lab 1

个人信息

学号：1911410

姓名：付文轩

专业：信息安全

学院：网络空间安全学院

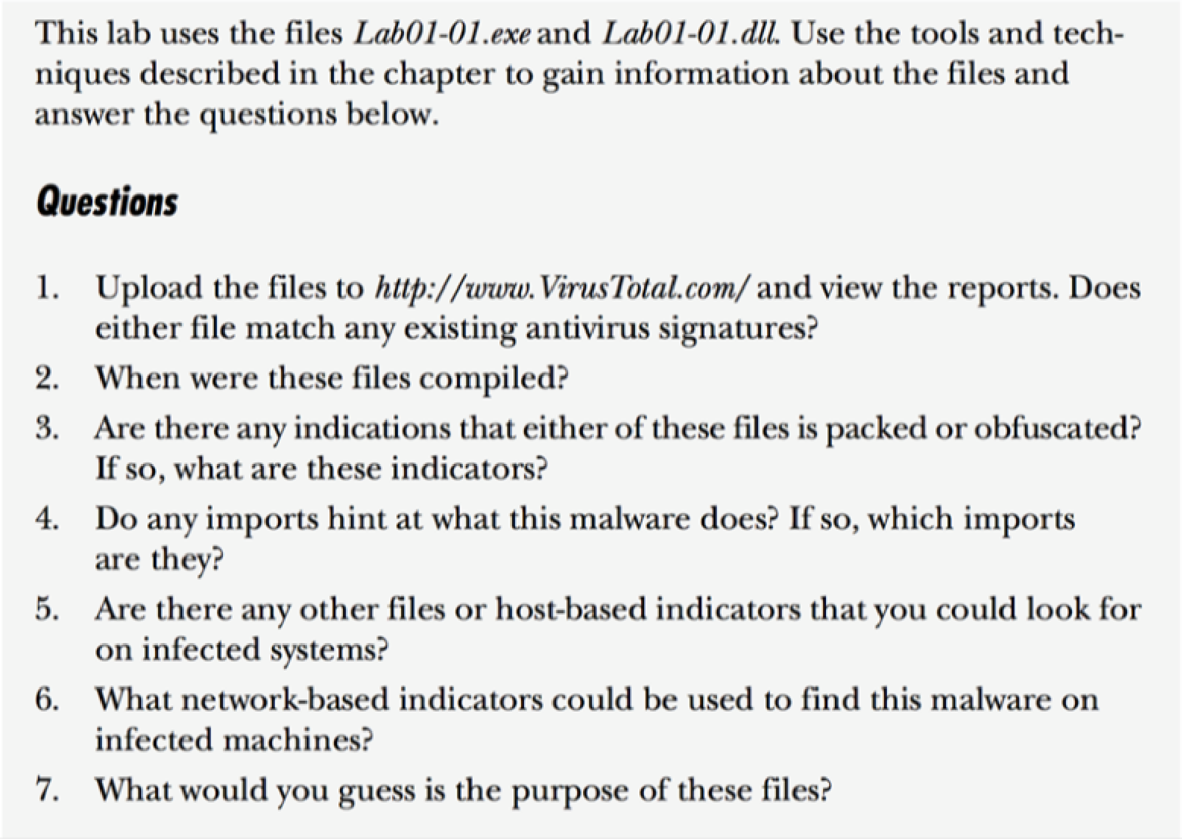
实验环境

虚拟机：Windows 7专业版

虚拟程序：VMware Workstation 16

lab 1-1

实验要求



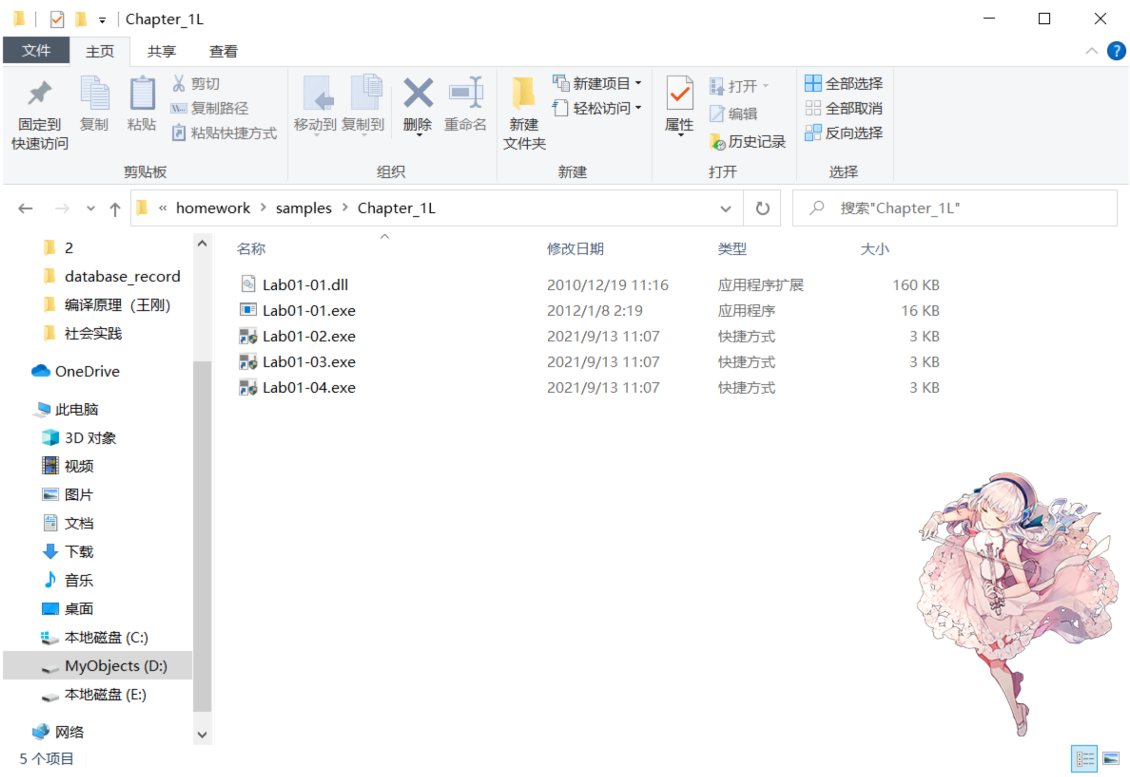
This lab uses the files *Lab01-01.exe* and *Lab01-01.dll*. Use the tools and techniques described in the chapter to gain information about the files and answer the questions below.

Questions

1. Upload the files to *http://www.VirusTotal.com/* and view the reports. Does either file match any existing antivirus signatures?
2. When were these files compiled?
3. Are there any indications that either of these files is packed or obfuscated? If so, what are these indicators?
4. Do any imports hint at what this malware does? If so, which imports are they?
5. Are there any other files or host-based indicators that you could look for on infected systems?
6. What network-based indicators could be used to find this malware on infected machines?
7. What would you guess is the purpose of these files?

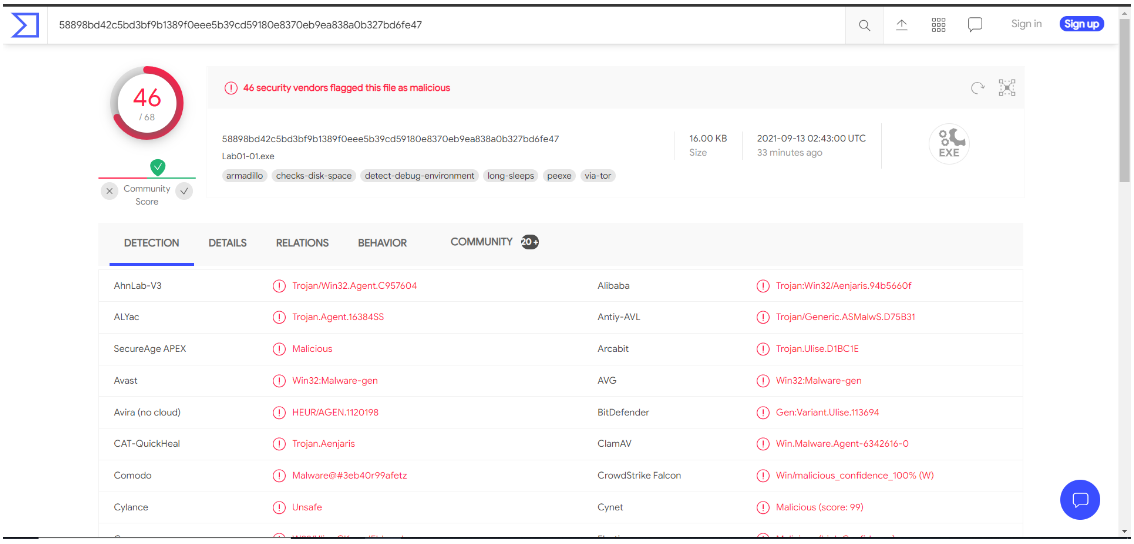
实验过程

1. 首先将下载好的样本进行解压，得到如下图所示目录



名称	修改日期	类型	大小
Lab01-01.dll	2010/12/19 11:16	应用程序扩展	160 KB
Lab01-01.exe	2012/1/8 2:19	应用程序	16 KB
Lab01-02.exe	2021/9/13 11:07	快捷方式	3 KB
Lab01-03.exe	2021/9/13 11:07	快捷方式	3 KB
Lab01-04.exe	2021/9/13 11:07	快捷方式	3 KB

2. 将`lab01-01.exe`提交到`virusTotal.com`，得到report



58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47

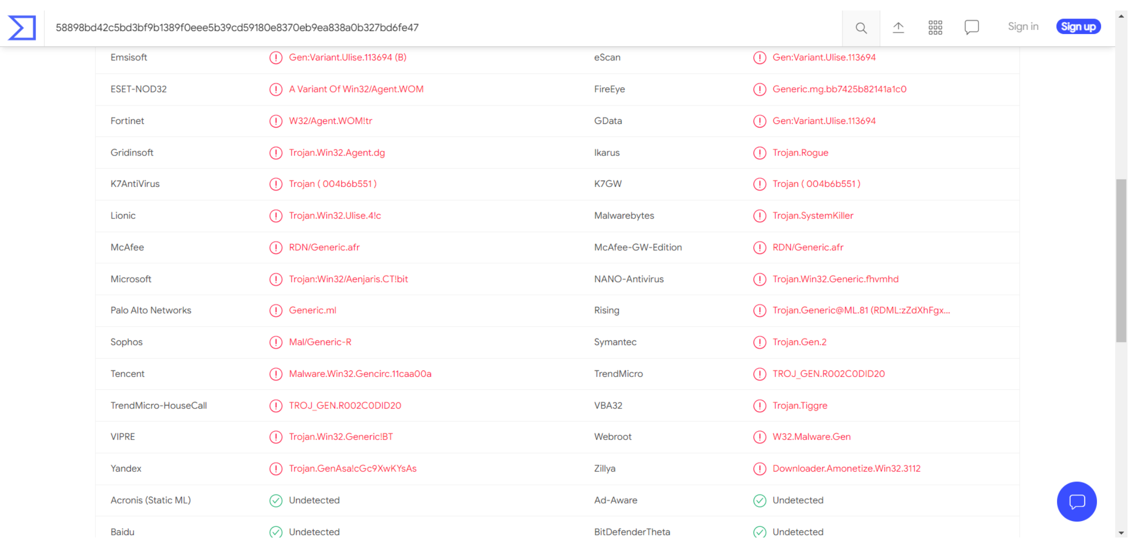
46 security vendors flagged this file as malicious

58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
Lab01-01.exe
armadillo checks-disk-space detect-debug-environment long-sleeps peexe via-tor

16.00 KB
Size

2021-09-13 02:43:00 UTC
33 minutes ago

AhnLab-V3	Trojan/Win32.Agent.C957604	Alibaba	Trojan:Win32/Aenjaris.94b5660f
ALYac	Trojan.Agent.16384SS	Antiy-AVL	Trojan/Generic.ASMalwS.D75B31
SecureAge APEX	Malicious	Arcabit	Trojan.Ulise.D1BC1E
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	HEUR/AGEN.1120198	BitDefender	Gen:Variant.Ulise.113694
CAT-QuickHeal	Trojan.Aenjaris	ClamAV	Win.Malware.Agent-6342616-0
Comodo	Malware@#3eb40r99afetz	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 99)

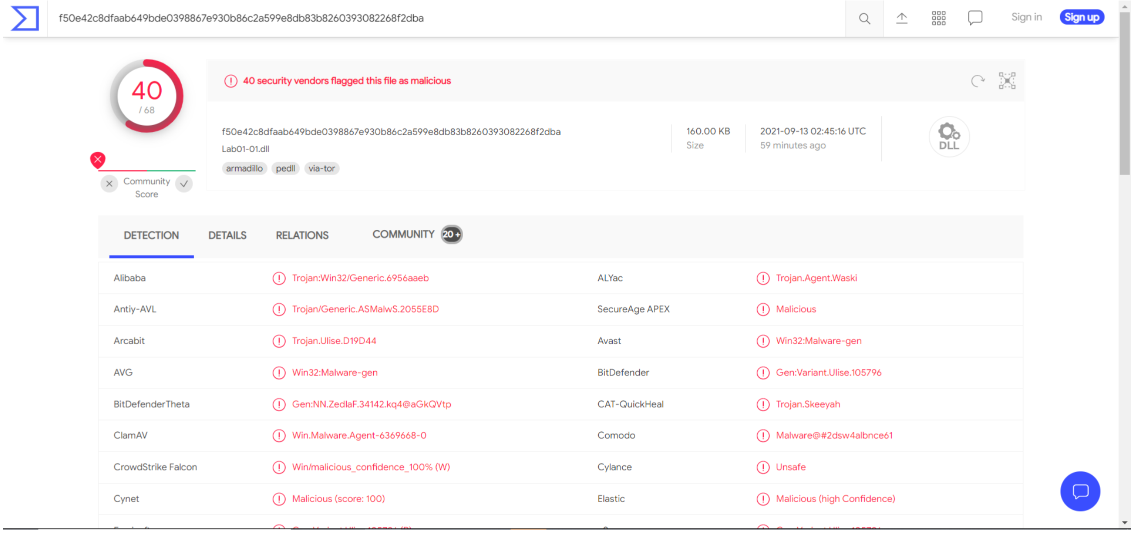


58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47

Emsisoft	Gen:Variant.Ulise.113694 (B)	eScan	Gen:Variant.Ulise.113694
ESET-NOD32	A Variant Of Win32/Agent.WOM	FireEye	Generic.mg.bb7425b82141a1c0
Fortinet	W32/Agent.WOM!tr	GData	Gen:Variant.Ulise.113694
Gridinsoft	Trojan.Win32.Agent.dg	Ikarus	Trojan.Rogue
K7AntiVirus	Trojan (004b6b551)	K7GW	Trojan (004b6b551)
Lionic	Trojan.Win32.Ulise.4!c	Malwarebytes	Trojan.SystemKiller
McAfee	RDN/Generic.afr	McAfee-GW-Edition	RDN/Generic.afr
Microsoft	Trojan:Win32/Aenjaris.CT!bit	NANO-Antivirus	Trojan.Win32.Generic.fhvmhd
Palo Alto Networks	Generic.ml	Rising	Trojan.Generic@ML.81 (RDML:zZdXhFgx...
Sophos	Mal/Generic-R	Symantec	Trojan.Gen.2
Tencent	Malware.Win32.Gencirc.11caa00a	TrendMicro	TROJ_GEN.R002C0DID20
TrendMicro-HouseCall	TROJ_GEN.R002C0DID20	VBA32	Trojan.Tiggre
VIPRE	Trojan.Win32.Generic!BT	Webroot	W32.Malware.Gen
Yandex	Trojan.GenAsa!cGc9XwKYsAs	Zillya	Downloader.Amonetize.Win32.3112
Acronis (Static ML)	Undetected	Ad-Aware	Undetected
Baidu	Undetected	BitDefenderTheta	Undetected

