Laboratorio 3:Forensics

Rodrigo Castillo

24 de agosto de 2020

1. Read the first paragraphs of the Section ”Malware Analysis in Virtual Machines”. Mention 1 advantage of using physical machines instead of virtual machines?

one of the advantages of using a physical machine is that it have full control of the resources of the machine, so it's faster.

2. Networking on VMs: Review the section Çonfigure Vmware”. Regarding the networking configuration of a virtual machine, mention one advantage and one disadvantage of each possible networking configuration:

2.1. Disconnected VM

2.1.1. Advantages

One of the advantages of having your virtual machine disconnected is that a worm wont be able to spread over your network

2.1.2. Disadvantages

By the way, the machine wont be able to connect to internet, so, for example, if a malware need internet to work, the analysis wont enought.

2.2. Host-Only

2.2.1. Advantages

Its usefull when you need to use internet in the virtual machine with the Ip of your real computer.

2.2.2. Disadvantages

malware can comunicate with host.

2.3. Multiple VMs inside an Internal Network

2.3.1. Advantages

its usefull to analyze the way that malware spreads.

2.3.2. Disadvantages

the machines wont be able to communicate out to the internet.

2.4. VM with Bridged network adapter

2.4.1. Advantages

It can be usefull to connect across the internet using an ip different to host.

2.4.2. Disadvantages

The malware can access to all machines in the network.

2.5. VM with NAT(Network Address Translation)

2.5.1. Advantages

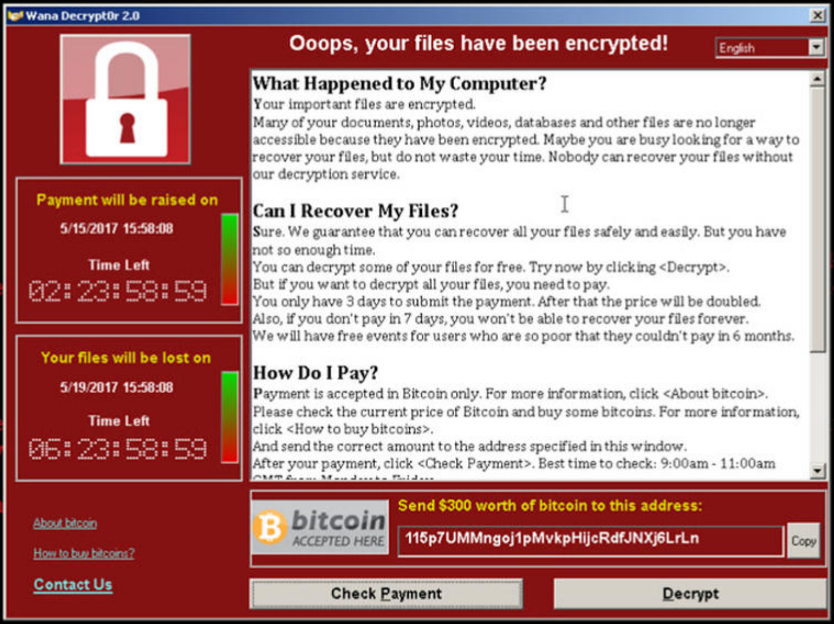
this mode is going to take the ip of the host machine.

2.5.2. Disadvantages

the malware can touch the host machine, also, internet is not safe, sometimes malware communicate with servers that are owned by mad people.

3. Wanna Cry

i'm having problems with my virtual machine right now :(, so i think i'll have to execute this file later, by the way, i've runned a lot of ransomwares before in competitions .
by the way, classic wannacry looks like this :



Ooops, your files have been encrypted!

Payment will be raised on
5/15/2017 15:58:08
Time Left
02:23:58:59

Your files will be lost on
5/19/2017 15:58:08
Time Left
06:23:58:59

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

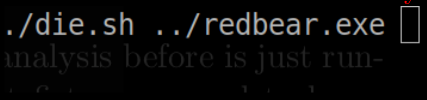
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

4. Read the first paragraphs of the section ”Basic Dynamic Analysis.ªnd indicate one disadvantage of doing ”dynamic analysis”without doing previously ”static analysis”.

