

## Analyze malicious files

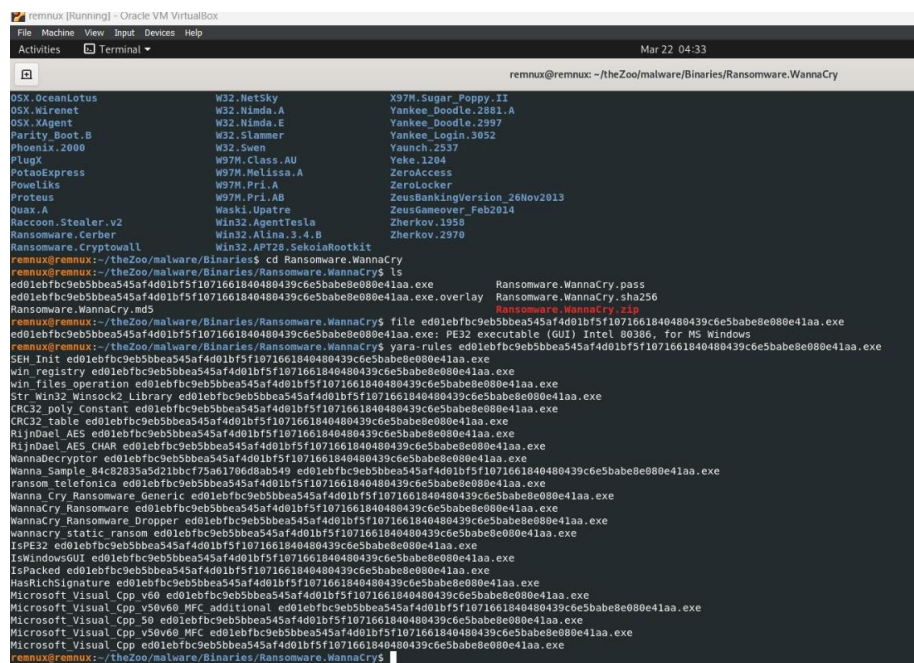
To analyze malicious file, I have used REMnux which is an open-source software.

About REMnux:

REMnux is a Linux-based operating system designed for malware analysis and reverse engineering. It is a lightweight, virtual appliance that comes pre-configured with a variety of powerful tools for analyzing and dissecting malware.

REMnux is built on top of the Ubuntu operating system and is designed to be used as a platform for investigating and analyzing malware in a safe and isolated environment. It includes a range of tools and utilities such as debuggers, disassemblers, memory analysis tools, and network traffic analysis tools that can help security professionals and researchers understand how malware works, identify its behavior, and develop ways to detect and mitigate it.

Pic-2.0



```
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$ ls
OSX.OceanLotus      W32.Netsky          X97M.Sugar_Poppy.II
OSX.Xirenet         W32.Nimda.A         Yankee.Doodle.2881.A
OSX.XAgent          W32.Nimda.E         Yankee.Doodle.2997
Parity_Boot.B       W32.Slammer         Yankee_Login.3052
Phoenix.2000        W32.Sven            Vaunch.2537
PlugX               W97M.Class.AU       Yeke.1204
PotatoExpress       W97M.Melissa.A      ZeroAccess
Poweliks            W97M.Pri.A          ZeroLocker
Proteus             W97M.Pri.AB         ZeusBankingVersion_26Nov2013
Quax.A              Waski.Upatre        ZeusGameover_Feb2014
Raccoon.Stealer.v2  Win32.AgentTesla    Zherkov.1958
Ransomware.Cerber   Win32.Alna.3.4.B     Zherkov.2970
Ransomware.Cryptowall
Win32.APT28.SekoiaRootkit
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$ cd Ransomware.WannaCry
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$ ls
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe  Ransomware.WannaCry.pass
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe.overlay  Ransomware.WannaCry.sha256
Ransomware.WannaCry.md5  Ransomware.WannaCry.zip
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$ file ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe: PE32 executable (GUI) Intel 80386, for MS Windows
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$ yara rules ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
SEH_Init ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
win_registry ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
win_files_operation ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
Str_win32_Winsock2_Library ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
CRC32_poly_constant ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
CRC32_table ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
Rijndael_AES ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
Rijndael_AES_CBC ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
WannaDecryptor ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
Wanna_Sample_84c82835a5d21bdcf75a61706d8ab549 ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
ransom_telefonica ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
WannaCry_Ransomware_Generic ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
WannaCry_Ransomware ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
WannaCry_Ransomware_Dropper ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
wannacry_static_ransom ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
ISPE32 ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
IsWindowsGUI ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
IsPacked ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
HasRchSignature ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
Microsoft_Visual_Cpp_v60 ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
Microsoft_Visual_Cpp_v50600_MFC_additional ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
Microsoft_Visual_Cpp_50 ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
Microsoft_Visual_Cpp_v50600_MFC ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
Microsoft_Visual_Cpp ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439ce5babe8e080e41aa.exe
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$
```