可以看到此时有46家杀毒公司都检测出来了这个文件是病毒

3. 将`lab01-01.dll`提交到`virusTotal.com`，得到report



f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba

40
/ 68

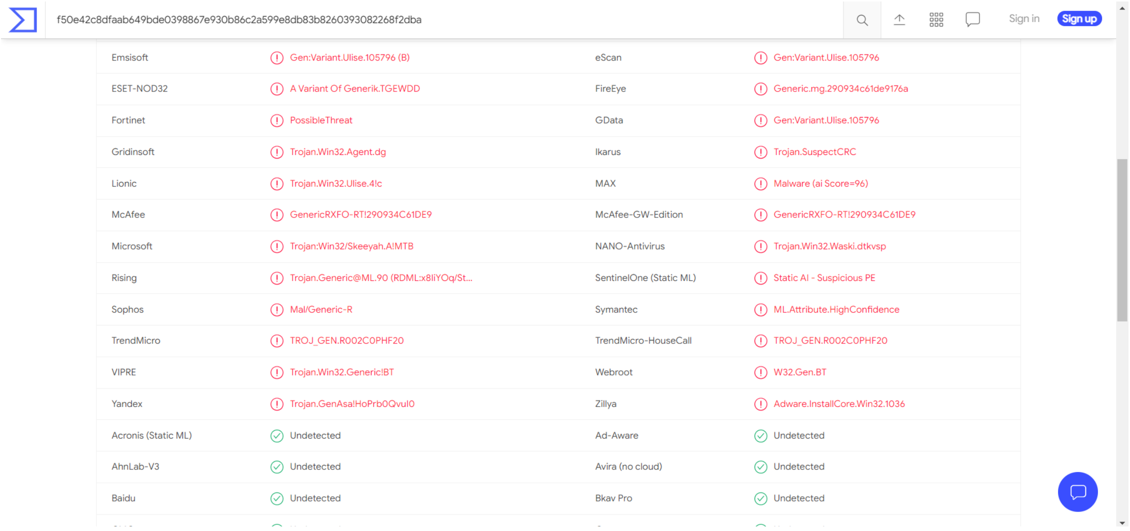
40 security vendors flagged this file as malicious

f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba
Lab01-01.dll
armadillo pedll via-tor

160.00 KB
Size

2021-09-13 02:45:16 UTC
59 minutes ago

Alibaba	Trojan:Win32/Generic.6956aaeb	ALYac	Trojan.Agent.Waski
Antiy-AVL	Trojan/Generic.ASMalwS.2055E8D	SecureAge APEX	Malicious
Arcabit	Trojan.Ulise.D19D44	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	BitDefender	Gen:Variant.Ulise.105796
BitDefenderTheta	Gen:NN.ZedlaF.34142.kq4@aGkQVtp	CAT-QuickHeal	Trojan.Skeeyah
ClamAV	Win.Malware.Agent-6369668-0	Comodo	Malware@#2dsw4albnce61
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe
Cynet	Malicious (score: 100)	Elastic	Malicious (high Confidence)



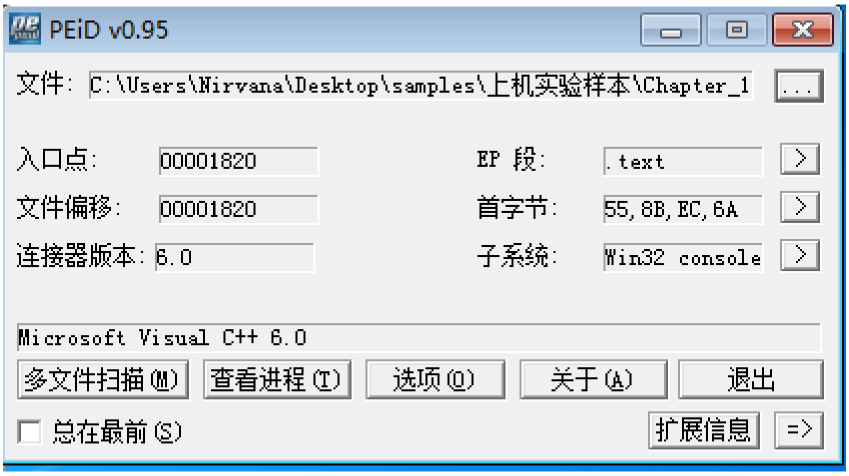
f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba

Emsisoft	Gen:Variant.Ulise.105796 (B)	eScan	Gen:Variant.Ulise.105796
ESET-NOD32	A Variant Of Generik.TGEWDD	FireEye	Generic.mg.290934c61de9176a
Fortinet	PossibleThreat	GData	Gen:Variant.Ulise.105796
Gridinsoft	Trojan.Win32.Agent.dg	Ikarus	Trojan.SuspectCRC
Lionic	Trojan.Win32.Ulise.4!c	MAX	Malware (ai Score=96)
McAfee	GenericRXFO-RT!290934C61DE9	McAfee-GW-Edition	GenericRXFO-RT!290934C61DE9
Microsoft	Trojan:Win32/Skeeyah.A!MTB	NANO-Antivirus	Trojan.Win32.Waski.dtkvsp
Rising	Trojan.Generic@ML.90 (RDML:x8IiYOq/St...	SentinelOne (Static ML)	Static AI - Suspicious PE
Sophos	Mal/Generic-R	Symantec	ML.Attribute.HighConfidence
TrendMicro	TROJ_GEN.R002C0PHF20	TrendMicro-HouseCall	TROJ_GEN.R002C0PHF20
VIPRE	Trojan.Win32.Generic!BT	Webroot	W32.Gen.BT
Yandex	Trojan.GenAsa!HoPrb0QvuI0	Zillya	Adware.InstallCore.Win32.1036
Acronis (Static ML)	Undetected	Ad-Aware	Undetected
AhnLab-V3	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	Bkav Pro	Undetected

可以看到此时有40家杀毒公司都检测出来了这个文件是病毒

4. 利用工具判断是否存在加壳

   1. 使用工具PEiD



PEiD v0.95

文件: C:\Users\Nirvana\Desktop\samples\上机实验样本\Chapter_1

入口点: 00001820

文件偏移: 00001820

连接器版本: 6.0

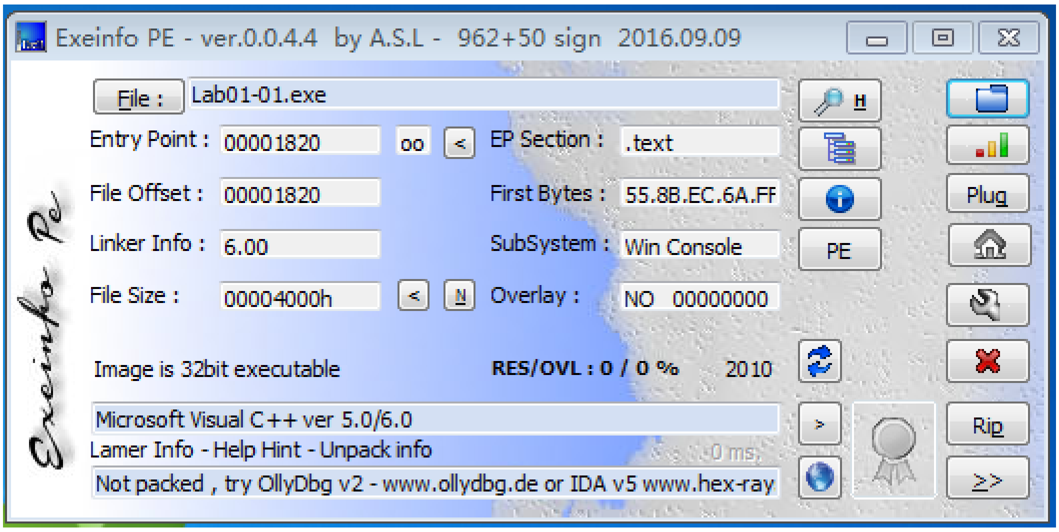
EP 段: .text

首字节: 55,8B,EC,6A

子系统: Win32 console

Microsoft Visual C++ 6.0

   2. 使用工具Exeinfo



File : Lab01-01.exe

Entry Point : 00001820

EP Section : .text

File Offset : 00001820

First Bytes : 55.8B.EC.6A.FF

Linker Info : 6.00

SubSystem : Win Console

File Size : 00004000h

Overlay : NO 00000000

Image is 32bit executable

RES/OVL : 0 / 0 % 2010

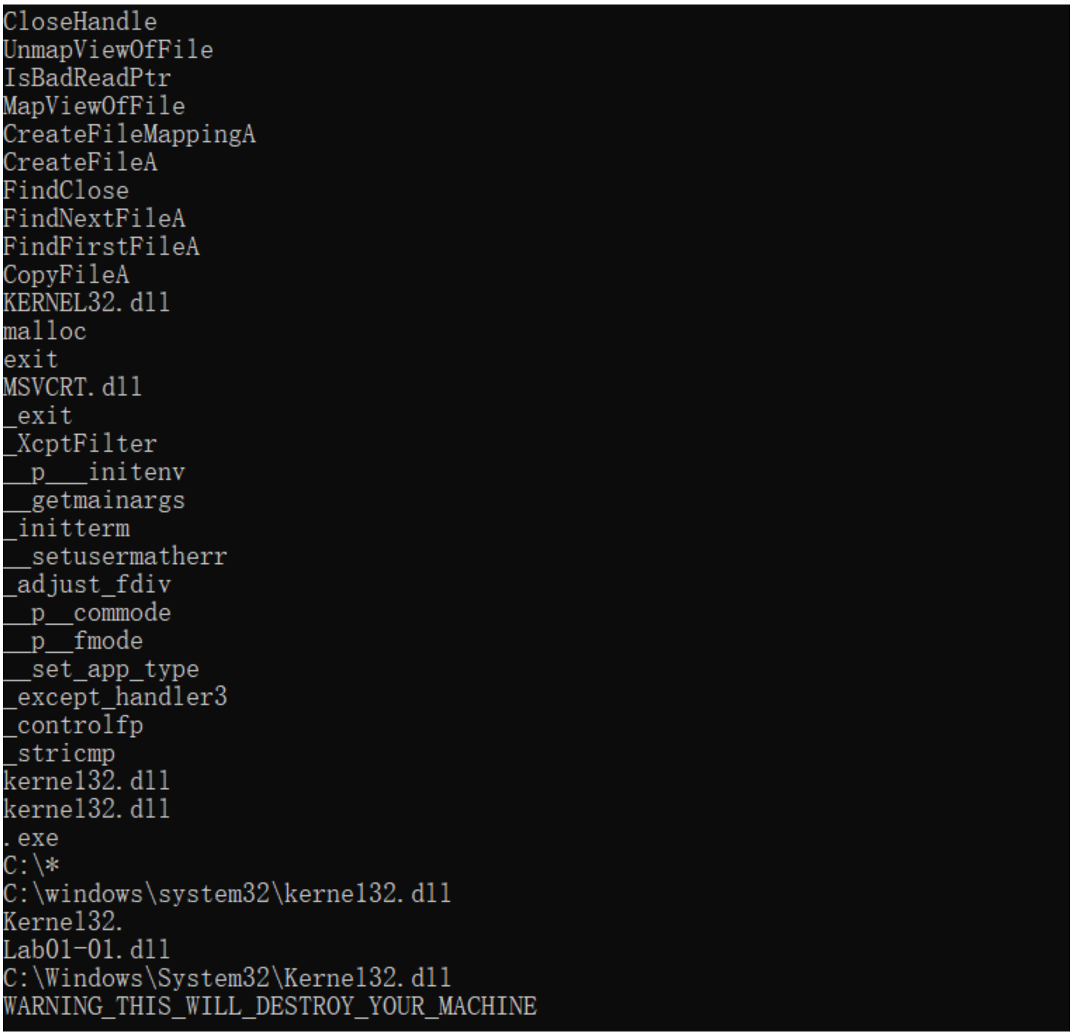
Microsoft Visual C++ ver 5.0/6.0

Lamer Info - Help Hint - Unpack info 0 ms.

Not packed , try OllyDbg v2 - www.ollydbg.de or IDA v5 www.hex-ray

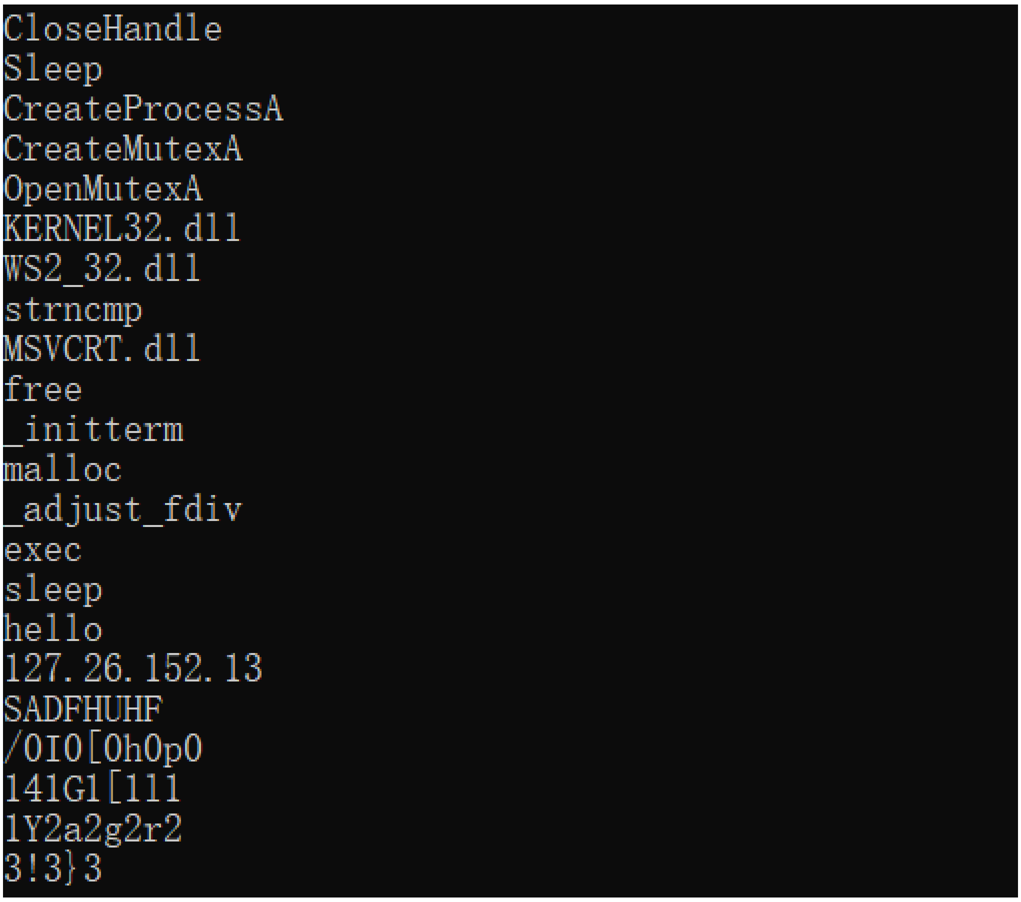
可以看出没有进行加壳

5. 使用strings工具
    1. 对`Lab01-01.exe`进行分析，得到如下结果（已忽略无效字符串）



```
CloseHandle
UnmapViewOfFile
IsBadReadPtr
MapViewOfFile
CreateFileMappingA
CreateFileA
FindClose
FindNextFileA
FindFirstFileA
CopyFileA
KERNEL32.dll
malloc
exit
MSVCRT.dll
_exit
_XcptFilter
__p___initenv
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
__set_app_type
_except_handler3
_controlfp
_stricmp
kerne132.dll
kerne132.dll
.exe
C:\*
C:\windows\system32\kerne132.dll
Kerne132.
Lab01-01.dll
C:\Windows\System32\Kerne132.dll
WARNING_THIS_WILL_DESTROY_YOUR_MACHINE
```

    2. 对`Lab01-01.dll`进行分析，得到如下结果（已忽略无效字符串）



```
CloseHandle
Sleep
CreateProcessA
CreateMutexA
OpenMutexA
KERNEL32.dll
WS2_32.dll
strncmp
MSVCRT.dll
free
_initterm
malloc
_adjust_fdiv
exec
sleep
hello
127.26.152.13
SADFHUHF
/0I0[0h0p0
141G1[111
1Y2a2g2r2
3!3}3
```