Performig Basic Dynamic Analysis without performing static analysis before is just running malware blindly . When you are gonna analyze malware, at firts, you need to know which kind of malware are you going to analyze and how, then you can running for analyze the way it works.

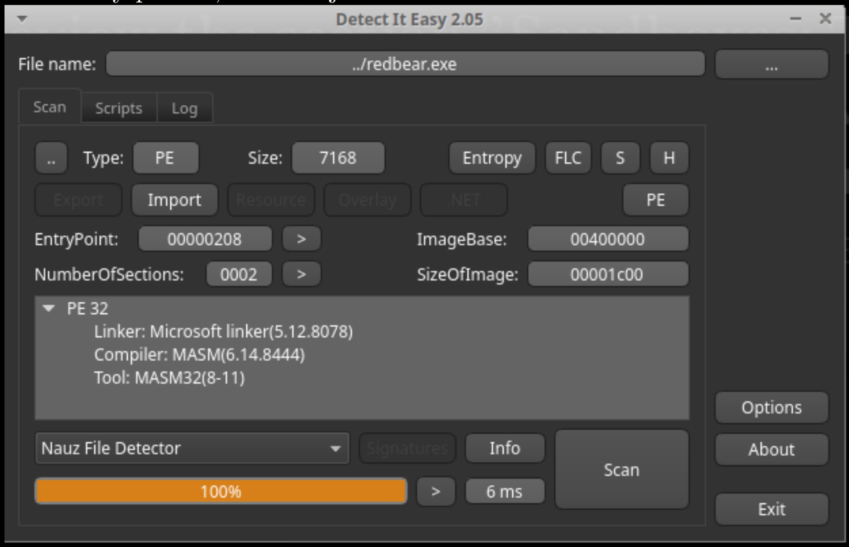
5. Review the section ”Sandboxes: The Quick-and-Dirty Approach”. Then do the following steps over the malware Redbear.exe”that you may download from here. Use the password: ”forense”to decompress:

because im having problem with my virtual machine, i cant use the tool PeID, so i’ll use a similar tool called ”Detect it easy”that works for linux .



```
./die.sh ../redbear.exe
```

from this tool, i can also check the memory of the malware, unfortunatly, even if the malware is obviusly packed, the tool just detects this:



