计算机病毒及其防治技术

Lab1

沙璇 1911562

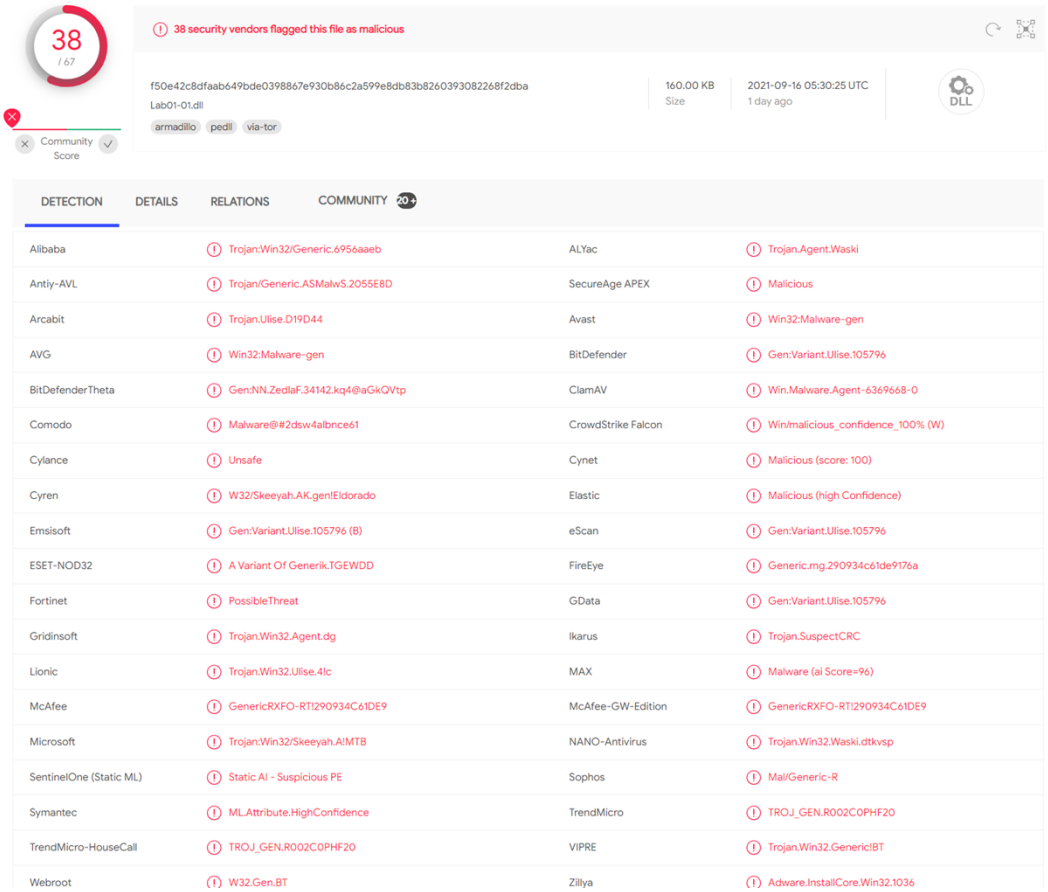
Lab 1-1

对 Lab01-01.exe 和 Lab01-01.dll 进行分析

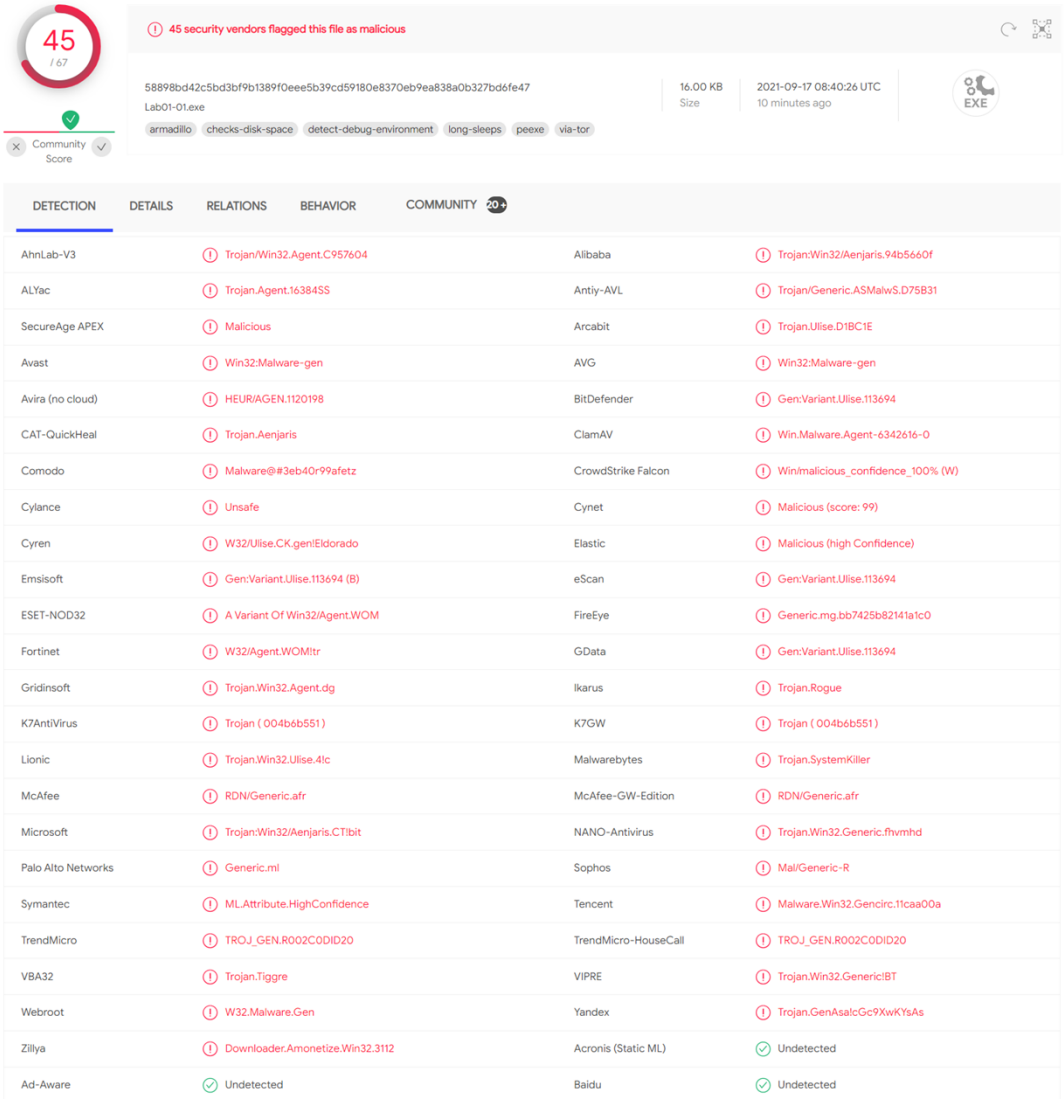
Q1: ***将文件上传至 http://www.VirusTotal.com 进行分析并查看报告。文件匹配到了已有的反病毒软件特征吗?***