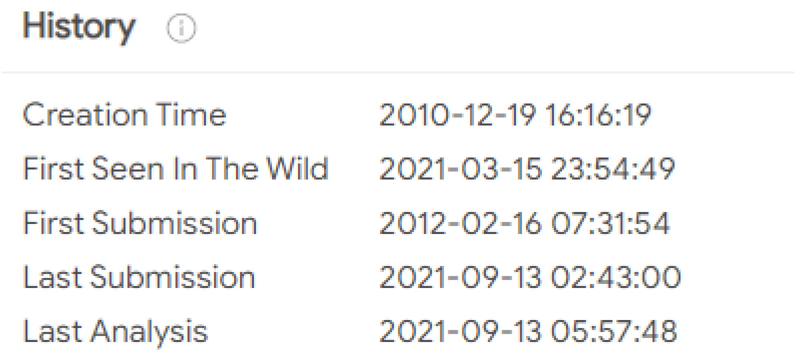
问题回答

Q1

通过实验过程2、3可以清晰的看见`lab01-01.exe`有46家杀毒公司检测出，`lab01-01.dll`有40家杀毒公司检测出

Q2

根据VirusTotal中的反馈，可以看出时间应该是在2020-12-19



History

Creation Time	2010-12-19 16:16:19
First Seen In The Wild	2021-03-15 23:54:49
First Submission	2012-02-16 07:31:54
Last Submission	2021-09-13 02:43:00
Last Analysis	2021-09-13 05:57:48

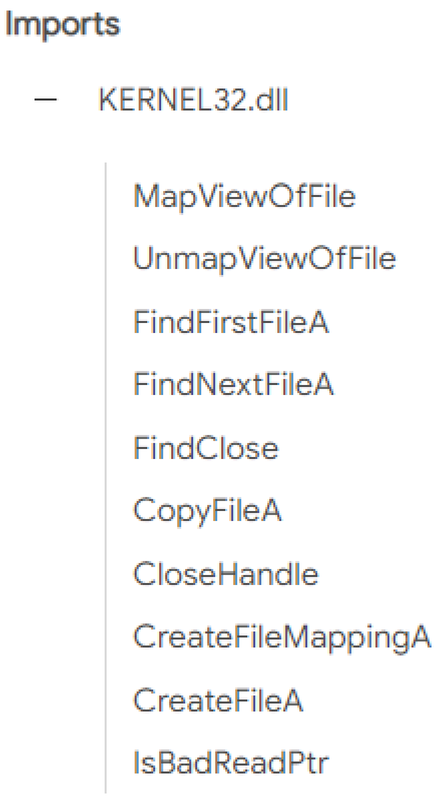
Q3

根据实验过程3、4可以看出本次实验的样本并没有进行加壳

Q4

根据VirusTotal的报告，可以看出

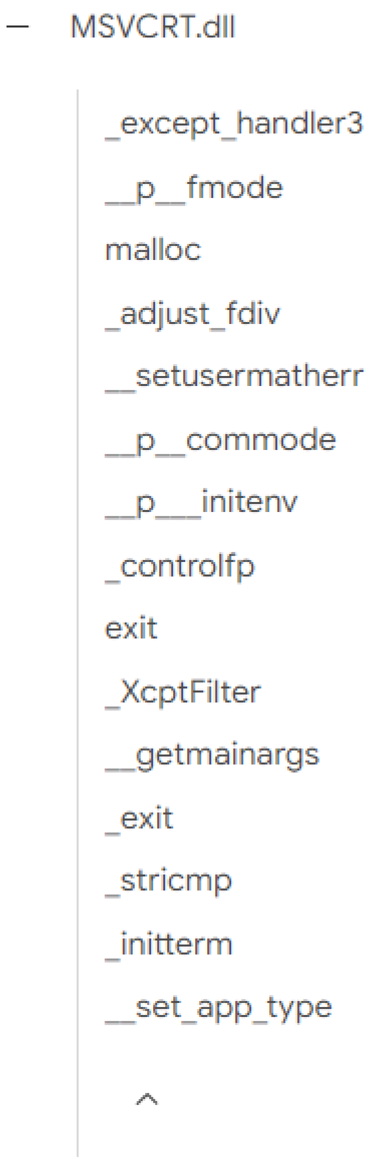
1. exe文件有`Kernel32.dll`和`MSVCRT.dll`



Imports

— KERNEL32.dll

MapViewOfFile
UnmapViewOfFile
FindFirstFileA
FindNextFileA
FindClose
CopyFileA
CloseHandle
CreateFileMappingA
CreateFileA
IsBadReadPtr



— MSVCRT.dll

_except_handler3

__p__fmode

malloc

_adjust_fdiv

__setusermatherr

__p__commode

__p___initenv

_controlfp

exit

_XcptFilter

__getmainargs

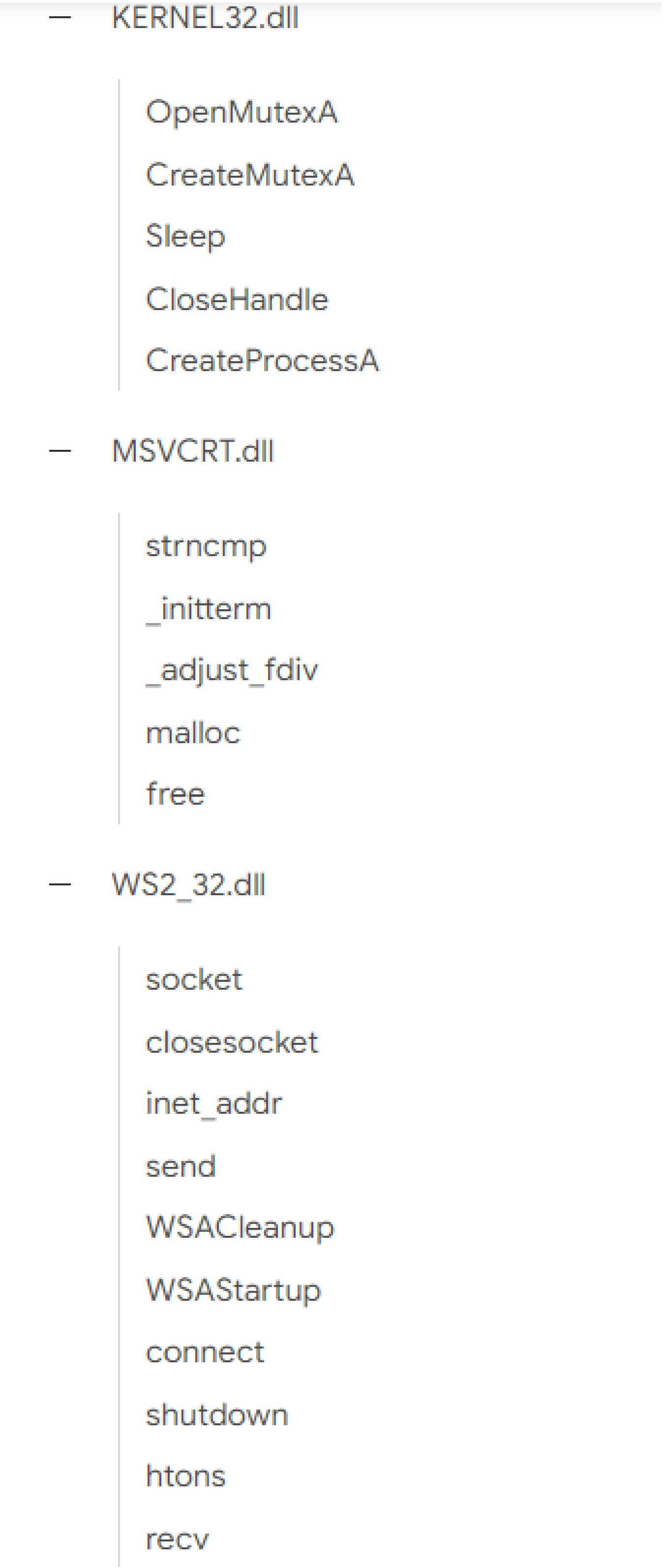
_exit

_stricmp

_initterm

__set_app_type

2. dll文件有`Kernel32.dll`、`MSVCRT.dll`和`WS2_32.dll`



- KERNEL32.dll
  - OpenMutexA
  - CreateMutexA
  - Sleep
  - CloseHandle
  - CreateProcessA
- MSVCRT.dll
  - strncmp
  - _initterm
  - _adjust_fdiv
  - malloc
  - free
- WS2_32.dll
  - socket
  - closesocket
  - inet_addr
  - send
  - WSACleanup
  - WSAStartup
  - connect
  - shutdown
  - htons
  - recv

Q5

VirutTotal反馈的相关检测报告如下：

```
File System Actions
Files Opened
C:\Windows\TEMP\CR_DB106.tmp
C:\Windows\TEMP\CR_DB106.tmp\CHROME_PATCH.PACKED.7Z
C:\Windows\TEMP\CR_DB106.tmp\SETUP_PATCH.PACKED.7Z
\??\MountPointManager
```

```
\SystemRoot\AppPatch\sysmain.sdb
C:\

Files Written
C:\Windows\Temp\CR_DB106.tmp\CHROME_PATCH.PACKED.7Z
C:\Windows\Temp\CR_DB106.tmp\SETUP_PATCH.PACKED.7Z
C:\Windows\TEMP\CR_DB106.tmp
C:\Windows\TEMP\CR_DB106.tmp\CHROME_PATCH.PACKED.7Z
C:\Windows\TEMP\CR_DB106.tmp\SETUP_PATCH.PACKED.7Z

Files Deleted
C:\Windows\Temp\CR_6BD02.tmp
C:\Windows\Temp\CR_6BD02.tmp\setup.exe

Registry Actions
Registry Keys Set
HKEY_LOCAL_MACHINE\SOFTWARE\Google\Update\ClientState\{8A69D345-D564-463C-AFF1-A69D9E530F96}\ap

Process And Service Actions
Shell Commands
"C:\Program Files\Google\Update\Install\{652D9351-3518-4014-9526-7C49A0F0D9B0}\69.0.3497.100_68.0.3440.106_chrome_updater.exe" --verbose-logging --do-not-launch-chrome --system-level
```

可以看出涉及到比较多的文件读写以及修改注册表和谷歌浏览器的更新操作

Q6

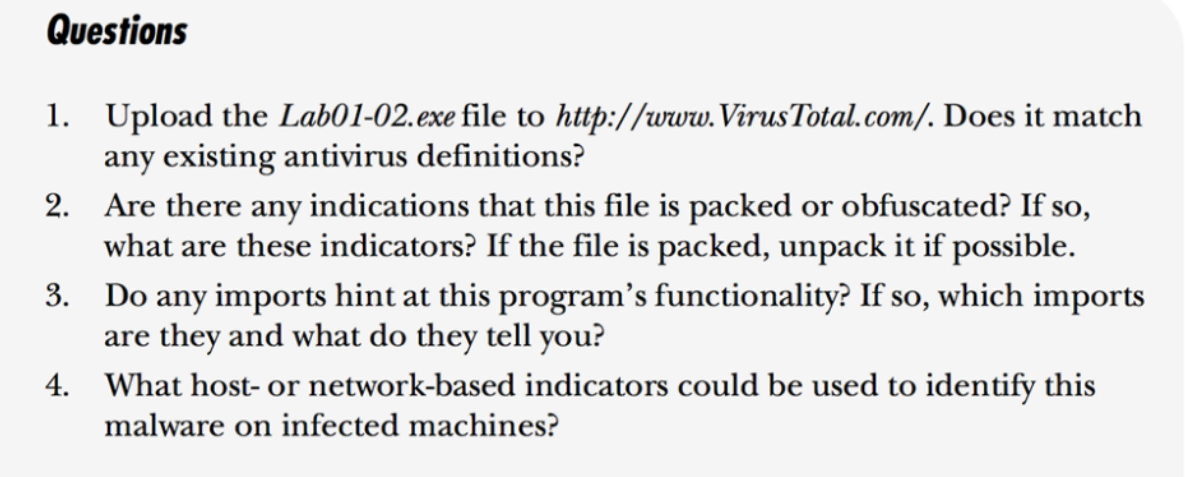
在对`Lab01-01.dll`使用strings工具进行检查时，发现了一个IP地址：127.26.152.13。猜测此exe在运行以后会对这个IP进行访问

Q7

根据反馈中其在命令行中的操作可以得出，此程序和dll的功能应该是更新Chorme，并且删除和修改一些默认的文件

lab 1-2

实验要求

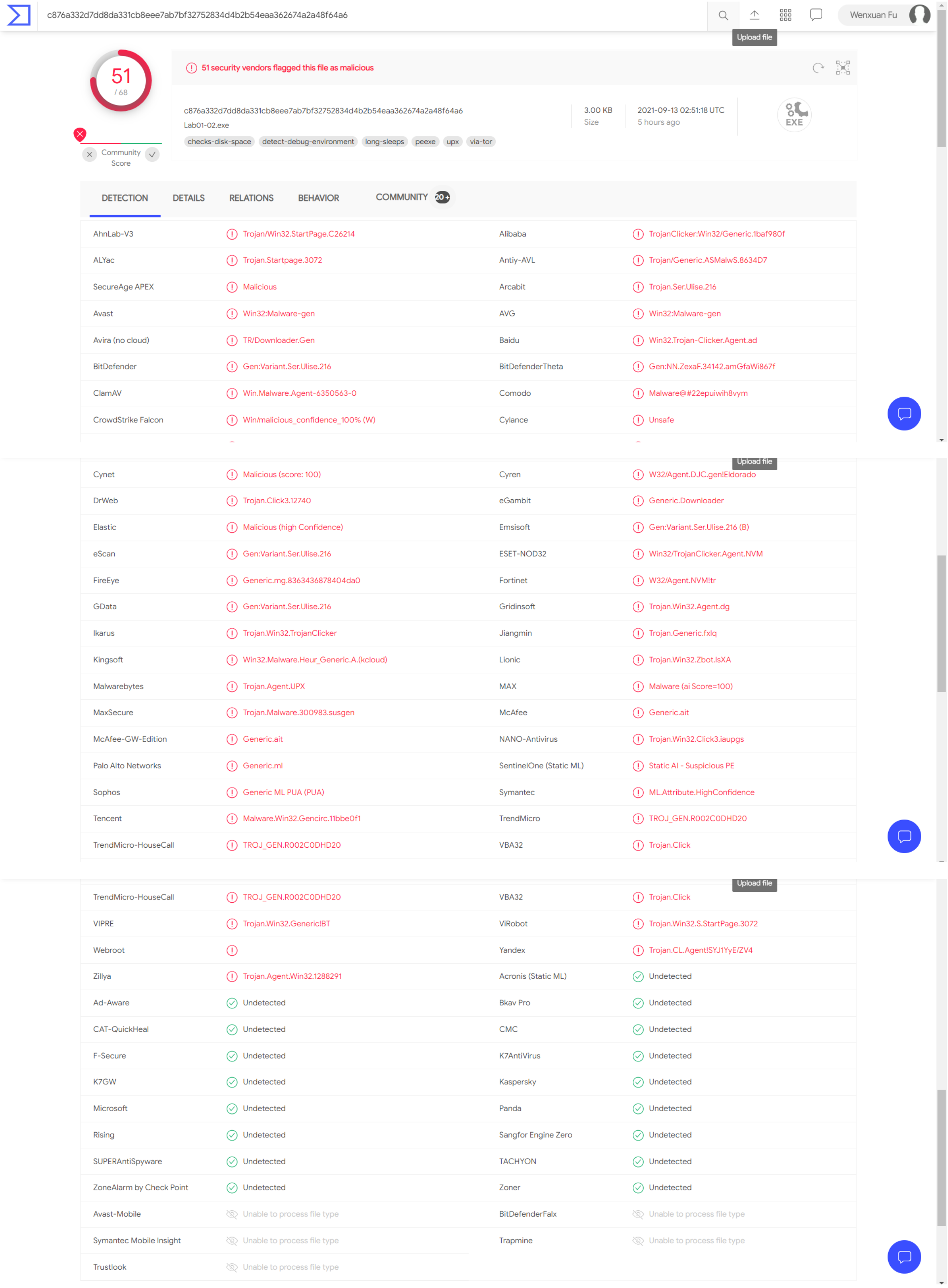


Questions

1. Upload the *Lab01-02.exe* file to *http://www.VirusTotal.com/*. Does it match any existing antivirus definitions?
2. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.
3. Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?
4. What host- or network-based indicators could be used to identify this malware on infected machines?

