

**恶意代码课程实验报告**

**实验三：基本动态分析**

****

学 院 网络安全学院

专 业 信息安全

学 号 2110688

姓 名 史文天

班 级 1063

1. **实验目的**

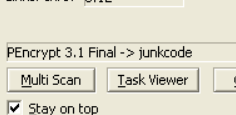
**完成教材Lab3的实验内容，编写Lab3样本的Yara引擎规则，并测试规则的执行效率。**

1. **实验原理**

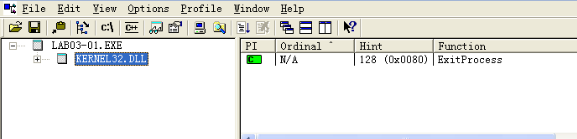
**配置XP虚拟机环境，安装动态、静态分析工具，使用动态分析工具。**

1. **实验过程**
2. **Lab03-01**
3. **找出这个恶意代码的导入函数与字符串列表？**

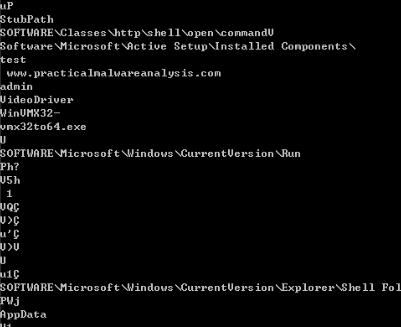
**使用PEiD打开，检测加壳信息。如图所示，可以看到壳为PEncrypt 3.1 Final -> junkcode**



**由于未进行脱壳，因此导入函数不完整，仅有一个ExitProcess。**

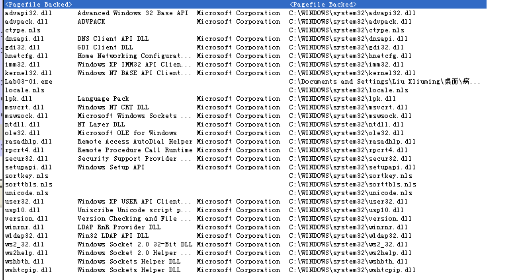


**下面使用Strings查看文件的字符串，可以看到一些诸如WinVMX32、VideoDriver、vmx32to64.exe、注册表位置、注册表键值、url等信息。如下图所示。**

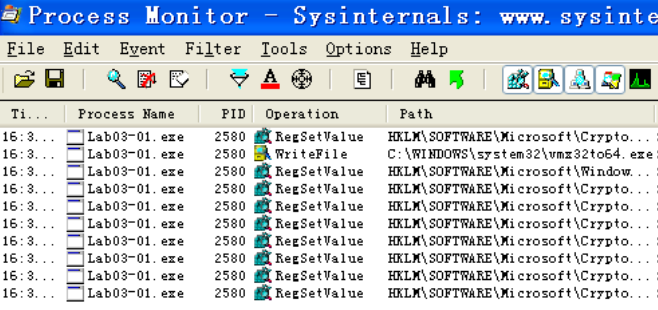


1. **这个恶意代码在主机上的感染迹象特征是什么？**

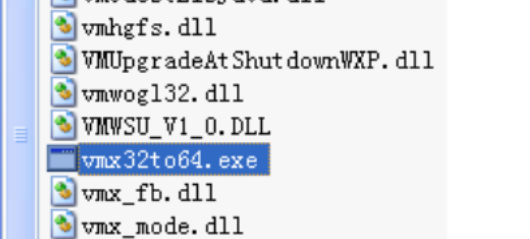
**打开Process Explorer，然后运行Lab03-01.exe，可以看到其对应的进程。选择查看其Handles，可以看到已经创建了互斥量WinVMX32，与字符串分析结果一致。选择查看其DLL，可以看到一些与联网功能有关的动态链接库。**



