

# 计算机病毒及其防治技术

## Lab4-Yara 引擎检测

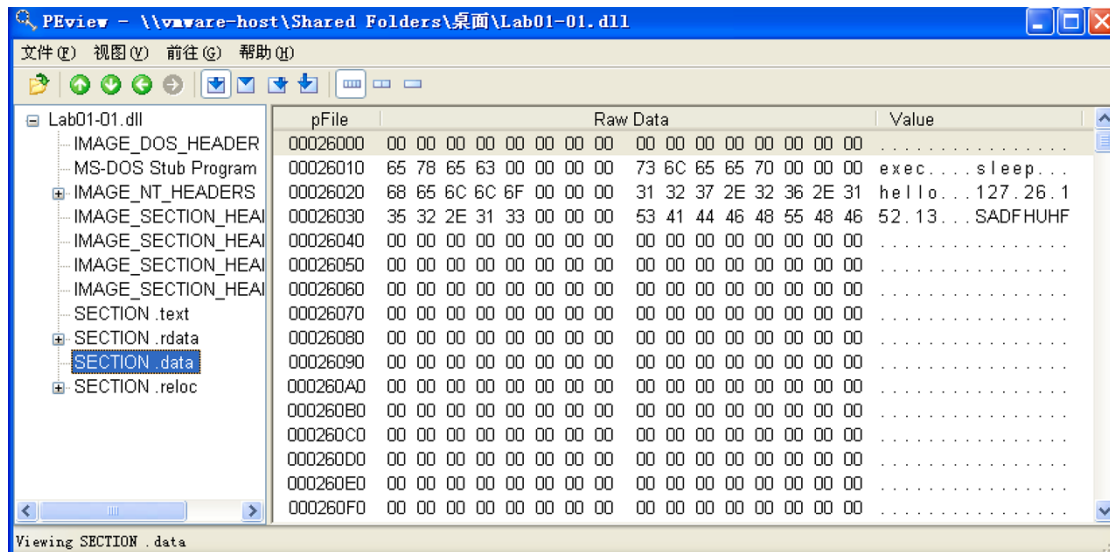
沙璇 1911562

### Lab 4

Q1:对Lab1 和Lab3 的样本编写Yara 规则

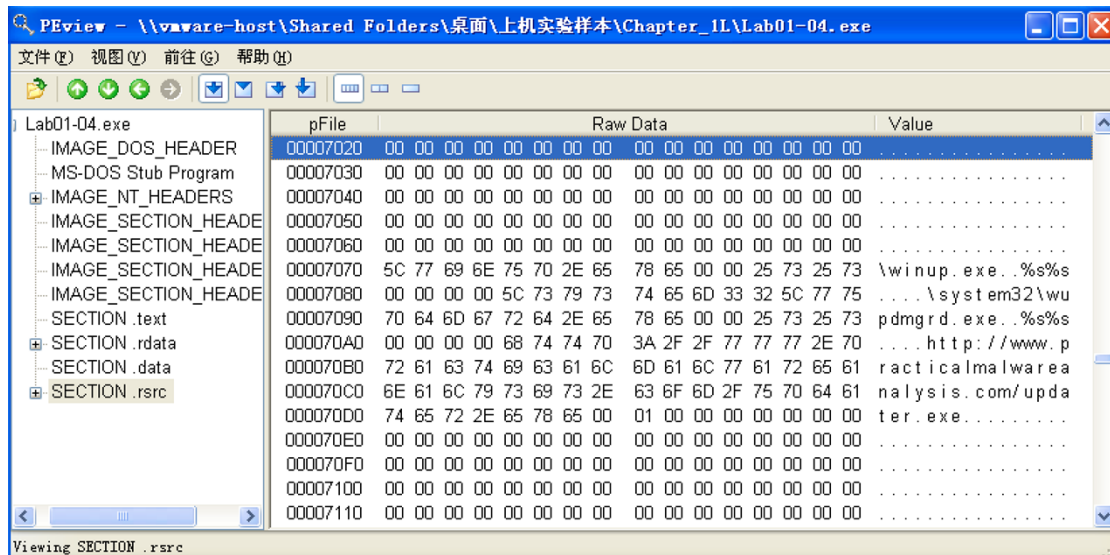
编写 yara 规则, 需要对病毒样本进行分析, 根据其特征进行编写。

根据实验报告 1, Lab01-01:



得到 ip 地址 127.26.13

Lab01-04:



得到字符串 <http://www.practicalmalwareanalysis.com>

以及 winup.exe

Yara 规则编写如下:

```
rule ll {
```

$$\}$$

根据实验报告 3, lab03-01:

IDA - C:\Documents and Settings\Administrator\Desktop\虚拟机实验样本\Chapter\_3L\Lab03-01.exe

