Analyze malicious files

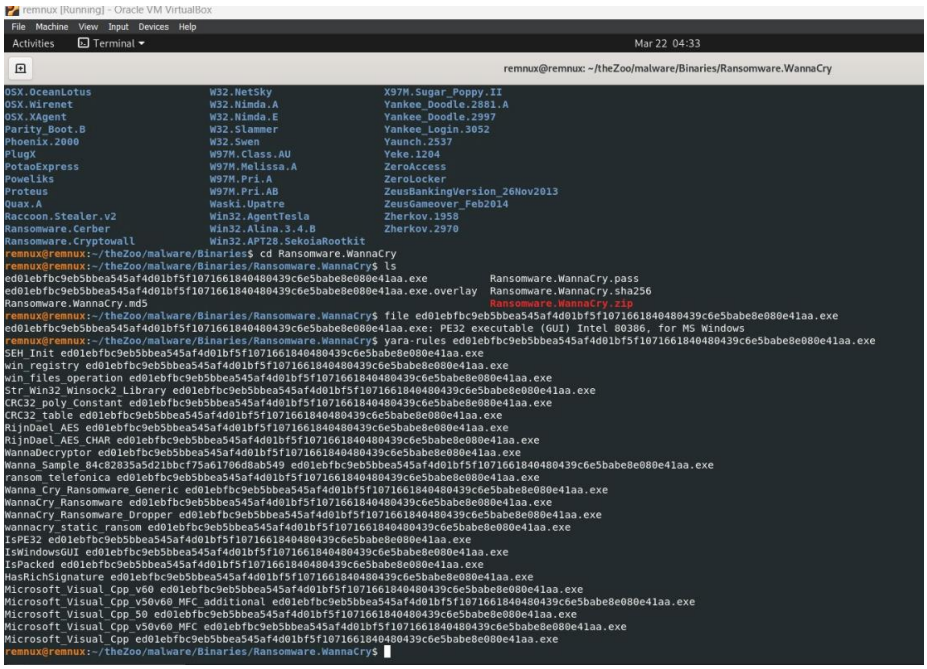
To analyze malicious file, I have used REMnux which is an open-source software.

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



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

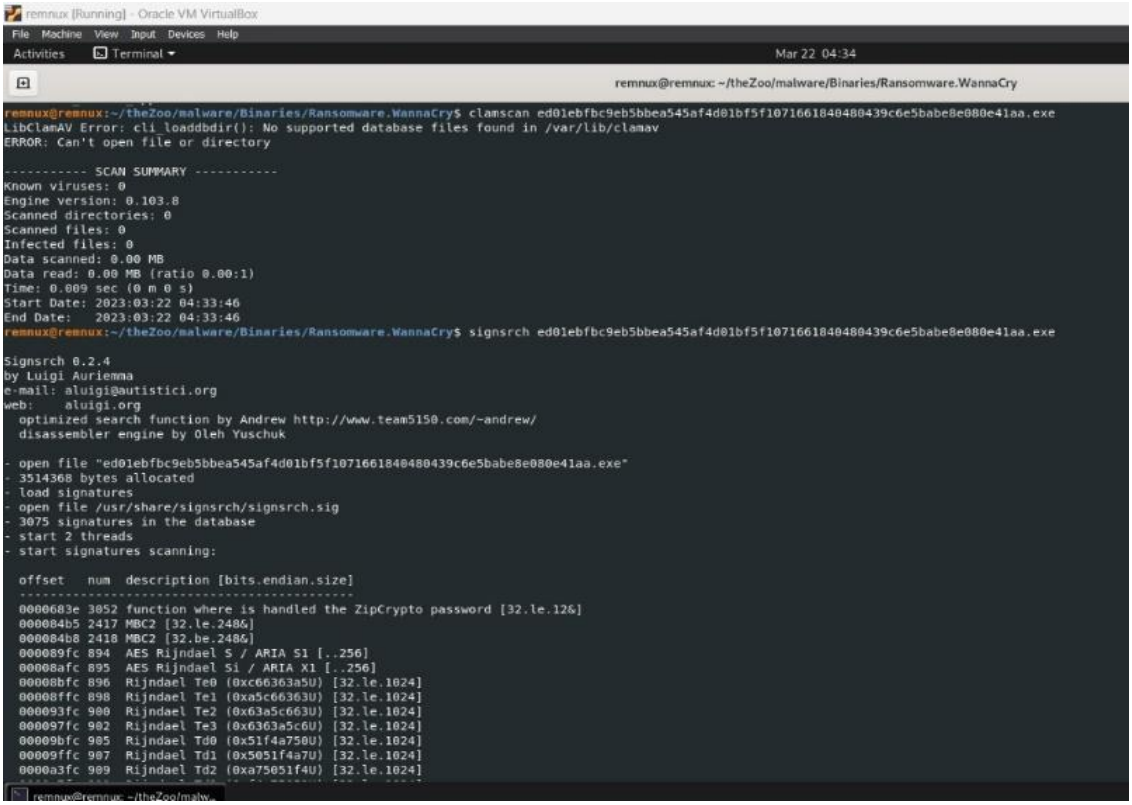
Shows about HTTP, registry, file operations, overlay

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.

