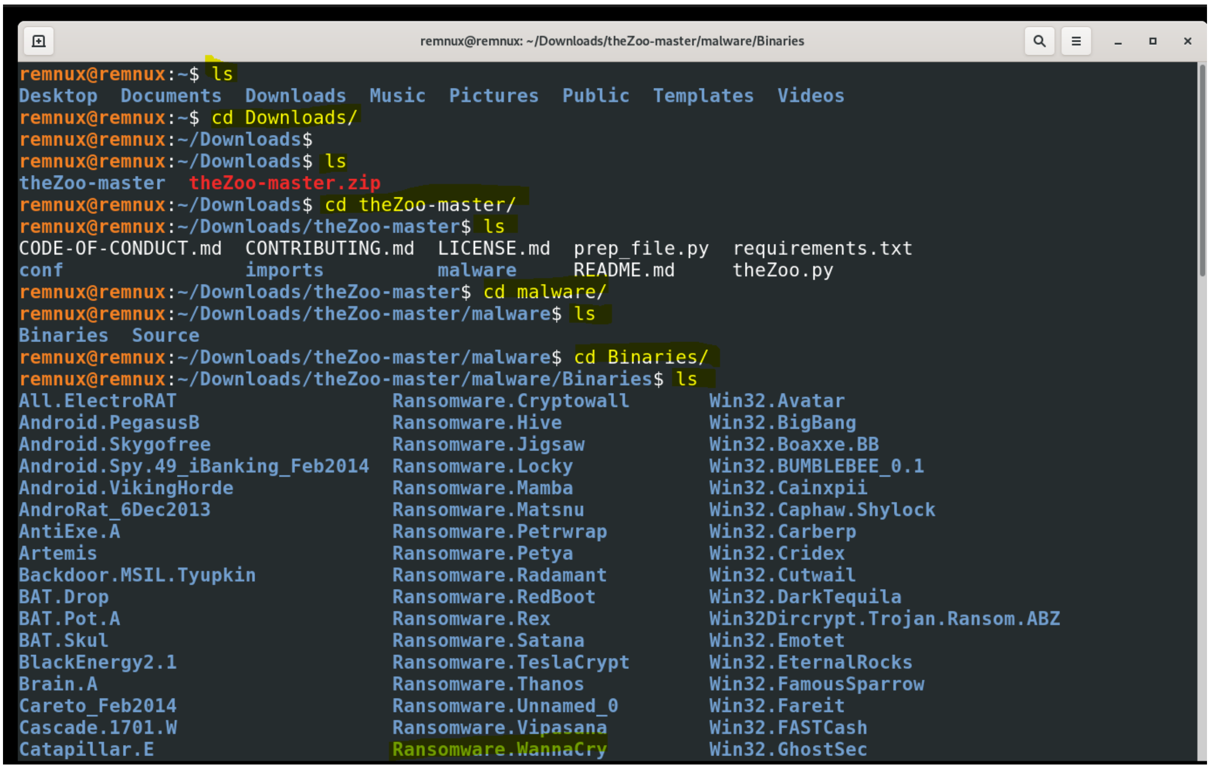
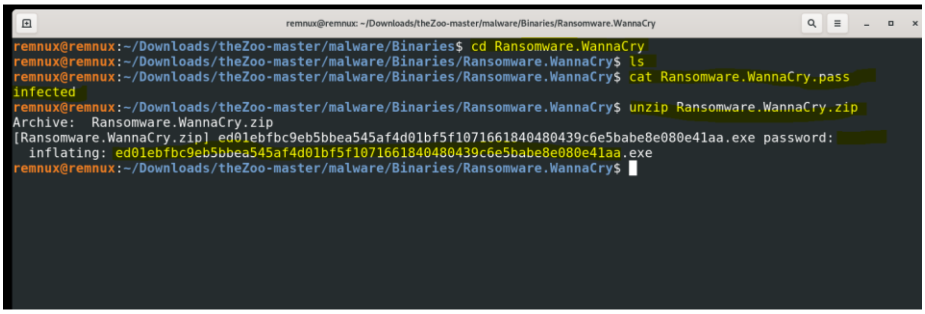
Static analysis using REMnux

- **Machine**: Launch the REMnux machine
- **Tools:** file and strings
- **Ransomware** – WannaCry
  - WannaCry is a ransomware worm that spread rapidly through across a number of computer networks in May of 2017. After infecting a Windows computer, it encrypts files on the PC's hard drive, making them impossible for users to access, then demands a ransom payment in bitcoin in order to decrypt them.
- Open the terminal and move to the location of the sample malware