可以看到文件匹配到已有的反病毒软件特征，部分截图如下：

Lab01-01.dll：



Lab01-01.exe：



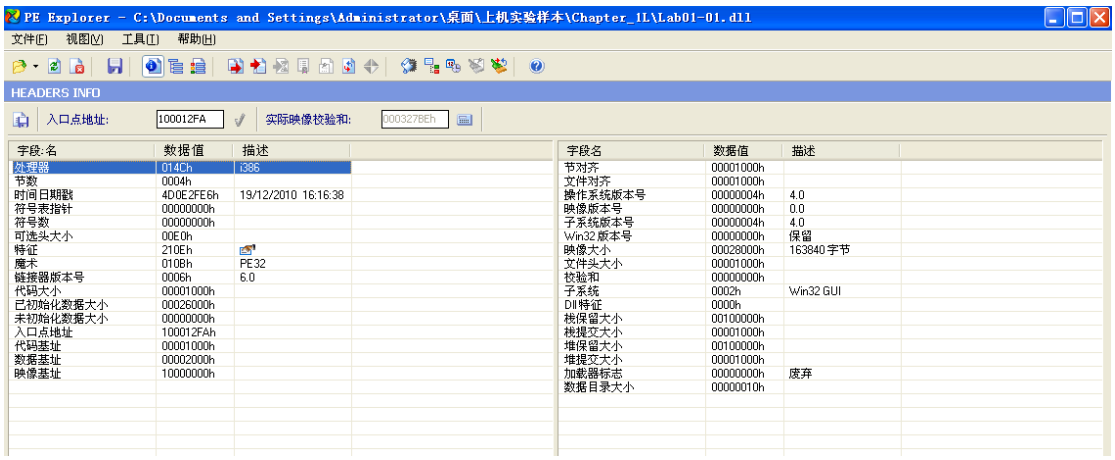
在 details 里可以看到基础属性、检测历史、命名、PE 信息(头、节、导入导出表等)

在 community 可以看到一些沙箱的分析报告等，有助于对样本加深理解

Q2:*这些文件是什么时候被编译的？*

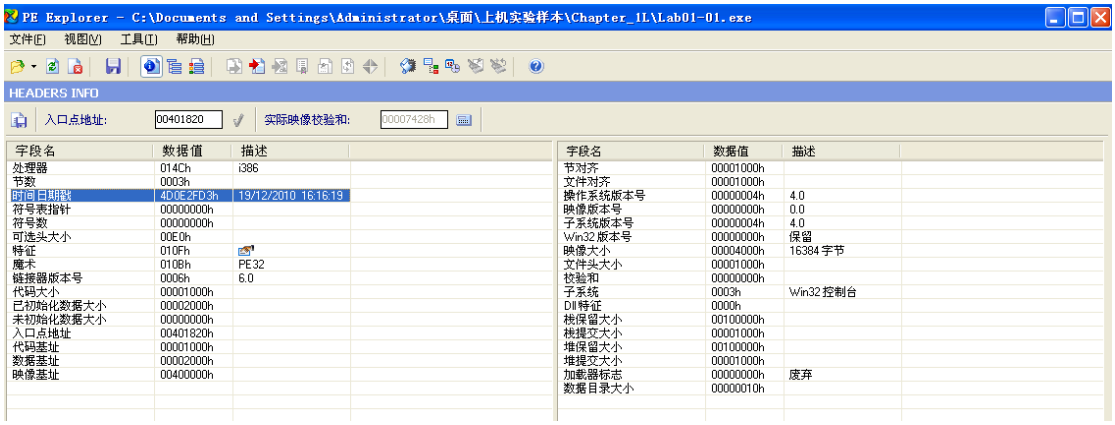
使用 PE Explorer 查看两个样例代码编译时间

Lab01-01.dll:



Compilation Timestamp 2010-12-19 16:16:38

Lab01-01.exe：



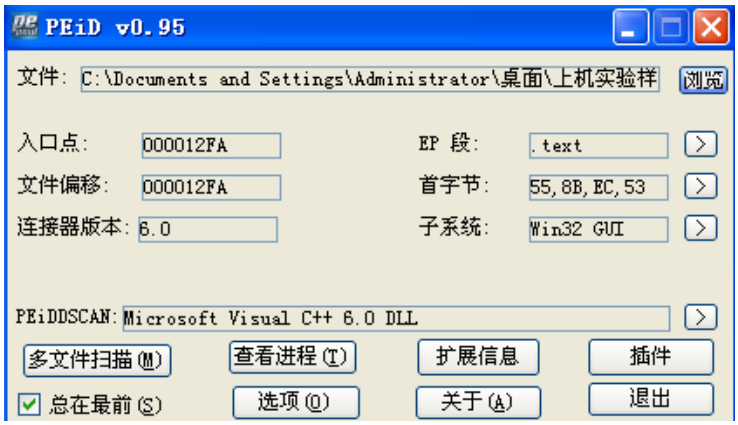
Compilation Timestamp 2010-12-19 16:16:19

Q3：*这两个文件中是否存在迹象说明它们是否被加壳或混淆？如果是，这些迹象在哪里？*

使用 PEID 查看是否有壳

Lab01-01.exe：

Lab01-01.dll：

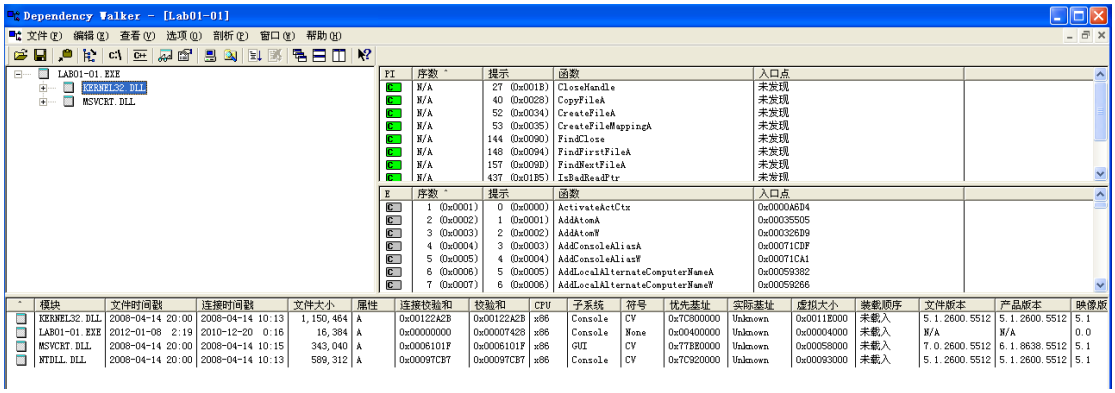


没有加壳和混淆

Q4：*利用 Dependency Walker 软件判断 Lab01-01.exe 这个样本代码中含有那些导入函数，他们可能是用来使得该样本程序完成什么功能的？*