The above picture-2.0 shows that :

Let's take sha256sum value(which is the file name) as sample.exe

**Command 1:** file sample.exe

It checks whether the file is PE32 executable file or PECompact2 compressed. A PE is a file format developed by Microsoft used for executables (. EXE, . SCR) and dynamic

link libraries (. DLL). A PE file infector is a malware family that propagates by appending or wrapping malicious code into other PE files on an infected system.

## Command 2: yara-rules sample.exe

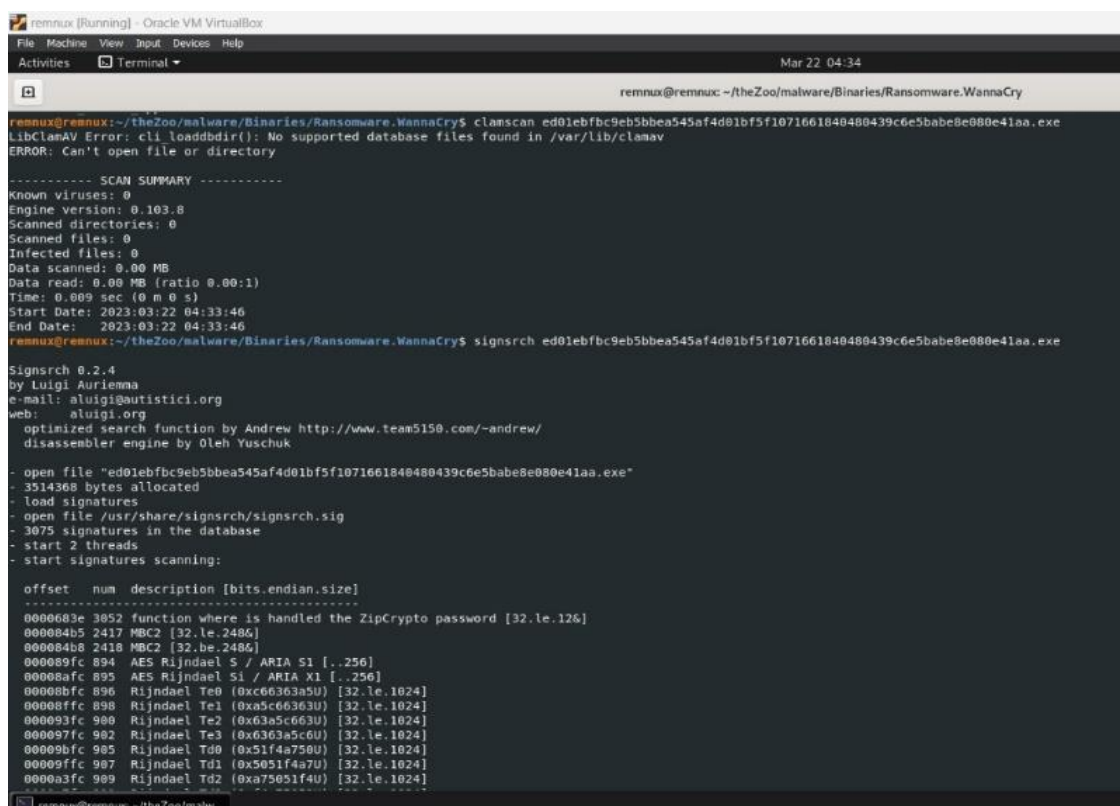
Shows about HTTP, registry, file operations, overlay

YARA is a tool used for identifying and classifying malware based on textual or binary patterns. YARA rules are the rules written in the YARA language to identify patterns of interest in files, processes, or network traffic.

