计算机病毒及其防治技术

Lab3

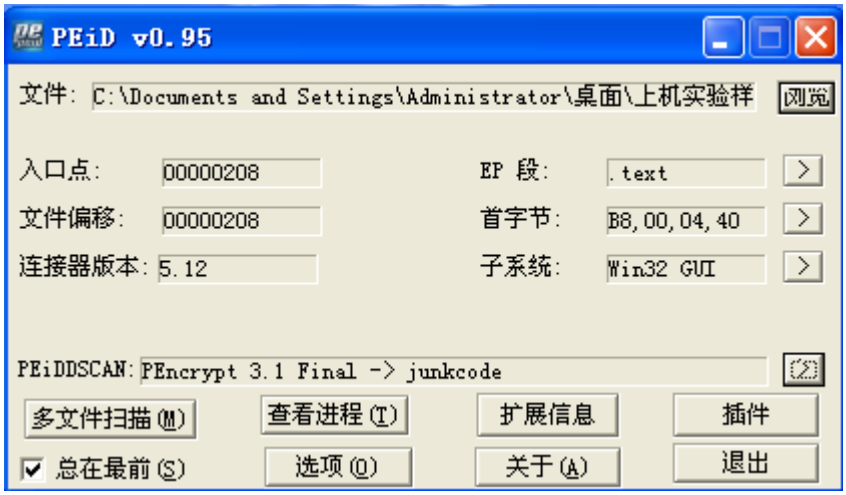
沙璇 1911562

Lab 3-1

用基本动态分析工具分析 lab03-01.exe 中的恶意代码

Q1: *此代码中的导入函数与字符串列表？*

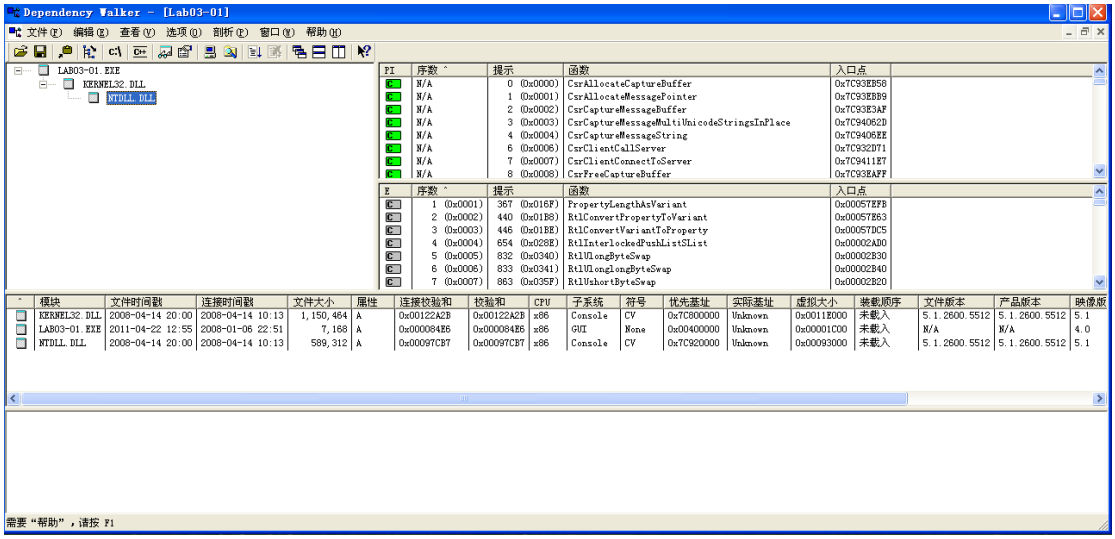
Peid 查看是否有壳：



可以看出文件被 PEncrypt 加密

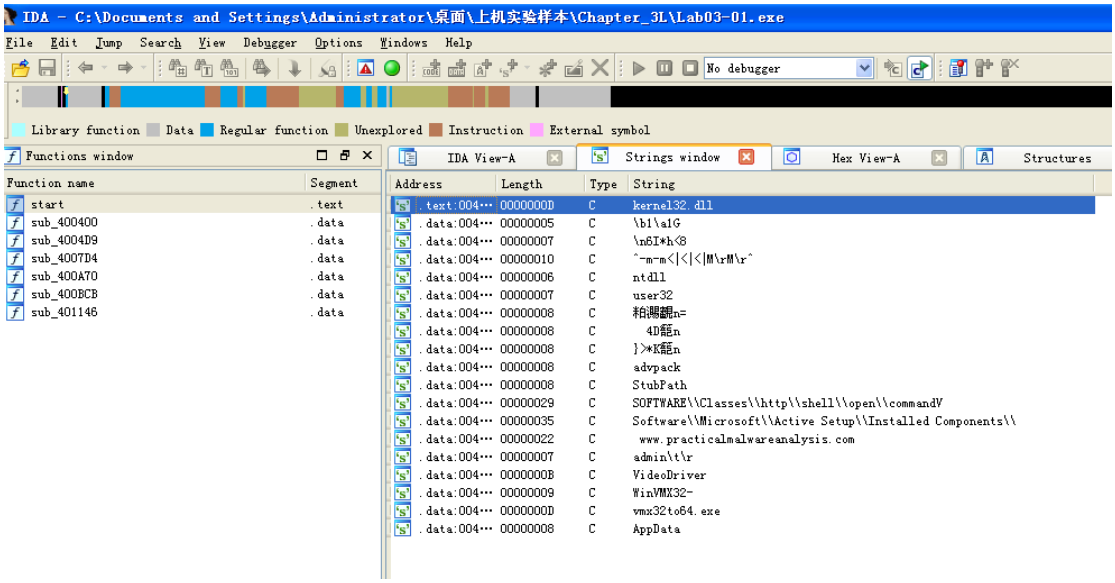
尝试脱壳。使用 Unpacker 脱壳失败。

使用 Dependency Walker 查看导入函数：



可以看到的是，此时的输入表里只有很少的函数。

使用 ida pro 查看字符串：



注册表

SOFTWARE\Classes\http\shell\open\commandV

Software\Microsoft\Active Setup\Installed Components

SOFTWARE\Microsoft\Windows\CurrentVersion\Run

SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

网址

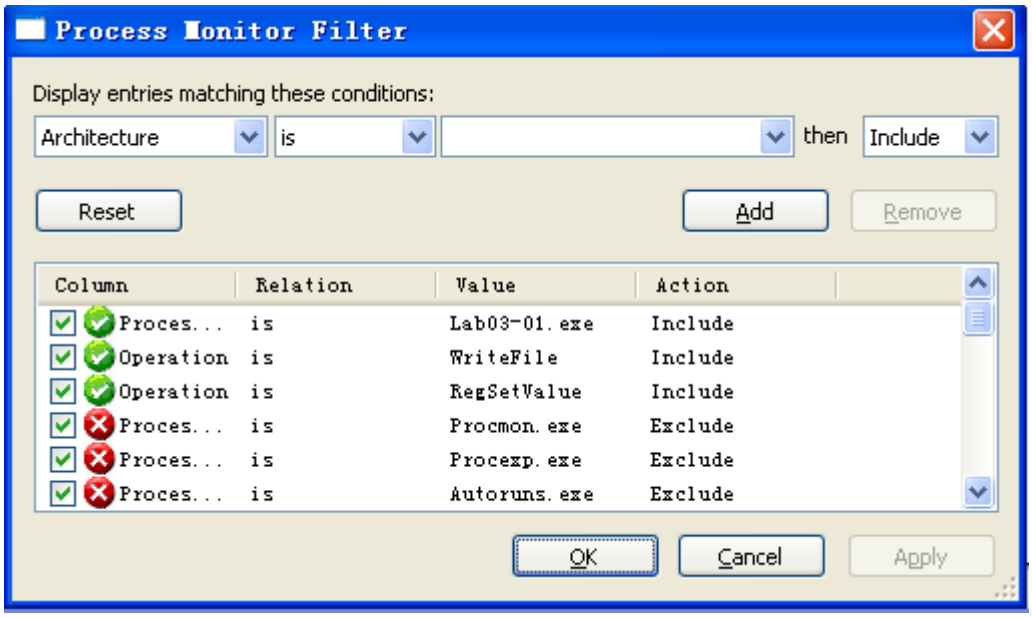
www.practicalmalwareanalysis.com

Q2: *这个恶意代码在主机上的感染迹象特征是什么？*

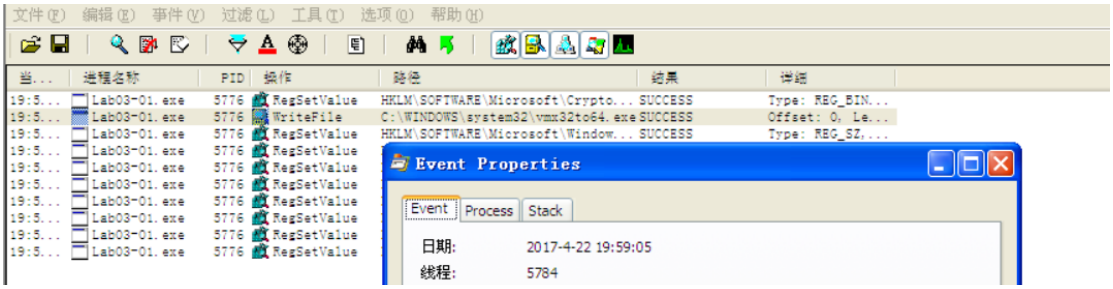
首先用 process monitor 打开该文件。

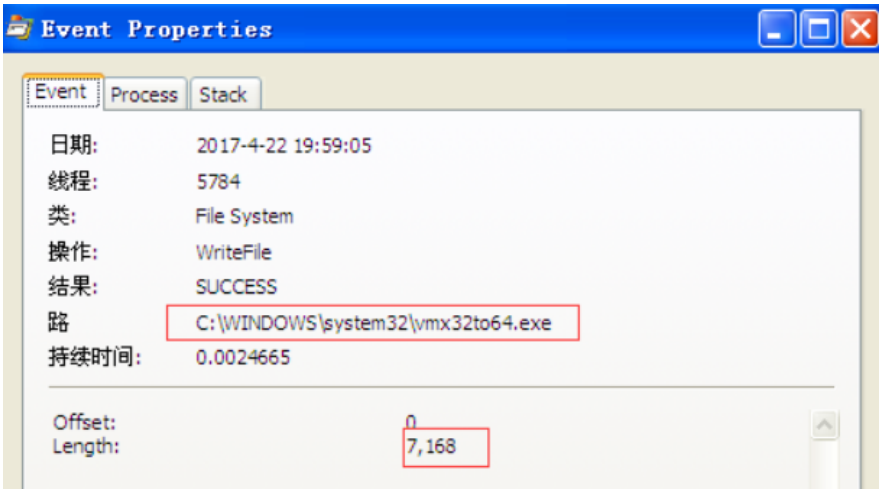
实际上由静态分析得到的字符串可以猜测该程序实际上是对注册表进行诸如写入之类操作实现的。