Detect It Easy 2.05

File name: ../redbear.exe

Type: PE

Size: 7168

EntryPoint: 00000208

ImageBase: 00400000

NumberOfSections: 0002

SizeOfImage: 00001c00

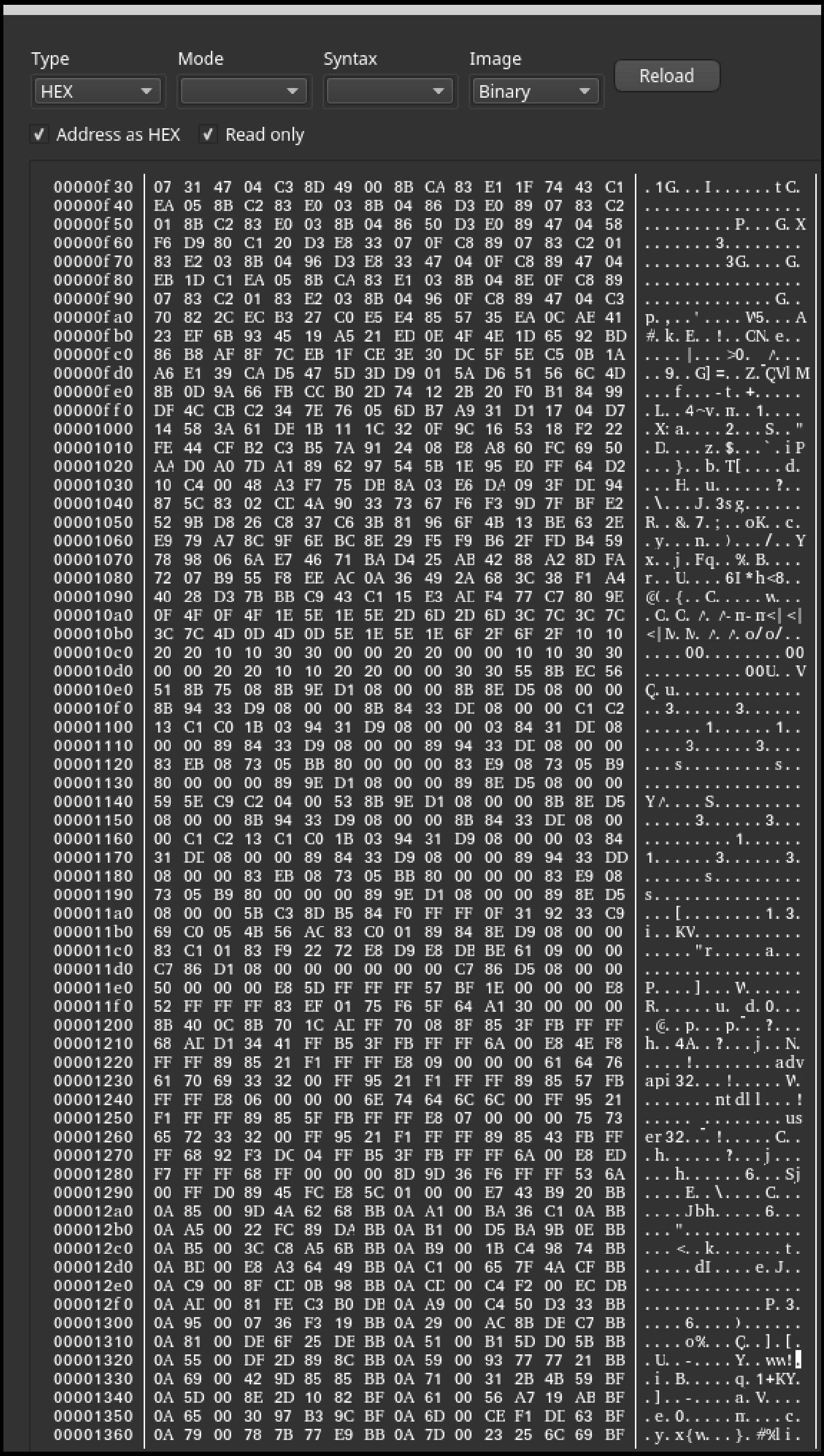
PE 32
    Linker: Microsoft linker(5.12.8078)