**返回Process Monitor，可以看到，此时已经监听到许多项目。进一步筛选，填入Operation is RegSetValue和Operation is WriteFile两个条件，可以检索到文件的相关操作记录。**



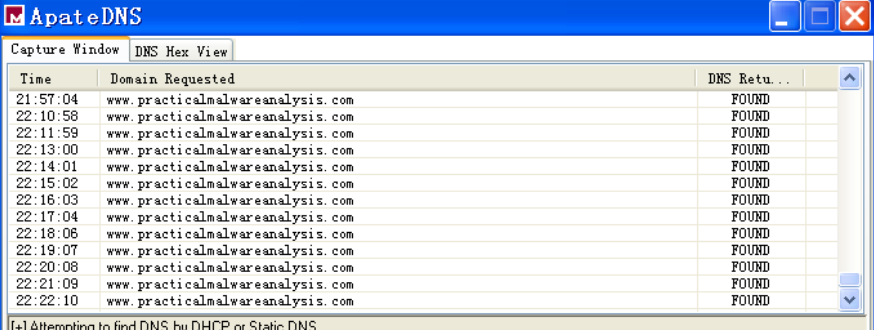
**点击查看相关操作记录，可以看到，文件向C:\WINDOWS\system32\vmx32to64.exe中写入了7168字节。按照其给定的路径，可以找到该文件。**



**除此之外，文件还将数据写入注册表项，命名为VideoDriver。分析可知，该文件将vmx32to64.exe写入到了开机启动的项目中。**

1. **这个恶意代码是否存在一些有用的网络特征吗？如果存在，它们是什么？**

**恶意代码执行了DNS请求，持续访问**[**www.praticalmalwareanalysis.com**](http://www.praticalmalwareanalysis.com)**，向该域名对应的服务器源源不断发送数据包。**



1. **Lab03-02**
2. **你怎样才能让这个恶意代码自行安装?**

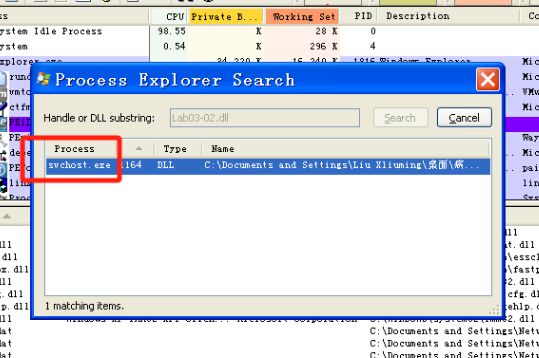
**使用rundll32.exe Lab03-02.dll,installA或rundll32.exe Lab03-02.dll,install指令。**

1. **在安装之后，你如何让这个恶意代码运行起来？**

**使用net start IPRIP指令。**

1. **你怎么能找到这个恶意代码是在哪个进程下运行的？**

**使用Process Explorer工具，检索Lab03-02.dll，就可以看到该恶意代码是svchost.exe进程下运行。**

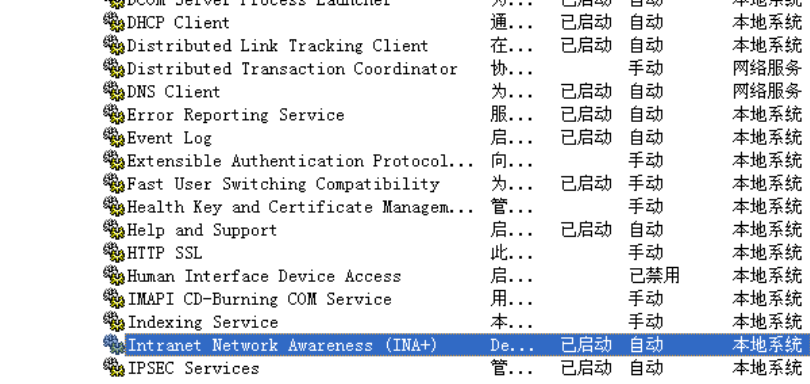


1. **你可以在procmon工具中设置什么样的过滤器，才能收集这个恶意代码的信息？**

**由上面分析可知，该恶意代码依附运行的进程的ID为1164，即设置PID is 1164即可收集该恶意代码的信息。**

1. **这个恶意代码在主机上的感染迹象特征是什么？**

**该恶意代码安装了IPRIP服务，并将其写入注册表，添加到开机启动项目中。**

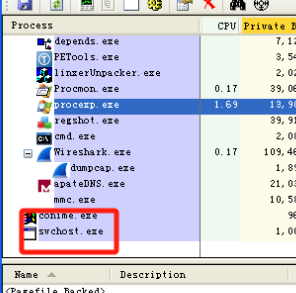


1. **这个恶意代码是否存在一些有用的网络特征码？**

**由上面分析可知，该恶意代码对practicalmalwareanalysis.com进行了访问，并向其发送数据交互请求，使用80端口HTTP协议。做一个GET 请求，请求的资源是serve.html，使用%ComputerName% Windows XP 6.11的用户代理。**

