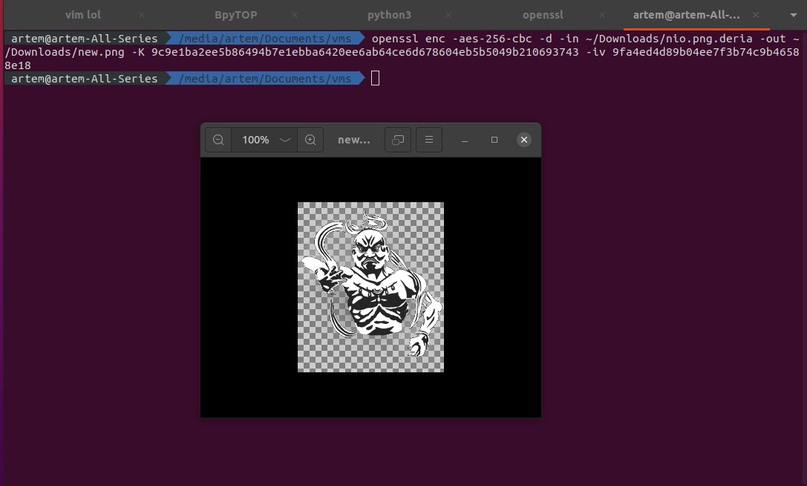


Рис. 17 – Полученное фото

**Вывод**

В ходе выполнения данной лабораторной работы были изучены основы использования ПО Yara, ILSpy. А также изучение работы вирусов.