    Compiler: MASM(6.14.8444)
    Tool: MASM32(8-11)

Nauz File Detector

100%

6 ms

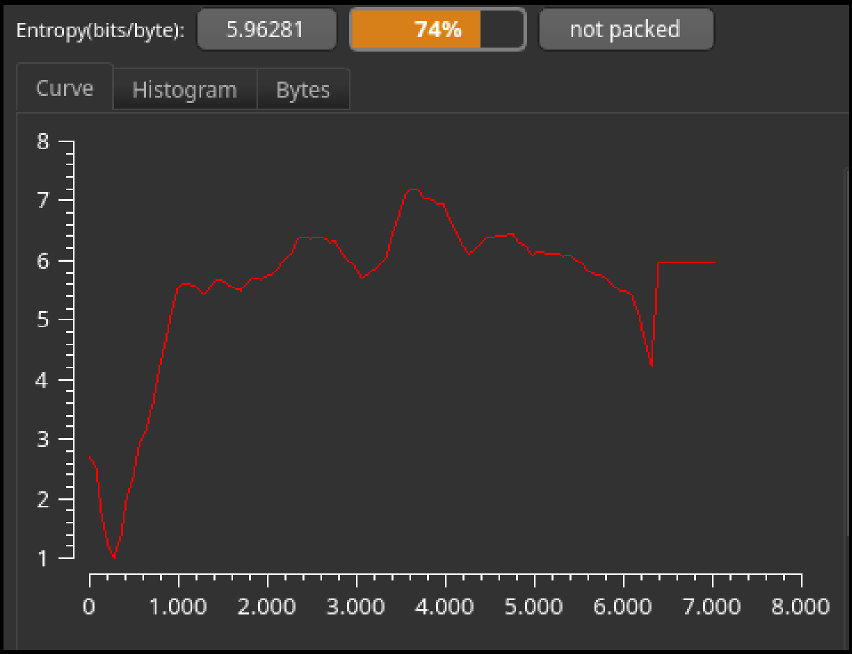
i also checked the memory of the malware searching for packages, but it looks like this :