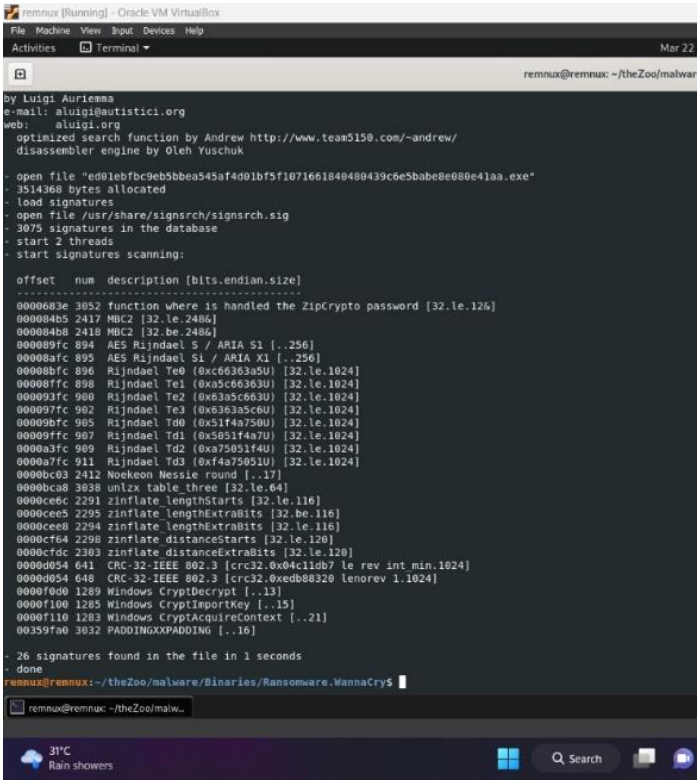
Command-3: clamscan sample.exe

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



Pic-2.2



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@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$ peframe ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
XLMMacroDeobfuscator: pywin32 is not installed (only is required if you want to use MS Excel)


------------------------------------------------------------------------------
File Information (time: 0:00:10.292882)
------------------------------------------------------------------------------
filename          ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
filetype          PE32 executable (GUI) Intel 80386, for MS Windows
filesize          3514368
hash sha256       ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
virustotal        /
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, antidbg, packer, crypto


------------------------------------------------------------------------------
Yara Plugins
------------------------------------------------------------------------------
IsPE32
IsWindowsGUI
IsPacked
HasRichSignature
CRC32 poly Constant
CRC32 table
RijnDael AES
RijnDael AES CHAR
RijnDael AES LONG


------------------------------------------------------------------------------
Behavior
------------------------------------------------------------------------------
Xor
win registry
win files operation