实验过程

1. 将`lab01-02.exe`提交到`virusTotal.com`，得到report



c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6
Wenxuan Fu
Upload file
51
/ 68
Community
Score
EXE

51 security vendors flagged this file as malicious

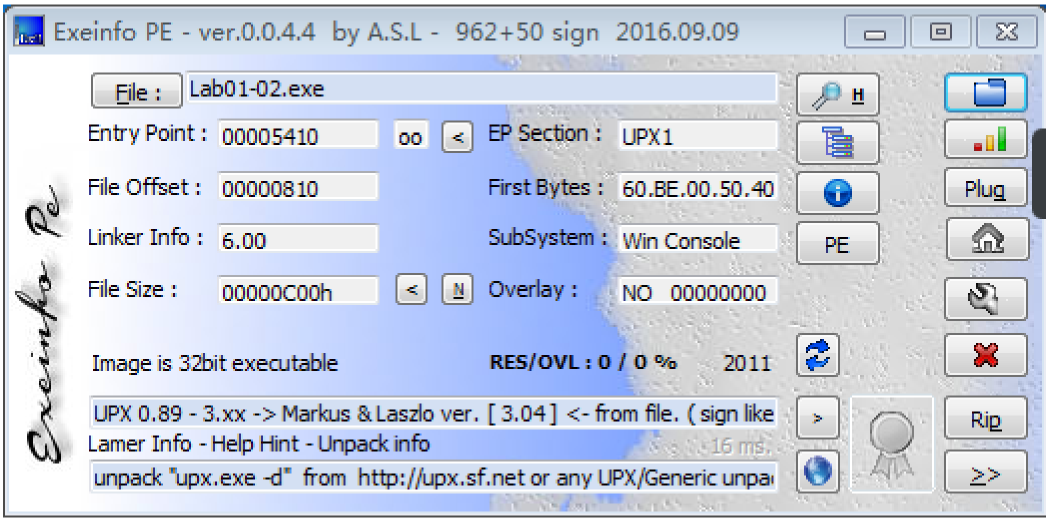
c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6
Lab01-02.exe
checks-disk-space detect-debug-environment long-sleeps peexe upx via-tor

3.00 KB
Size

2021-09-13 02:51:18 UTC
5 hours ago

AhnLab-V3	Trojan/Win32.StartPage.C26214	Alibaba	TrojanClicker:Win32/Generic.1baf980f
ALYac	Trojan.Startpage.3072	Antiy-AVL	Trojan/Generic.ASMalwS.8634D7
SecureAge APEX	Malicious	Arcabit	Trojan.Ser.Ulise.216
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	TR/Downloader.Gen	Baidu	Win32.Trojan-Clicker.Agent.ad
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)	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Agent.DJC.gen!Eldorado
DrWeb	Trojan.Click3.12740	eGambit	Generic.Downloader
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)
MaxSecure	Trojan.Malware.300983.susgen	McAfee	Generic.ait
McAfee-GW-Edition	Generic.ait	NANO-Antivirus	Trojan.Win32.Click3.iaupgs
Palo Alto Networks	Generic.ml	SentinelOne (Static ML)	Static AI - Suspicious PE
Sophos	Generic ML PUA (PUA)	Symantec	ML.Attribute.HighConfidence
Tencent	Malware.Win32.Gencirc.11bbe0f1	TrendMicro	TROJ_GEN.R002C0DHD20
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	Acronis (Static ML)	Undetected
Ad-Aware	Undetected	Bkav Pro	Undetected
CAT-QuickHeal	Undetected	CMC	Undetected
F-Secure	Undetected	K7AntiVirus	Undetected
K7GW	Undetected	Kaspersky	Undetected
Microsoft	Undetected	Panda	Undetected
Rising	Undetected	Sangfor Engine Zero	Undetected
SUPERAntiSpyware	Undetected	TACHYON	Undetected
ZoneAlarm by Check Point	Undetected	Zoner	Undetected
Avast-Mobile	Unable to process file type	BitDefenderFalx	Unable to process file type
Symantec Mobile Insight	Unable to process file type	Trapmine	Unable to process file type
Trustlook	Unable to process file type		

2. 使用工具分析是否加壳
    1. 使用Exeinfo检测



File : Lab01-02.exe

Entry Point : 00005410 EP Section : UPX1

File Offset : 00000810 First Bytes : 60.BE.00.50.40

Linker Info : 6.00 SubSystem : Win Console

File Size : 00000C00h Overlay : NO 00000000

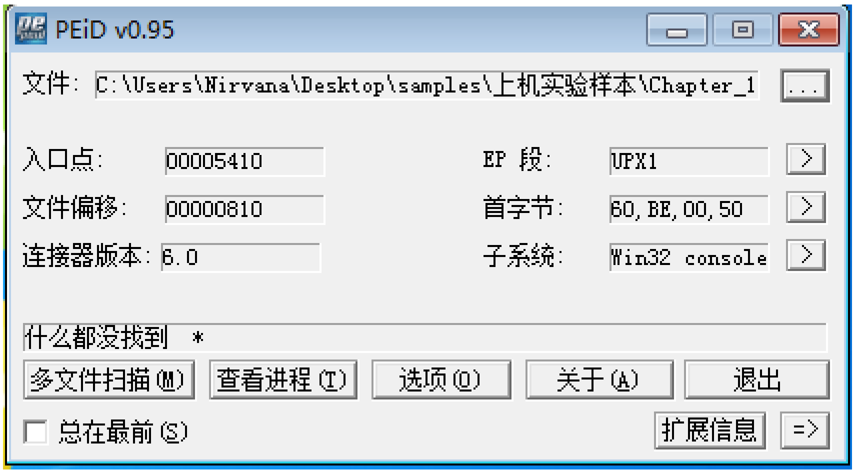
Image is 32bit executable RES/OVL : 0 / 0 % 2011

UPX 0.89 - 3.xx -> Markus & Laszlo ver. [3.04] <- from file. (sign like

Lamer Info - Help Hint - Unpack info 16 ms.

unpack "upx.exe -d" from http://upx.sf.net or any UPX/Generic unpa

2. 使用PEiD检测



文件: C:\Users\Nirvana\Desktop\samples\上机实验样本\Chapter_1

入口点: 00005410 EP 段: UPX1

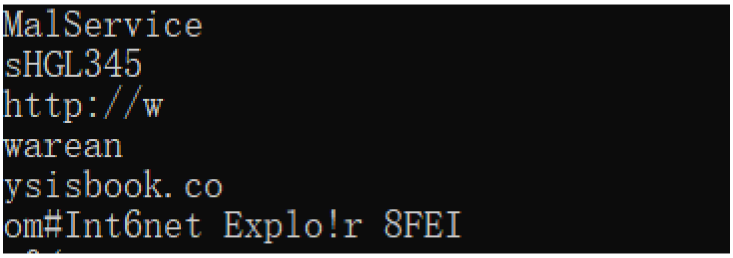
文件偏移: 00000810 首字节: 60,BE,00,50

连接器版本: 6.0 子系统: Win32 console

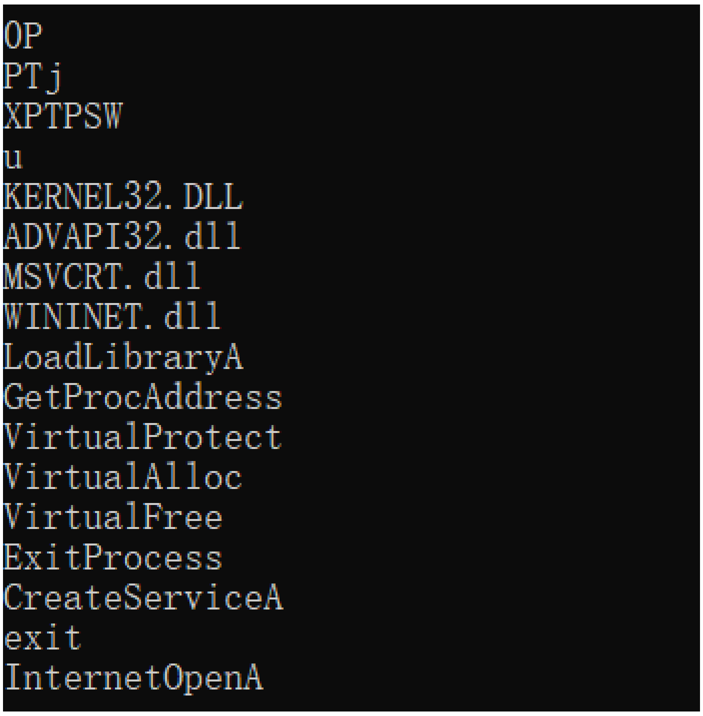
什么都没找到 *

□ 总在最前 (S)

3. 使用strings工具进行分析，得到如下截图

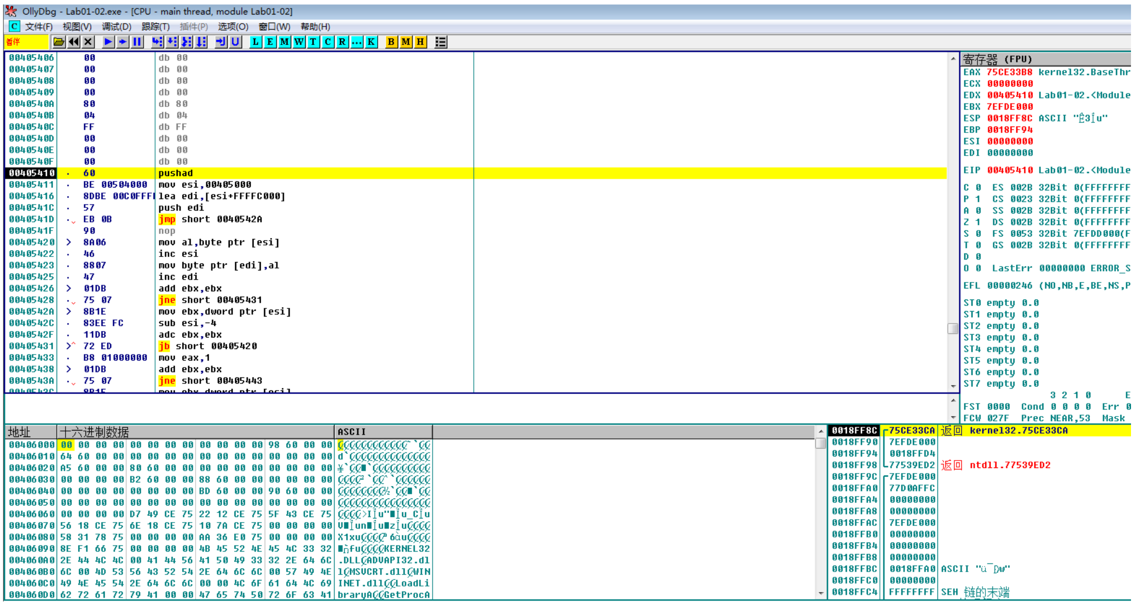


```
MalService
sHGL345
http://w
warean
ysisbook.co
om#Int6net Explo!r 8FEI
```



```
0P
PTj
XPTPSW
u
KERNEL32.DLL
ADVAPI32.dll
MSVCRT.dll
WININET.dll
LoadLibraryA
GetProcAddress
VirtualProtect
VirtualAlloc
VirtualFree
ExitProcess
CreateServiceA
exit
InternetOpenA
```

4. 使用OllyDbg进行反汇编


OllyDbg - Lab01-02.exe - [CPU - main thread, module Lab01-02]
C 文件(F) 视图(V) 调试(D) 跟踪(T) 插件(P) 选项(O) 窗口(W) 帮助(H)
暂停
L E M W T C R ... K B M H

```
00405406     00          db 00
00405407     00          db 00
00405408     00          db 00
00405409     00          db 00
0040540A     80          db 80
0040540B     04          db 04
0040540C     FF          db FF
0040540D     00          db 00
0040540E     00          db 00
0040540F     00          db 00
00405410   . 60          pushad
00405411   . BE 00504000 mov esi,00405000
00405416   . 8DBE 00C0FFFIlea edi,[esi+FFFFC000]
0040541C   . 57          push edi
0040541D   .v EB 0B      jmp short 0040542A
0040541F     90          nop
00405420   > 8A06        mov al,byte ptr [esi]
00405422   . 46          inc esi
00405423   . 8807        mov byte ptr [edi],al
00405425   . 47          inc edi
00405426   > 01DB        add ebx,ebx
00405428   .v 75 07      jne short 00405431
0040542A   > 8B1E        mov ebx,dword ptr [esi]
0040542C   . 83EE FC     sub esi,-4
0040542F   . 11DB        adc ebx,ebx
00405431   >^ 72 ED      jb short 00405420
00405433   . B8 01000000 mov eax,1
00405438   > 01DB        add ebx,ebx
0040543A   .v 75 07      jne short 00405443
```

```
寄存器 (FPU)
EAX 75CE33B8 kernel32.BaseThr
ECX 00000000
EDX 00405410 Lab01-02.<Module
EBX 7EFDE000
ESP 0018FF8C ASCII "Ê3Îu"
EBP 0018FF94
ESI 00000000
EDI 00000000

EIP 00405410 Lab01-02.<Module

C 0  ES 002B 32Bit 0(FFFFFFFF
P 1  CS 0023 32Bit 0(FFFFFFFF
A 0  SS 002B 32Bit 0(FFFFFFFF
Z 1  DS 002B 32Bit 0(FFFFFFFF
S 0  FS 0053 32Bit 7EFDD000(F
T 0  GS 002B 32Bit 0(FFFFFFFF
D 0
O 0  LastErr 00000000 ERROR_S

EFL 00000246 (NO,NB,E,BE,NS,P

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E
FST 0000  Cond 0 0 0 0  Err 0
FCW 027F  Prec NEAR,53  Mask
```

```
地址     十六进制数据                                      ASCII
00406000 00 00 00 00 00 00 00 00 00 00 00 00 98 60 00 00 ............˜`..
00406010 64 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d`..............
00406020 A5 60 00 00 80 60 00 00 00 00 00 00 00 00 00 00 ¥`..■`..........
00406030 00 00 00 00 B2 60 00 00 88 60 00 00 00 00 00 00 ....²`..ˆ`......
00406040 00 00 00 00 00 00 00 00 BD 60 00 00 90 60 00 00 ........½`..■`..
00406050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00406060 00 00 00 00 D7 49 CE 75 22 12 CE 75 5F 43 CE 75 ....×IÎu"■Îu_CÎu
00406070 56 18 CE 75 6E 18 CE 75 10 7A CE 75 00 00 00 00 V■Îun■Îu■zÎu....
00406080 58 31 78 75 00 00 00 00 AA 36 E0 75 00 00 00 00 X1xu....ª6àu....
00406090 8E F1 66 75 00 00 00 00 4B 45 52 4E 45 4C 33 32 ■ñfu....KERNEL32
004060A0 2E 44 4C 4C 00 41 44 56 41 50 49 33 32 2E 64 6C .DLL.ADVAPI32.dl
004060B0 6C 00 4D 53 56 43 52 54 2E 64 6C 6C 00 57 49 4E l.MSVCRT.dll.WIN
004060C0 49 4E 45 54 2E 64 6C 6C 00 00 4C 6F 61 64 4C 69 INET.dll..LoadLi
004060D0 62 72 61 72 79 41 00 00 47 65 74 50 72 6F 63 41 braryA..GetProcA
```

```
0018FF8C  75CE33CA  返回 kernel32.75CE33CA
0018FF90  7EFDE000
0018FF94  0018FFD4
0018FF98  77539ED2  返回 ntdll.77539ED2
0018FF9C  7EFDE000
0018FFA0  77D0AFFC
0018FFA4  00000000
0018FFA8  00000000
0018FFAC  7EFDE000
0018FFB0  00000000
0018FFB4  00000000
0018FFB8  00000000
0018FFBC  0018FFA0  ASCII "ü¯Ðw"
0018FFC0  00000000
0018FFC4  FFFFFFFF  SEH 链的末端
```