☑ Address as HEX ☑ Read only

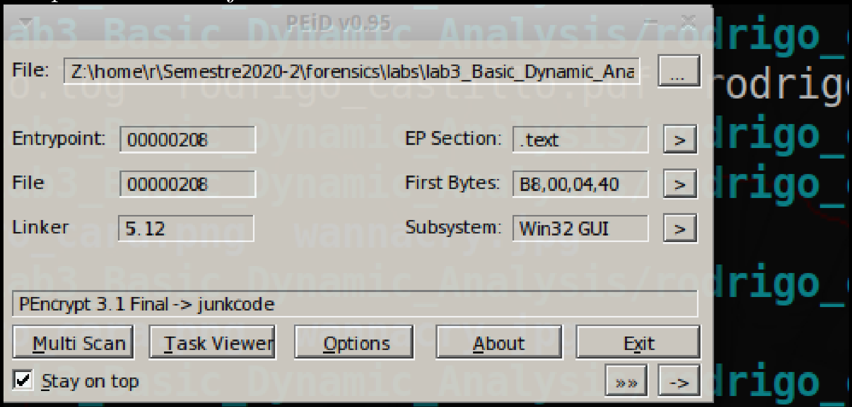
```
00000f30  07 31 47 04 C3 8D 49 00 8B CA 83 E1 1F 74 43 C1  .1G...I......tC.
00000f40  EA 05 8B C2 83 E0 03 8B 04 86 D3 E0 89 07 83 C2  ................
00000f50  01 8B C2 83 E0 03 8B 04 86 50 D3 E0 89 47 04 58  .........P...G.X
00000f60  F6 D9 80 C1 20 D3 E8 33 07 0F C8 89 07 83 C2 01  .......3........
00000f70  83 E2 03 8B 04 96 D3 E8 33 47 04 0F C8 89 47 04  ........3G....G.
00000f80  EB 1D C1 EA 05 8B CA 83 E1 03 8B 04 8E 0F C8 89  ................
00000f90  07 83 C2 01 83 E2 03 8B 04 96 0F C8 89 47 04 C3  .............G..
00000fa0  70 82 2C EC B3 27 C0 E5 E4 85 57 35 EA 0C AE 41  p.,..'....W5...A
00000fb0  23 EF 6B 93 45 19 A5 21 ED 0E 4F 4E 1D 65 92 BD  #.k.E..!..ON.e..
00000fc0  86 B8 AF 8F 7C EB 1F CE 3E 30 DC 5F 5E C5 0B 1A  ....|...>0._^...
00000fd0  A6 E1 39 CA D5 47 5D 3D D9 01 5A D6 51 56 6C 4D  ..9..G]=..Z.QVlM
00000fe0  8B 0D 9A 66 FB CC B0 2D 74 12 2B 20 F0 B1 84 99  ...f...-t.+.....
00000ff0  DF 4C CB C2 34 7E 76 05 6D B7 A9 31 D1 17 04 D7  .L..4~v.m..1....
00001000  14 58 3A 61 DE 1B 11 1C 32 0F 9C 16 53 18 F2 22  .X:a....2...S.."
00001010  FE 44 CF B2 C3 B5 7A 91 24 08 E8 A8 60 FC 69 50  .D....z.$...`.iP
00001020  AA D0 A0 7D A1 89 62 97 54 5B 1E 95 E0 FF 64 D2  ...}..b.T[....d.
00001030  10 C4 00 48 A3 F7 75 DB 8A 03 E6 DA 09 3F DD 94  ...H..u......?..
00001040  87 5C 83 02 CD 4A 90 33 73 67 F6 F3 9D 7F BF E2  .\...J.3sg......
00001050  52 9B D8 26 C8 37 C6 3B 81 96 6F 4B 13 BE 63 2E  R..&.7.;..oK..c.
00001060  E9 79 A7 8C 9F 6E BC 8E 29 F5 F9 B6 2F FD B4 59  .y...n..)..../..Y
00001070  78 98 06 6A E7 46 71 BA D4 25 AB 42 88 A2 8D FA  x..j.Fq..%.B....
00001080  72 07 B9 55 F8 EE AC 0A 36 49 2A 68 3C 38 F1 A4  r..U....6I*h<8..
00001090  40 28 D3 7B BB C9 43 C1 15 E3 AD F4 77 C7 80 9E  @(.{..C.....w...
000010a0  0F 4F 0F 4F 1E 5E 1E 5E 2D 6D 2D 6D 3C 7C 3C 7C  .O.O.^.^-m-m<|<|
000010b0  3C 7C 4D 0D 4D 0D 5E 1E 5E 1E 6F 2F 6F 2F 10 10  <|M.M.^.^.o/o/..
000010c0  20 20 10 10 30 30 00 00 20 20 00 00 10 10 30 30  ....00........00
000010d0  00 00 20 20 10 10 20 20 00 00 30 30 55 8B EC 56  ..........00U..V
000010e0  51 8B 75 08 8B 9E D1 08 00 00 8B 8E D5 08 00 00  Q.u.............
000010f0  8B 94 33 D9 08 00 00 8B 84 33 DD 08 00 00 C1 C2  ..3......3......
00001100  13 C1 C0 1B 03 94 31 D9 08 00 00 03 84 31 DD 08  ......1......1..
00001110  00 00 89 84 33 D9 08 00 00 89 94 33 DD 08 00 00  ....3......3....
00001120  83 EB 08 73 05 BB 80 00 00 00 83 E9 08 73 05 B9  ...s.........s..
00001130  80 00 00 00 89 9E D1 08 00 00 89 8E D5 08 00 00  ................
00001140  59 5E C9 C2 04 00 53 8B 9E D1 08 00 00 8B 8E D5  Y^....S.........