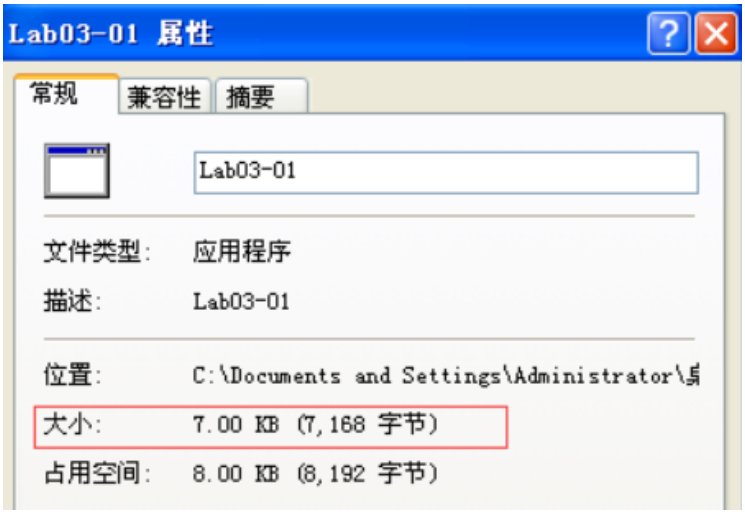
由于这个工具监视的项目过多，进行过滤操作：对程序对注册表的更改、写文件。



过滤得：

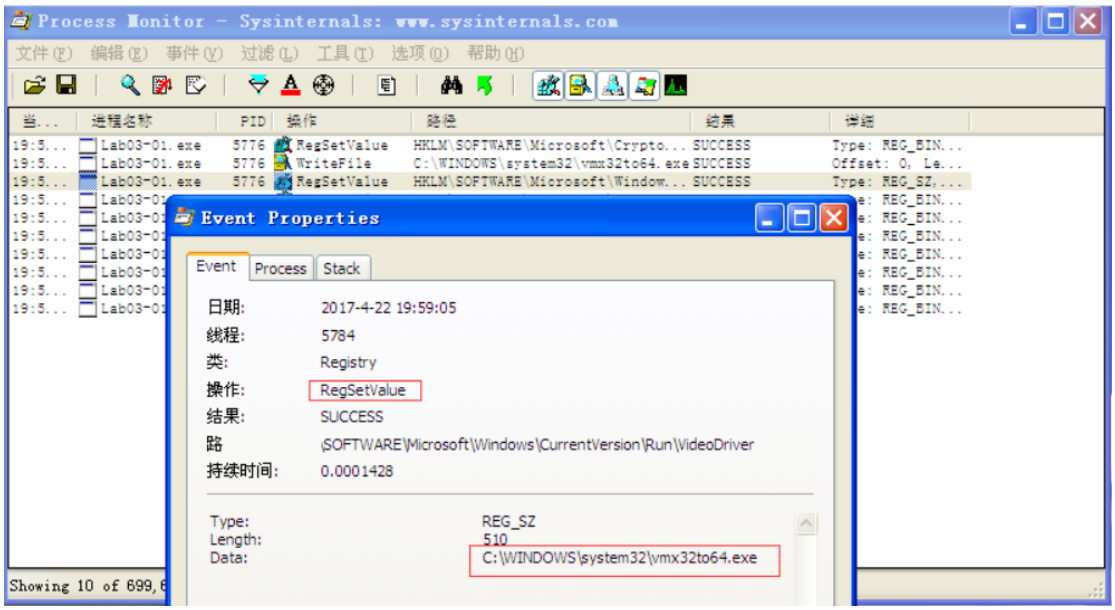






恶意代码在系统中写入了一个新程序叫做 vmx32to64.exe，这个新的可执行程序的长度为 7168。与 Lab03-01.exe 程序本身长度是一致的。

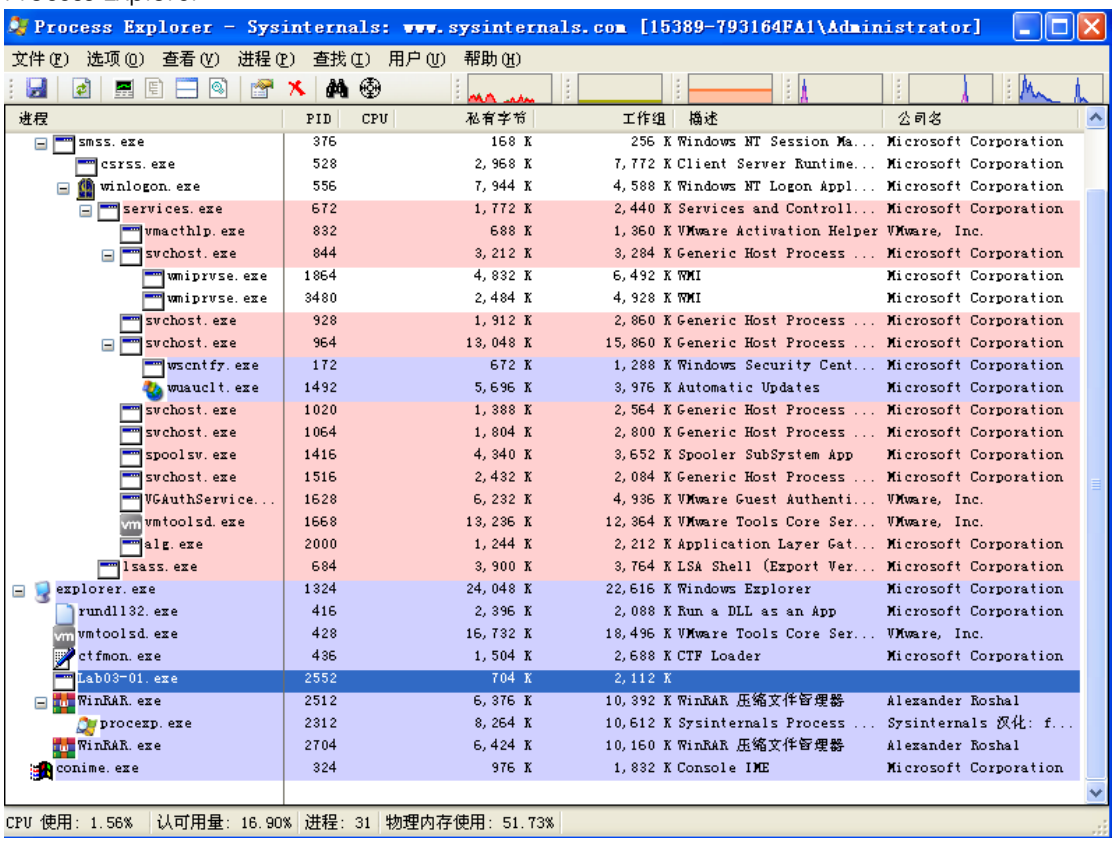
再看过滤出的写入注册表值：



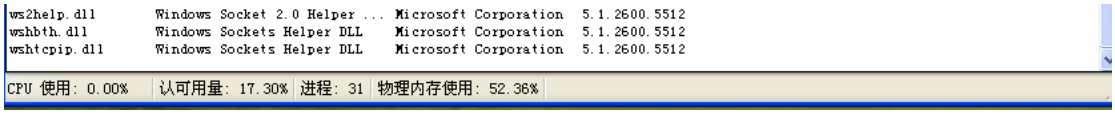
可以看到写入的注册表自启动项键值的数据，路径就是刚创建的那个可执行程序。

Q3: *这个恶意代码是否存在一些有用的网络特征码？如果存在，它们是什么？*

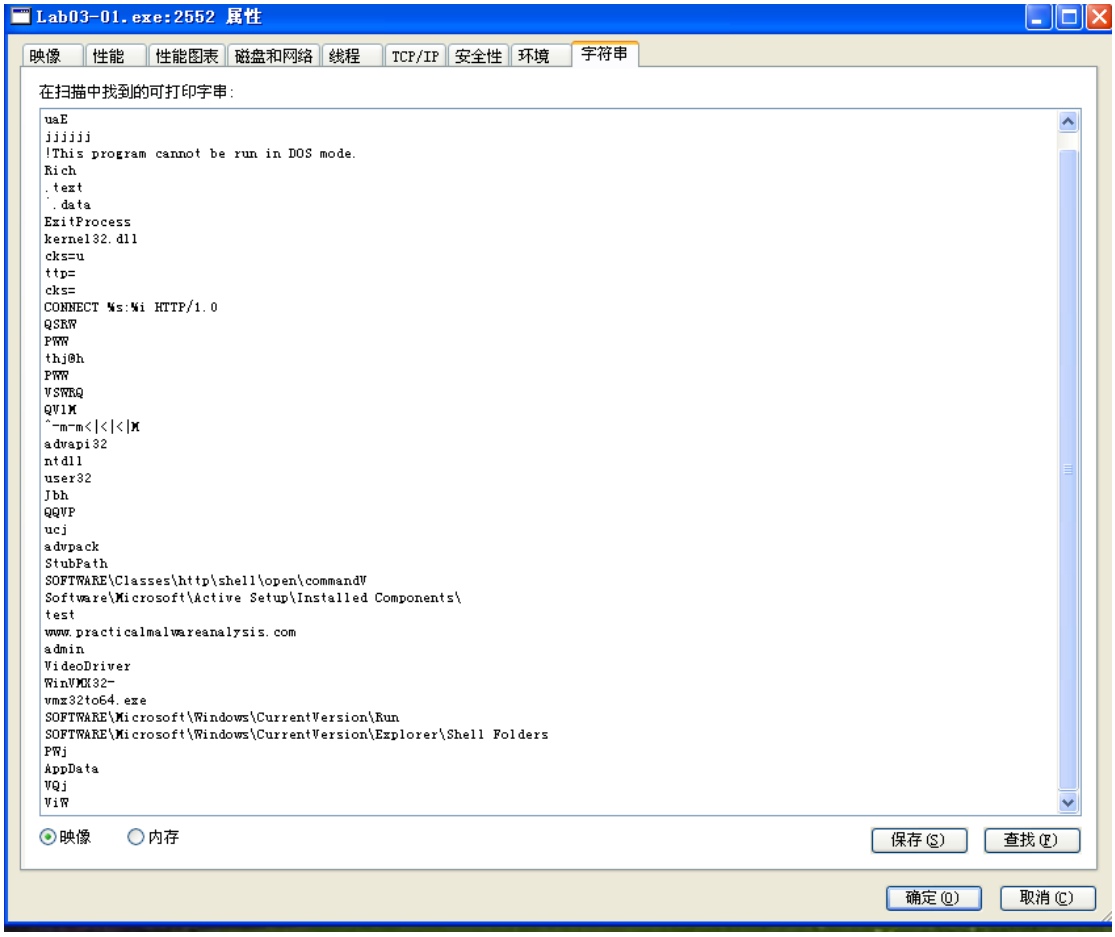
Process Explorer



可以看到 Lab03-01.exe 是一个已经运行的进程。查看 dlls：



发现有进行联网操作的相关 dll
