Rz-pipe, is a python wrapper for Rizin an open-source disassembler which replaces Radare2.

The wrapper allows to use the usual commands in python which is very handy for automation and analysis.

Info of the current file :

```
fd       3
file     static/files/Malware.exe
size     0x1c00
humansz  7K
mode     r-x
format   pe64
iorw     false
block    0x100
type     EXEC (Executable file)
arch     x86
cpu      N/A
baddr    0x140000000
binsz    0x00001c00
bintype  pe
bits     64
retguard false
class    PE32+
cmp.csum 0x0000a270
compiled Thu Apr 15 01:06:53 2010 UTC+3
compiler N/A
dbg_file N/A
endian   LE
hdr.csum 0x0000a0b8
guid     N/A
intrp    N/A
laddr    0x00000000
lang     c
machine  AMD 64
maxopsz  16
minopsz  1
os       windows
overlay  false
cc       ms
pcalign  0
```

rpath N/A

signed false

subsys Windows GUI

stripped false

crypto false

havecode true

va true

sanitiz false

static false

linenum false

lsyms false

canary false

PIE false

RELROCS true

NX false

Summary of all info imports, exports, sections, etc. :

[Info]

arch x86

cpu N/A

baddr 0x140000000

binsz 0x00001c00

bintype pe

bits 64

retguard false

class PE32+

cmp.csum 0x0000a270

compiled Thu Apr 15 01:06:53 2010 UTC+3

compiler N/A

dbg_file N/A

endian LE

hdr.csum 0x0000a0b8

guid N/A

intrp N/A

laddr 0x00000000

lang c

machine AMD 64

maxopsz 16

minopsz 1

os windows

overlay false

cc ms

pcalign 0

rpath N/A

signed false

subsys Windows GUI

stripped false

crypto false

havecode true

va true

sanitiz false

static false

linenum false

lsyms false

canary false

PIE false

RELROCS true

NX false

[Imports]

nth vaddr bind type lib name

---

1 0x140003000 NONE FUNC KERNEL32.dll VirtualAlloc

2 0x140003008 NONE FUNC KERNEL32.dll ExitProcess

[Entries]

vaddr paddr hvaddr haddr type

0x140004000 0x00001800 ---------- 0x000000f0 program

[Exports]

nth paddr vaddr bind type size lib name

[Classes]

address min max name super

[Symbols]

nth paddr vaddr bind type size lib name

---

1 0x00001600 0x140003000 NONE FUNC 0 KERNEL32.dll imp.VirtualAlloc

2 0x00001608 0x140003008 NONE FUNC 0 KERNEL32.dll imp.ExitProcess

[Sections]

paddr size vaddr vsize align perm name type flags

0x00000400 0x1200 0x140001000 0x2000 0x0 -r-x .text CNT_CODE

0x00001600 0x200 0x140003000 0x1000 0x0 -r-- .rdata CNT_INITIALIZED_DATA

0x00001800 0x400 0x140004000 0x1000 0x0 -rwx .admx CNT_CODE

[Memory]

name size address flags mirror

[Strings]

nth paddr vaddr len size section type string

---

0 0x0000165a 0x14000305a 11 12 .rdata ascii ExitProcess

1 0x00001668 0x140003068 12 13 .rdata ascii VirtualAlloc

2 0x00001676 0x140003076 12 13 .rdata ascii KERNEL32.dll

Binary fields :

