

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 d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe:
PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
```

```
remnux@remnux:~/Downloads$ file e2a68f7a348b8b2598f0c8baa29aeafd5c5ec4d0f703120beleca3f6e68be12c.xls
e2a68f7a348b8b2598f0c8baa29aeafd5c5ec4d0f703120beleca3f6e68be12c.xls:
Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: Dream, Last Saved By: RHRSDJTJDGHT, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Sun Jun 12 19:21:36 2022, Security: 0
```

Yara-rules

```
remnux@remnux:~/Downloads$ yara-rules e2a68f7a348b8b2598f0c8baa29aeafd5c5ec4d0f703120beleca3f6e68be12c.xls
remnux@remnux:~/Downloads$ yara-rules d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.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 d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
Microsoft_Visual_C_Basic_NET d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
Microsoft_Visual_Studio_NET_additional d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
Microsoft_Visual_C_v70_Basic_NET d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
NET_executable d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
NET_executable d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab.exe
remnux@remnux:~/Downloads$
```

Clamscan

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

```
remnux@remnux:~/Downloads$ clamscan e2a68f7a348b8b2598f0c8baa29aeafd5c5ec4d0f703120beleca3f6e68be12c.xls
e2a68f7a348b8b2598f0c8baa29aeafd5c5ec4d0f703120beleca3f6e68be12c.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    0x1fff2e
imphash       f34d5f2d4577ed6d9ceec516c1f5a744
datetime      2022-04-26 23:43:30
dll           False
directories     import, tls, resources, relocations
sections      .text, .rsrc, .reloc
features      packer, crypto
```

38 / 65

Оценка сообщества

38 поставщиков средств безопасности и 5 изолированных программ отметили этот файл как вредоносный

Повторный анализ | Скачать | Похоже на | Еще

d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab

YFGGCYufgtwfyuTGFWTVFAUYVF.exe

Размер

125.50 КБ

Дата последнего анализа

11 месяцев назад

EXE

peexe

распространитель

оборка

прямой доступ к тактовой частоте процессора

проверяет сетевые адаптеры

обнаружение отладки-среда

среда выполнения-модули

ОБНАРУЖЕНИЕ

ПОДРОБНЫЕ СВЕДЕНИЯ

ОТНОШЕНИЯ

ПОВЕДЕНИЕ

СООБЩЕСТВО 7

Присоединяйтесь к сообществу VT и наслаждайтесь дополнительной информацией сообщества и обнаружениями с помощью краудсорсинга, а также ключом API для автоматизации проверок.

Популярный ярлык угрозы

trojan.msl/snakekeylogger

Категории угроз

троянец

шпионское ПО

Семейные метки

msl

snakekeylogger

pwix

Сообщить

Отчет по жалобе

d1d04ea545fb3b5028dbc6f362928a4ce78ea70400c40afe6c332c44559f83ab

Вредоносное ПО

Обзор

Обращения

≈ 10

Впервые увиденный

9 июня 2022 19:54

Последний просмотр

9 августа 2022 г. 20:06

Формат

exe x32

Размер

125,50 КБ (128512 Б)

Подписано

—

Упаковано

—

MD5

1F179811D03857BB6D43DAFFD6A284AB

SHA-1

67B3783180A57F333A620092D261046640B81A18

SHA-256

D1D04EA545FB3B5028DBC6F362928A4CE78EA70400C40AFE6C332C44559F83AB

Категории

Общая информация

```
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    /
```

31
157

Оценка сообщества

31 поставщик средств безопасности и 3 изолированных хранилища отметили этот файл как вредоносный

Повторный анализ | Скачать | Похоже на | Еще

e2a68f7a348b8b2598f0c8baa29aeafd5c5ec4d0f703120be1eca3f6e68be12c

51849189224252789195825550.xls

Размер

60,50 КБ

Дата последнего анализа

11 месяцев назад

XLS

ОБНАРУЖЕНИЕ

ПОДРОБНЫЕ СВЕДЕНИЯ

ОТНОШЕНИЯ

ПОВЕДЕНИЕ

СООБЩЕСТВО 6

Присоединяйтесь к сообществу VT и наслаждайтесь дополнительной информацией сообщества и обнаружениями с помощью краудсорсинга, а также ключом API для автоматизации проверок.

Популярный ярлык угрозы

trojan.abracadabra/x97m

Категории угроз

тройнец

загрузчик

Семейные метки

абракадабра

x97m

emotet

Сообщить

Отчет по хэшу

e2a68f7a348b8b2598f0c8baa29aeafd5c5ec4d0f703120be1eca3f6e68be12c

Вредоносное ПО

Обзор

Обращения

≈ 100

Впервые увиденный

13 июня 2022 03:09

Последний просмотр

23 февраля 2023 01:28

Формат

xls

Размер

125,50 КБ (128512 B)

Подписано

—

Упаковано

—

MD5

99A08A7A25337BDC8D3F61967DF8C568

SHA-1

4D458E143F5C4E6316AB3C365375696754735AF7

SHA-256

E2A68F7A348B8B2598F0C8BAA29AEAFD5C5EC4D0F703120BE1ECA3F6E68BE12C

Категории

Общая информация