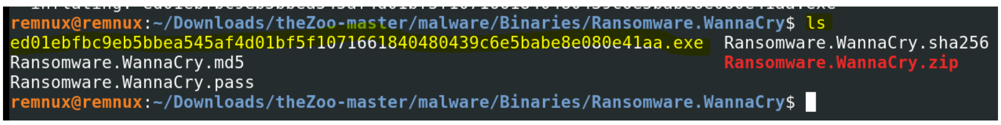
```
remnux@remnux:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
remnux@remnux:~$ cd Downloads/
remnux@remnux:~/Downloads$
remnux@remnux:~/Downloads$ ls
theZoo-master  theZoo-master.zip
remnux@remnux:~/Downloads$ cd theZoo-master/
remnux@remnux:~/Downloads/theZoo-master$ ls
CODE-OF-CONDUCT.md  CONTRIBUTING.md  LICENSE.md  prep_file.py  requirements.txt
conf                imports          malware     README.md     theZoo.py
remnux@remnux:~/Downloads/theZoo-master$ cd malware/
remnux@remnux:~/Downloads/theZoo-master/malware$ ls
Binaries  Source
remnux@remnux:~/Downloads/theZoo-master/malware$ cd Binaries/
remnux@remnux:~/Downloads/theZoo-master/malware/Binaries$ ls
All.ElectroRAT                   Ransomware.Cryptowall      Win32.Avatar
Android.PegasusB                 Ransomware.Hive            Win32.BigBang
Android.Skygofree                Ransomware.Jigsaw          Win32.Boaxxe.BB
Android.Spy.49_iBanking_Feb2014  Ransomware.Locky           Win32.BUMBLEBEE_0.1
Android.VikingHorde              Ransomware.Mamba           Win32.Cainxpii
AndroRat_6Dec2013                Ransomware.Matsnu          Win32.Caphaw.Shylock
AntiExe.A                        Ransomware.Petrwrap        Win32.Carberp
Artemis                          Ransomware.Petya           Win32.Cridex
Backdoor.MSIL.Tyupkin            Ransomware.Radamant        Win32.Cutwail
BAT.Drop                         Ransomware.RedBoot         Win32.DarkTequila
BAT.Pot.A                        Ransomware.Rex             Win32Dircrypt.Trojan.Ransom.ABZ
BAT.Skul                         Ransomware.Satana          Win32.Emotet
BlackEnergy2.1                   Ransomware.TeslaCrypt      Win32.EternalRocks
Brain.A                          Ransomware.Thanos          Win32.FamousSparrow
Careto_Feb2014                   Ransomware.Unnamed_0       Win32.Fareit
Cascade.1701.W                   Ransomware.Vipasana        Win32.FASTCash
Catapillar.E                     Ransomware.WannaCry        Win32.GhostSec
```

- For this activity we shall use Ransomware.WannaCry malware
- We need to unzip the password protected file Ransomware.WannCry.zip. Obtain the password and then use the password to unzip



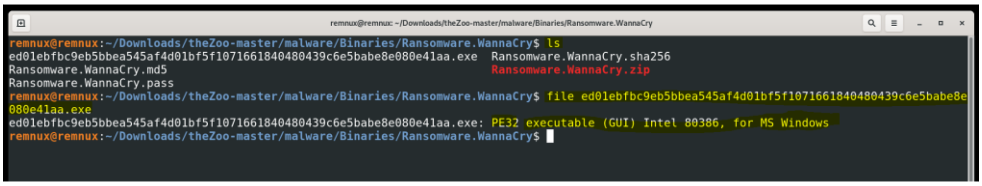
remnux@remnux: ~/Downloads/theZoo-master/malware/Binaries/Ransomware.WannaCry

```
remnux@remnux:~/Downloads/theZoo-master/malware/Binaries$ cd Ransomware.WannaCry
remnux@remnux:~/Downloads/theZoo-master/malware/Binaries/Ransomware.WannaCry$ ls
remnux@remnux:~/Downloads/theZoo-master/malware/Binaries/Ransomware.WannaCry$ cat Ransomware.WannaCry.pass
infected
remnux@remnux:~/Downloads/theZoo-master/malware/Binaries/Ransomware.WannaCry$ unzip Ransomware.WannaCry.zip
Archive:  Ransomware.WannaCry.zip
[Ransomware.WannaCry.zip] ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe password:
  inflating: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
remnux@remnux:~/Downloads/theZoo-master/malware/Binaries/Ransomware.WannaCry$ 
```



```
remnux@remnux:~/Downloads/theZoo-master/malware/Binaries/Ransomware.WannaCry$ ls
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe  Ransomware.WannaCry.sha256
Ransomware.WannaCry.md5                                                Ransomware.WannaCry.zip
Ransomware.WannaCry.pass
remnux@remnux:~/Downloads/theZoo-master/malware/Binaries/Ransomware.WannaCry$ 
```