使用 Dependency Walker 打开 Lab01_01.exe

如下：



从 KERNEL32.DLL 中可以看到 10 个导入函数，进行搜索后得到相关结果如下：

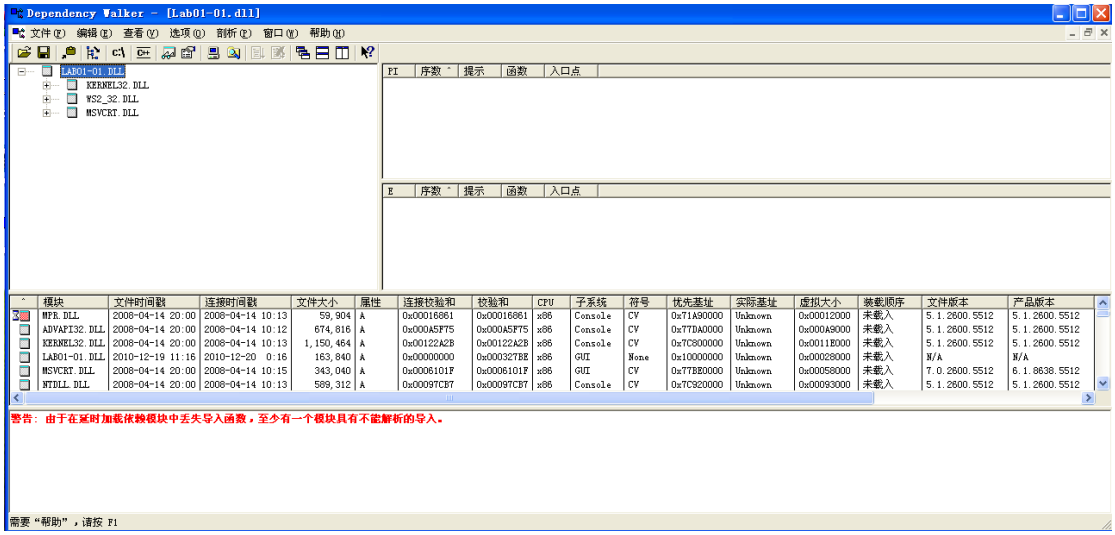
- CloseHandle：关闭一个内核对象
- CopyFile：拷贝（覆盖）文件
- CreateFileMapping：创建一个新的文件映射内核对象
- FindClose：关闭 FindFirstFile 创建的搜索句柄
- FindFirstFile：根据文件名查找文件
- FindNextFile：此函数用于遍历目录或文件时，判断当前目录下是否有下一个目录或文件
- IsBadReadPtr：判断一个内存是否能够被读取
- MapViewOfFile：将一个文件映射对象映射到当前应用程序的地址空间
- UnmapViewOfFile：在当前应用程序的内存地址空间解除对一个文件映射对象的映射

Q5：*是否有其他文件或基于主机的指示符，可以帮助你在被该恶意代码感染的主机上进行搜索？*

猜测运行 Lab01-01.exe 则会导入 kerne132.dll 以及 Lab01-01.dll 文件。所以如果在主机上找到了 kerne132.dll 则可以说明该主机感染了此病毒。

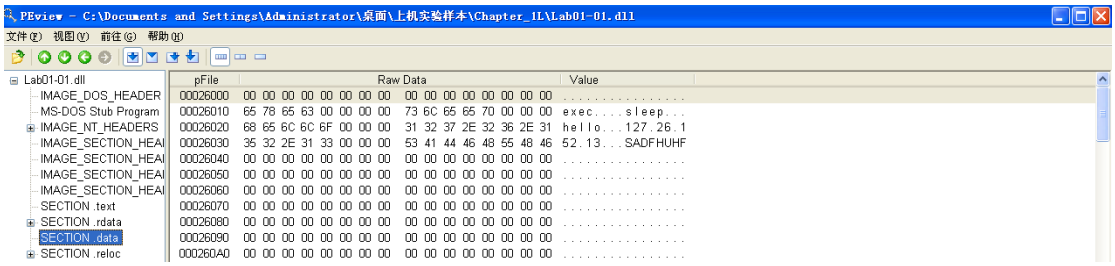
Q6：*是否有基于网络连接的线索可以用来探查这个恶意代码？*

使用 Dependency Walker 打开 Lab01_01.dll 如下所示



观察到输入表函数中多了一个 WS2_32.dll。查阅后知该函数 WS2_32.dll 是 Windows Sockets 应用程序接口，用于支持 Internet 和网络应用程序。

接着使用 peview 软件打开，如下：



找到一个 ip 地址 127.26.1

Q7: ***猜测这些文件的目的是什么？***

查询发现 kernel32.dll 是非常重要的 32 位动态链接库文件，属于内核级文件。它控制着系统的内存管理、数据的输入输出操作和中断处理。而此 dll 文件中有 Kernel23.dll 文件,因此推测这此文件主要的功能应该是把系统盘 c:\windows\system32 中的 kernel123.dll 文件换成这个程序中的 Kernel23.dll 文件，非法获得系统权限。

Lab 1-2

对 Lab01-02.exe 进行分析

Q1:

上传并检测 Lab01-02.exe

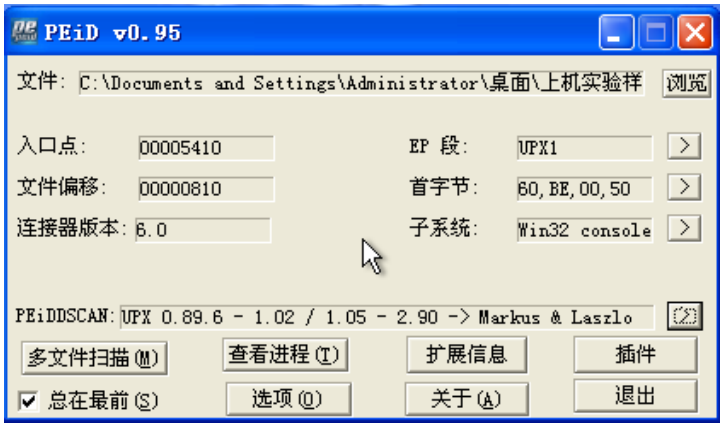
DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 20+