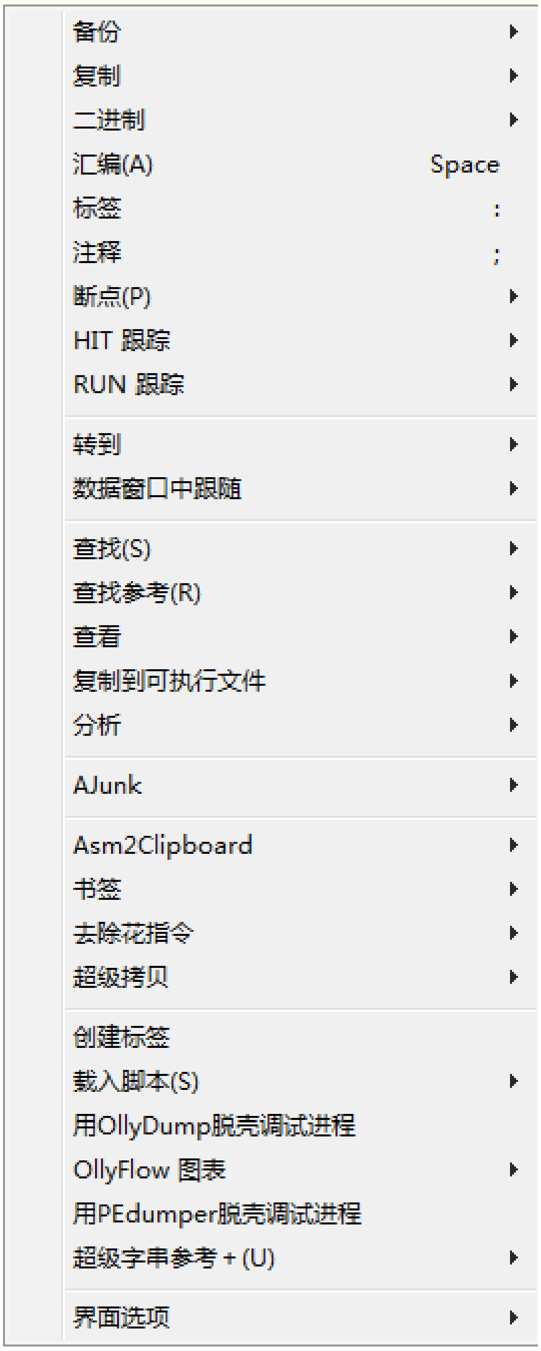
问题回答

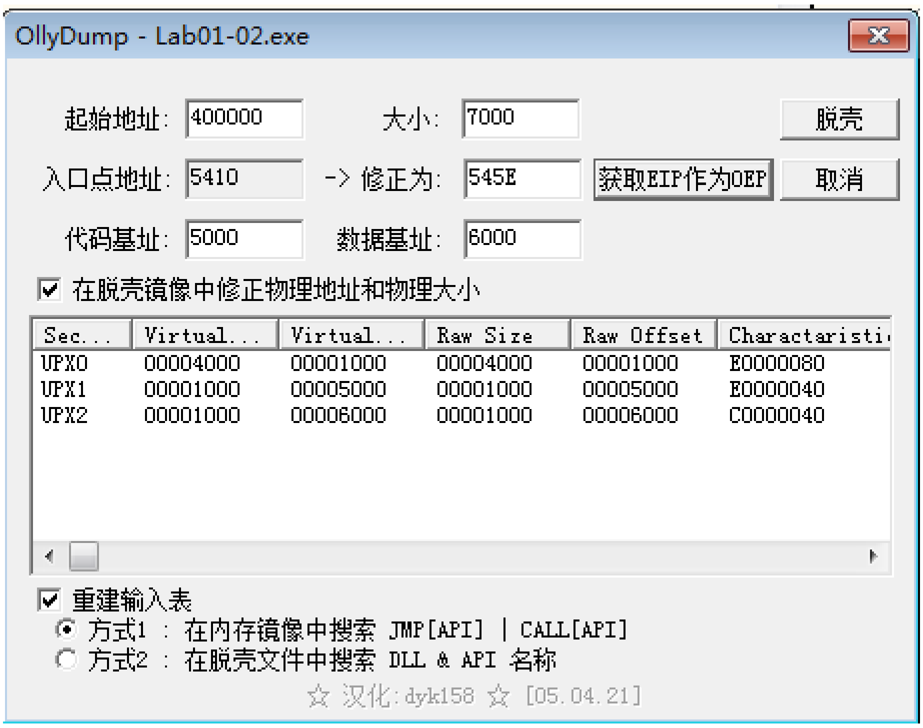
Q1

可以看出有51家杀毒公司检测出此病毒

Q2

通过Exeinfo可以看出，此样本应该是进行了加壳操作，使用的壳应该是UPX 0.89。利用OD的插件OllyDump可以进行脱壳





起始地址: 400000　大小: 7000

入口点地址: 5410　-> 修正为: 545E

代码基址: 5000　数据基址: 6000

☑ 在脱壳镜像中修正物理地址和物理大小

Sec...	Virtual...	Virtual...	Raw Size	Raw Offset	Characteristi
UPX0	00004000	00001000	00004000	00001000	E0000080
UPX1	00001000	00005000	00001000	00005000	E0000040
UPX2	00001000	00006000	00001000	00006000	C0000040

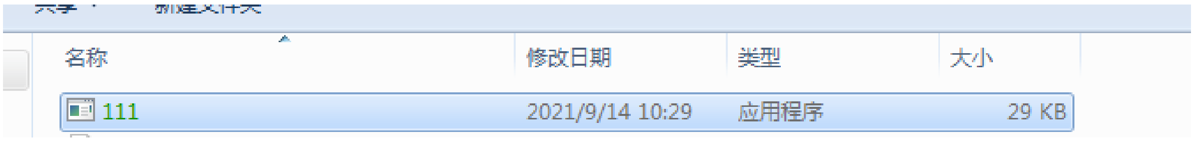
☑ 重建输入表

● 方式1 ： 在内存镜像中搜索 JMP[API] | CALL[API]

○ 方式2 ： 在脱壳文件中搜索 DLL & API 名称

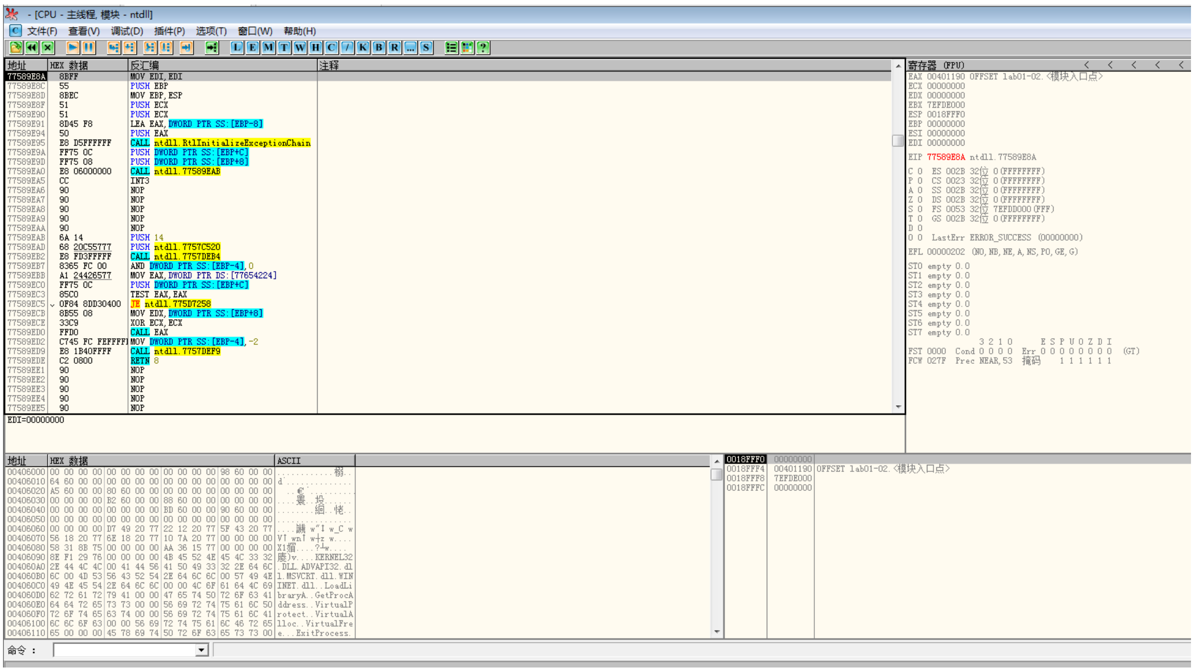
☆ 汉化:dyk158 ☆ [05.04.21]

得到脱壳后的程序：



名称	修改日期	类型	大小
111	2021/9/14 10:29	应用程序	29 KB

并可以使用OD进行反汇编


- [CPU - 主线程, 模块 - ntdll]
文件(F) 查看(V) 调试(D) 插件(P) 选项(T) 窗口(W) 帮助(H)
L E M T W H C / K B R ... S

```
地址      HEX 数据          反汇编                                   注释
77589E8A  8BFF              MOV EDI, EDI
77589E8C  55                PUSH EBP
77589E8D  8BEC              MOV EBP, ESP
77589E8F  51                PUSH ECX
77589E90  51                PUSH ECX
77589E91  8D45 F8           LEA EAX, DWORD PTR SS:[EBP-8]
77589E94  50                PUSH EAX
77589E95  E8 D5FFFFFF       CALL ntdll.RtlInitializeExceptionChain
77589E9A  FF75 0C           PUSH DWORD PTR SS:[EBP+C]
77589E9D  FF75 08           PUSH DWORD PTR SS:[EBP+8]
77589EA0  E8 06000000       CALL ntdll.77589EAB
77589EA5  CC                INT3
77589EA6  90                NOP
77589EA7  90                NOP
77589EA8  90                NOP
77589EA9  90                NOP
77589EAA  90                NOP
77589EAB  6A 14             PUSH 14
77589EAD  68 20C55777       PUSH ntdll.7757C520
77589EB2  E8 FD3FFFFF       CALL ntdll.7757DEB4
77589EB7  8365 FC 00        AND DWORD PTR SS:[EBP-4], 0
77589EBB  A1 24426577       MOV EAX, DWORD PTR DS:[77654224]
77589EC0  FF75 0C           PUSH DWORD PTR SS:[EBP+C]
77589EC3  85C0              TEST EAX, EAX
77589EC5 ⌄ 0F84 8DD30400    JE ntdll.775D7258
77589ECB  8B55 08           MOV EDX, DWORD PTR SS:[EBP+8]
77589ECE  33C9              XOR ECX, ECX
77589ED0  FFD0              CALL EAX
77589ED2  C745 FC FEFFFFI   MOV DWORD PTR SS:[EBP-4], -2
77589ED9  E8 1B40FFFF       CALL ntdll.7757DEF9
77589EDE  C2 0800           RETN 8
77589EE1  90                NOP
77589EE2  90                NOP
77589EE3  90                NOP
77589EE4  90                NOP
77589EE5  90                NOP
EDI=00000000
```

```
寄存器 (FPU)
EAX 00401190 OFFSET lab01-02.<模块入口点>
ECX 00000000
EDX 00000000
EBX 7EFDE000
ESP 0018FFF0
EBP 00000000
ESI 00000000
EDI 00000000

EIP 77589E8A ntdll.77589E8A

C 0  ES 002B 32位 0(FFFFFFFF)
P 0  CS 0023 32位 0(FFFFFFFF)
A 0  SS 002B 32位 0(FFFFFFFF)
Z 0  DS 002B 32位 0(FFFFFFFF)
S 0  FS 0053 32位 7EFDD000(FFF)
T 0  GS 002B 32位 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  掩码    1 1 1 1 1 1
```

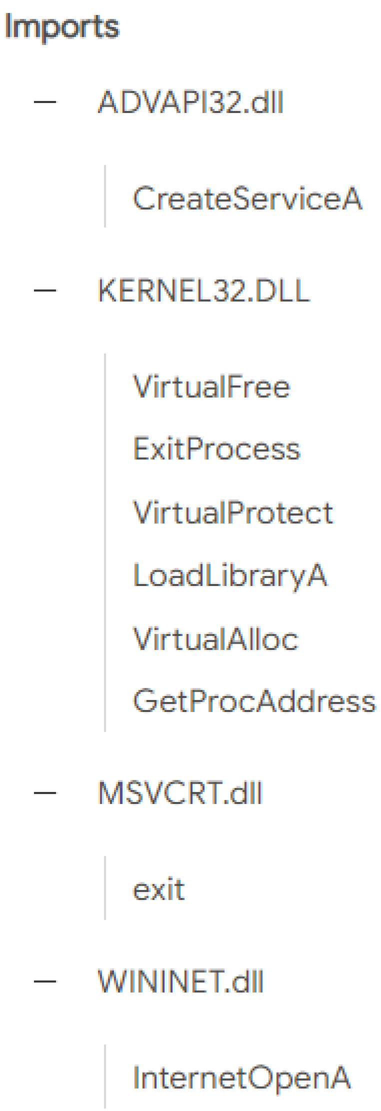
```
地址      HEX 数据                                         ASCII
00406000  00 00 00 00 00 00 00 00 00 00 00 00 98 60 00 00  ............榒..
00406010  64 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00  d`..............
00406020  A5 60 00 00 80 60 00 00 00 00 00 00 00 00 00 00  ..€`............
00406030  00 00 00 00 B2 60 00 00 88 60 00 00 00 00 00 00  ....瞏..坄......
00406040  00 00 00 00 00 00 00 00 BD 60 00 00 90 60 00 00  ........絗..恅..
00406050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00406060  00 00 00 00 D7 49 20 77 22 12 20 77 5F 43 20 77  ....譏 w" w_C w
00406070  56 18 20 77 6E 18 20 77 10 7A 20 77 00 00 00 00  V w n w z w....
00406080  58 31 8B 75 00 00 00 00 AA 36 15 77 00 00 00 00  X1媢....?w....
00406090  8E F1 29 76 00 00 00 00 4B 45 52 4E 45 4C 33 32  庱)v....KERNEL32
004060A0  2E 44 4C 4C 00 41 44 56 41 50 49 33 32 2E 64 6C  .DLL.ADVAPI32.dl
004060B0  6C 00 4D 53 56 43 52 54 2E 64 6C 6C 00 57 49 4E  l.MSVCRT.dll.WIN
004060C0  49 4E 45 54 2E 64 6C 6C 00 00 4C 6F 61 64 4C 69  INET.dll..LoadLi
004060D0  62 72 61 72 79 41 00 00 47 65 74 50 72 6F 63 41  braryA..GetProcA
004060E0  64 64 72 65 73 73 00 00 56 69 72 74 75 61 6C 50  ddress..VirtualP
004060F0  72 6F 74 65 63 74 00 00 56 69 72 74 75 61 6C 41  rotect..VirtualA
00406100  6C 6C 6F 63 00 00 56 69 72 74 75 61 6C 46 72 65  lloc..VirtualFre
00406110  65 00 00 00 45 78 69 74 50 72 6F 63 65 73 73 00  e...ExitProcess.
```

```
0018FFF0  00000000
0018FFF4  00401190  OFFSET lab01-02.<模块入口点>
0018FFF8  7EFDE000
0018FFFC  00000000
```

程序的开始就是Push EBP等对栈的操作，脱壳应该是成功了

Q3

关于imports，VirusTotal的报告如下：



Imports

- ADVAPI32.dll
  - CreateServiceA
- KERNEL32.DLL
  - VirtualFree
  - ExitProcess
  - VirtualProtect
  - LoadLibraryA
  - VirtualAlloc
  - GetProcAddress
- MSVCRT.dll
  - exit
- WININET.dll
  - InternetOpenA

从这些dll文件中函数的名字可以猜测，该程序有创建虚拟内存、保护、创建服务和联网的操作

Q4

在使用strings工具进行分析时，发现在`Lab01-02.exe`中出现有http://字样，由此将其后面的字符串进行拼接，猜测会进行问网络访问，访问网址大概为：`http://www.wareanysisbook.com`

lab 1-3

实验要求

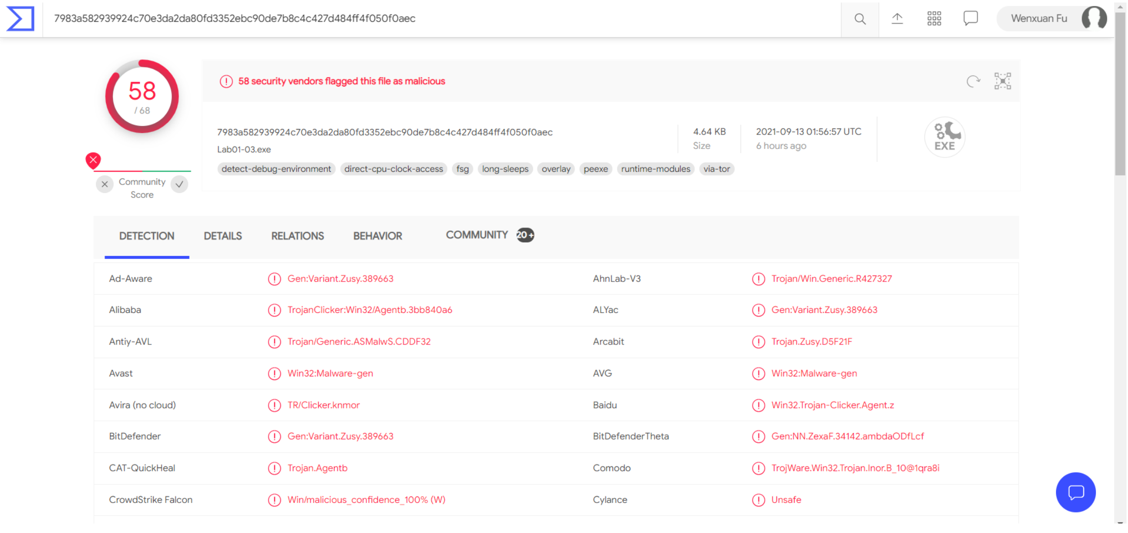
Analyze the file *Lab01-03.exe.*

Questions

1. Upload the *Lab01-03.exe* file to *http://www.VirusTotal.com/*. Does it match any existing antivirus definitions?
2. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.
3. Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?
4. What host- or network-based indicators could be used to identify this malware on infected machines?