## Command-3: clamscan sample.exe

The clamscan command is a command-line antivirus scanner for Linux-based operating systems. It is part of the ClamAV open-source antivirus software package and is used to scan files, directories, and entire filesystems for viruses, malware, and other malicious software.

Pic-2.1



```
remnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mar 22 04:34
remnux@remnux: ~/theZoo/malware/Binaries/Ransomware.WannaCry

remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$ clamscan ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
LibClamAV Error: cli_loaddbdir(): No supported database files found in /var/lib/clamav
ERROR: Can't open file or directory

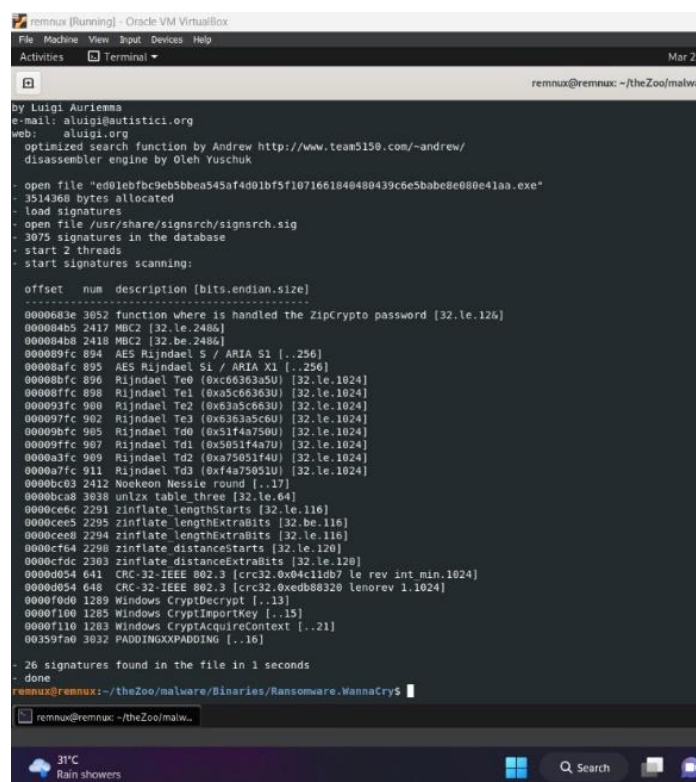
----- SCAN SUMMARY -----
Known viruses: 0
Engine version: 0.103.8
Scanned directories: 0
Scanned files: 0
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 0.009 sec (0 m 0 s)
Start Date: 2023:03:22 04:33:46
End Date: 2023:03:22 04:33:46
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$ signsrch ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

Signsrch 0.2.4
by Luigi Auriemma
e-mail: luigi@autistici.org
web: luigi.org
optimized search function by Andrew http://www.team5150.com/~andrew/
disassembler engine by Oleh Yuschuk

- open file "ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe"
- 3514368 bytes allocated
- load signatures
- open file /usr/share/signsrch/signsrch.sig
- 3075 signatures in the database
- start 2 threads
- start signatures scanning:

offset num description [bits.endian.size]
-----
0000683e 3852 function where is handled the ZipCrypto password [32.le.126]
000084b5 2417 MBC2 [32.le.2486]
000084b8 2418 MBC2 [32.be.2486]
000089fc 894 AES Rijndael S / ARIA S1 [...256]
00008afc 895 AES Rijndael S1 / ARIA X1 [...256]
00008bfc 896 Rijndael Te0 (0xc66363a5U) [32.le.1024]
00008ffc 898 Rijndael Te1 (0xa5c66363U) [32.le.1024]
000093fc 900 Rijndael Te2 (0x63a5c663U) [32.le.1024]
000097fc 902 Rijndael Te3 (0x6363a5c6U) [32.le.1024]
00009bfc 905 Rijndael Td0 (0x51f4a759U) [32.le.1024]
00009ffc 907 Rijndael Td1 (0x5051f4a7U) [32.le.1024]
0000a3fc 909 Rijndael Td2 (0xa75051f4U) [32.le.1024]
```

