**МИНОБРНАУКИ РОССИИ**
**САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ**
**ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**
**«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)**
**Кафедра информационной безопасности**

# ОТЧЕТ

**по практической работе №1**

**по дисциплине «Введение в специальность»**

**Тема: Создание сигнатуры для свободного антивирусного ПО ClamAV**

Студент гр. 8363 _____ Нерсисян А.С.

Преподаватель _____ Халиуллин Р.А.

Санкт-Петербург

2020

## 1. Задание для практической работы

Необходимо выделить сигнатуру из безопасного исполняемого файла формата PE (Portable Executable) по выбору студента и создать файл с пользовательской сигнатурой для антивирусного ПО ClamAV. Созданная сигнатура должна обеспечивать детектирование выбранного исполняемого файла без ложных срабатываний (false positives).

## 2. Описание процесса выполнения практической работы

Для работы был выбран безопасный исполняемый файл AgentService.exe формата PE (Portable Executable) из директории C:\\Window\System32. Для выделения сигнатуры был использован hex-редактор Hex Editor Neo. Выделенная сигнатура представлена на рисунке 1.

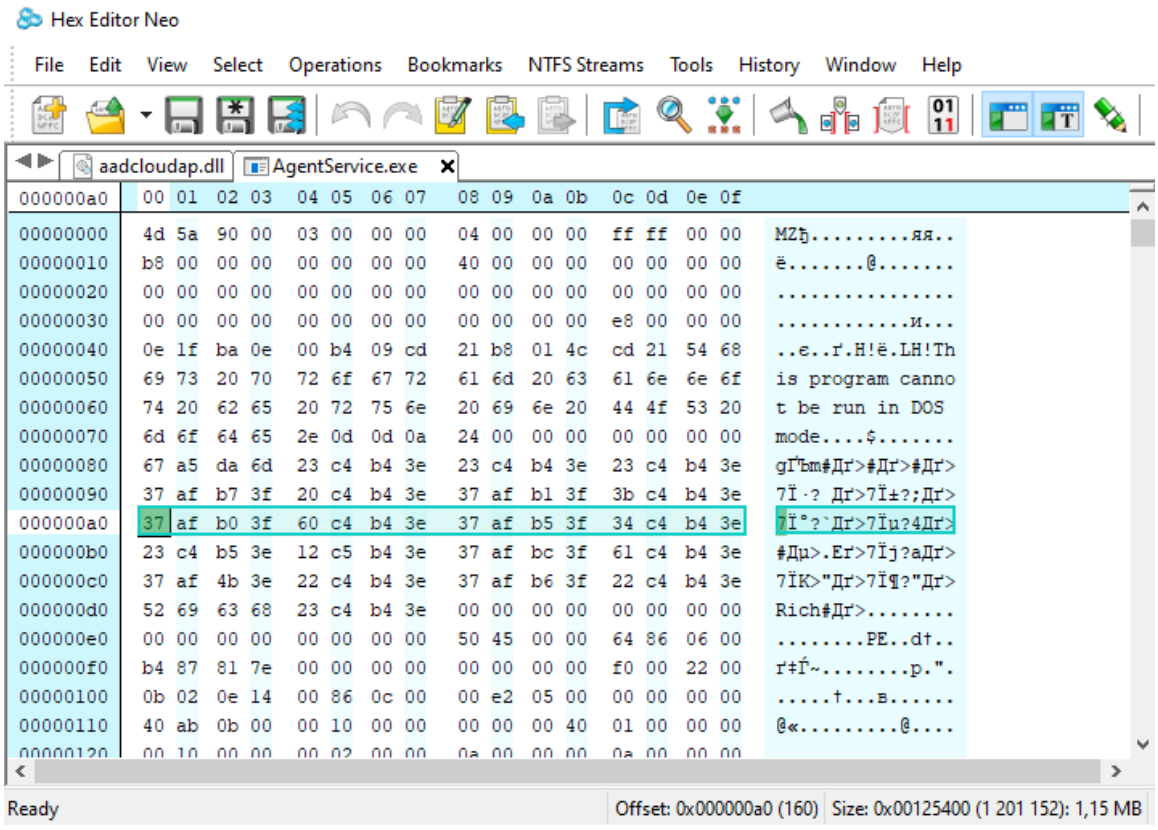


Рисунок 1 — Выделенная сигнатура из безопасного файла

Для выделения сигнатуры открыл в hex-редакторе Hex Editor Neo исполняемый файл AgentService.exe формата PE (Portable Executable), выделил

16-байт шестнадцатеричного кода и скопировал в буфер обмена. Далее создал файл с расширением .ndb, открыл его в текстовом редакторе Microsoft Visual Studio Code и согласно структуре ndb-файла написал имя, тип и другие данные сигнатуры. Содержимое формата сигнатуры представлен на рисунке 2.