AhnLab-V3	Trojan/Win32.StartPage.C26214	Alibaba	TrojanClicker:Win32/Generic.1baf980f
ALYac	Trojan.Startpage.3072	Antiy-AVL	Trojan/Generic.ASMalwS.8634D7
SecureAge APEX	Malicious	Avira (no cloud)	TR/Downloader.Gen
BitDefender	Gen:Variant.Ser.Ulise.216	BitDefenderTheta	Gen:NN.ZexaF.34142.amGfaWi867f
ClamAV	Win.Malware.Agent-6350563-0	Comodo	Malware@#22epuiwih8vym
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cynet	Malicious (score: 100)
Cyren	W32/Agent.DJC.gen!Eldorado	DrWeb	Trojan.Click3.12740
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Variant.Ser.Ulise.216 (B)
eScan	Gen:Variant.Ser.Ulise.216	ESET-NOD32	Win32/TrojanClicker.Agent.NVM
FireEye	Generic.mg.8363436878404da0	Fortinet	W32/Agent.NVM!tr
GData	Gen:Variant.Ser.Ulise.216	Gridinsoft	Trojan.Win32.Agent.dg
Ikarus	Trojan.Win32.TrojanClicker	Jiangmin	Trojan.Generic.fxlq
Kingsoft	Win32.Malware.Heur_Generic.A.(kcloud)	Lionic	Trojan.Win32.Zbot.lsXA
Malwarebytes	Trojan.Agent.UPX	MAX	Malware (ai Score=100)
McAfee	Generic.ait	NANO-Antivirus	Trojan.Win32.Click3.iaupgs
Palo Alto Networks	Generic.ml	SentinelOne (Static ML)	Static AI - Suspicious PE
Sophos	Mal/Generic-S	Symantec	ML.Attribute.HighConfidence
Tencent	Malware.Win32.Gencirc.11bbe0f1	TrendMicro-HouseCall	TROJ_GEN.R002C0DHD20
VBA32	Trojan.Click	VIPRE	Trojan.Win32.Generic!BT
ViRobot	Trojan.Win32.S.StartPage.3072	Webroot	
Yandex	Trojan.CL.Agent!SYJ1YyE/ZV4	Zillya	Trojan.Agent.Win32.1288291

Q2：

探索是否有加壳

用 peid 探测如下图



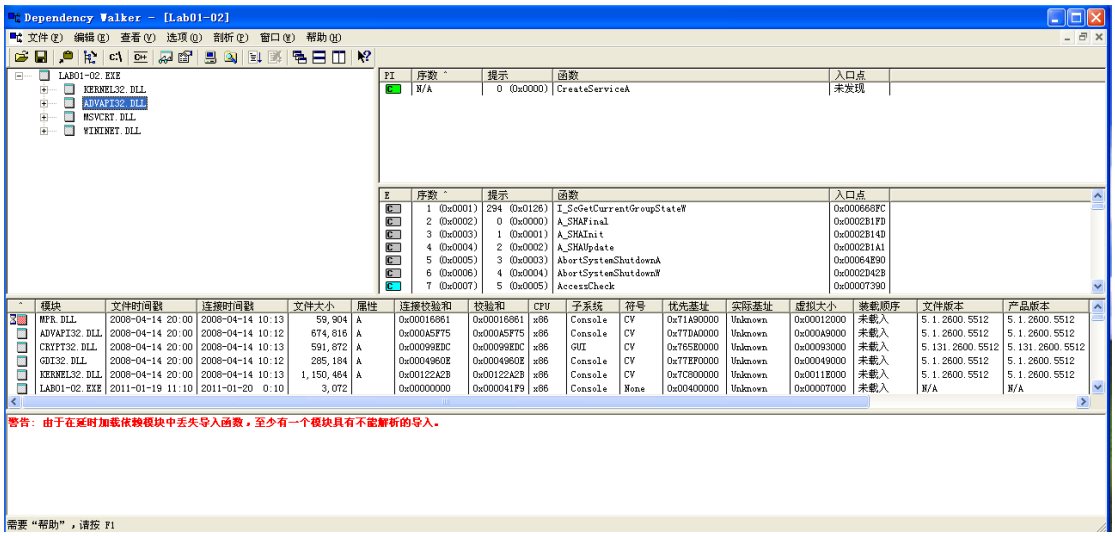
Upx 加壳

使用 wsnupacker 脱壳

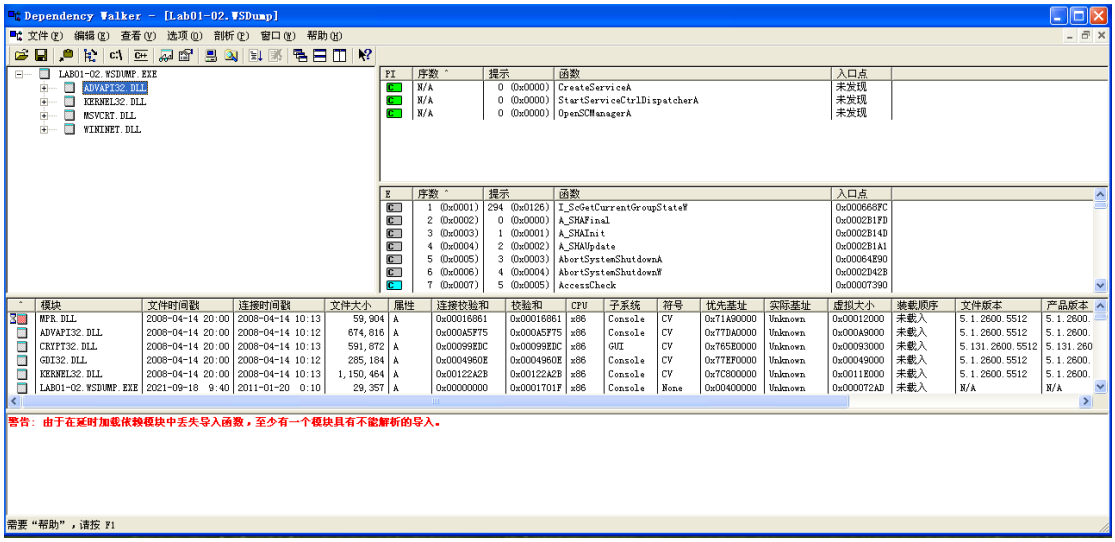
检测如下：

Q3：

脱壳前：



脱壳后：



脱壳后有更多导入函数显示。

Q4：

使用 IDAPRO 打开脱壳后文件，打开函数调用窗口：

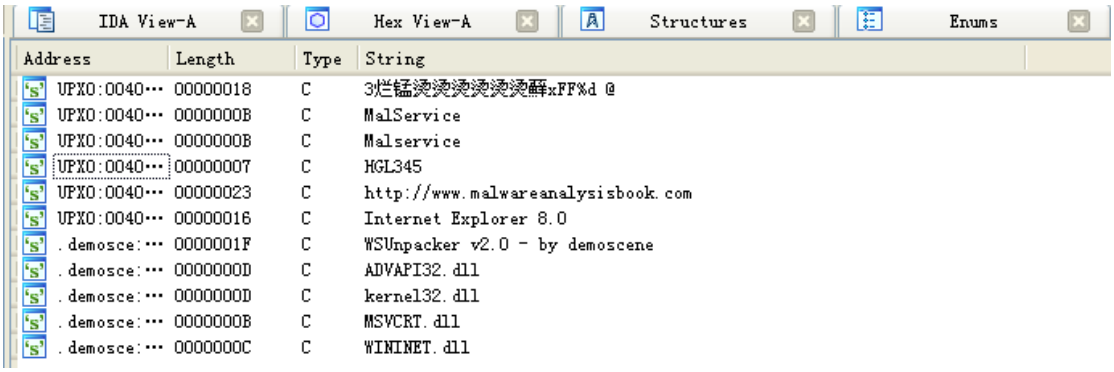
根据如下函数名推理该程序首先创建相关服务函数：

Address	Ordinal	Name	Library
00402000		CreateServiceA	ADVAPI32
00402004		StartServiceCtrlDispatcherA	ADVAPI32
00402008		OpenSCManagerA	ADVAPI32