查看字符串



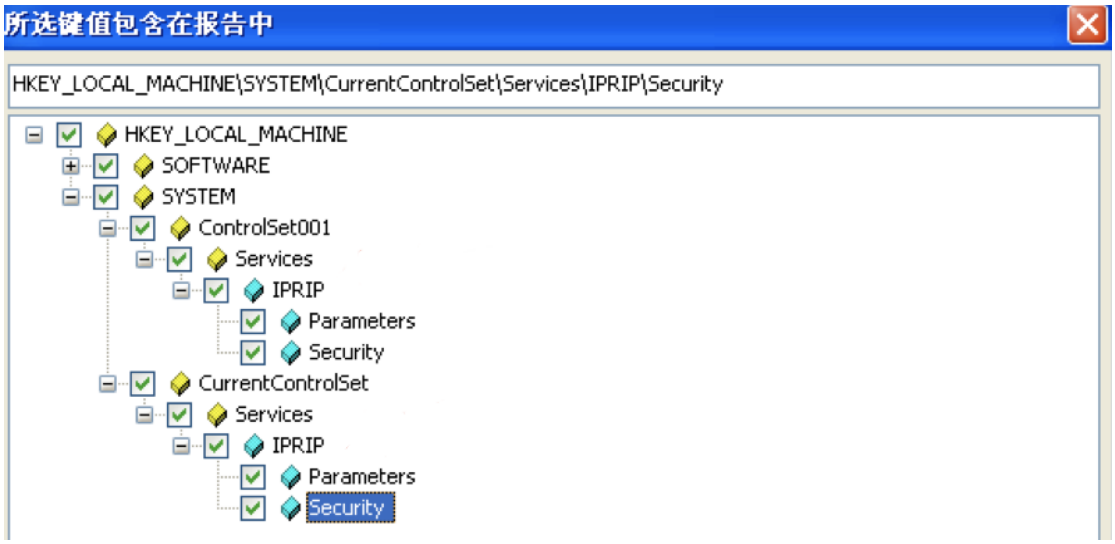
访问 www.practicalmalwareanalysis.com 网址
CONNECT %s:%i HTTP/1.0 联网

Lab 3-2

使用动态分析基础技术分析在 Lab03-02.dll 文件中发现的恶意代码。

Q1:*你怎样才能让这个恶意代码自行安装？*

Windows 系统中的 rundll32.exe 专用于运行 dll 程序。在该 dll 目录下运行 `rundll32.exe Lab03-02.dll,installA` 即可安装。我们使用 regshot 查看安装前后变化：



发现了这个 iprip 服务。

新添加键 (6) 快照 B

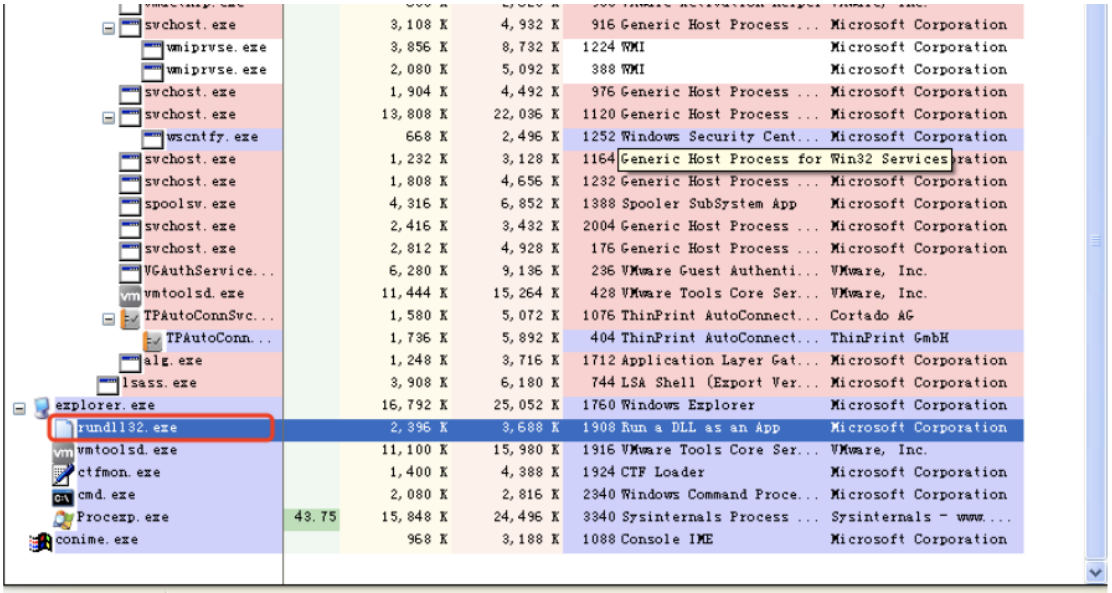
```
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\IPRIP]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IPRIP]
```