00001150  08 00 00 8B 94 33 D9 08 00 00 8B 84 33 DD 08 00  .....3......3...
00001160  00 C1 C2 13 C1 C0 1B 03 94 31 D9 08 00 00 03 84  .........1......
00001170  31 DD 08 00 00 89 84 33 D9 08 00 00 89 94 33 DD  1......3......3.
00001180  08 00 00 83 EB 08 73 05 BB 80 00 00 00 83 E9 08  ......s.........
00001190  73 05 B9 80 00 00 00 89 9E D1 08 00 00 89 8E D5  s...............
000011a0  08 00 00 5B C3 8D B5 84 F0 FF FF 0F 31 92 33 C9  ...[........1.3.
000011b0  69 C0 05 4B 56 AC 83 C0 01 89 84 8E D9 08 00 00  i..KV...........
000011c0  83 C1 01 83 F9 22 72 E8 D9 E8 DB BE 61 09 00 00  ....."r.....a...
000011d0  C7 86 D1 08 00 00 00 00 00 00 C7 86 D5 08 00 00  ................
000011e0  50 00 00 00 E8 5D FF FF FF 57 BF 1E 00 00 00 E8  P....]...W......
000011f0  52 FF FF FF 83 EF 01 75 F6 5F 64 A1 30 00 00 00  R......u._d.0...
00001200  8B 40 0C 8B 70 1C AD FF 70 08 8F 85 3F FB FF FF  .@..p...p...?...
00001210  68 AD D1 34 41 FF B5 3F FB FF FF 6A 00 E8 4E F8  h..4A..?...j..N.
00001220  FF FF 89 85 21 F1 FF FF E8 09 00 00 00 61 64 76  ....!........adv
00001230  61 70 69 33 32 00 FF 95 21 F1 FF FF 89 85 57 FB  api32...!.....W.
00001240  FF FF E8 06 00 00 00 6E 74 64 6C 6C 00 FF 95 21  .......ntdll...!
00001250  F1 FF FF 89 85 5F FB FF FF E8 07 00 00 00 75 73  ....._........us
00001260  65 72 33 32 00 FF 95 21 F1 FF FF 89 85 43 FB FF  er32...!.....C..
00001270  FF 68 92 F3 DC 04 FF B5 3F FB FF FF 6A 00 E8 ED  .h......?...j...
00001280  F7 FF FF 68 FF 00 00 00 8D 9D 36 F6 FF FF 53 6A  ...h......6...Sj
00001290  00 FF D0 89 45 FC E8 5C 01 00 00 E7 43 B9 20 BB  ....E..\....C...
000012a0  0A 85 00 9D 4A 62 68 BB 0A A1 00 BA 36 C1 0A BB  ....Jbh.....6...
000012b0  0A A5 00 22 FC 89 DA BB 0A B1 00 D5 BA 9B 0E BB  ..."............
000012c0  0A B5 00 3C C8 A5 6B BB 0A B9 00 1B C4 98 74 BB  ...<..k.......t.
000012d0  0A BD 00 E8 A3 64 49 BB 0A C1 00 65 7F 4A CF BB  .....dI....e.J..
000012e0  0A C9 00 8F CD 0B 98 BB 0A CD 00 C4 F2 00 EC DB  ................
000012f0  0A AD 00 81 FE C3 B0 DB 0A A9 00 C4 50 D3 33 BB  ............P.3.
00001300  0A 95 00 07 36 F3 19 BB 0A 29 00 AC 8B DE C7 BB  ....6....)......
00001310  0A 81 00 DE 6F 25 DE BB 0A 51 00 B1 5D D0 5B BB  ....o%...Q.].[.
00001320  0A 55 00 DF 2D 89 8C BB 0A 59 00 93 77 77 21 BB  .U..-....Y..ww!.
00001330  0A 69 00 42 9D 85 85 BB 0A 71 00 31 2B 4B 59 BF  .i.B.....q.1+KY.
00001340  0A 5D 00 8E 2D 10 82 BF 0A 61 00 56 A7 19 AB BF  .]..-....a.V....
00001350  0A 65 00 30 97 B3 9C BF 0A 6D 00 CE F1 DD 63 BF  .e.0.....m....c.
00001360  0A 79 00 78 7B 77 E9 BB 0A 7D 00 23 25 6C 69 BF  .y.x{w...}.#%li.
```