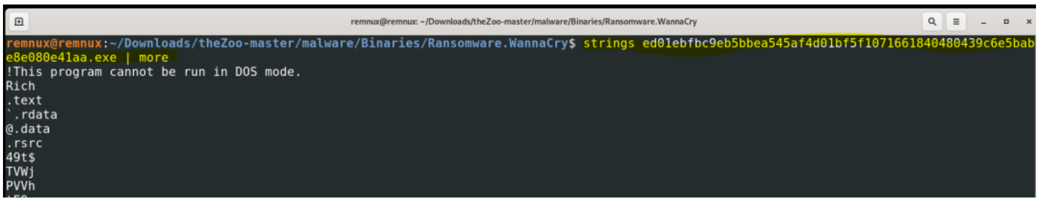
- Use the tool - file to find the file type


remnux@remnux: ~/Downloads/theZoo-master/malware/Binaries/Ransomware.WannaCry

```
remnux@remnux:~/Downloads/theZoo-master/malware/Binaries/Ransomware.WannaCry$ ls
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe  Ransomware.WannaCry.sha256
Ransomware.WannaCry.md5                                               Ransomware.WannaCry.zip
Ransomware.WannaCry.pass
remnux@remnux:~/Downloads/theZoo-master/malware/Binaries/Ransomware.WannaCry$ file ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e
080e41aa.exe
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe: PE32 executable (GUI) Intel 80386, for MS Windows
remnux@remnux:~/Downloads/theZoo-master/malware/Binaries/Ransomware.WannaCry$ 
```

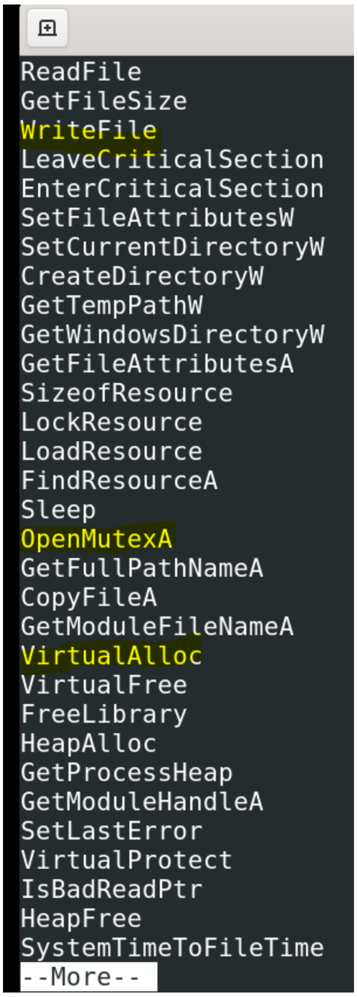
  - **Observation**: it is a PE file written for 32 bit MS Windows machine

- Use the tool – strings to get further information about the malware


remnux@remnux: ~/Downloads/theZoo-master/malware/Binaries/Ransomware.WannaCry

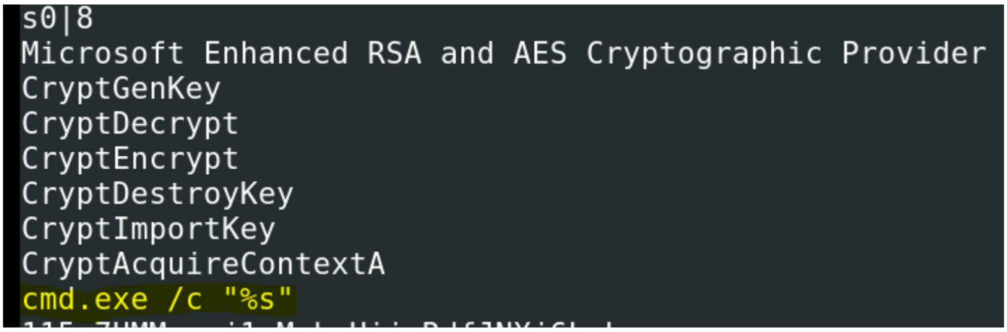
```
remnux@remnux:~/Downloads/theZoo-master/malware/Binaries/Ransomware.WannaCry$ strings ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5bab
e8e080e41aa.exe | more
!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.rsrc
49t$
TVWj
PVVh
```