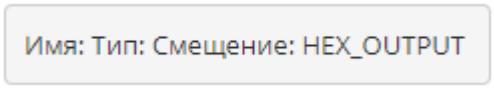


Рисунок 2 – Содержимое ndb-файла

Полученная сигнатура представлена на рисунке 3.

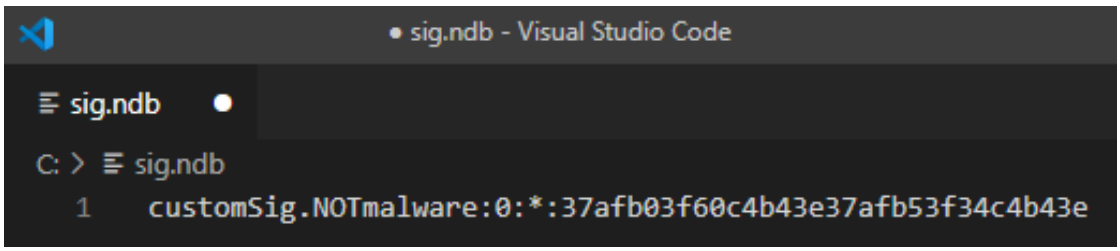


Рисунок 3 – Полученная сигнатура

Имя сигнатуры: `customSig.NOTmalware`

Тип: `0` (любой)

Смещение: `*` (любое)

HEX-OUTPUT: `37afb03f60c4b43e37afb53f34c4b43e`

Далее скачиваем базу вирусных сигнатур "main.cvd". Используя файловой менеджер 7-zip откроем файл "main.cvd". На рисунке 4 показано содержимое файла "main.cvd".

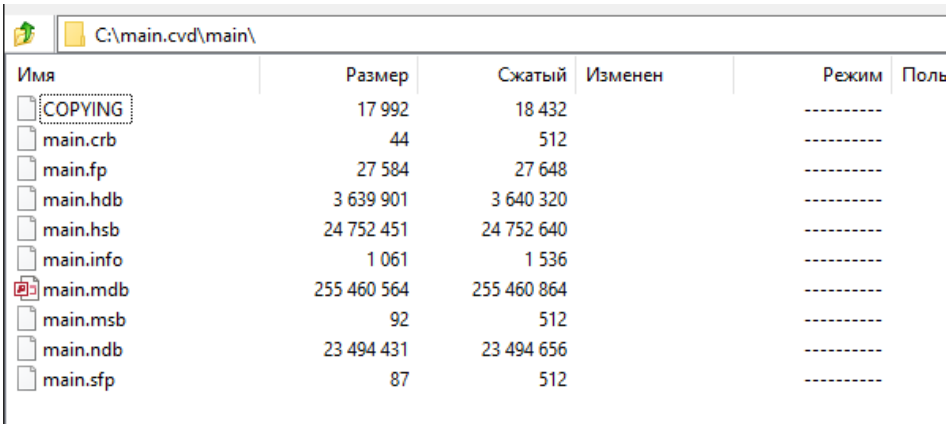


Рисунок 4 – Содержимое файла "main.cvd".

Теперь добавляем в вирусную базу main.ndb выделенную сигнатуру, открыв ее с помощью текстового редактора. Результат добавления представлен на рисунке 5.