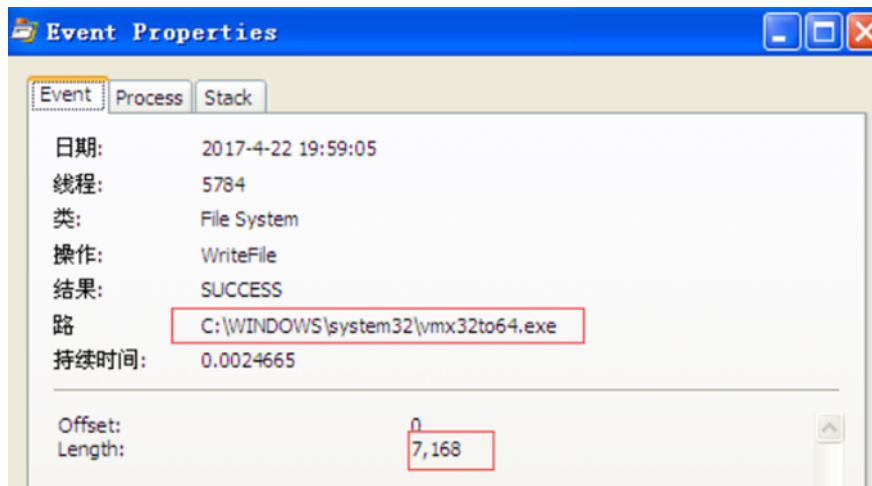
File Edit Jump Search View Debugger Options Windows Help

Library function Data Regular function Unexplored Instruction External symbol

Functions window IDA View-A Strings window Hex View-A Structures

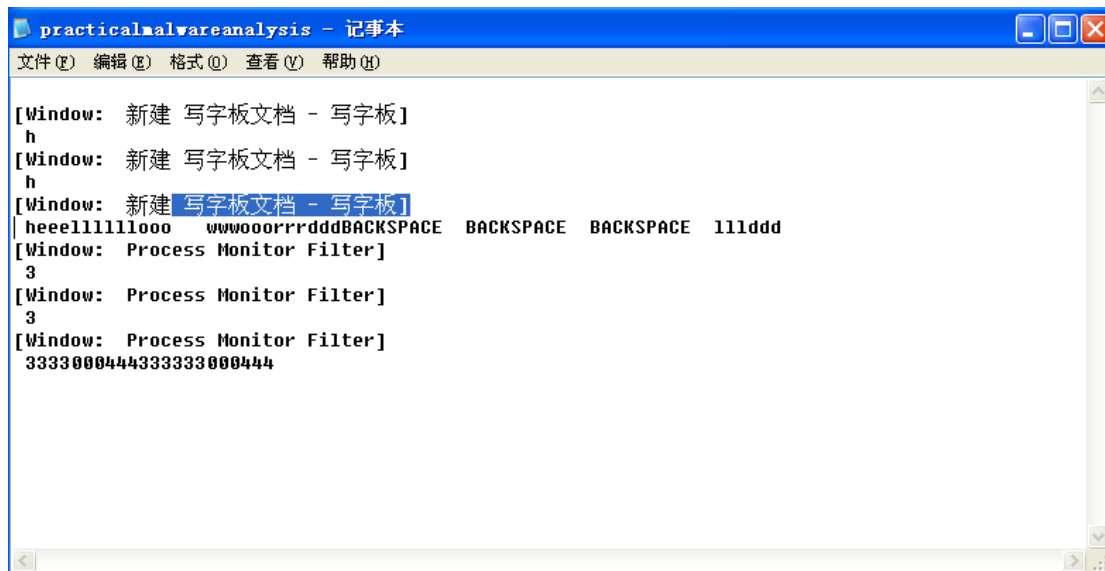
Function name	Segment	Address	Length	Type	String
start	.text	text:00400000	0000000D	C	kernel32.dll
sub_400400	.data	.data:00400000	00000005	C	\b\alG
sub_4004D9	.data	.data:00400007	00000007	C	\nSI*hG
sub_4007D4	.data	.data:00400010	00000010	C	~-m< < < M\rM\r
sub_400A70	.data	.data:00400008	00000008	C	ntdll
sub_400BCB	.data	.data:00400007	00000007	C	user32
sub_401146	.data	.data:00400008	00000008	C	柏湖湖n=
		.data:00400008	00000008	C	4D能n
		.data:00400008	00000008	C	}>K能n
		.data:00400008	00000008	C	advpack
		.data:00400008	00000008	C	StubPath
		.data:004000029	00000029	C	SOFTWARE\\Classes\\http\\shell\\open\\commandV
		.data:004000035	00000035	C	Software\\Microsoft\\Active Setup\\Installed Components\\
		.data:004000022	00000022	C	www.practicalmalwareanalysis.com
		.data:004000007	00000007	C	admin\\tr
		.data:004000008	00000008	C	VideoDriver
		.data:004000009	00000009	C	WinVMX32-
		.data:00400000D	0000000D	C	vmx32to64.exe
		.data:004000008	00000008	C	AppData

网址 [www.practicalmalwareanalysis.com](http://www.practicalmalwareanalysis.com)



写入的新程序 vmx32to64.exe

Lab03-03:



找到同一个目录下生成的 log 文件 : practicalmalwareanalysis.log

Yara 规则编写如下:

```
rule 13 {
  meta:
    description="lab3 "
  strings:
    $a="www.practicalmalwareanalysis.com"wide ascii
    $b="vmx32to64.exe"wide ascii
    $c="practicalmalwareanalysis.log"wide ascii

  condition:
    $a or $b or $c
}
```