Pic-2.2



```
remnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mar 22
remnux@remnux: ~/theZoo/malware

by Luigi Auriemma
e-mail: aluigi@autistici.org
web: aluigi.org
optimized search function by Andrew http://www.team5150.com/~andrew/
disassembler engine by Oleh Yuschuk

- open file "ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe"
- 3514968 bytes allocated
- load signatures
- open file /usr/share/signsrch/signsrch.sig
- 3075 signatures in the database
- start 2 threads
- start signatures scanning:

offset num description [bits.endian.size]
-----
0000683e 3052 function where is handled the ZipCrypto password [32.le.126]
000084b5 2417 MBC2 [32.le.2486]
000084b8 2418 MBC2 [32.be.2486]
000089fc 894 AES Rijndael S / ARIA S1 [..256]
00008afc 895 AES Rijndael S1 / ARIA X1 [..256]
00008bfc 896 Rijndael Te0 (0xc66363a5U) [32.le.1024]
00008ffc 898 Rijndael Te1 (0xa5c66363U) [32.le.1024]
000093fc 900 Rijndael Te2 (0xa3a5c663U) [32.le.1024]
000097fc 902 Rijndael Te3 (0x6363a5c6U) [32.le.1024]
00009bfc 905 Rijndael Td0 (0x51f4a750U) [32.le.1024]
00009ffc 907 Rijndael Td1 (0x5051f4a7U) [32.le.1024]
0000a3fc 909 Rijndael Td2 (0xa75051f4U) [32.le.1024]
0000a7fc 911 Rijndael Td3 (0xf4a75051U) [32.le.1024]
0000bc03 2412 Nookeon Nessie round [..17]
0000bc08 3038 unLzx table three [32.le.64]
0000cec6 2291 zlib lengthStarts [32.le.116]
0000cee5 2295 zlib lengthExtraBits [32.be.116]
0000cee8 2294 zlib lengthExtraBits [32.le.116]
0000cf64 2290 zlib distanceStarts [32.le.120]
0000cfdc 2303 zlib distanceExtraBits [32.le.120]
0000d054 641 CRC-32-IEEE 802.3 [crc32.0x04c11db7 le rev int min.1024]
0000d054 648 CRC-32-IEEE 802.3 [crc32.0xedb88320 lenorev 1.1024]
0000f0d0 1289 Windows CryptDecrypt [..13]
0000f100 1285 Windows CryptImportKey [..15]
0000f110 1283 Windows CryptAcquireContext [..21]
00359fa0 3032 PADDINGXXPADDING [..16]

- 26 signatures found in the file in 1 seconds
- done
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$
```

Command-4: signsrch sample.exe

we can verify that the file has been signed using this specific digital signature algorithm.

A digital signature is a cryptographic technique used to ensure the authenticity and integrity of a digital document or file. In the case of executable files, a digital signature can be used to verify that the file has not been tampered with and was signed by a trusted entity.

```
remnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mar 22 04:35
remnux@remnux: ~/theZoo/malware/Binaries/Ransomware.WannaCry
$ ./wannaCry
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$ peframe ed01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
XLMacroDeobfuscator: pywin32 is not installed (only is required if you want to use MS Excel)

-----
File Information (time: 0:00:10.292882)
-----
filename      ed01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
filetype      PE32 executable (GUI) Intel 80386, for MS Windows
filesize      3514368
hash sha256   ed01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa
virus total   /
imagebase     0x400000
entrypoint    0x77ba
imphash       68f013d7437aa653a8a98a05807afeb1
datetime     2010-11-20 09:05:05
dll           False
directories    import, tls, resources, relocations
sections      .data, .text *, .rdata *, .rsrc *
features      mutex, antidebug, packer, crypto

-----
Yara Plugins
-----
IsPE32
IsWindowsGUI
IsPacked
HashRichSignature
CRC32 poly Constant
CRC32 table
Rijndael AES
Rijndael AES CHAR
Rijndael AES LONG

-----
Behavior
-----
xor
win registry
win files operation

-----
Crypto
-----
remnux@remnux: ~/theZoo/malw...
```