paddr name vaddr comment

0x00000090 RICH_ENTRY_NAME 0x00000090 Linker900

0x00000090 RICH_ENTRY_ID 0x00000090 0x00000091

0x00000092 RICH_ENTRY_VERSION 0x00000092 0x00007809

0x00000094 RICH_ENTRY_TIMES 0x00000094 0x00000001

0x00000098 RICH_ENTRY_NAME 0x00000098 Masm900

0x00000098 RICH_ENTRY_ID 0x00000098 0x00000095

0x0000009a RICH_ENTRY_VERSION 0x0000009a 0x00007809

0x0000009c RICH_ENTRY_TIMES 0x0000009c 0x00000001

0x000000a0 RICH_ENTRY_NAME 0x000000a0 Import0

0x000000a0 RICH_ENTRY_ID 0x000000a0 0x00000001

0x000000a2 RICH_ENTRY_VERSION 0x000000a2 0x00000000

0x000000a4 RICH_ENTRY_TIMES 0x000000a4 0x00000002

0x000000a8 RICH_ENTRY_NAME 0x000000a8 Implib800

0x000000a8 RICH_ENTRY_ID 0x000000a8 0x0000007b

0x000000aa RICH_ENTRY_VERSION 0x000000aa 0x0000c627

0x000000ac RICH_ENTRY_TIMES 0x000000ac 0x00000003

0x000000b0 Signature 0x000000b0 0x00004550

0x000000b4 Machine 0x000000b4 0x00008664

0x000000b6 NumberOfSections 0x000000b6 0x00000003

0x000000b8 TimeDateStamp 0x000000b8 0x4bc63c7d

0x000000bc PointerToSymbolTable 0x000000bc 0x00000000

0x000000c0 NumberOfSymbols 0x000000c0 0x00000000

0x000000c4 SizeOfOptionalHeader 0x000000c4 0x000000f0

0x000000c6 Characteristics 0x000000c6 0x00000023

0x000000c8 Magic 0x000000c8 0x0000020b

0x000000ca MajorLinkerVersion 0x000000ca 0x00000001

0x000000cb MinorLinkerVersion 0x000000cb 0x00000000

0x000000cc SizeOfCode 0x000000cc 0x00003000

0x000000d0 SizeOfInitializedData 0x000000d0 0x00001000

0x000000d4 SizeOfUninitializedData 0x000000d4 0x00000000

0x000000d8 AddressOfEntryPoint 0x000000d8 0x00004000

0x000000dc BaseOfCode 0x000000dc 0x00001000

0x000000e0 ImageBase 0x000000e0 0x140000000

0x000000e4 SectionAlignment 0x000000e4 0x00001000

0x000000e8 FileAlignment 0x000000e8 0x00000200

0x000000ec MajorOperatingSystemVersion 0x000000ec 0x00000004

0x000000ee MinorOperatingSystemVersion 0x000000ee 0x00000000

0x000000f0 MajorImageVersion 0x000000f0 0x00000000

0x000000f2 MinorImageVersion 0x000000f2 0x00000000

0x000000f4 MajorSubsystemVersion 0x000000f4 0x00000004

0x000000f6 MinorSubsystemVersion 0x000000f6 0x00000000

0x000000f8 Win32VersionValue 0x000000f8 0x00000000

0x000000fc SizeOfImage 0x000000fc 0x00004248

0x00000100 SizeOfHeaders 0x00000100 0x00000248

0x00000104 CheckSum 0x00000104 0x0000a0b8

0x00000108 Subsystem 0x00000108 0x00000002

0x0000010a DllCharacteristics 0x0000010a 0x00008000

0x0000010c SizeOfStackReserve 0x0000010c 0x00100000

0x00000110 SizeOfStackCommit 0x00000110 0x00001000

0x00000114 SizeOfHeapReserve 0x00000114 0x00100000

0x00000118 SizeOfHeapCommit 0x00000118 0x00001000

0x0000011c LoaderFlags 0x0000011c 0x00000000

0x00000120 NumberOfRvaAndSizes 0x00000120 0x00000010

0x0000012c IMAGE_DIRECTORY_ENTRY_IMPORT 0x0000012c 0x000041d0

0x00000130 SIZE_IMAGE_DIRECTORY_ENTRY_IMPORT 0x00000130 0x0000006c

0x0000014c IMAGE_DIRECTORY_ENTRY_BASERELOC 0x0000014c 0x00004240

0x00000150 SIZE_IMAGE_DIRECTORY_ENTRY_BASERELOC 0x00000150 0x00000008

0x00000184 IMAGE_DIRECTORY_ENTRY_IAT 0x00000184 0x00003000

0x00000188 SIZE_IMAGE_DIRECTORY_ENTRY_IAT 0x00000188 0x00000018

0x0000018c IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT 0x0000018c 0x00000000

0x00000190 SIZE_IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT 0x00000190 0x0000ffff

Binary headers :

PE file header:

IMAGE_NT_HEADERS

Signature : 0x4550

IMAGE_FILE_HEADERS

Machine : 0x8664

NumberOfSections : 0x3

TimeDateStamp : 0x4bc63c7d

PointerToSymbolTable : 0x0

NumberOfSymbols : 0x0

SizeOfOptionalHeader : 0xf0

Characteristics : 0x23

IMAGE_OPTIONAL_HEADERS

Magic : 0x20b

MajorLinkerVersion : 0x1

MinorLinkerVersion : 0x0

SizeOfCode : 0x3000

SizeOfInitializedData : 0x1000

SizeOfUninitializedData : 0x0

AddressOfEntryPoint : 0x4000

BaseOfCode : 0x1000

ImageBase : 0x140000000

SectionAlignment : 0x1000

FileAlignment : 0x200

MajorOperatingSystemVersion : 0x4

MinorOperatingSystemVersion : 0x0

MajorImageVersion : 0x0

MinorImageVersion : 0x0

MajorSubsystemVersion : 0x4

MinorSubsystemVersion : 0x0

Win32VersionValue : 0x0

SizeOfImage : 0x4248

SizeOfHeaders : 0x248

CheckSum : 0xa0b8

Subsystem : 0x2

DllCharacteristics : 0x8000

SizeOfStackReserve : 0x100000

SizeOfStackCommit : 0x1000

SizeOfHeapReserve : 0x100000

SizeOfHeapCommit : 0x1000

LoaderFlags : 0x0

NumberOfRvaAndSizes : 0x10

RICH_FIELDS

Product: 145 Name: Linker900 Version: 30729 Times: 1

Product: 149 Name: Masm900 Version: 30729 Times: 1

Product: 1 Name: Import0 Version: 0 Times: 2

Product: 123 Name: Implib800 Version: 50727 Times: 3

IMAGE_DIRECTORY_ENTRY_IMPORT

VirtualAddress : 0x41d0

Size : 0x6c

IMAGE_DIRECTORY_ENTRY_BASERELOC

VirtualAddress : 0x4240

Size : 0x8

IMAGE_DIRECTORY_ENTRY_IAT

VirtualAddress : 0x3000

Size : 0x18

IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT

VirtualAddress : 0x0

Size : 0xffff

file hashes :

md5 b4ecb4d98af207511145ffa9715747a8

sha1 62f232157086170f094c3a233d5bf90a426766df

sha256 fb2d8bb6909090b2ac00bd32e915f3fc59856e1d0438fcb347042120201cd3c7

crc32 2ee088cf

entropy 1.260004