1. **Lab03-03**
2. **当你使用Process Explorer 工具进行监视时，你注意到了什么？**

**文件运行时创建了一个子进程，接着结束掉自己的进程，留下了之前创建的子进程独立运行。**

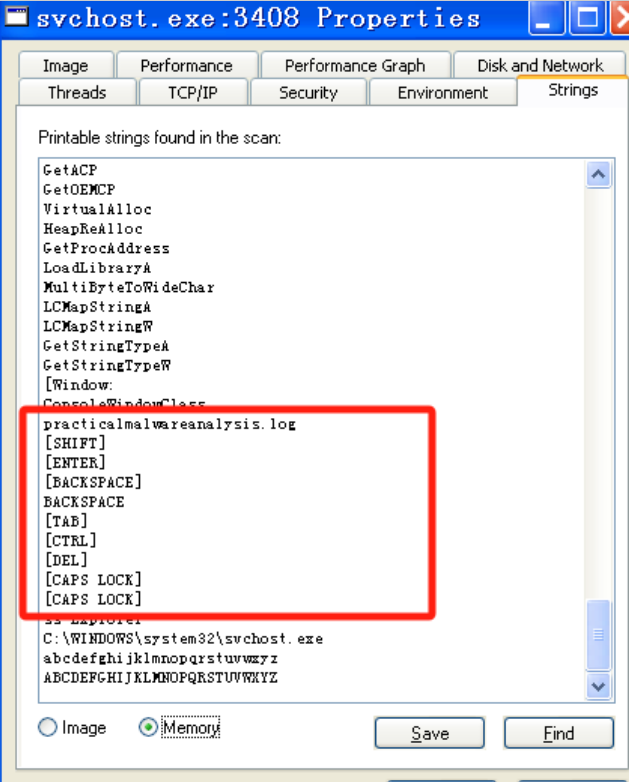


1. **你可以找出任何的内存修改行为吗？**

**该恶意代码将svchost.exe留下运行，而该进程在内存与磁盘中的字符串存在区别。**

1. **这个恶意代码在主机上的感染迹象特征是什么？**

**主机内存中多出了practicalmalwareanalysis.log 和[SHIFT]、[ENTER]、[BACKSPACE]等不该出现的字符串。基于以上字符，推测是一个敲击键盘的记录器，将键盘键入的信息保存到practicalmalwareanalysis.log文件中。**