实验过程

1. 将`lab01-03.exe`提交到`virusTotal.com`，得到report


7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec
Wenxuan Fu
58
/ 68
Community
Score
EXE

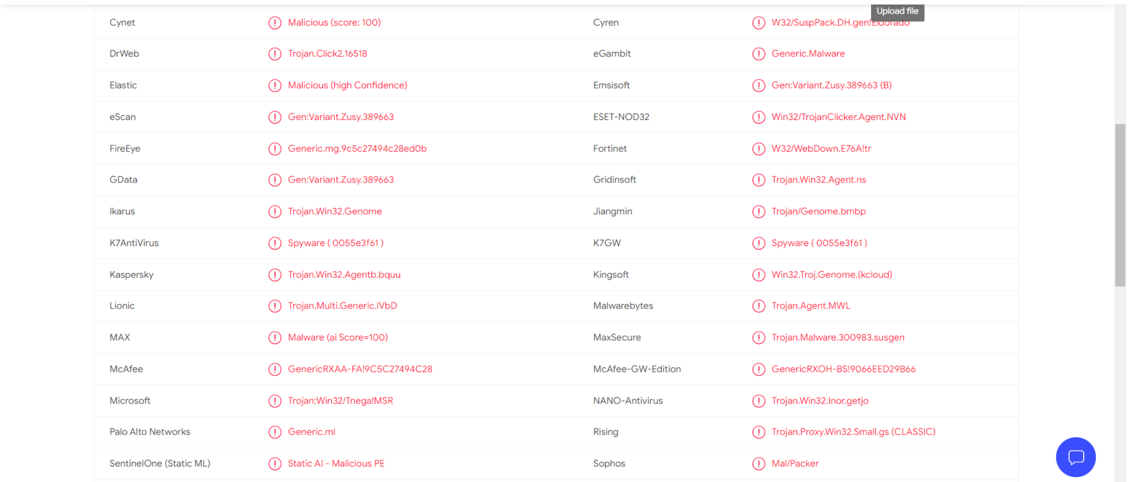
58 security vendors flagged this file as malicious

7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec
Lab01-03.exe

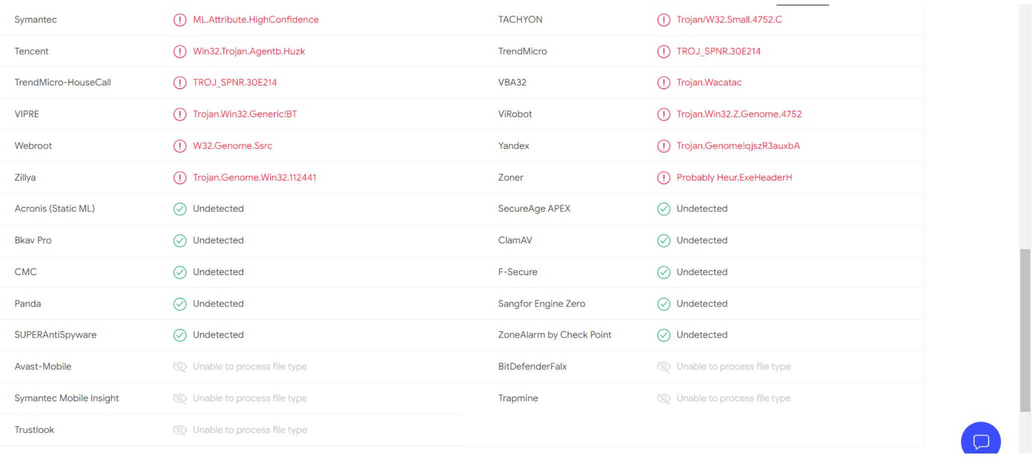
4.64 KB
Size

2021-09-13 01:56:57 UTC
6 hours ago

detect-debug-environment direct-cpu-clock-access fsg long-sleeps overlay peexe runtime-modules via-tor



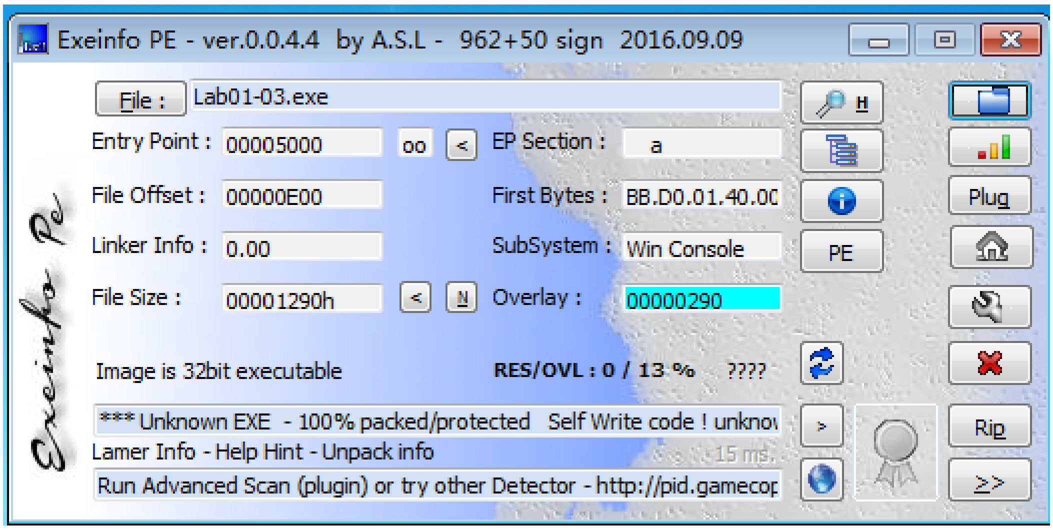
Ad-Aware	Gen:Variant.Zusy.389663	AhnLab-V3	Trojan/Win.Generic.R427327
Alibaba	TrojanClicker:Win32/Agentb.3bb840a6	ALYac	Gen:Variant.Zusy.389663
Antiy-AVL	Trojan/Generic.ASMalwS.CDDF32	Arcabit	Trojan.Zusy.D5F21F
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	TR/Clicker.knmor	Baidu	Win32.Trojan-Clicker.Agent.z
BitDefender	Gen:Variant.Zusy.389663	BitDefenderTheta	Gen:NN.ZexaF.34142.ambdaODfLcf
CAT-QuickHeal	Trojan.Agentb	Comodo	TrojWare.Win32.Trojan.Inor.B_10@1qra8i
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/SuspPack.DH.gen!Eldorado
DrWeb	Trojan.Click2.16518	eGambit	Generic.Malware
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Variant.Zusy.389663 (B)
eScan	Gen:Variant.Zusy.389663	ESET-NOD32	Win32/TrojanClicker.Agent.NVN
FireEye	Generic.mg.9c5c27494c28ed0b	Fortinet	W32/WebDown.E76A!tr
GData	Gen:Variant.Zusy.389663	Gridinsoft	Trojan.Win32.Agent.ns
Ikarus	Trojan.Win32.Genome	Jiangmin	Trojan/Genome.bmbp
K7AntiVirus	Spyware (0055e3f61)	K7GW	Spyware (0055e3f61)
Kaspersky	Trojan.Win32.Agentb.bquu	Kingsoft	Win32.Troj.Genome.(kcloud)
Lionic	Trojan.Multi.Generic.lVbD	Malwarebytes	Trojan.Agent.MWL
MAX	Malware (ai Score=100)	MaxSecure	Trojan.Malware.300983.susgen
McAfee	GenericRXAA-FA!9C5C27494C28	McAfee-GW-Edition	GenericRXOH-BS!9066EED29B66
Microsoft	Trojan:Win32/Tnega!MSR	NANO-Antivirus	Trojan.Win32.Inor.getjo
Palo Alto Networks	Generic.ml	Rising	Trojan.Proxy.Win32.Small.gs (CLASSIC)
SentinelOne (Static ML)	Static AI - Malicious PE	Sophos	Mal/Packer



Symantec	ML.Attribute.HighConfidence	TACHYON	Trojan/W32.Small.4752.C
Tencent	Win32.Trojan.Agentb.Huzk	TrendMicro	TROJ_SPNR.30E214
TrendMicro-HouseCall	TROJ_SPNR.30E214	VBA32	Trojan.Wacatac
VIPRE	Trojan.Win32.Generic!BT	ViRobot	Trojan.Win32.Z.Genome.4752
Webroot	W32.Genome.Ssrc	Yandex	Trojan.Genome!qjszR3auxbA
Zillya	Trojan.Genome.Win32.112441	Zoner	Probably Heur.ExeHeaderH
Acronis (Static ML)	Undetected	SecureAge APEX	Undetected
Bkav Pro	Undetected	ClamAV	Undetected
CMC	Undetected	F-Secure	Undetected
Panda	Undetected	Sangfor Engine Zero	Undetected
SUPERAntiSpyware	Undetected	ZoneAlarm by Check Point	Undetected
Avast-Mobile	Unable to process file type	BitDefenderFalx	Unable to process file type
Symantec Mobile Insight	Unable to process file type	Trapmine	Unable to process file type
Trustlook	Unable to process file type		

2. 使用工具判断是否加壳

   1. Exeinfo



Exeinfo PE - ver.0.0.4.4 by A.S.L - 962+50 sign 2016.09.09

File : Lab01-03.exe

Entry Point : 00005000 oo

EP Section : a

File Offset : 00000E00

First Bytes : BB.D0.01.40.00

Linker Info : 0.00

SubSystem : Win Console

File Size : 00001290h

Overlay : 00000290

Image is 32bit executable

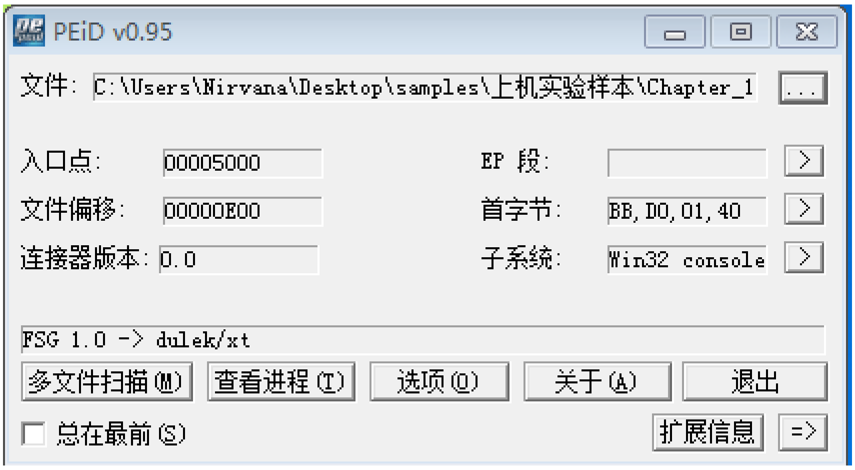
RES/OVL : 0 / 13 % ????

*** Unknown EXE - 100% packed/protected Self Write code ! unknow

Lamer Info - Help Hint - Unpack info 15 ms.

Run Advanced Scan (plugin) or try other Detector - http://pid.gamecop

   2. PEiD



PEiD v0.95

文件: C:\Users\Nirvana\Desktop\samples\上机实验样本\Chapter_1

入口点: 00005000

EP 段:

文件偏移: 00000E00

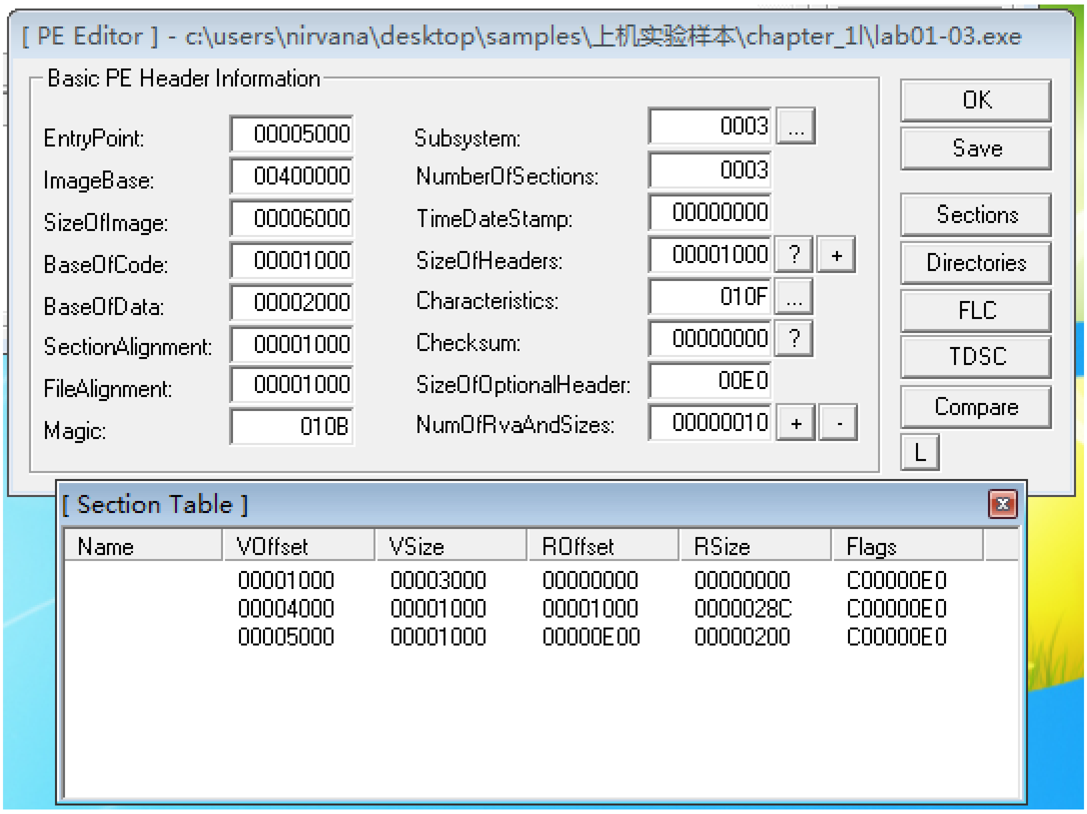
首字节: BB, D0, 01, 40

连接器版本: 0.0

子系统: Win32 console

FSG 1.0 -> dulek/xt

3. 使用LordPE查看程序的节的信息



[PE Editor] - c:\users\nirvana\desktop\samples\上机实验样本\chapter_1l\lab01-03.exe

Basic PE Header Information

EntryPoint: 00005000
ImageBase: 00400000
SizeOfImage: 00006000
BaseOfCode: 00001000
BaseOfData: 00002000
SectionAlignment: 00001000
FileAlignment: 00001000
Magic: 010B
Subsystem: 0003
NumberOfSections: 0003
TimeDateStamp: 00000000
SizeOfHeaders: 00001000
Characteristics: 010F
Checksum: 00000000
SizeOfOptionalHeader: 00E0
NumOfRvaAndSizes: 00000010