根据如下函数名推测该程序会打开一个链接：

00402070	InternetOpenUrlA	WININET
00402074	InternetOpenA	WININET

在字符串窗口查找如下：



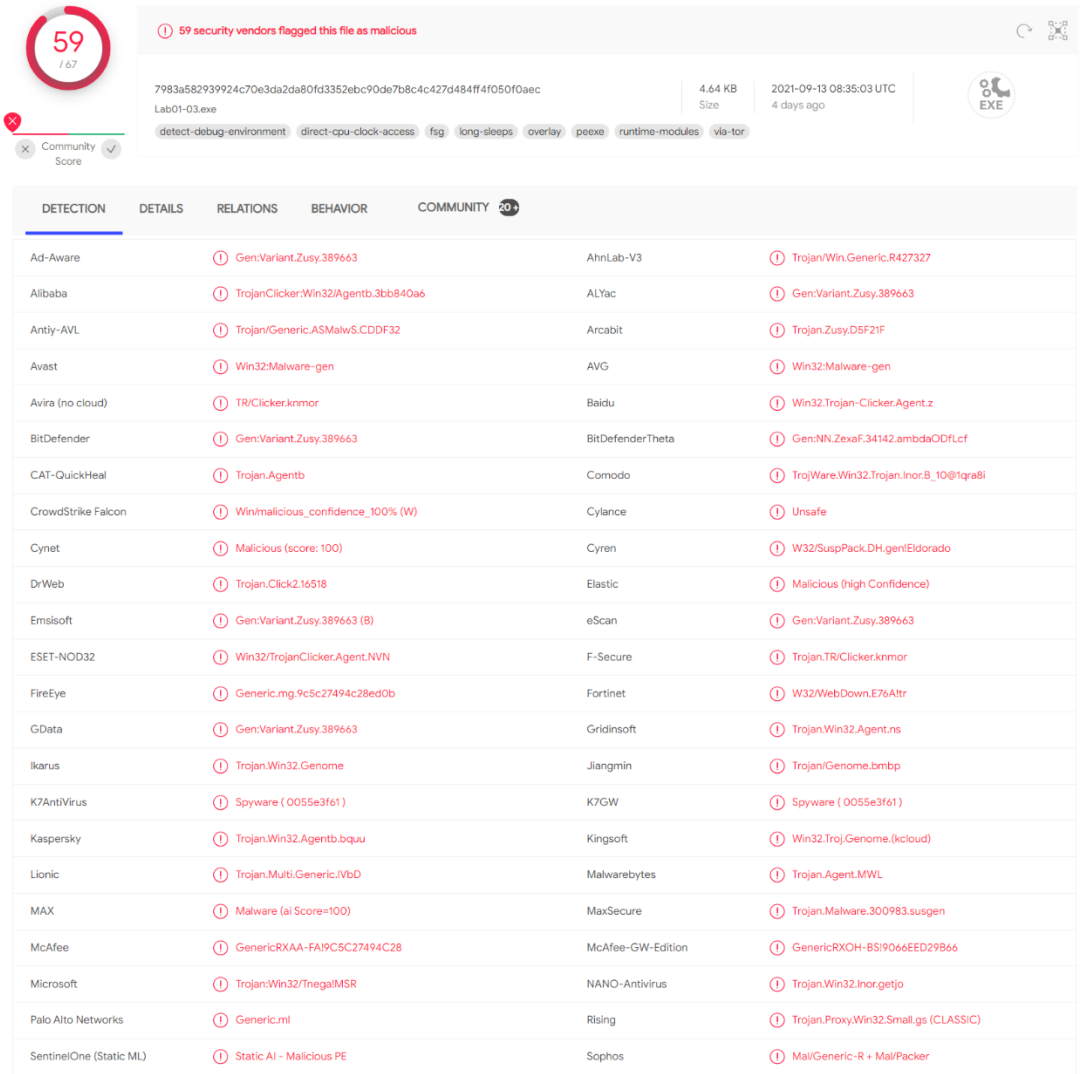
出现可疑的 URL: www.malwareanalysisbook.com，以及 IE8.0，推测应该是使用 IE 打开该网站。

Lab 1-3

对 Lab01-03.exe 进行分析

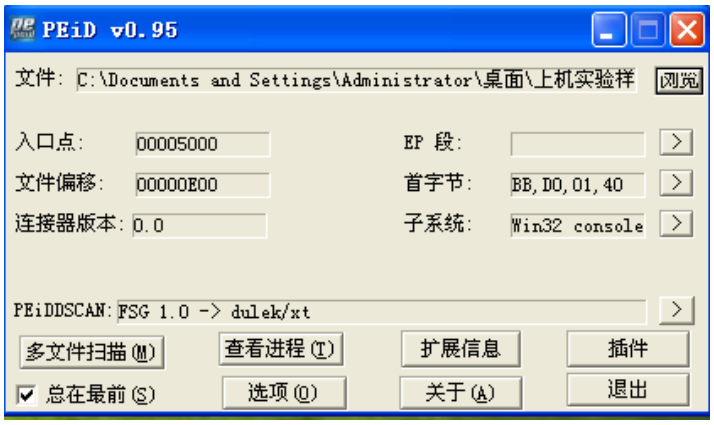
Q1:

检测如下：



Q2:

使用 peid 探测是否加壳



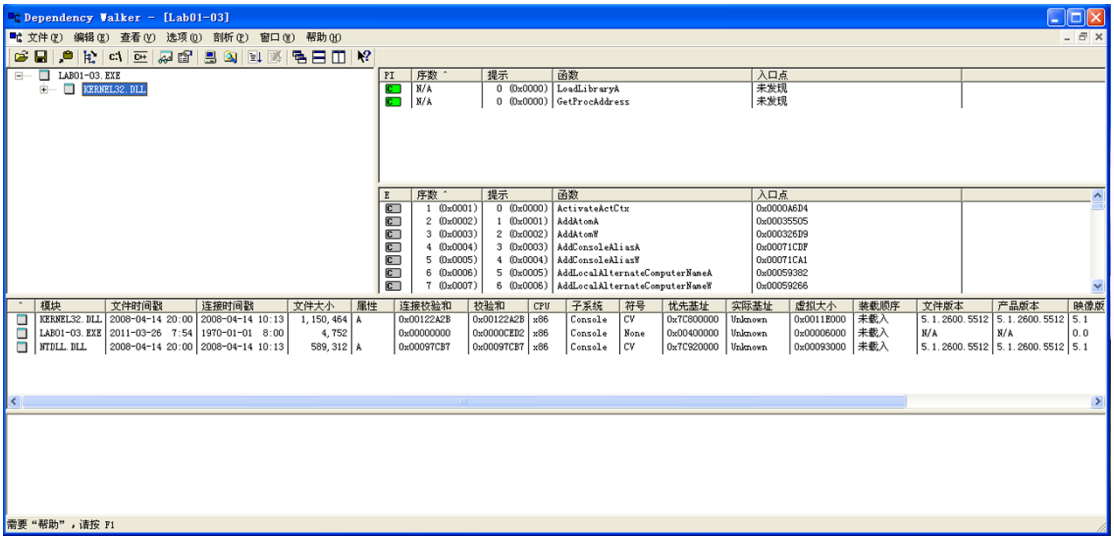
使用 FSG 加壳

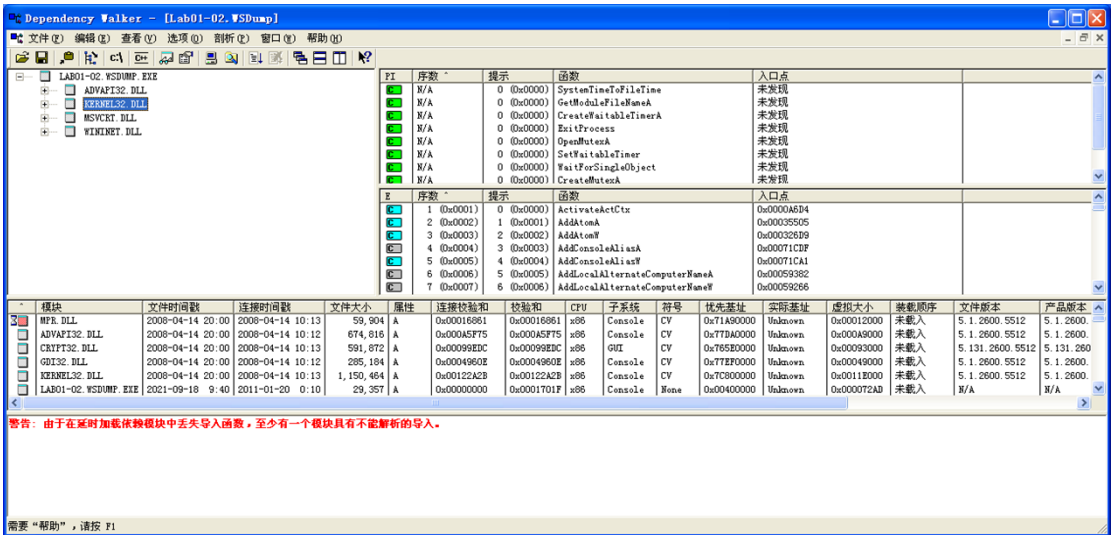
Wsunpacker 脱壳:

再次检测:

Q3:

比较前后导入函数:





Q4:

Idapro 打开该文件调用函数显示如下:

Address	Ordinal	Name	Library
00402000		__getmainargs	msvcrt
00402004		_controlfp	msvcrt
00402008		_except_handler3	msvcrt
0040200C		__set_app_type	msvcrt
00402010		__p__fmode	msvcrt
00402014		__p__commode	msvcrt
00402018		_exit	msvcrt
0040201C		_XcptFilter	msvcrt
00402020		exit	msvcrt
00402024		__p___initenv	msvcrt
00402028		_initterm	msvcrt
0040202C		__setusermatherr	msvcrt
00402030		_adjust_fdiv	msvcrt
00402038		VariantInit	OLEAUT32
0040203C		SysAllocString	OLEAUT32
00402040		SysFreeString	OLEAUT32
00402048		OleInitialize	ole32
0040204C		CoCreateInstance	ole32
00402050		OleUninitialize	ole32

查询知 OleInitialize 是一个 Windows API 函数。它的作用是在当前单元(apartment)初始化组件对象模型(COM)库;CoCreateInstance 函数用指定的类标识符创建一个 Com 对象,用指定的类标识符创建一个未初始化的对象;OleInitialize 是一个 Windows API 函数，它的作用是在当前单元(apartment)初始化组件对象模型(COM)库，将当前的并发模式标识为 STA(single-thread apartment——单线程单元)。

再主函数中找到一个地址如下：

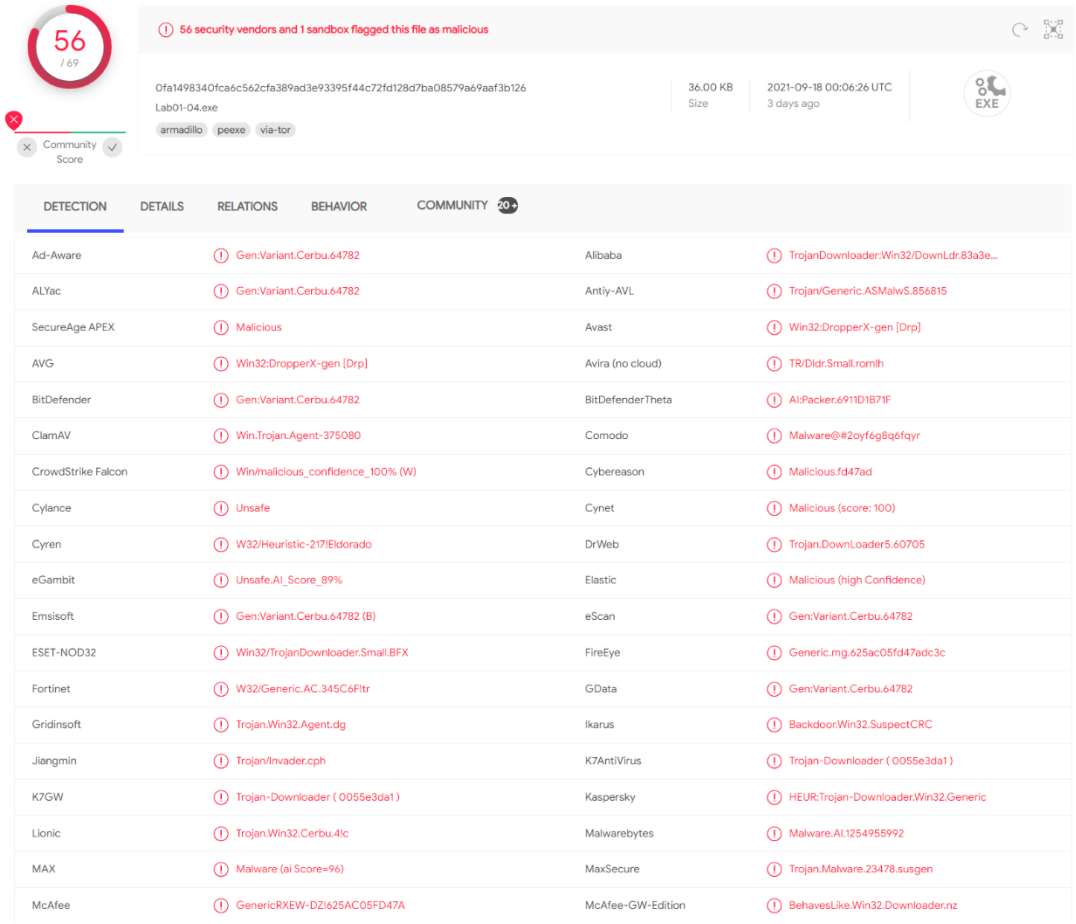
```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  OLECHAR *v3; // esi@3
  LPVOID ppv; // [sp+0h] [bp-24h]@2
  VARIANTARG pvarg; // [sp+4h] [bp-20h]@3
  __int16 v7; // [sp+14h] [bp-10h]@3
  int v8; // [sp+1Ch] [bp-8h]@3

  if ( OleInitialize(NULL) >= 0 )
  {
    CoCreateInstance(&rclsid, NULL, 4u, &riid, &ppv);
    if ( ppv )
    {
      VariantInit(&pvarg);
      v7 = 3;
      v8 = 1;
      v3 = SysAllocString(L"http://www.malwareanalysisbook.com/ad.html");
      (*(void (__stdcall **)(LPVOID, OLECHAR *, __int16 *, VARIANTARG *, VARIANTARG *, VARIANTARG *))(*(_DWORD *)ppv + 44))(
        ppv,
        v3,
        &v7,
        &pvarg,
        &pvarg,
        &pvarg);
      SysFreeString(v3);
    }
    OleUninitialize();
  }
```