已删除值 (0) 快照 A

新添加值 (20) 快照 B

```
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\IPRIP]
"Type"=dword:00000020
"Start"=dword:00000002
"ErrorControl"=dword:00000001
"ImagePath"=hex(2):25,00,53,00,79,00,73,00,74,00,65,00,6d,00,52,00,6f,00,6f,00,\
```

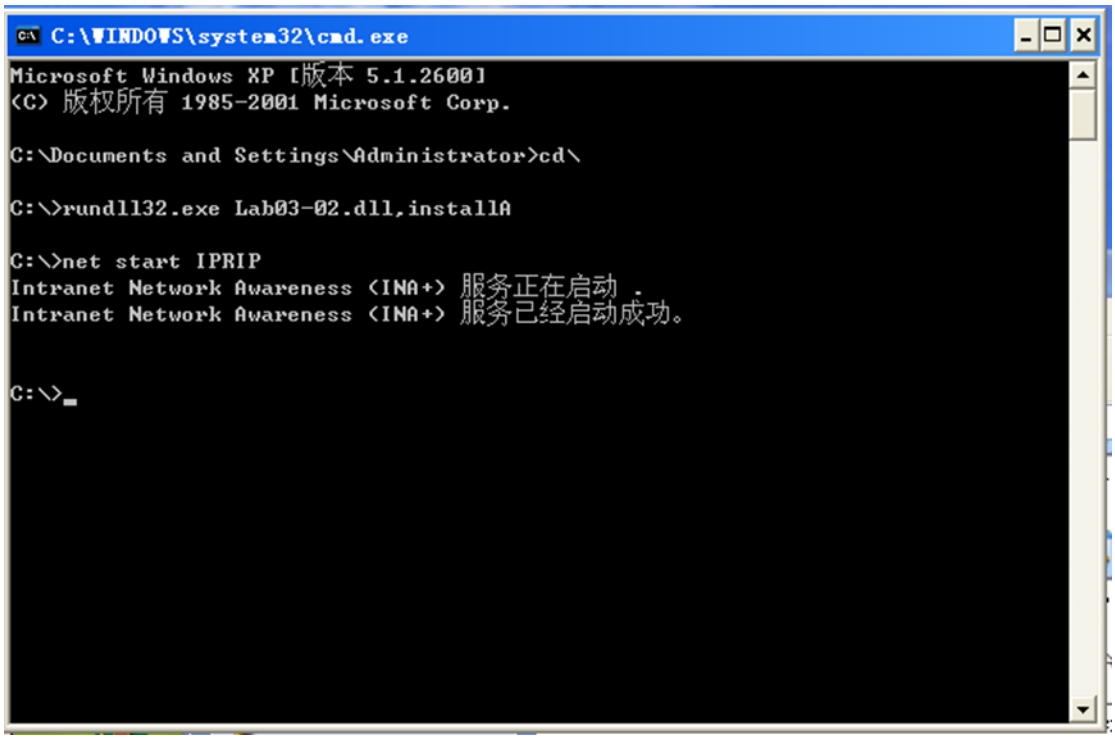
process explorer 查看：



发现 rundll32.exe 正在运行。

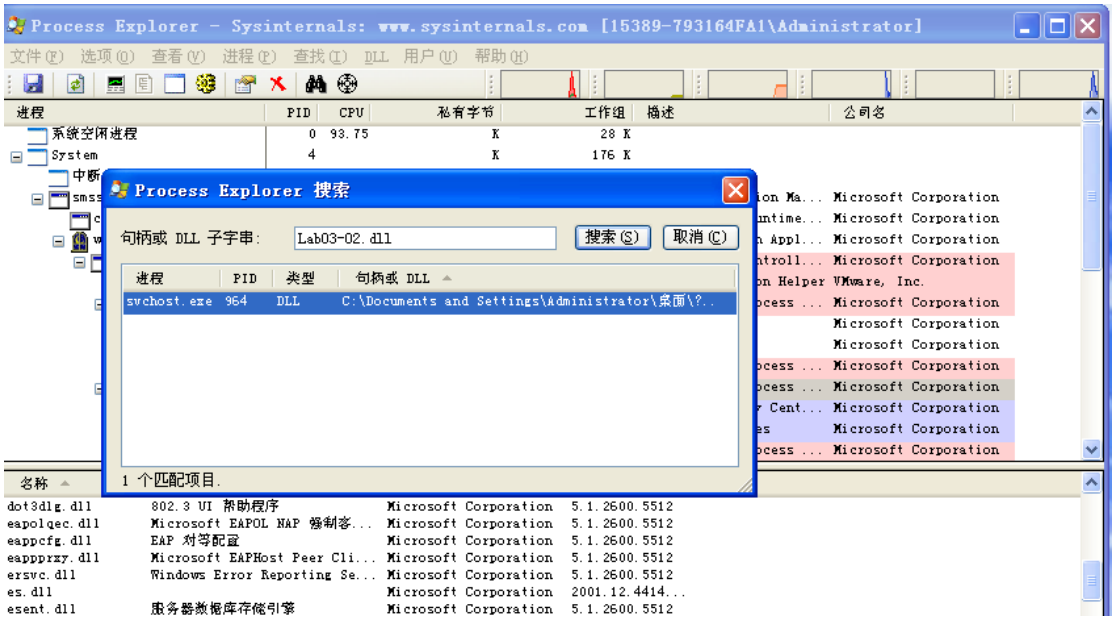
Q2:*你怎样才能让这个恶意代码运行起来？*

在安装过程中发现了 iprip 服务，net start IPRIP



Q3: *你怎么可以找到这个恶意代码在哪个进程下运行的？*

使用 process explorer 搜索 dll

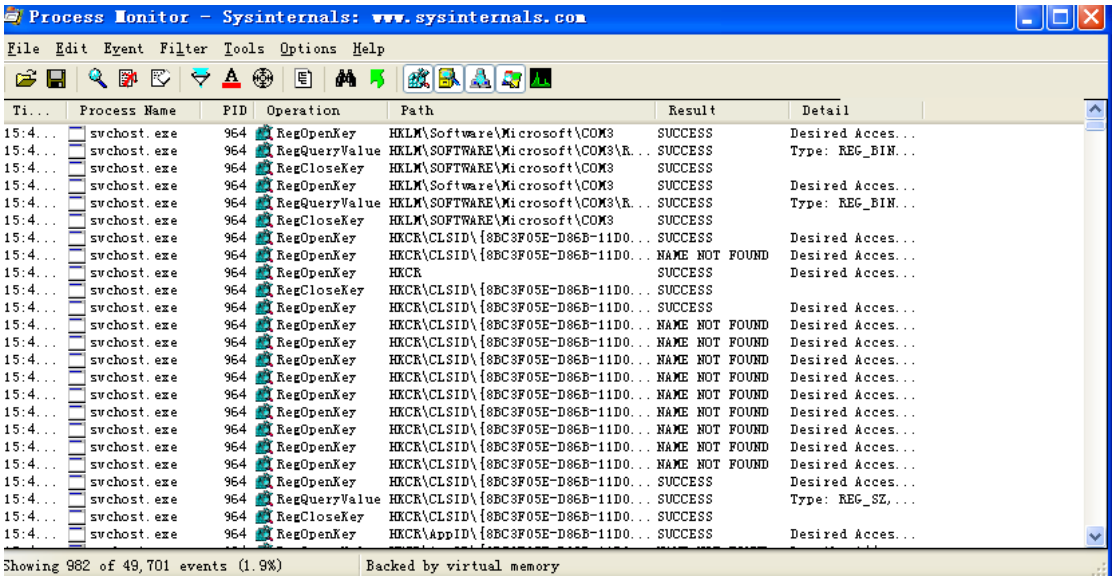


在 svchost.exe 进程下。

Q4: *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？*

在 procmon 里，打开 filter

然后设置 PID 为刚刚发现的值 964，就可以收集这个恶意代码的信息



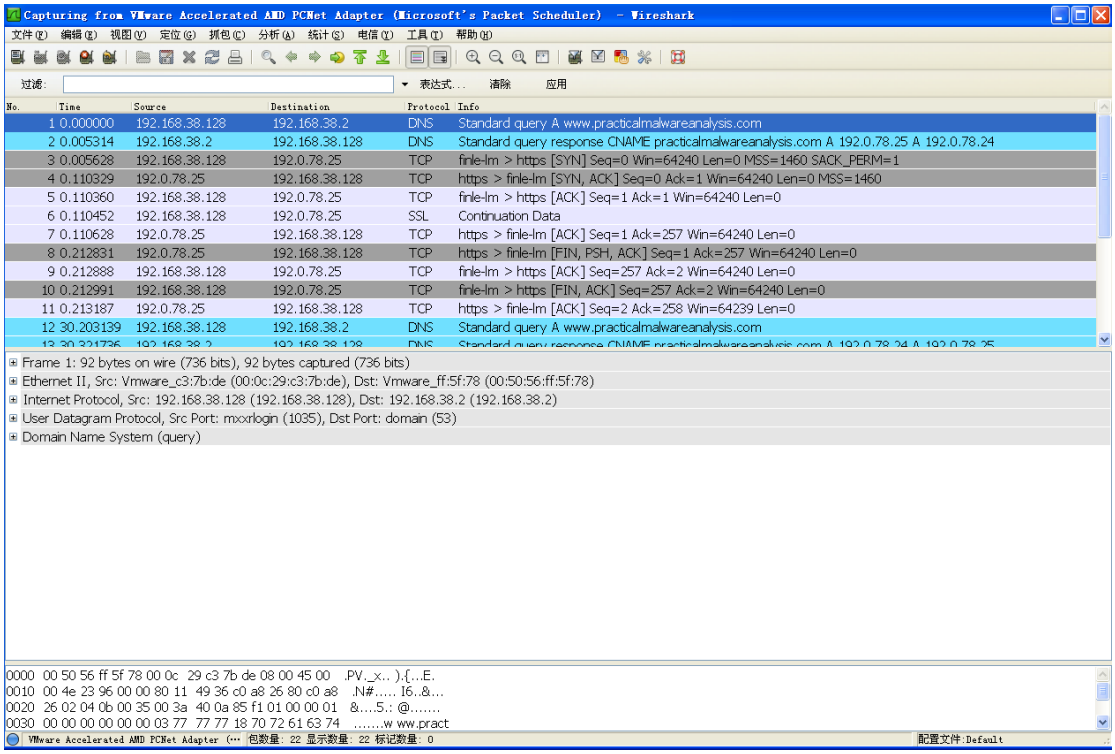
```
Process Monitor - Sysinternals: www.sysinternals.com
Ti...  Process Name  PID  Operation      Path                                Result          Detail
15:4...  svchost.exe  964  RegOpenKey     HKLM\Software\Microsoft\COM3        SUCCESS         Desired Acces...
15:4...  svchost.exe  964  RegQueryValue  HKLM\SOFTWARE\Microsoft\COM3\R...   SUCCESS         Type: REG_BIN...
15:4...  svchost.exe  964  RegCloseKey    HKLM\SOFTWARE\Microsoft\COM3        SUCCESS
15:4...  svchost.exe  964  RegOpenKey     HKLM\Software\Microsoft\COM3        SUCCESS         Desired Acces...
15:4...  svchost.exe  964  RegQueryValue  HKLM\SOFTWARE\Microsoft\COM3\R...   SUCCESS         Type: REG_BIN...
15:4...  svchost.exe  964  RegCloseKey    HKLM\SOFTWARE\Microsoft\COM3        SUCCESS
15:4...  svchost.exe  964  RegOpenKey     HKCR\CLSID\{8BC3F05E-D86B-11D0...   SUCCESS         Desired Acces...
15:4...  svchost.exe  964  RegOpenKey     HKCR\CLSID\{8BC3F05E-D86B-11D0...   NAME NOT FOUND  Desired Acces...