[Section Table]

Name	VOffset	VSize	ROffset	RSize	Flags
	00001000	00003000	00000000	00000000	C00000E0
	00004000	00001000	00001000	0000028C	C00000E0
	00005000	00001000	00000E00	00000200	C00000E0

可以发现有三个区段，并且区段名都抹去了

问题回答

Q1

可以看出有58家杀毒公司检测出此病毒

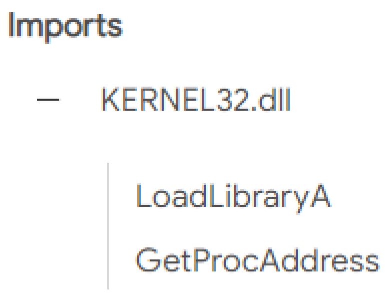
Q2

在VirusTotal得到的报告中，其检测出来的Imports中只有对`Kernel32.dll`中的`LoadLibrary`和`GetProcAddress`，由此猜测应当是存在有加壳或者混淆操作

通过工具对文件的检查，可以看出明显样本进行了加壳操作，并且判断出加壳版本是`FSG 1.0`，不会手动脱壳

Q3

VirusTotal反馈报告如下



Imports

— KERNEL32.dll

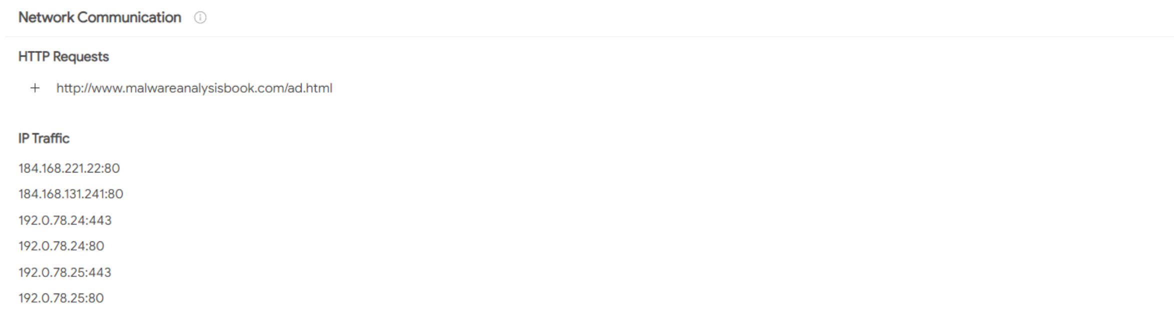
LoadLibraryA

GetProcAddress

可以看见这个程序只调用了`Kernel32.dll`，并且使用的函数是`LoadLibrary`和`GetProcAddress`，猜测这个程序应当做了加壳处理

Q4

VirusTotal中关于病毒行为表现的报告如下：



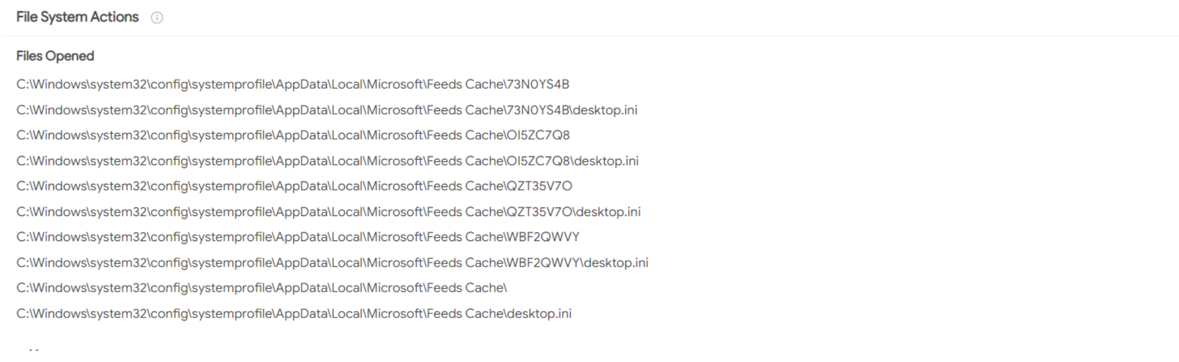
Network Communication

HTTP Requests

```
+ http://www.malwareanalysisbook.com/ad.html
```

IP Traffic

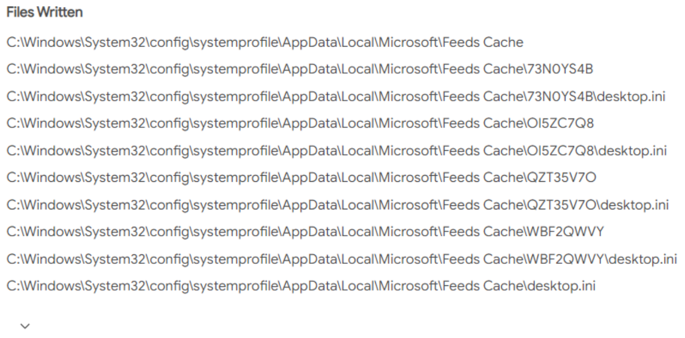
```
184.168.221.22:80
184.168.131.241:80
192.0.78.24:443
192.0.78.24:80
192.0.78.25:443
192.0.78.25:80
```



File System Actions

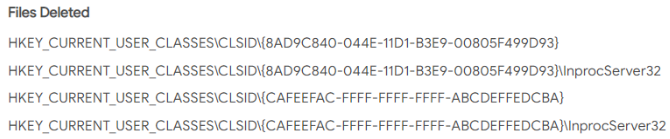
Files Opened

```
C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\Feeds Cache\73N0YS4B
C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\Feeds Cache\73N0YS4B\desktop.ini
C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\Feeds Cache\OI5ZC7Q8
C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\Feeds Cache\OI5ZC7Q8\desktop.ini
C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\Feeds Cache\QZT35V7O
C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\Feeds Cache\QZT35V7O\desktop.ini
C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\Feeds Cache\WBF2QWVY
C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\Feeds Cache\WBF2QWVY\desktop.ini
C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\Feeds Cache\
C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\Feeds Cache\desktop.ini
```



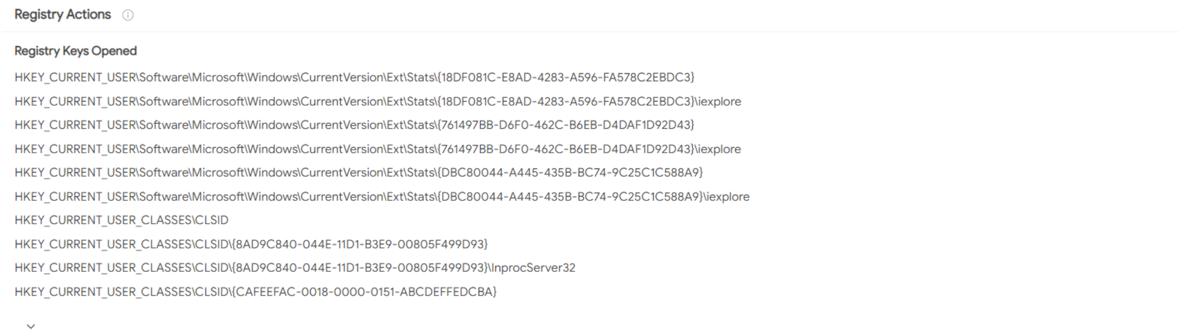
Files Written

```
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Feeds Cache
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Feeds Cache\73N0YS4B
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Feeds Cache\73N0YS4B\desktop.ini
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Feeds Cache\OI5ZC7Q8
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Feeds Cache\OI5ZC7Q8\desktop.ini
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Feeds Cache\QZT35V7O
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Feeds Cache\QZT35V7O\desktop.ini
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Feeds Cache\WBF2QWVY
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Feeds Cache\WBF2QWVY\desktop.ini
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Feeds Cache\desktop.ini
```



Files Deleted

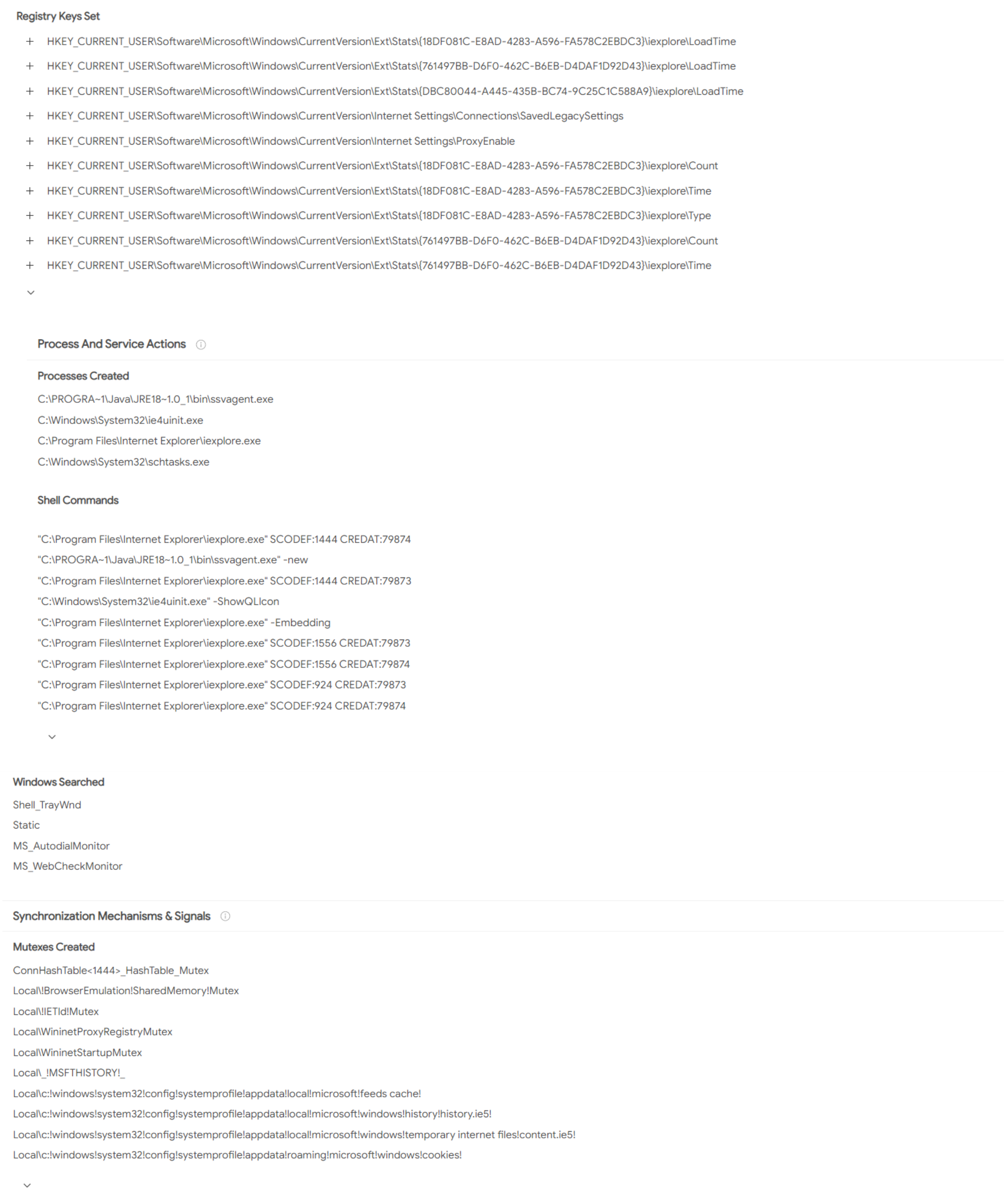
```
HKEY_CURRENT_USER_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93}
HKEY_CURRENT_USER_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93}\InprocServer32
HKEY_CURRENT_USER_CLASSES\CLSID\{CAFEEFAC-FFFF-FFFF-FFFF-ABCDEFFEDCBA}
HKEY_CURRENT_USER_CLASSES\CLSID\{CAFEEFAC-FFFF-FFFF-FFFF-ABCDEFFEDCBA}\InprocServer32
```