因此推测该程序通过调用 com 接口访问如上的网址。

Lab 1-4

对 Lab01-04.exe 进行分析

Q1: ***将文件上传至 http://www.VirusTotal.com 进行分析并查看报告。文件匹配到了已有的反病毒软件特征吗?***

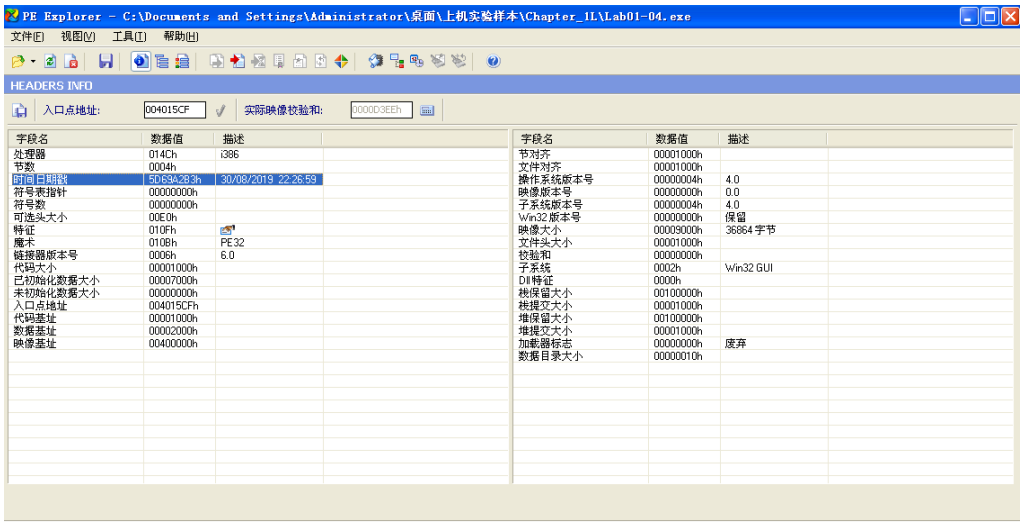


Q2:

通过 PEiD 的检测，如下所示：

说明文件没有加壳，是通过 Microsoft Visual C++编译的

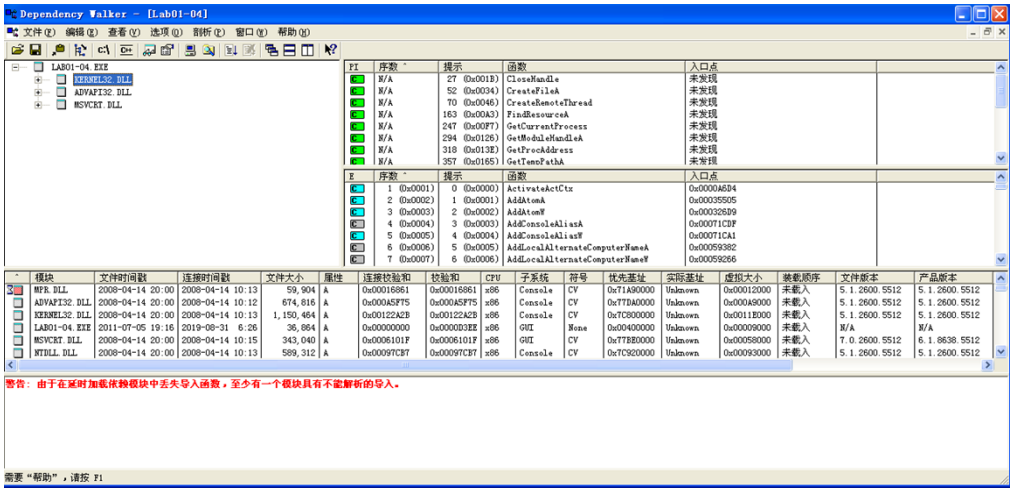
Q3:

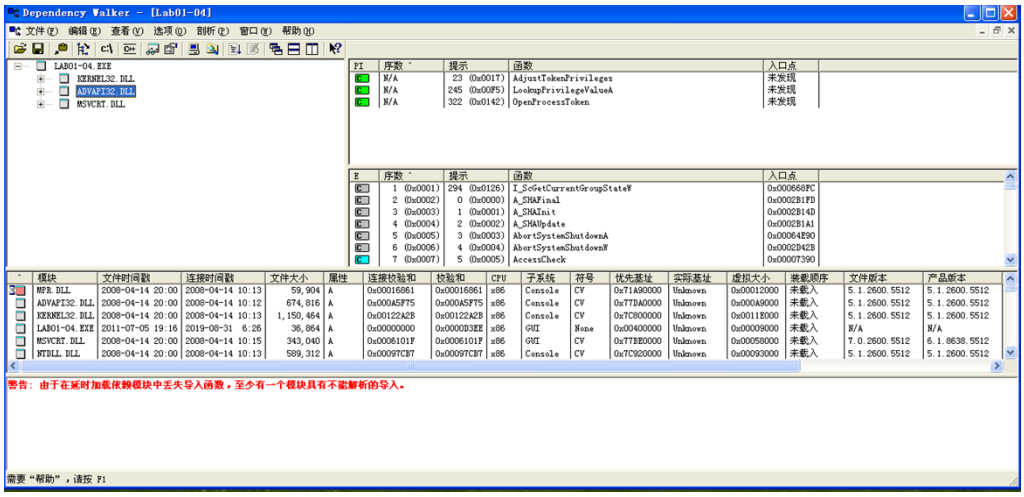


使用 PE Explorer 查看样例代码编时间 2019/08/30 22:26:59

Q4:

使用 Dependency Walker 打开 Lab01_01.exe





Lab01_04.exe 中有三个 dll 文件：KERNEL32.DLL、ADVAPI32.DLL 和 MSVCRT.DLL

查阅资料后知

KERNEL32.DLL 中的一些关键导入函数：

1. - CreateFileA：打开或创建对象
2. - CreateRemoteThread：创建一个在其它进程地址空间中运行的线程(也称:创建远程线程)
3. - FindResource：确定指定模块中指定类型和名称的资源所在位置
4. - GetWindowsDirectory：获取 Windows 目录的完整路径名
5. - LoadLibrary：加载动态连接库
6. - LoadResource：装载指定资源到全局存储器
7. - SizeofResource：返回指定资源节的大小
8. - WinExec：运行指定程序

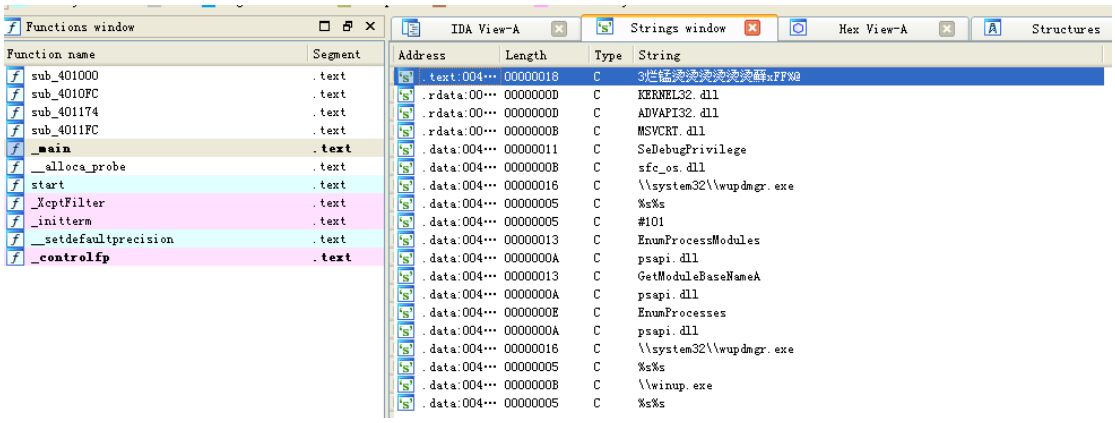
ADVAPI32.DLL 中的一些关键导入函数：

1. - AdjustTokenPrivileges：用于启用或禁止，指定访问令牌的特权
2. - LookupPrivilegeValueA：函数查看系统权限的特权值
3. - OpenProcessToken：数用来打开与进程相关联的访问令牌

推测该程序使用 ADVAPI32.DLL 中三个函数获取访问令牌的特权，然后创建一个远程线程，找到一个特权能访问的资源，加载到全局储存器后运行程序。

Q5:

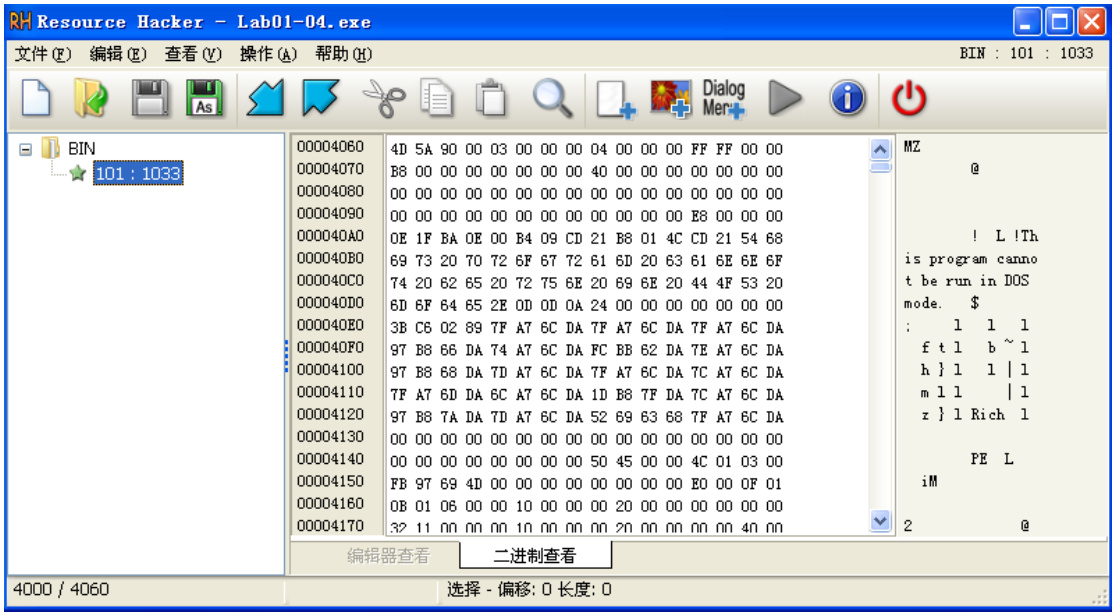
用 ida 打开该文件，得到字符串如下：



推测恶意代码会在 C:\windows\system32\wupdmgr.exe 这个位置创建或者修改文件

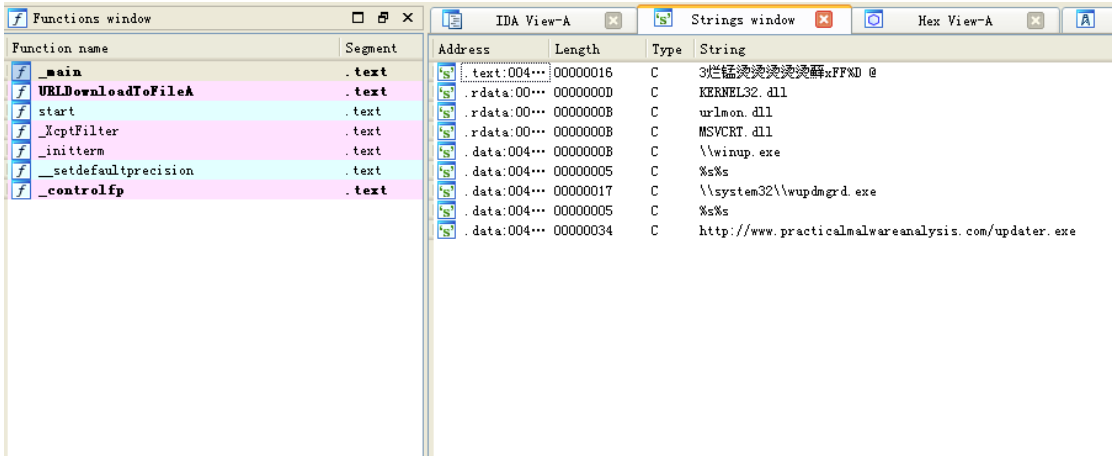
Q6:

使用 resource hacker 载入



资源节里存储着另一个可执行文件，我们可以将其另存为一个可执行文件，命名为 bin01-04.exe

再使用 idapro 载入，得到字符串如下所示：



得到一个网址 http://www.practicalmalwareanalysis.com/updater.exe

推测 wupdmgrd.exe 程序就是从这个链接下载得到