15:4...  svchost.exe  964  RegOpenKey     HKCR                                SUCCESS         Desired Acces...
15:4...  svchost.exe  964  RegCloseKey    HKCR\CLSID\{8BC3F05E-D86B-11D0...   SUCCESS
15:4...  svchost.exe  964  RegOpenKey     HKCR\CLSID\{8BC3F05E-D86B-11D0...   SUCCESS         Desired Acces...
15:4...  svchost.exe  964  RegOpenKey     HKCR\CLSID\{8BC3F05E-D86B-11D0...   NAME NOT FOUND  Desired Acces...
15:4...  svchost.exe  964  RegOpenKey     HKCR\CLSID\{8BC3F05E-D86B-11D0...   NAME NOT FOUND  Desired Acces...
15:4...  svchost.exe  964  RegOpenKey     HKCR\CLSID\{8BC3F05E-D86B-11D0...   NAME NOT FOUND  Desired Acces...
15:4...  svchost.exe  964  RegOpenKey     HKCR\CLSID\{8BC3F05E-D86B-11D0...   NAME NOT FOUND  Desired Acces...
15:4...  svchost.exe  964  RegOpenKey     HKCR\CLSID\{8BC3F05E-D86B-11D0...   NAME NOT FOUND  Desired Acces...
15:4...  svchost.exe  964  RegOpenKey     HKCR\CLSID\{8BC3F05E-D86B-11D0...   NAME NOT FOUND  Desired Acces...
15:4...  svchost.exe  964  RegOpenKey     HKCR\CLSID\{8BC3F05E-D86B-11D0...   NAME NOT FOUND  Desired Acces...
15:4...  svchost.exe  964  RegOpenKey     HKCR\CLSID\{8BC3F05E-D86B-11D0...   NAME NOT FOUND  Desired Acces...
15:4...  svchost.exe  964  RegOpenKey     HKCR\CLSID\{8BC3F05E-D86B-11D0...   NAME NOT FOUND  Desired Acces...
15:4...  svchost.exe  964  RegOpenKey     HKCR\CLSID\{8BC3F05E-D86B-11D0...   SUCCESS         Desired Acces...
15:4...  svchost.exe  964  RegQueryValue  HKCR\CLSID\{8BC3F05E-D86B-11D0...   SUCCESS         Type: REG_SZ,...
15:4...  svchost.exe  964  RegCloseKey    HKCR\CLSID\{8BC3F05E-D86B-11D0...   SUCCESS
15:4...  svchost.exe  964  RegOpenKey     HKCR\AppID\{8BC3F05E-D86B-11D0...   SUCCESS         Desired Acces...
Showing 982 of 49,701 events (1.9%)        Backed by virtual memory
```