1. **这个恶意代码的目的是什么？**

**该恶意代码利用进程替换技术，将内存中的svchost.exe进程替换成一个键盘键入记录器，将键盘键入的信息记录在了practicalmalwareanalysis.log文件中。**

1. **Lab03-04**
2. **当你运行这个文件时，会发生什么呢？**

**文件会自己删除。**

1. **是什么原因造成动态分析无法有效实施？**

**怀疑是因为缺少命令行参数或是程序内容有残缺。**

1. **是否有其他方式来运行这个程序？**

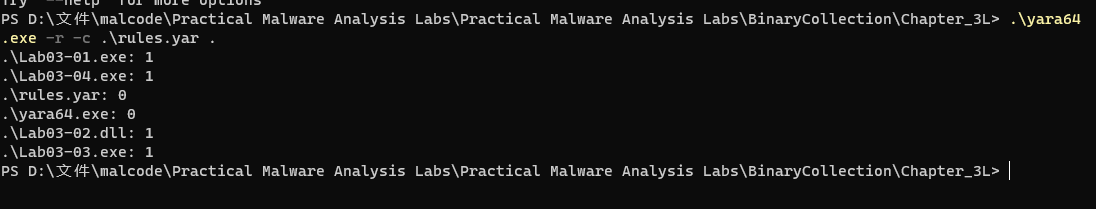
**尝试使用命令行并加入参数等方式运行程序，但依旧无法成功运行。**

1. **Yara规则**

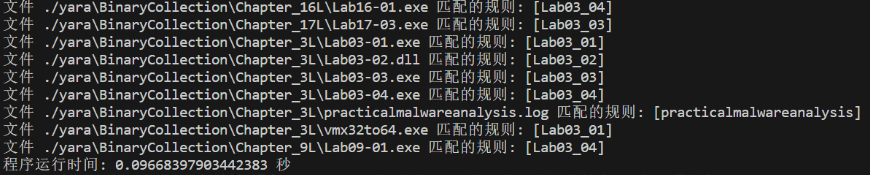
**根据以上分析结果，同时利用Yaragen工具，得到Yara规则如下。**

1. rule Lab03\_01 {
2. meta:
3. description = " - file Lab03-01.exe"
4. author = "yarGen Rule Generator"
5. reference = "https://github.com/Neo23x0/yarGen"
6. date = "2023-09-25"
7. hash1 = "eb84360ca4e33b8bb60df47ab5ce962501ef3420bc7aab90655fd507d2ffcedd"
8. strings:
9. $s1 = "vmx32to64.exe" fullword ascii
10. $s2 = "SOFTWARE\\Classes\\http\\shell\\open\\commandV" fullword ascii
11. $s3 = " www.practicalmalwareanalysis.com" fullword ascii
12. $s4 = "CONNECT %s:%i HTTP/1.0" fullword ascii
13. $s5 = "advpack" fullword ascii
14. $s6 = "VideoDriver" fullword ascii
15. $s7 = "AppData" fullword ascii */\* Goodware String - occured 74 times \*/*
16. $s8 = "6I\*h<8" fullword ascii */\* Goodware String - occured 1 times \*/*
17. $s9 = "StubPath" fullword ascii */\* Goodware String - occured 1 times \*/*
18. $s10 = "WinVMX32-" fullword ascii
19. $s11 = "Software\\Microsoft\\Active Setup\\Installed Components\\" fullword ascii */\* Goodware String - occured 4 times \*/*
20. $s12 = "^-m-m<|<|<|M" fullword ascii
21. condition:
22. uint16(0) == 0x5a4d and filesize < 20KB and 8 of them
23. }
24. rule Lab03\_02 {
25. meta:
26. description = " - file Lab03-02.dll"
27. author = "yarGen Rule Generator"
28. reference = "https://github.com/Neo23x0/yarGen"
29. date = "2023-09-25"
30. hash1 = "5eced7367ed63354b4ed5c556e2363514293f614c2c2eb187273381b2ef5f0f9"
31. strings:
32. $x1 = "%SystemRoot%\\System32\\svchost.exe -k " fullword ascii
33. $x2 = "cmd.exe /c " fullword ascii
34. $s3 = "RegOpenKeyEx(%s) KEY\_QUERY\_VALUE error ." fullword ascii
35. $s4 = "Lab03-02.dll" fullword ascii
36. $s5 = "practicalmalwareanalysis.com" fullword ascii
37. $s6 = "RegOpenKeyEx(%s) KEY\_QUERY\_VALUE success." fullword ascii
38. $s7 = "GetModuleFileName() get dll path" fullword ascii
39. $s8 = "dW5zdXBwb3J0" fullword ascii */\* base64 encoded string 'unsupport' \*/*
40. $s9 = "Y29ubmVjdA==" fullword ascii */\* base64 encoded string 'connect' \*/*
41. $s10 = "OpenService(%s) error 2" fullword ascii
42. $s11 = "OpenService(%s) error 1" fullword ascii
43. $s12 = "CreateService(%s) error %d" fullword ascii
44. $s13 = "You specify service name not in Svchost//netsvcs, must be one of following:" fullword ascii
45. $s14 = "RegQueryValueEx(Svchost\\netsvcs)" fullword ascii
46. $s15 = "netsvcs" fullword ascii
47. $s16 = "serve.html" fullword ascii
48. $s17 = "DependOnService" fullword ascii
49. $s18 = ":$:2:K:U:\\:l:" fullword ascii
50. $s19 = "uninstall is starting" fullword ascii
51. $s20 = "uninstall success" fullword ascii
52. condition:
53. uint16(0) == 0x5a4d and filesize < 70KB and 1 of ($x\*) and 4 of them
54. }
