МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение

высшего образования

«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»

ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ

Кафедра компьютерной инженерии и моделирования

Расследование вредоносных программ в REMnux

Отчет по лабораторной работе 1

по дисциплине «**Информационная безопасность**»

студента 3 курса группы ИВТ-б-о-202

Шор Константина Александровича

Направления подготовки 09.03.01«Информатика и вычислительная техника»

Симферополь, 2023

File

```
remnux@remnux:~/Downloads$ file d1d04ea545fb3b5028dbc6f362928a4ce78ea7
0400c40afe6c332c44559f83ab.exe
d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe:
PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
```

```
remnux@remnux:~/Downloads$ file e2a68f7a348b8b2598f0c8baa29aeafd5c5ec4
d0f703120be1eca3f6e68be12c.xls
e2a68f7a348b8b2598f0c8baa29aeafd5c5ec4d0f703120be1eca3f6e68be12c.xls:
Composite Document File V2 Document, Little Endian, Os: Windows, Versi
on 10.0, Code page: 1251, Author: Dream, Last Saved By: RHRSDJTJDGHT,
Name of Creating Application: Microsoft Excel, Create Time/Date: Fri J
un  5 19:19:34 2015, Last Saved Time/Date: Sun Jun 12 19:21:36 2022, S
ecurity: 0
```

Yara-rules

```
remnux@remnux:~/Downloads$ yara-rules e2a68f7a348b8b2598f0c8baa29aeafd5c5ec4d0f703120be1eca3f6e68be1
2c.xls
remnux@remnux:~/Downloads$ yara-rules d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83
ab.exe
win_hook d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
network_smtp_dotNet d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
keylogger d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
Big_Numbers1 d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
NETexecutableMicrosoft d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
IsPE32 d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
IsNET_EXE d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
IsWindowsGUI d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
Microsoft_Visual_Studio_NET d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
Microsoft_Visual_C_v70_Basic_NET_additional d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44
559f83ab.exe
Microsoft_Visual_C_Basic_NET d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
Microsoft_Visual_Studio_NET_additional d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f8
3ab.exe
Microsoft_Visual_C_v70_Basic_NET d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.ex
e
NET_executable_ d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
NET_executable d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
remnux@remnux:~/Downloads$
```

Clamscan

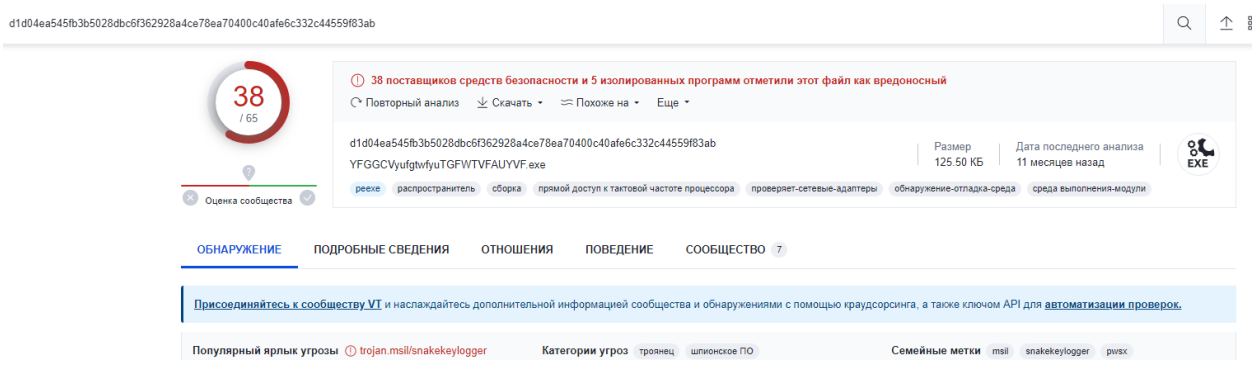
```
remnux@remnux:~/Downloads$ clamscan d1d04ea545fb3b5028dbc6f362928a4ce7
8ea70400c40afe6c332c44559f83ab.exe
d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe:
Win.Malware.Snake-9953539-0 FOUND
```

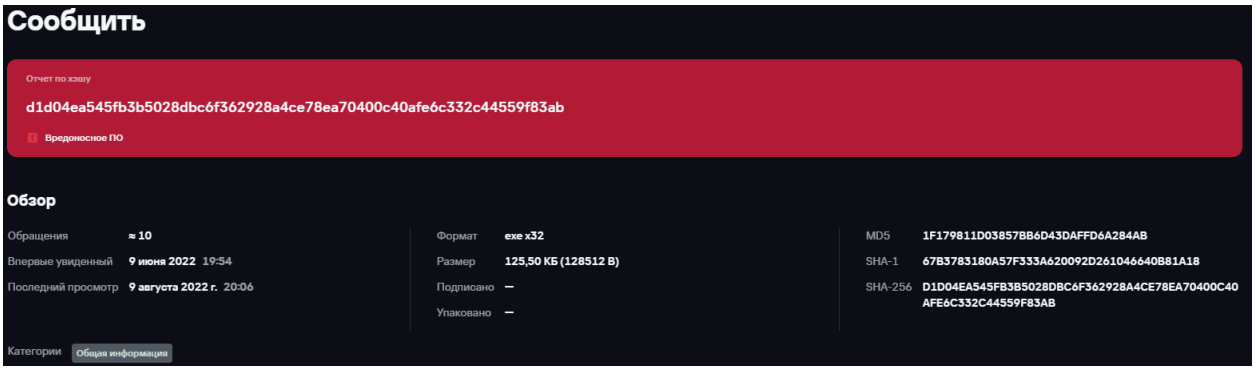
```
remnux@remnux:~/Downloads$ clamscan e2a68f7a348b8b2598f0c8baa29aeafd5
5ec4d0f703120be1eca3f6e68be12c.xls
e2a68f7a348b8b2598f0c8baa29aeafd5c5ec4d0f703120be1eca3f6e68be12c.xls:
OK
```

PEframe

```
remnux@remnux:~/Downloads$ peframe d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
XLMMacroDeobfuscator: pywin32 is not installed (only is required if you want to use MS Excel)


------------------------------------------------------------------------------
File Information (time: 0:00:01.281736)
------------------------------------------------------------------------------
filename          d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
filetype          PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Wi
filesize          128512
hash sha256       d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab
virustotal        /
imagebase         0x400000
entrypoint        0x1ff2e
imphash           f34d5f2d4577ed6d9ceec516c1f5a744
datetime          2022-04-26 23:43:30
dll               False
directories       import, tls, resources, relocations
sections          .text, .rsrc, .reloc
features          packer, crypto
```





```
remnux@remnux:~/Downloads$ peframe e2a68f7a348b8b2598f0c8baa29aeafd5c5ec4d0f703120be1eca3f6e68be12c.xls
XLMMacroDeobfuscator: pywin32 is not installed (only is required if you want to use MS Excel)


-------------------------------------------------------------------------------
File Information (time: 0:00:05.440266)
-------------------------------------------------------------------------------
filename          e2a68f7a348b8b2598f0c8baa29aeafd5c5ec4d0f703120be1eca3f6e68be12c.xls
filetype          Composite Document File V2 Document, Little Endian, Os: Windows
filesize          61952
hash sha256       e2a68f7a348b8b2598f0c8baa29aeafd5c5ec4d0f703120be1eca3f6e68be12c
virustotal        /
```