Q5 *这个恶意代码在主机上的感染迹象特征是什么？*

在第一问发现他会创建一个服务叫 IPRIP，所以感染迹象就是会有创建一个服务叫 IPRIP

Q6: *这个恶意代码是否存在一些有用的网络特征码？*

Wireshark 抓包



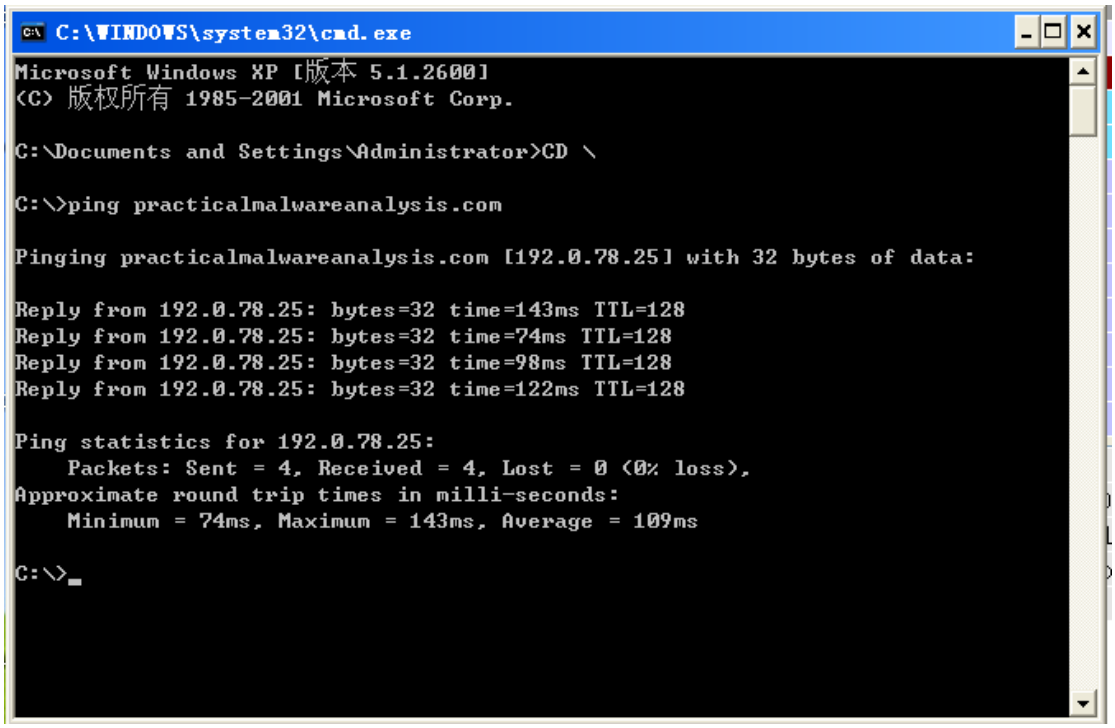
```
Capturing from VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) - Wireshark
No.  Time       Source          Destination     Protocol Info
  1 0.000000    192.168.38.128  192.168.38.2    DNS      Standard query A www.practicalmalwareanalysis.com
  2 0.005314    192.168.38.2    192.168.38.128  DNS      Standard query response CNAME practicalmalwareanalysis.com A 192.0.78.25 A 192.0.78.24
  3 0.005628    192.168.38.128  192.0.78.25     TCP      finle-lm > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
  4 0.110329    192.0.78.25     192.168.38.128  TCP      https > finle-lm [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
  5 0.110360    192.168.38.128  192.0.78.25     TCP      finle-lm > https [ACK] Seq=1 Ack=1 Win=64240 Len=0
  6 0.110452    192.168.38.128  192.0.78.25     SSL      Continuation Data
  7 0.110628    192.0.78.25     192.168.38.128  TCP      https > finle-lm [ACK] Seq=1 Ack=257 Win=64240 Len=0
  8 0.212831    192.0.78.25     192.168.38.128  TCP      https > finle-lm [FIN, PSH, ACK] Seq=1 Ack=257 Win=64240 Len=0
  9 0.212888    192.168.38.128  192.0.78.25     TCP      finle-lm > https [ACK] Seq=257 Ack=2 Win=64240 Len=0
 10 0.212991    192.168.38.128  192.0.78.25     TCP      finle-lm > https [FIN, ACK] Seq=257 Ack=2 Win=64240 Len=0
 11 0.213187    192.0.78.25     192.168.38.128  TCP      https > finle-lm [ACK] Seq=2 Ack=258 Win=64239 Len=0
 12 30.203139   192.168.38.128  192.168.38.2    DNS      Standard query A www.practicalmalwareanalysis.com

⊞ Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
⊞ Ethernet II, Src: Vmware_c3:7b:de (00:0c:29:c3:7b:de), Dst: Vmware_ff:5f:78 (00:50:56:ff:5f:78)
⊞ Internet Protocol, Src: 192.168.38.128 (192.168.38.128), Dst: 192.168.38.2 (192.168.38.2)
⊞ User Datagram Protocol, Src Port: mxxrlogin (1035), Dst Port: domain (53)
⊞ Domain Name System (query)

0000  00 50 56 ff 5f 78 00 0c  29 c3 7b de 08 00 45 00   .PV._x.. ).{...E.
0010  00 4e 23 96 00 00 80 11  49 36 c0 a8 26 80 c0 a8   .N#..... I6..&...
0020  26 02 04 0b 00 35 00 3a  40 0a 85 f1 01 00 00 01   &....5.: @.......
0030  00 00 00 00 00 00 03 77  77 77 18 70 72 61 63 74   .......w ww.pract

VMware Accelerated AMD PCNet Adapter (…  包数量: 22 显示数量: 22 标记数量: 0        配置文件:Default
```

可以看到第一个是一个 DNS 解析，网址仍是 practicalmalwareanalysis.com



找到 ip 192.0.78.25

进行过滤

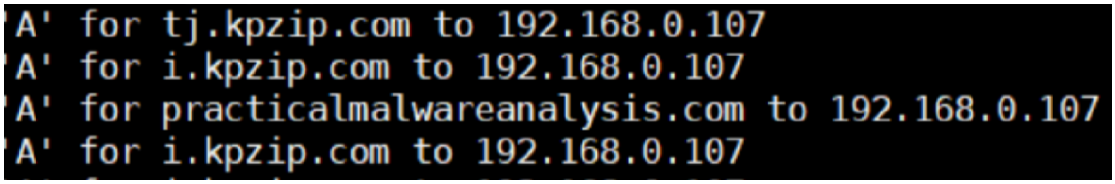
但是得到的结果里面并没有 http 协议。只有无法解析的 ssl 协议（continuation Data）。

不知道问题出在哪里。

换种方法。

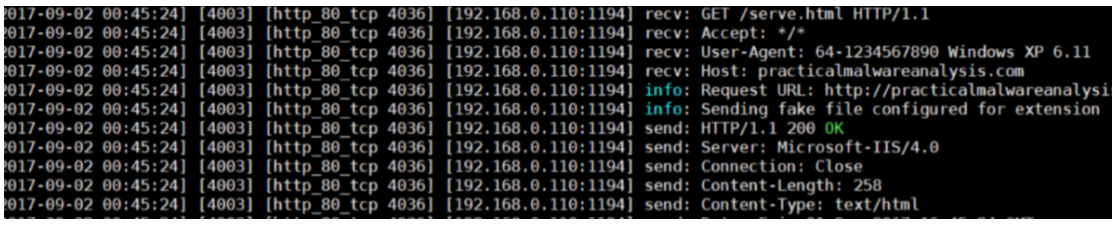
查看 DNSChef 和 INetSim 服务器上的记录

先检查一下 dns 的解析记录，用 DNSChef 虚拟机



和前面发现的恶意域名是对应的

然后我们在看看 INetSIm 虚拟机上的记录，记录在 log/service.log 里面



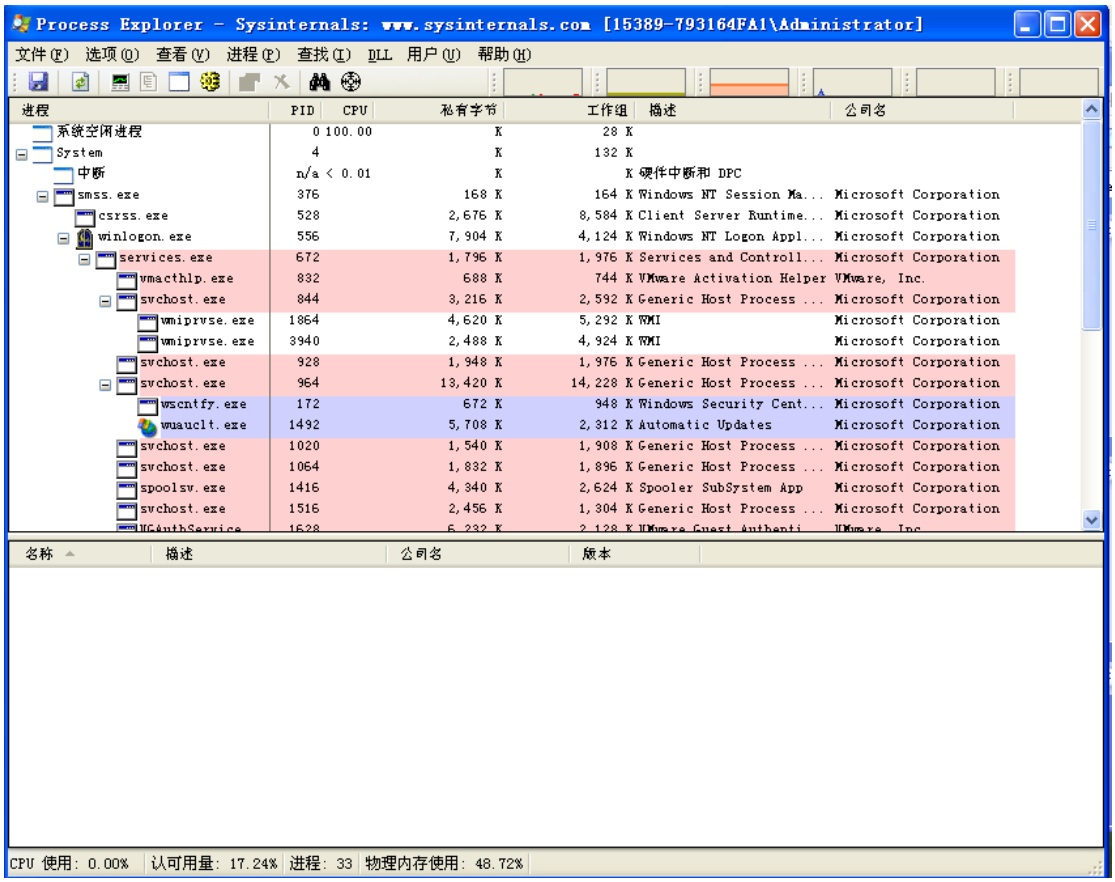
注意到

```
recv: GET /serve.html HTTP/1.1
recv: Accept: */*
recv: User-Agent: 64-1234567890 Windows XP 6.11
recv: Host: practicalmalwareanalysis.com
info: Request URL: http://practicalmalwareanalysis.com/serve.html
info: Sending fake file configured for extension 'html'.
send: HTTP/1.1 200 OK
send: Server: Microsoft-IIS/4.0
send: Connection: Close
send: Content-Length: 258
send: Content-Type: text/html
```