55. rule Lab03\_03 {
56. meta:
57. description = " - file Lab03-03.exe"
58. author = "yarGen Rule Generator"
59. reference = "https://github.com/Neo23x0/yarGen"
60. date = "2023-09-25"
61. hash1 = "ae8a1c7eb64c42ea2a04f97523ebf0844c27029eb040d910048b680f884b9dce"
62. strings:
63. $s1 = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA" ascii
64. $s2 = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA" ascii
65. $s3 = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA" ascii
66. $s4 = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA" ascii
67. $s5 = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA" ascii
68. $s6 = "aAAAAAAAAAAAAAAAAAAAAAAA" ascii
69. $s7 = "\\svchost.exe" fullword ascii
70. $s8 = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA" ascii
71. $s9 = "BAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA" ascii
72. $s10 = "AAAAAAAAAAAAAAAAAAAAAAAAAAA" ascii
73. $s11 = "AAAAAABAAAAA" ascii "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA" ascii
74. $s13 = "AAAqAAApAAAsAAArAAAuAAAtAAAwAAAvAAAyAAAxAAA" fullword ascii
75. $s14 = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA" ascii
76. $s15 = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAq" fullword ascii
77. $s16 = "wqpwLKla/.5a$/.4&)a21 \"$a'.3a5)3$ %a% 5 LKALK #/.3, -a13.&3 ,a5$3,(/ 5(./LKAAAA" fullword ascii
78. $s17 = "- 22AA13 \"5(\" -, -6 3$ / -82(2o-.&AAAAaAAA" fullword ascii
79. $s18 = "+A+A+A+A" fullword ascii */\* reversed goodware string 'A+A+A+A+' \*/*
80. $s19 = "(\"3.2.'5a" fullword ascii */\* hex encoded string '2Z' \*/*
81. $s20 = "wqswLKla/.5a$/.4&)a21 \"$a'.3a25%(.a(/(5( -(; 5(./LKAAAA" fullword ascii
82. condition:
83. uint16(0) == 0x5a4d and filesize < 200KB and 8 of them
84. }
85. rule Lab03\_04 {
86. meta:
87. description = " - file Lab03-04.exe"
88. author = "yarGen Rule Generator"
89. reference = "https://github.com/Neo23x0/yarGen"
90. date = "2023-09-25"
91. hash1 = "6ac06dfa543dca43327d55a61d0aaed25f3c90cce791e0555e3e306d47107859"
92. strings:
93. $s1 = "http://www.practicalmalwareanalysis.com" fullword ascii
94. $s2 = "%SYSTEMROOT%\\system32\\" fullword ascii
95. $s3 = " HTTP/1.0" fullword ascii
96. $s4 = " Manager Service" fullword ascii
97. $s5 = "UPLOAD" fullword ascii */\* Goodware String - occured 1 times \*/*
98. $s6 = "DOWNLOAD" fullword ascii */\* Goodware String - occured 26 times \*/*
99. $s7 = "command.com" fullword ascii */\* Goodware String - occured 55 times \*/*
100. $s8 = "COMSPEC" fullword ascii */\* Goodware String - occured 140 times \*/*
101. $s9 = "\"WWSh(" fullword ascii */\* Goodware String - occured 1 times \*/*
102. $s10 = "SOFTWARE\\Microsoft \\XPS" fullword ascii
103. $s11 = "k:%s h:%s p:%s per:%s" fullword ascii
104. $s12 = " >> NUL" fullword ascii
105. $s13 = "/c del " fullword ascii
106. $s14 = "6KRich" fullword ascii
107. condition:
108. uint16(0) == 0x5a4d and filesize < 200KB and 8 of them
109. }

**运行结果如下，可看到成功匹配所有文件。**



**在存放所有样例的文件夹下测试其检测效率，结果如下。**



1. **实验结论及心得体会**
2. **尝试了各种动态分析工具，对动态分析有了一定了解。**
3. **了解了更多恶意代码的形式和特征。**