**Q2: 使用自己编写的规则对自己电脑的C盘进行Yara引擎的扫描, 记录扫描所用时间**

Lab1 规则通过 yara64 运行, 输入 C:/目录和-r 全文件指令, 对本机的 C 盘进行扫描, 记录扫描时间大约为 10 分钟。

```
选择命令提示符 - yara64 lab1 C:\-r
Microsoft Windows [版本 10.0.19042.1237]
(c) Microsoft Corporation. 保留所有权利。

C:\Users\15389>cd Desktop\yara-v4.1.2-1693-win64

C:\Users\15389\Desktop\yara-v4.1.2-1693-win64>echo rule 11{meta:description="lab1" strings:$a="127.26.152.13"wide ascii
$b="http://www.practicalmalwareanalysis.com" wide ascii $c="winup.exe" wide ascii condition: $a or $b or $c}>lab1

C:\Users\15389\Desktop\yara-v4.1.2-1693-win64>yara64 lab1 C:\ -r
11 C:\\$Recycle.Bin\\S-1-5-21-3074820558-2449994026-59155067-1001\\$ROHPHKS\\Lab01-01.dll
11 C:\\$Recycle.Bin\\S-1-5-21-3074820558-2449994026-59155067-1001\\$ROHPHKS\\Lab01-04.exe
error scanning C:\\DumpStack.log.tmp: could not open file
error scanning C:\\hiberfil.sys: could not open file
error scanning C:\\KRECYCLE\\00019290.KVQ: could not open file
error scanning C:\\pagefile.sys: could not open file
error scanning C:\\Program Files\\Common Files\\mcafee\\amcore\\EM\\EMSystemWideDataStore_00.PTF: could not open file
```

Lab2 规则 yara64 运行, 输入 C:/目录和-r 全文件指令, 对本机的 C 盘进行扫描, 记录扫描时间大约为 8 分钟。

```
命令提示符 - yara64 lab3 C:\-r
Microsoft Windows [版本 10.0.19042.1237]
(c) Microsoft Corporation. 保留所有权利。

C:\Users\15389>cd Desktop\yara-v4.1.2-1693-win64

C:\Users\15389\Desktop\yara-v4.1.2-1693-win64>echo rule 13{meta:description="lab3" strings:$a="www.practicalmalwareanalysis.com"wide ascii $b="vmx32to64.exe"wide ascii $c="practicalmalwareanalysis.log"wide ascii condition:$a or $b or $c}>lab3

C:\Users\15389\Desktop\yara-v4.1.2-1693-win64>yara64 lab3 C:\ -r
13 C:\\$Recycle.Bin\\S-1-5-21-3074820558-2449994026-59155067-1001\\$ROHPHKS\\Lab01-04.exe
error scanning C:\\DumpStack.log.tmp: could not open file
error scanning C:\\hiberfil.sys: could not open file
error scanning C:\\KRECYCLE\\00019290.KVQ: could not open file
error scanning C:\\pagefile.sys: could not open file
error scanning C:\\Program Files\\Common Files\\mcafee\\amcore\\EM\\EMSystemWideDataStore_00.PTF: could not open file
error scanning C:\\Program Files\\Microsoft SQL Server\\MSSQL10.SQLEXPRESS\\MSSQL\\Template Data\\tempdb.mdf: could not open file
error scanning C:\\Program Files\\Microsoft SQL Server\\MSSQL10.SQLEXPRESS\\MSSQL\\Template Data\\templog.ldf: could not open file
error scanning C:\\Program Files\\Microsoft SQL Server\\MSSQL10.SQLEXPRESS\\MSSQL\\Template Data\\MS_AgentSigningCertificate.cer: could not open file
error scanning C:\\Program Files\\Microsoft SQL Server\\MSSQL15.SQLEXPRESS01\\MSSQL\\Template Data\\tempdb.mdf: could not open file
error scanning C:\\Program Files\\Microsoft SQL Server\\MSSQL15.SQLEXPRESS01\\MSSQL\\Template Data\\templog.ldf: could not open file
error scanning C:\\Program Files (x86)\\Steam\\steamapps\\common\\The Witcher 3\\Blood and Wine extras\\Blood and Wine OST\\flac\\09 The Musty Scent of Fresh Pat .flac: could not open file
error scanning C:\\Program Files (x86)\\Steam\\steamapps\\common\\The Witcher 3\\Blood and Wine extras\\Blood and Wine OST\\mp3\\
```

**Q3: 讨论哪些 Yara 条件执行效率高, 哪些 Yara 条件执行效率低。如何改进那些执行效率低的 Yara 条件?**

- ☐ 低效的 yara 规则可以匹配当前的样本, 但匹配不了其他相似的恶意样本(如同一个家族的)。
- ☐ yara 规则太过具体, 也同样不能匹配多个样本。
- ☐ 生成高效通用的 yara 规则, 能通用地匹配恶意软件, 不会出现在合法软件中。同时, 给扫描样本加上大小限制, 达到更精确的效果。