Pic-2.3

```
remnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mar 22 04:3
remnux@remnux: ~/theZoo/malware/Bin
Crypto
-----
CRC32 poly Constant
CRC32 table
Rijndael AES
Rijndael AES CHAR
Rijndael AES LONG

-----
Packer
-----
Microsoft Visual Cpp v60
Microsoft Visual Cpp v50v60 MFC additional
Microsoft Visual Cpp 50
Microsoft Visual Cpp v50v60 MFC
Microsoft Visual Cpp

-----
Mutex Api
-----
OpenMutexA
WaitForSingleObject

-----
Anti Debug
-----
TerminateProcess

-----
Sections Suspicious
-----
.text      0.40
.rdata     0.40
.rsrc      7.99

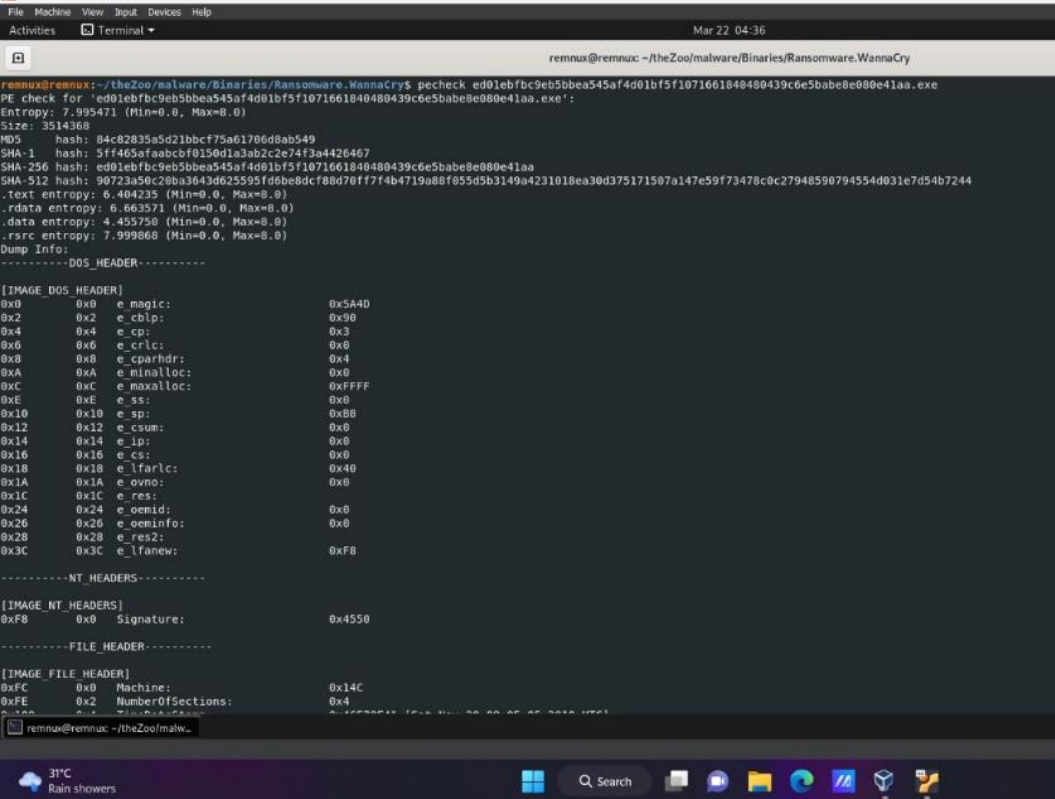
-----
Metadata
-----
CompanyName      Microsoft Corporation
FileDescription   DiskPart
FileVersion       6.1.7601.17514 (win7sp1 rtm.101119-1850)
remnux@remnux: ~/theZoo/malw...
```

Pic-2.4

**Command-5:** peframe sample.exe

It gives output of behaviour of files and clear report , file information,crypto,Hashes, sections code and .rsrc, entropy of .rsrc high, suspicious API references.