------------------------------------------------------------------------------
Crypto
```

Pic-2.3

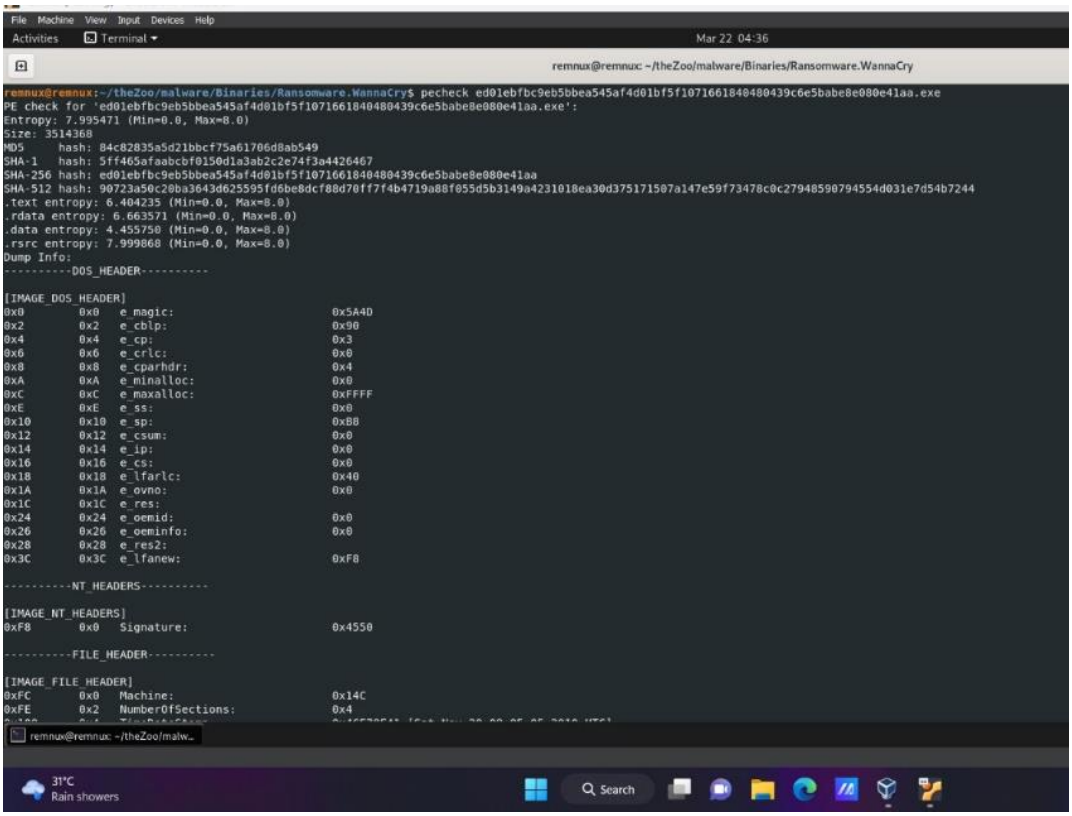
```
------------------------------------------------------------------------------
Crypto
------------------------------------------------------------------------------
CRC32 poly Constant
CRC32 table
RijnDael AES
RijnDael AES CHAR
RijnDael AES LONG


------------------------------------------------------------------------------
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           6.40
.rdata          6.66
.rsrc           7.99


------------------------------------------------------------------------------
Metadata
------------------------------------------------------------------------------
CompanyName     Microsoft Corporation
FileDescription DiskPart
FileVersion     6.1.7601.17514 (win7sp1 rtm.101119-1850)
```

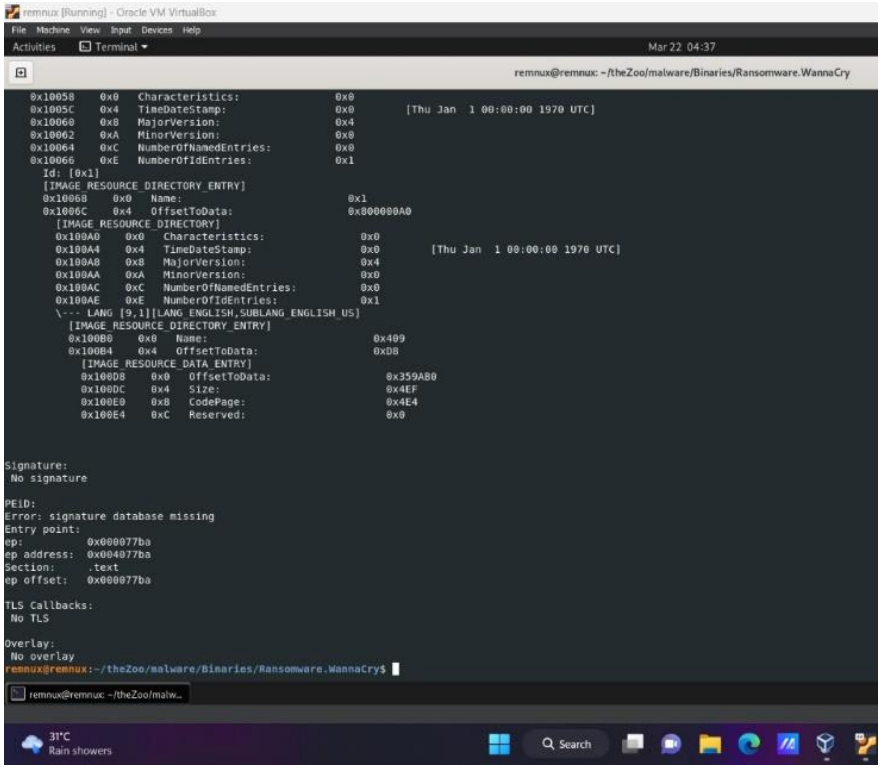
Pic-2.4

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





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.