Lab 3-3

用基本动态分析工具分析 lab03-03.exe 中的恶意代码

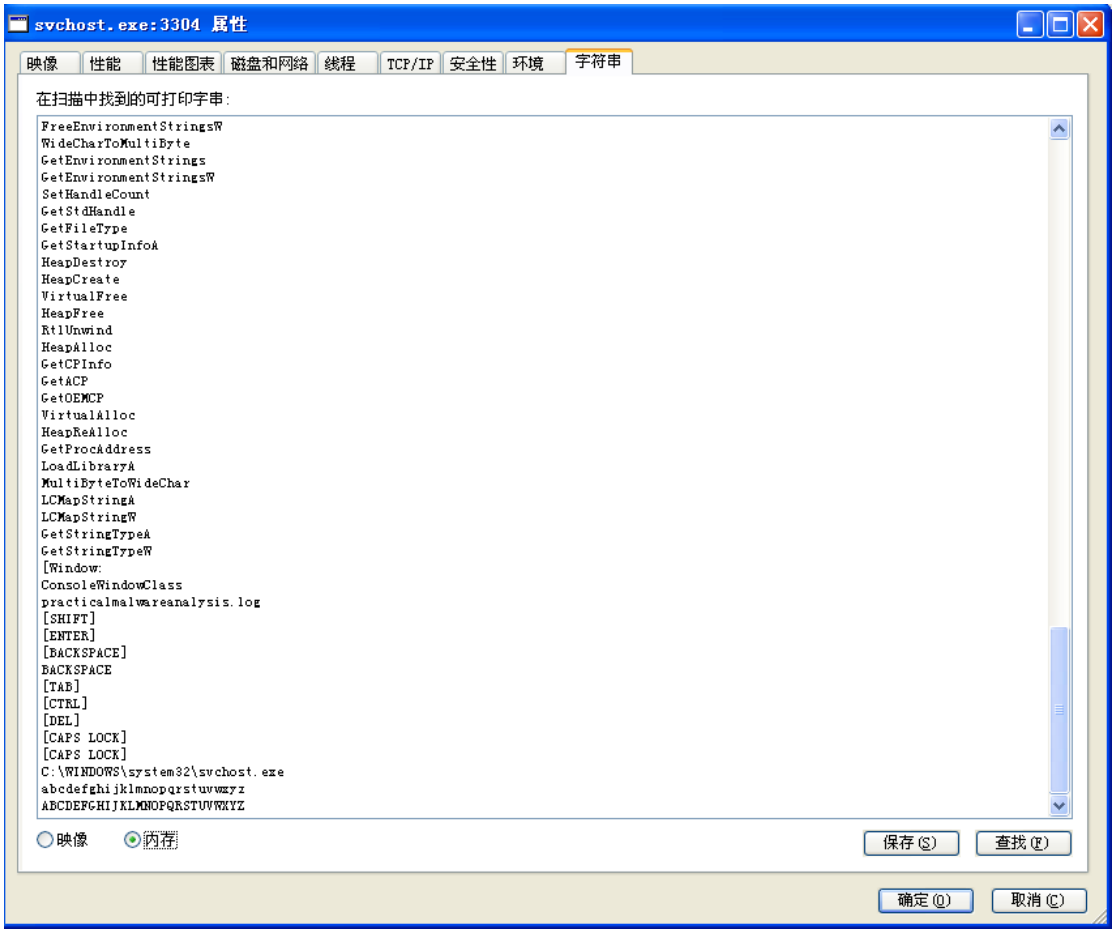
Q1: *当你使用 Process Explorer 工具进行监视的时候，你注意到了什么？*