if you check for the entropy of the character of the malware, is obviusly packaged :



Entropy(bits/byte): 5.96281 74% not packed

finally, i found a way to run PeID on linux, and i know that the malware is packed in a compression called junkcode



File: Z:\home\r\Semestre2020-2\forensics\labs\lab3_Basic_Dynamic_Ana

Entrypoint: 00000208
EP Section: .text

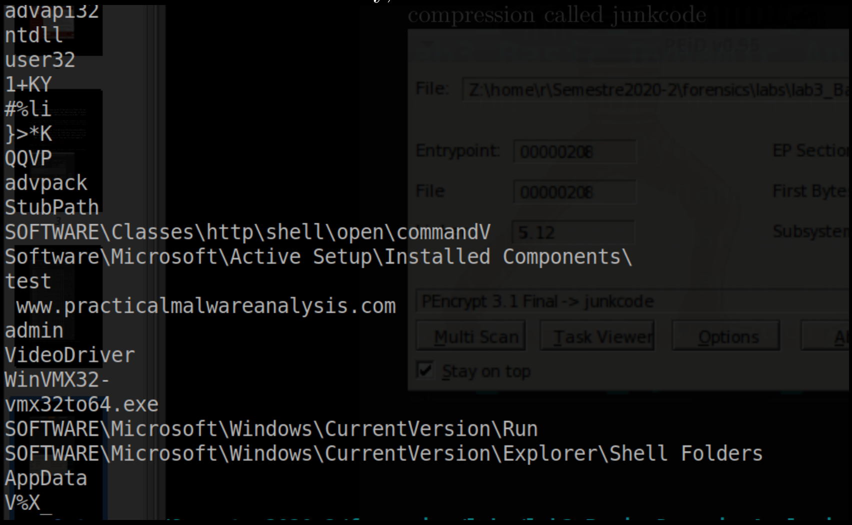
File 00000208
First Bytes: B8,00,04,40

Linker 5.12
Subsystem: Win32 GUI

PEncrypt 3.1 Final -> junkcode

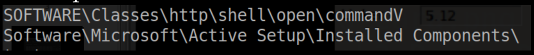
☑ Stay on top

we can see that is a malware from "www.practicalmalwareanalysis.com", its a trojan that connects to this domain.Actually, we can see that is a reverse shell.



```
advapi32
ntdll
user32
1+KY
#%li
}>*K
QQVP
advpack
StubPath
SOFTWARE\Classes\http\shell\open\commandV
Software\Microsoft\Active Setup\Installed Components\
test
 www.practicalmalwareanalysis.com
admin
VideoDriver
WinVMX32-
vmx32to64.exe
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
AppData
V%X_
```

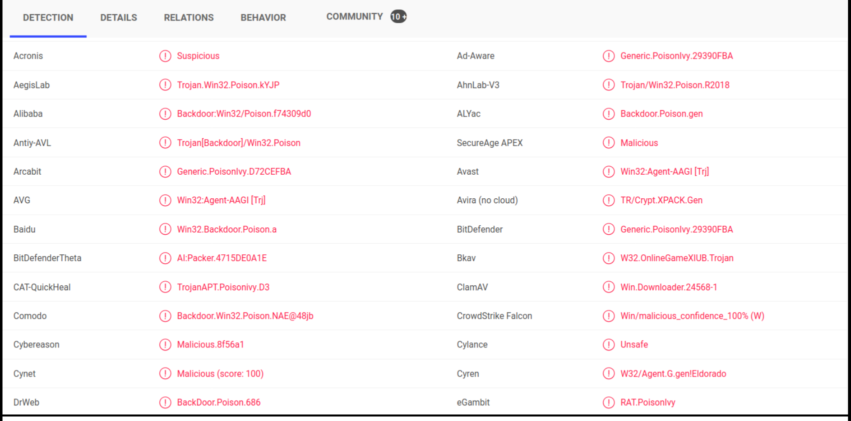
we also can see that it imports kernel32 library so its dangerous, in the binary we can see those paths :