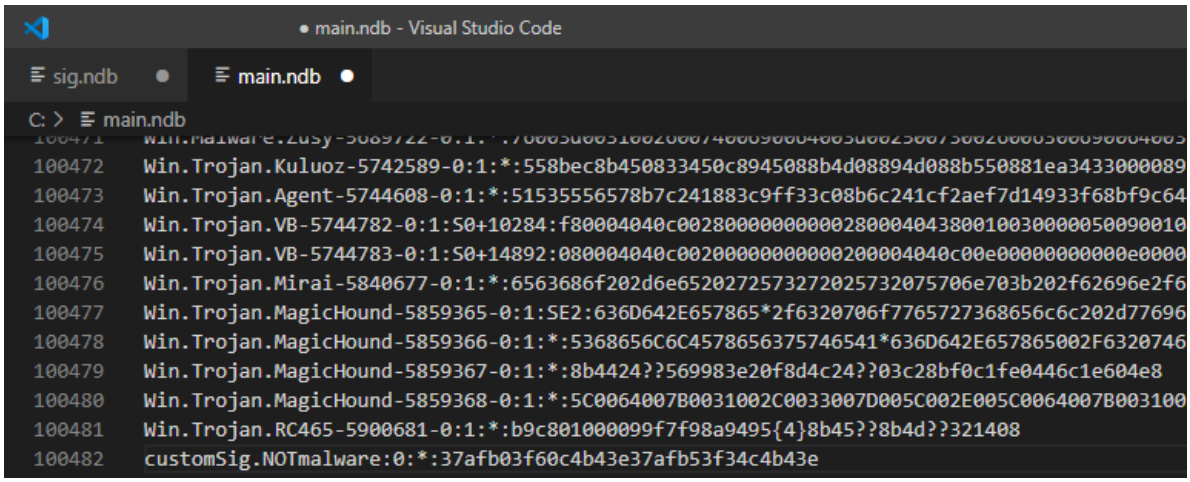


Рисунок 5 – Список сигнатур после добавления собственной сигнатуры

Сохраняем и копируем файл main.ndb в директорию, где установлен антивирус ClamAV:

```
C:\Program Files\ClamAV\
```

### 3. Результаты выполнения практической работы

Для удобства направим вывод результатов сканирования в текстовый файл с помощью команды представленной ниже:

```
clamscan.exe -d main.ndb >> scanlog.txt
```

Результаты сканирования были направлены в текстовой файл "scanlog.txt". Содержимое текстового файла представлен в листинге 1.

C:\Program Files\ClamAV\AgentService.exe: customSig.NOTmalware.UNOFFICIAL FOUND
C:\Program Files\ClamAV\clam.ico: OK
C:\Program Files\ClamAV\clambc.exe: OK
C:\Program Files\ClamAV\clamconf.exe: OK
C:\Program Files\ClamAV\clamd.conf: OK
C:\Program Files\ClamAV\clamd.exe: OK
C:\Program Files\ClamAV\clamdscan.exe: OK
C:\Program Files\ClamAV\clamscan.exe: OK

C:\Program Files\ClamAV\clamsubmit.exe: OK

C:\Program Files\ClamAV\freshclam.conf: OK

C:\Program Files\ClamAV\freshclam.exe: OK

C:\Program Files\ClamAV\json-c.dll: OK

C:\Program Files\ClamAV\libbz2.dll: OK

C:\Program Files\ClamAV\libclamav.dll: OK

C:\Program Files\ClamAV\libclamunrar.dll: OK

C:\Program Files\ClamAV\libclamunrar_iface.dll: OK

C:\Program Files\ClamAV\libcrypto-1_1-x64.dll: OK

C:\Program Files\ClamAV\libcurl.dll: OK

C:\Program Files\ClamAV\libfreshclam.dll: OK

C:\Program Files\ClamAV\libssh2.dll: OK

C:\Program Files\ClamAV\libssl-1_1-x64.dll: OK

C:\Program Files\ClamAV\libxml2.dll: OK

C:\Program Files\ClamAV\main.ndb: OK

C:\Program Files\ClamAV\mspack.dll: OK

C:\Program Files\ClamAV\mysig.ndb: OK

C:\Program Files\ClamAV\nghttp2.dll: OK

C:\Program Files\ClamAV\pcre2-8.dll: OK

C:\Program Files\ClamAV\pthreadVC2.dll: OK

C:\Program Files\ClamAV\README.md: OK

C:\Program Files\ClamAV\scanlog.txt: OK

C:\Program Files\ClamAV\sigtool.exe: OK

C:\Program Files\ClamAV\unins000.dat: OK

C:\Program Files\ClamAV\unins000.exe: OK

---------- SCAN SUMMARY ----------

Known viruses: 100320

Engine version: 0.102.1

Scanned directories: 1

Scanned files: 34

Infected files: 1

Data scanned: 38.10 MB

Data read: 38.59 MB (ratio 0.99:1)

Time: 3.777 sec (0 m 3 s)

Листинг 1 – Результат сканирования

Как видим, при сканировании сообщается об обнаружении зараженного файла и выведено название вредоносного ПО. Также представлены результаты тестирования на любых других файлах и продемонстрировано отсутствие ложных срабатываний (false positives) антивирусного ПО ClamAV.

**Заключение**

В рзультате выполнения данной практической работы научились выделить сигнатуру из безопасного исполняемого файла формата PE (Portable Executable) и создать файл с пользовательской сигнатурой для антивирусного ПО ClamAV. Созданная сигнатура обеспечивало детектирование выбранного исполняемого файла без ложных срабатываний (false positives).

**Приложение 1. Исходный код**

Содержимое ndb-файла:

```
customSig.NOTmalware:0:*:37afb03f60c4b43e37afb53f34c4b43e
```

Использованная команда:

```
clamscan.exe -d main.ndb >> scanlog.txt
```