  - Let us analyse the output and look for IOC (of course a guess)
  - It uses many functions, may be some of them are suspicious – WriteFile, OpenMutexA, VirtualAlloc



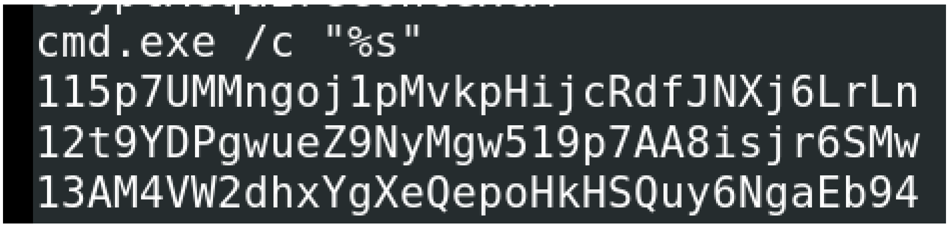
```
ReadFile
GetFileSize
WriteFile
LeaveCriticalSection
EnterCriticalSection
SetFileAttributesW
SetCurrentDirectoryW
CreateDirectoryW
GetTempPathW
GetWindowsDirectoryW
GetFileAttributesA
SizeofResource
LockResource
LoadResource
FindResourceA
Sleep
OpenMutexA
GetFullPathNameA
CopyFileA
GetModuleFileNameA
VirtualAlloc
VirtualFree
FreeLibrary
HeapAlloc
GetProcessHeap
GetModuleHandleA
SetLastError
VirtualProtect
IsBadReadPtr
HeapFree
SystemTimeToFileTime
--More--
```

- Look if the malware is trying to open the command line



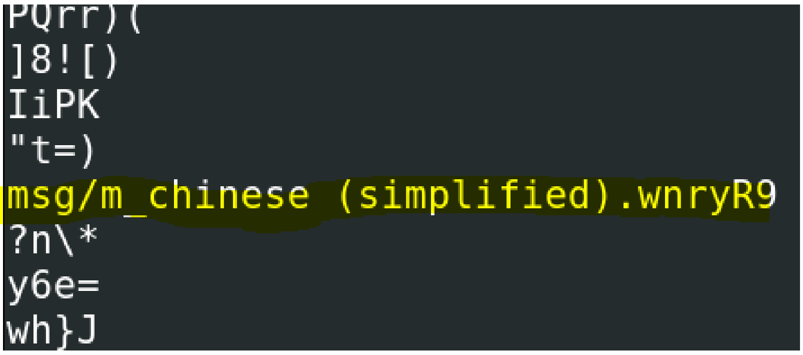
```
s0|8
Microsoft Enhanced RSA and AES Cryptographic Provider
CryptGenKey
CryptDecrypt
CryptEncrypt
CryptDestroyKey
CryptImportKey
CryptAcquireContextA
cmd.exe /c "%s"
```

- Look for Random strings – used to confuse malware analysts



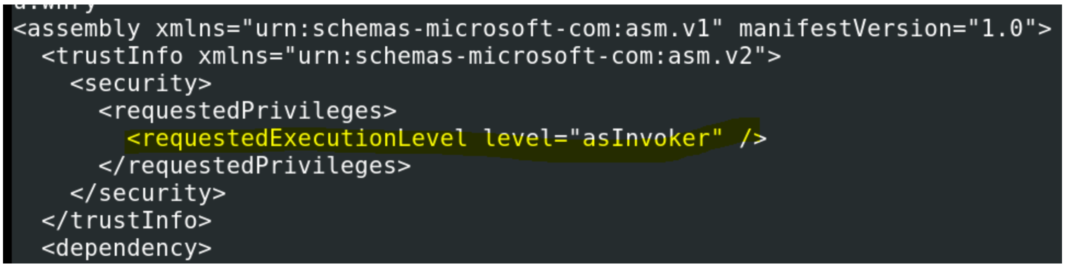
```
cmd.exe /c "%s"
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
```

- To display messages about the ransomware attack



```
PQrr)(
]8![)
IiPK
"t=)
msg/m_chinese (simplified).wnryR9
?n\*
y6e=
wh}J
```

- Trying to get privileges as Invoker



```
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
    <security>
      <requestedPrivileges>
        <requestedExecutionLevel level="asInvoker" />
      </requestedPrivileges>
    </security>
  </trustInfo>
  <dependency>
```