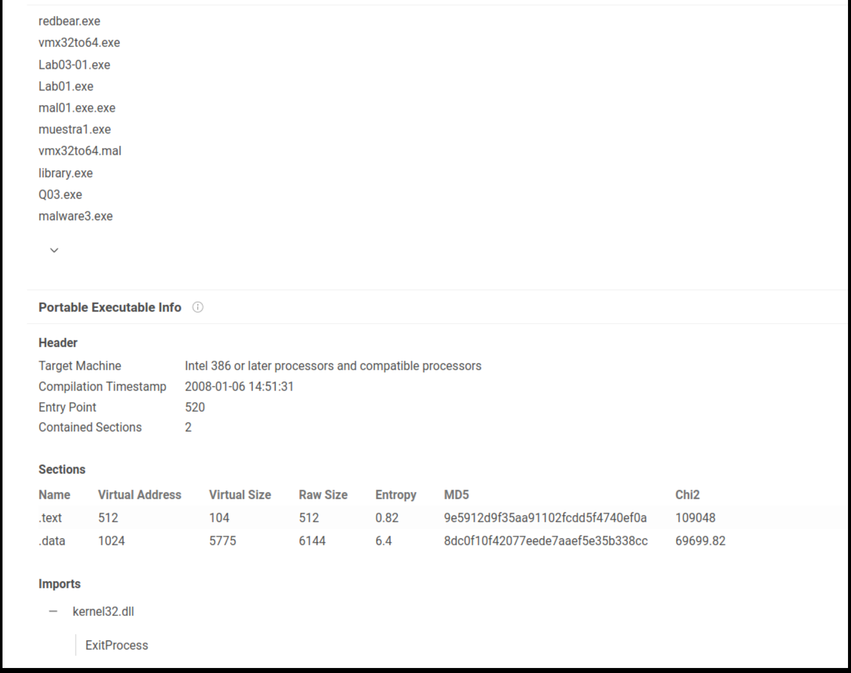
```
SOFTWARE\Classes\http\shell\open\commandV
Software\Microsoft\Active Setup\Installed Components\
```

i dont know too much about windows 32 architecture, but, those path can mean 2 things, the firstone is that he es creating this file for adding malware there, or the secondone is that the malware is modifying this file for addding malware there.

i checked that my analysis was ok in virus total and i was ok. Its a trojan for malware analysis.



Acronis	ⓘ Suspicious	Ad-Aware	ⓘ Generic.PoisonIvy.29390FBA
AegisLab	ⓘ Trojan.Win32.Poison.kYJP	AhnLab-V3	ⓘ Trojan/Win32.Poison.R2018
Alibaba	ⓘ Backdoor:Win32/Poison.f74309d0	ALYac	ⓘ Backdoor.Poison.gen
Antiy-AVL	ⓘ Trojan[Backdoor]/Win32.Poison	SecureAge APEX	ⓘ Malicious
Arcabit	ⓘ Generic.PoisonIvy.D72CEFBA	Avast	ⓘ Win32:Agent-AAGI [Trj]
AVG	ⓘ Win32:Agent-AAGI [Trj]	Avira (no cloud)	ⓘ TR/Crypt.XPACK.Gen
Baidu	ⓘ Win32.Backdoor.Poison.a	BitDefender	ⓘ Generic.PoisonIvy.29390FBA
BitDefenderTheta	ⓘ AI:Packer.4715DE0A1E	Bkav	ⓘ W32.OnlineGameXIUB.Trojan
CAT-QuickHeal	ⓘ TrojanAPT.Poisonivy.D3	ClamAV	ⓘ Win.Downloader.24568-1
Comodo	ⓘ Backdoor.Win32.Poison.NAE@48jb	CrowdStrike Falcon	ⓘ Win/malicious_confidence_100% (W)
Cybereason	ⓘ Malicious.8f56a1	Cylance	ⓘ Unsafe
Cynet	ⓘ Malicious (score: 100)	Cyren	ⓘ W32/Agent.G.gen!Eldorado
DrWeb	ⓘ BackDoor.Poison.686	eGambit	ⓘ RAT.PoisonIvy



redbear.exe
vmx32to64.exe
Lab03-01.exe
Lab01.exe
mal01.exe.exe
muestra1.exe
vmx32to64.mal
library.exe
Q03.exe
malware3.exe

Portable Executable Info ⓘ

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2008-01-06 14:51:31
Entry Point	520
Contained Sections	2

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	512	104	512	0.82	9e5912d9f35aa91102fcdd5f4740ef0a	109048
.data	1024	5775	6144	6.4	8dc0f10f42077eede7aaef5e35b338cc	69699.82

Imports

— kernel32.dll

ExitProcess