注意到 explore 下面多了一个不成寻常进程 svchost.exe

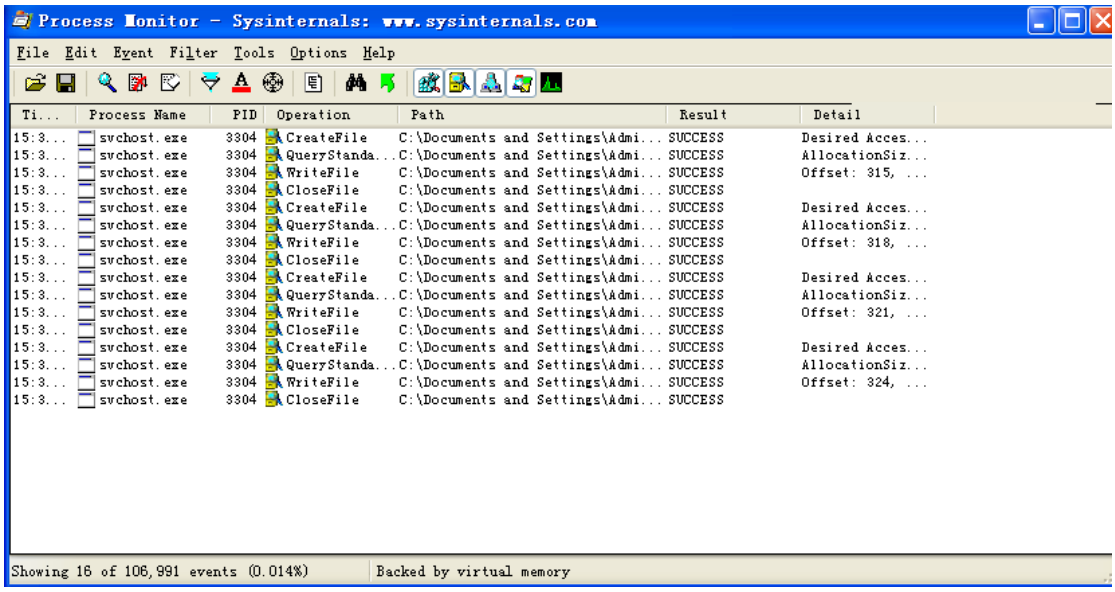
Q2: *你可以找到任何的内存修改的行为吗？*

双击 svchost 进程，在 strings 中查看 memory，发现一个 log 文件，有键盘特殊按键的标识



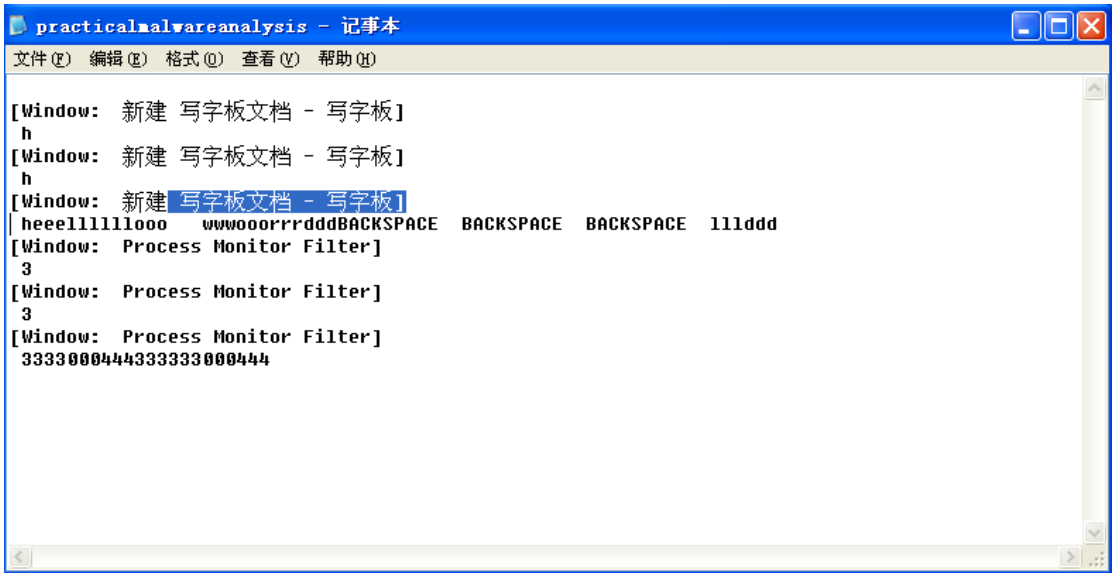
出现了[ENTER]这些字符串，可能是击键记录器

我们随便打开虚拟机界面开一个文本，然后据 PID 来在 procmon 中创建一个过滤器



发现这个程序一直在不断的 CreateFile 和 WriteFile

找到这个 log 文件，在可执行程序的同一个目录下。打开：



Q3: *这个恶意代码在主机上的感染迹象特征是什么？*

根据上面的分析，迹象就是创建了一个 praticalmalwareanalysis.log 文件

Q4: *这个恶意代码的目的是什么？*

根据上面的分析，是键盘记录器。

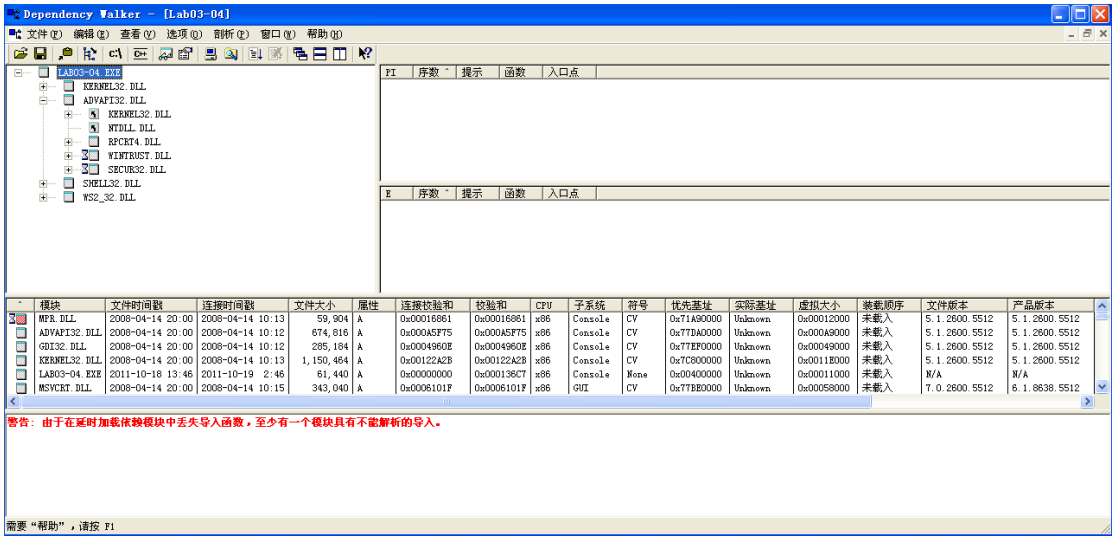
Lab 3-4

用基本动态分析工具分析 lab03-04.exe 中的恶意代码

Q1: *当你运行这个文件时，会发生什么呢？*

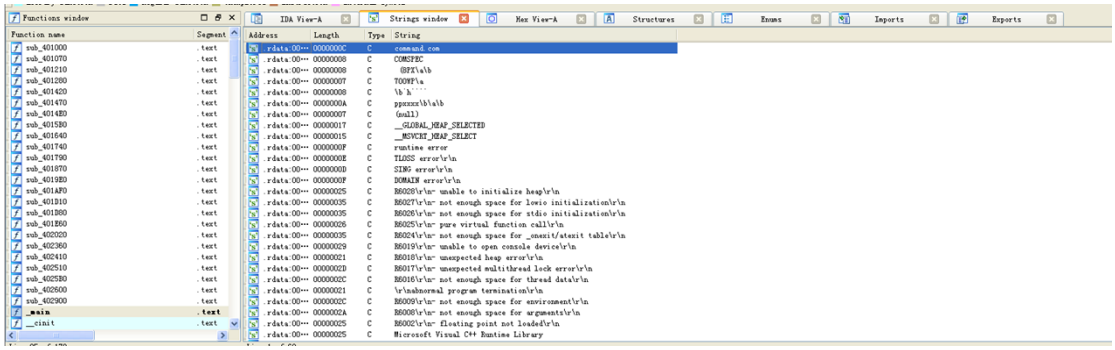
首先静态分析：
使用 PEiD 查看发现**未加壳**

使用 Dependency Walker 查看：



Advapi32.dll 提供核心 Windows 组件访问，如服务管理器和注册表
Kernel32.dll 提供系统核心功能，访问和操作内存、文件、硬件等
Shell32.dll 是 Windows 的 32 位外壳动态链接库文件，用于打开网页和文件，建立文件时的默认文 件名的设置等大量功能。
Wsock32.dll 用于联网，或执行网络相关操作

打开 idapro 分析字符串



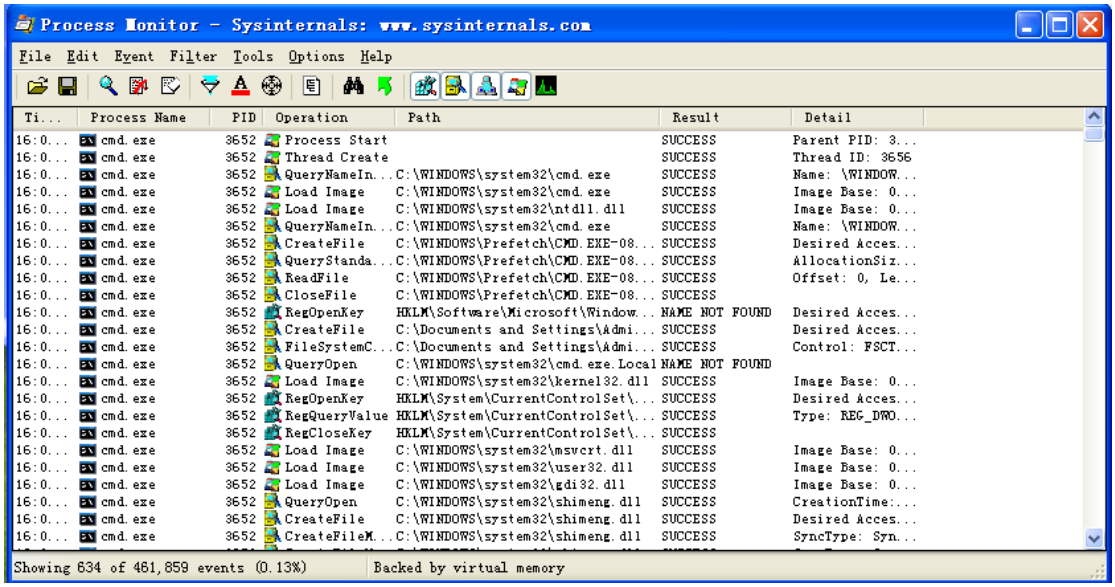
1. 可疑网站 http://www.practialmalwareanalysis.com
2. 可疑指令：Get CMD UPLOAD SLEEP

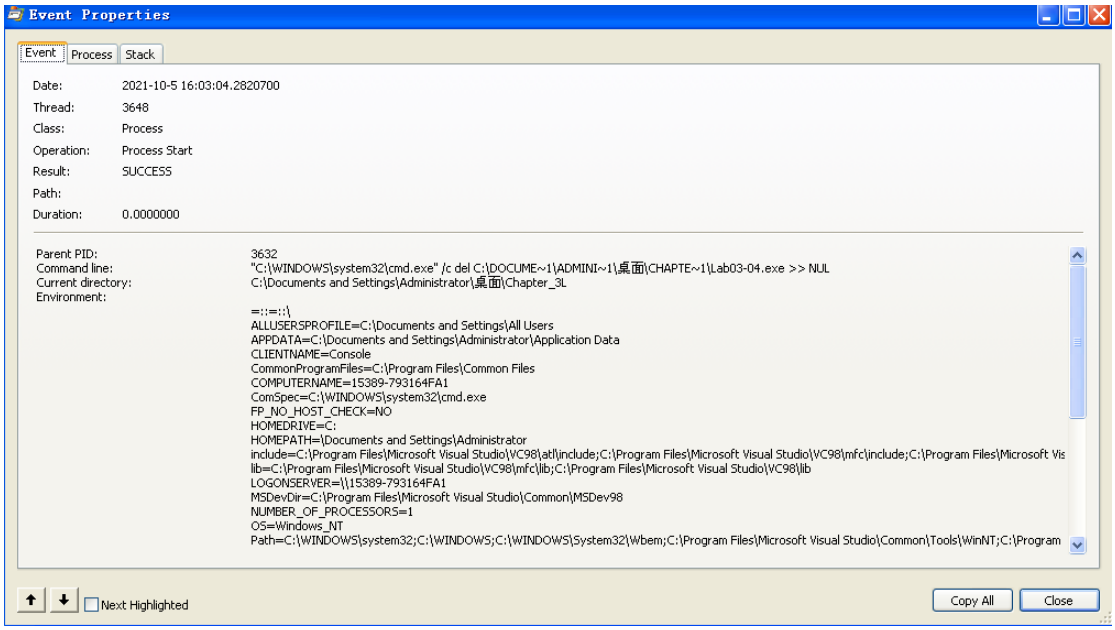
然后试图进行动态分析。
双击该程序，该程序删除了自身。

Q2: *是什么原因造成动态分析无法有效实施？*

Process Explorer 找到运行 lab03-04 时一闪而过的 pid

然后据 PID 来在 procmon 中创建一个过滤器





得知文件删除过程通过“C:\WINDOWS\system32\cmd.exe" /c del C:\.....\Lab03-04.exe >> NUL”完成

Q2: *是否有其他方式来运行这个程序？*

再次运行 Lab03-04.exe，并添加上命令行参数（例如-cc、-in、-re 等），程序依然删除自身。