Pic-2.5



```
remnux@remnux: ~/theZoo/malware/Binaries/Ransomware.WannaCry
peframe ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
PE check for 'ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe':
Entropy: 7.995471 (Min=0.0, Max=8.0)
Size: 3514368
MD5 hash: 84c02835a5d21bbc775a61706d8ab549
SHA-1 hash: 5ff468afaabcf0150d1a3ab2c2e74f3a4426467
SHA-256 hash: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
SHA-512 hash: 90723a50c20ba3643d625595fd6be8dcf80d70ff774b4719a88f055d5b3149a4231018ea30d375171507a147e59f73478c0c27948590794554d031e7d54b7244
.text entropy: 6.404235 (Min=0.0, Max=8.0)
.rdata entropy: 6.663571 (Min=0.0, Max=8.0)
.data entropy: 4.455750 (Min=0.0, Max=8.0)
.rsrc entropy: 7.999860 (Min=0.0, Max=8.0)
Dump Info:
-----DOS_HEADER-----
[IMAGE_DOS_HEADER]
0x0 0x0 e_magic: 0x5A4D
0x2 0x2 e_cblp: 0x90
0x4 0x4 e_cp: 0x3
0x6 0x6 e_crlc: 0x0
0x8 0x8 e_cparhdr: 0x4
0xA 0xA e_minalloc: 0x0
0xC 0xC e_maxalloc: 0xFFFF
0xE 0xE e_ss: 0x0
0x10 0x10 e_sp: 0xB8
0x12 0x12 e_csum: 0x0
0x14 0x14 e_ip: 0x0
0x16 0x16 e_cs: 0x0
0x18 0x18 e_lfarlc: 0x40
0x1A 0x1A e_ovno: 0x0
0x1C 0x1C e_res: 0x0
0x24 0x24 e_oemid: 0x0
0x26 0x26 e_oeminfo: 0x0
0x28 0x28 e_res2: 0x0
0x3C 0x3C e_lfanew: 0xF8
-----NT_HEADERS-----
[IMAGE_NT_HEADERS]
0xF8 0x0 Signature: 0x4550
-----FILE_HEADER-----
[IMAGE_FILE_HEADER]
0xFC 0x0 Machine: 0x14C
0xFE 0x2 NumberOfSections: 0x4
```

```
remnux@remnux: ~/theZoo/malware/Binaries/Ransomware.WannaCry
0x10058 0x0 Characteristics: 0x0
0x1005C 0x4 TimeDateStamp: 0x0 [Thu Jan 1 00:00:00 1970 UTC]
0x10060 0x0 MajorVersion: 0x4
0x10062 0xA MinorVersion: 0x0
0x10064 0xC NumberOfNamedEntries: 0x0
0x10066 0xE NumberOfIdEntries: 0x1
Id: [0x1]
[IMAGE_RESOURCE_DIRECTORY_ENTRY]
0x10068 0x0 Name: 0x1
0x1006C 0x4 OffsetToData: 0x800000A0
[IMAGE_RESOURCE_DIRECTORY]
0x100A0 0x0 Characteristics: 0x0
0x100A4 0x4 TimeDateStamp: 0x0 [Thu Jan 1 00:00:00 1970 UTC]
0x100A8 0x8 MajorVersion: 0x4
0x100AA 0xA MinorVersion: 0x0
0x100AC 0xC NumberOfNamedEntries: 0x0
0x100AE 0xE NumberOfIdEntries: 0x1
\\- LANG [9:1][LANG_ENGLISH;SUBLANG_ENGLISH_US]
[IMAGE_RESOURCE_DIRECTORY_ENTRY]
0x100B0 0x0 Name: 0x409
0x100B4 0x4 OffsetToData: 0xD8
[IMAGE_RESOURCE_DATA_ENTRY]
0x100D0 0x0 OffsetToData: 0x359AB0
0x100DC 0x4 Size: 0x4EF
0x100E0 0x0 CodePage: 0x4E4
0x100E4 0xC Reserved: 0x0

Signature:
No signature

PEID:
Error: signature database missing
Entry point:
ep: 0x000077ba
ep address: 0x004077ba
Section: .text
ep offset: 0x000077ba

TLS Callbacks:
No TLS

Overlay:
No overlay
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$
```

Pic-2.6

Command-6: pecheck sample.exe

It gives output about Hashes, suspicious API references, overlay.

PECheck is a command-line tool that can be used to verify the PE header and section headers of PE files. It checks the file signature, the size of the image, the entry point, and other information in the PE header. It can also validate the section headers by checking their names, sizes, and attributes.