Registry Actions

Registry Keys Opened

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
HKEY_CURRENT_USER_CLASSES\CLSID
HKEY_CURRENT_USER_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93}
HKEY_CURRENT_USER_CLASSES\CLSID\{8AD9C840-044E-11D1-B3E9-00805F499D93}\InprocServer32
HKEY_CURRENT_USER_CLASSES\CLSID\{CAFEEFAC-0018-0000-0151-ABCDEFFEDCBA}
```



Registry Keys Set

+ HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore\LoadTime
+ HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore\LoadTime
+ HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore\LoadTime
+ HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
+ HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
+ HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore\Count
+ HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore\Time
+ HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore\Type
+ HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore\Count
+ HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore\Time

Process And Service Actions

Processes Created

C:\PROGRA~1\Java\JRE18~1.0_1\bin\ssvagent.exe
C:\Windows\System32\ie4uinit.exe
C:\Program Files\Internet Explorer\iexplore.exe
C:\Windows\System32\schtasks.exe

Shell Commands

"C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:1444 CREDAT:79874
"C:\PROGRA~1\Java\JRE18~1.0_1\bin\ssvagent.exe" -new
"C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:1444 CREDAT:79873
"C:\Windows\System32\ie4uinit.exe" -ShowQLIcon
"C:\Program Files\Internet Explorer\iexplore.exe" -Embedding
"C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:1556 CREDAT:79873
"C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:1556 CREDAT:79874
"C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:924 CREDAT:79873
"C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:924 CREDAT:79874

Windows Searched

Shell_TrayWnd
Static
MS_AutodialMonitor
MS_WebCheckMonitor

Synchronization Mechanisms & Signals

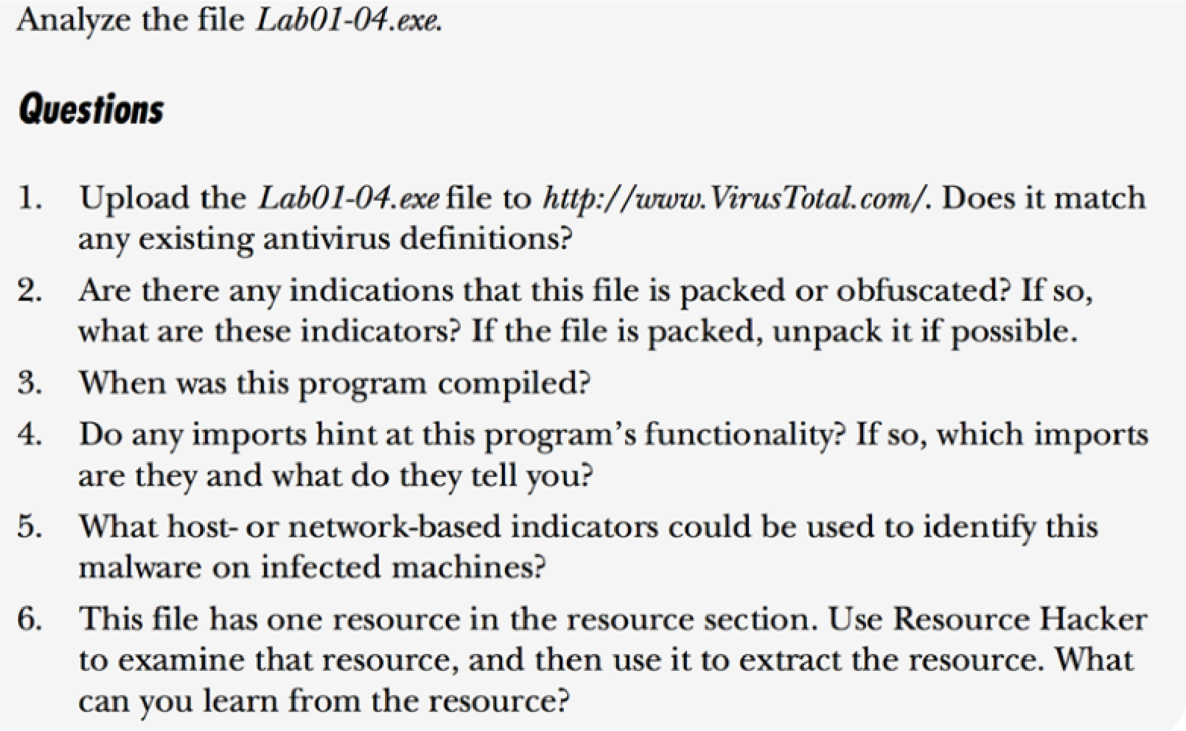
Mutexes Created

ConnHashTable<1444>_HashTable_Mutex
Local\!BrowserEmulation!SharedMemory!Mutex
Local\!IETld!Mutex
Local\WininetProxyRegistryMutex
Local\WininetStartupMutex
Local_!MSFTHISTORY!_
Local\c:!windows!system32!config!systemprofile!appdata!local!microsoft!feeds cache!
Local\c:!windows!system32!config!systemprofile!appdata!local!microsoft!windows!history!history.ie5!
Local\c:!windows!system32!config!systemprofile!appdata!local!microsoft!windows!temporary internet files!content.ie5!
Local\c:!windows!system32!config!systemprofile!appdata!roaming!microsoft!windows!cookies!

根据报告显示，这个文件存在有网络行为：链接`http://www.malwareanalysisbook.com/ad.html`、对桌面的一些配置信息进行修改、修改注册表信息

lab 1-4

实验要求



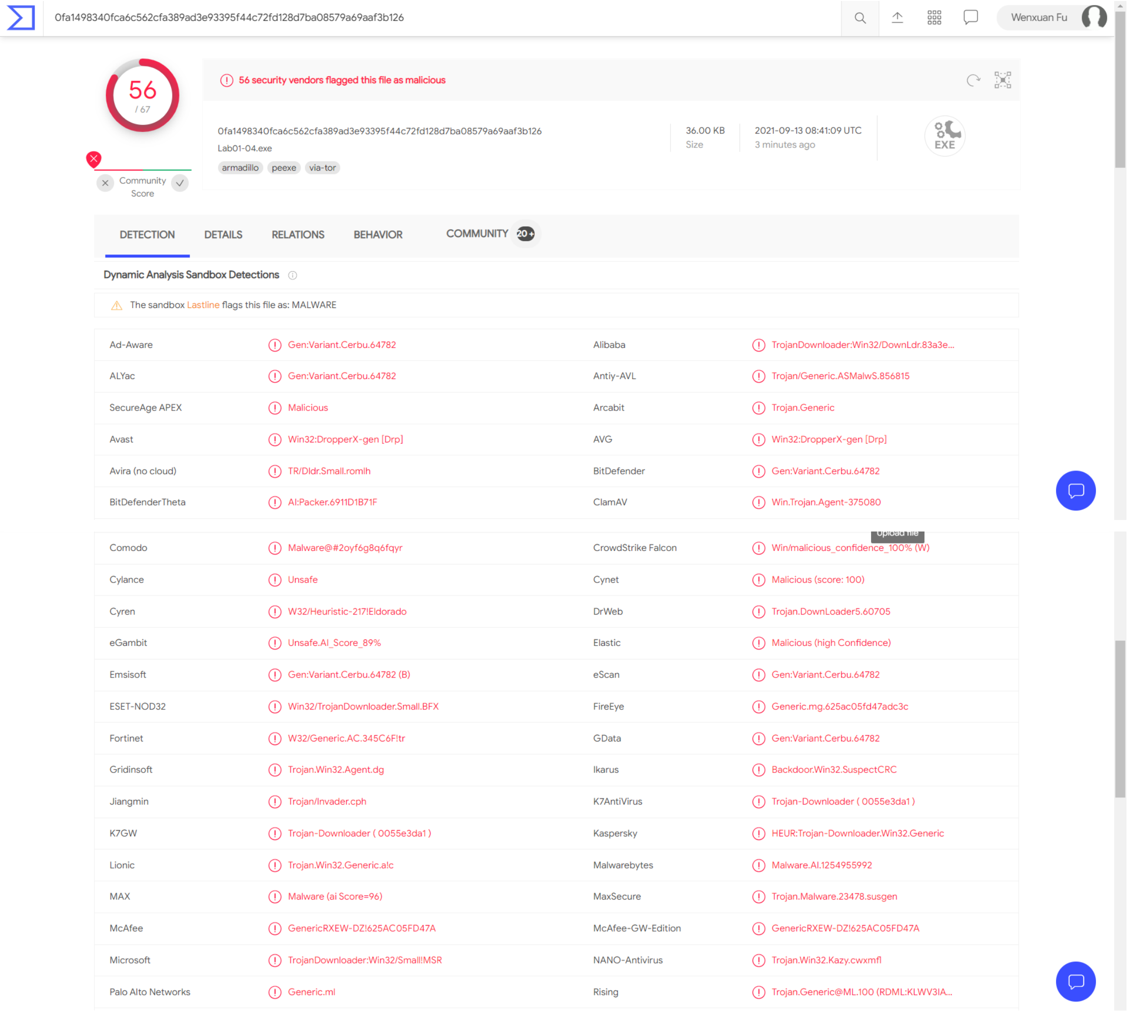
Analyze the file *Lab01-04.exe.*

Questions

1. Upload the *Lab01-04.exe* file to *http://www.VirusTotal.com/*. Does it match any existing antivirus definitions?
2. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.
3. When was this program compiled?
4. Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?
5. What host- or network-based indicators could be used to identify this malware on infected machines?
6. This file has one resource in the resource section. Use Resource Hacker to examine that resource, and then use it to extract the resource. What can you learn from the resource?

实验过程

1. 将`lab01-04.exe`提交到`virusTotal.com`，得到report



0fa1498340fca6c562cfa389ad3e93395f44c72fd128d7ba08579a69aaf3b126
Wenxuan Fu
56
/ 67
Community
Score
EXE

56 security vendors flagged this file as malicious

0fa1498340fca6c562cfa389ad3e93395f44c72fd128d7ba08579a69aaf3b126
Lab01-04.exe
armadillo peexe via-tor

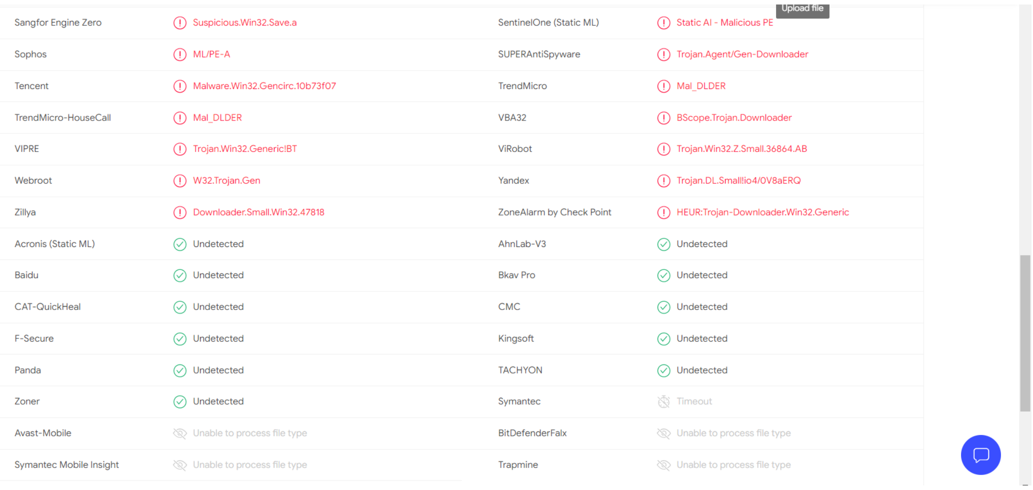
36.00 KB
Size

2021-09-13 08:41:09 UTC
3 minutes ago

Dynamic Analysis Sandbox Detections

⚠ The sandbox Lastline flags this file as: MALWARE

Ad-Aware	Gen:Variant.Cerbu.64782	Alibaba	TrojanDownloader:Win32/DownLdr.83a3e...
ALYac	Gen:Variant.Cerbu.64782	Antiy-AVL	Trojan/Generic.ASMalwS.856815
SecureAge APEX	Malicious	Arcabit	Trojan.Generic
Avast	Win32:DropperX-gen [Drp]	AVG	Win32:DropperX-gen [Drp]
Avira (no cloud)	TR/Dldr.Small.romlh	BitDefender	Gen:Variant.Cerbu.64782
BitDefenderTheta	AI:Packer.6911D1B71F	ClamAV	Win.Trojan.Agent-375080
Comodo	Malware@#2oyf6g8q6fqyr	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)
Cyren	W32/Heuristic-217!Eldorado	DrWeb	Trojan.DownLoader5.60705
eGambit	Unsafe.AI_Score_89%	Elastic	Malicious (high Confidence)
Emsisoft	Gen:Variant.Cerbu.64782 (B)	eScan	Gen:Variant.Cerbu.64782
ESET-NOD32	Win32/TrojanDownloader.Small.BFX	FireEye	Generic.mg.625ac05fd47adc3c
Fortinet	W32/Generic.AC.345C6F!tr	GData	Gen:Variant.Cerbu.64782
Gridinsoft	Trojan.Win32.Agent.dg	Ikarus	Backdoor.Win32.SuspectCRC
Jiangmin	Trojan/Invader.cph	K7AntiVirus	Trojan-Downloader (0055e3da1)
K7GW	Trojan-Downloader (0055e3da1)	Kaspersky	HEUR:Trojan-Downloader.Win32.Generic
Lionic	Trojan.Win32.Generic.a!c	Malwarebytes	Malware.AI.1254955992
MAX	Malware (ai Score=96)	MaxSecure	Trojan.Malware.23478.susgen
McAfee	GenericRXEW-DZ!625AC05FD47A	McAfee-GW-Edition	GenericRXEW-DZ!625AC05FD47A
Microsoft	TrojanDownloader:Win32/Small!MSR	NANO-Antivirus	Trojan.Win32.Kazy.cwxmfl
Palo Alto Networks	Generic.ml	Rising	Trojan.Generic@ML.100 (RDML:KLWV3IA...

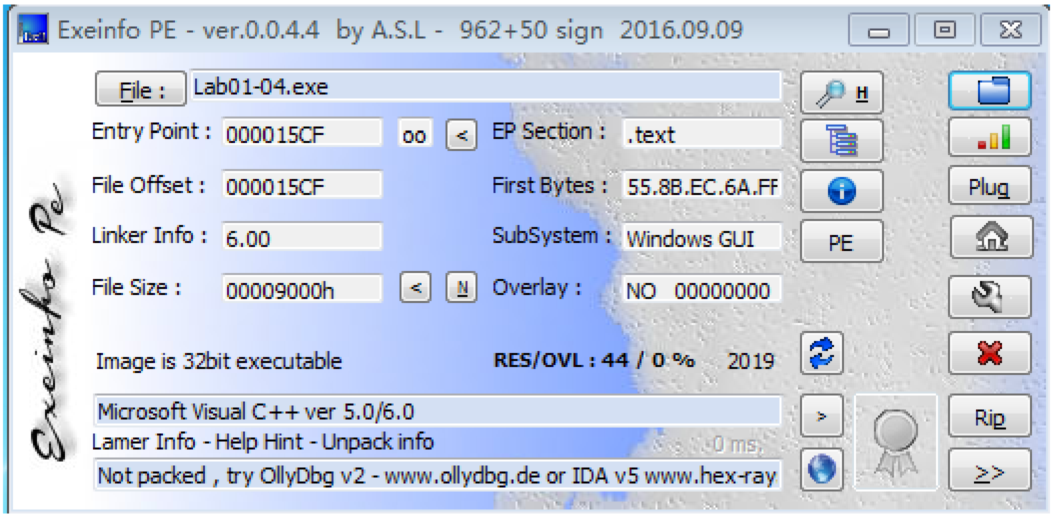


Upload file

Sangfor Engine Zero	Suspicious.Win32.Save.a	SentinelOne (Static ML)	Static AI - Malicious PE
Sophos	ML/PE-A	SUPERAntiSpyware	Trojan.Agent/Gen-Downloader
Tencent	Malware.Win32.Gencirc.10b73f07	TrendMicro	Mal_DLDER
TrendMicro-HouseCall	Mal_DLDER	VBA32	BScope.Trojan.Downloader
VIPRE	Trojan.Win32.Generic!BT	ViRobot	Trojan.Win32.Z.Small.36864.AB
Webroot	W32.Trojan.Gen	Yandex	Trojan.DL.Small!io4/0V8aERQ
Zillya	Downloader.Small.Win32.47818	ZoneAlarm by Check Point	HEUR:Trojan-Downloader.Win32.Generic
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Baidu	Undetected	Bkav Pro	Undetected
CAT-QuickHeal	Undetected	CMC	Undetected
F-Secure	Undetected	Kingsoft	Undetected
Panda	Undetected	TACHYON	Undetected
Zoner	Undetected	Symantec	Timeout
Avast-Mobile	Unable to process file type	BitDefenderFalx	Unable to process file type
Symantec Mobile Insight	Unable to process file type	Trapmine	Unable to process file type

2. 使用工具判断是否加壳

   1. Exeinfo



Exeinfo PE - ver.0.0.4.4 by A.S.L - 962+50 sign 2016.09.09

File : Lab01-04.exe

Entry Point : 000015CF oo < EP Section : .text

File Offset : 000015CF First Bytes : 55.8B.EC.6A.FF

Linker Info : 6.00 SubSystem : Windows GUI

File Size : 00009000h < N Overlay : NO 00000000

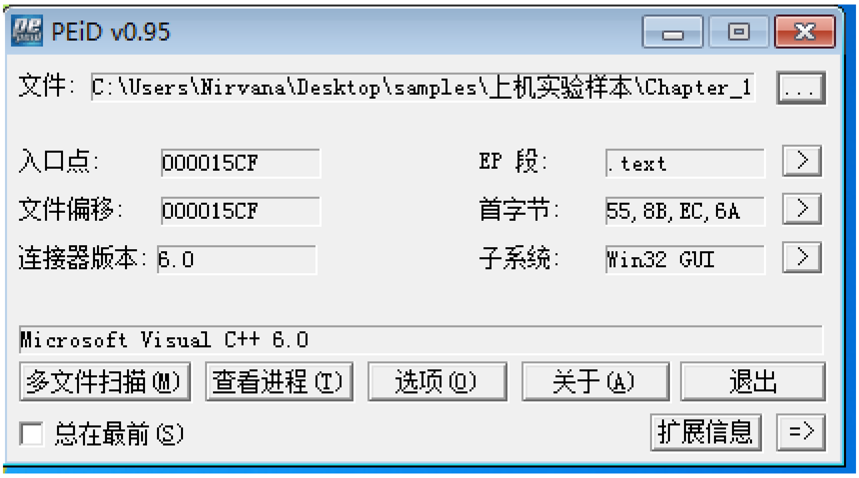
Image is 32bit executable RES/OVL : 44 / 0 % 2019

Microsoft Visual C++ ver 5.0/6.0

Lamer Info - Help Hint - Unpack info 0 ms.

Not packed , try OllyDbg v2 - www.ollydbg.de or IDA v5 www.hex-ray

   2. PEiD



PEiD v0.95

文件: C:\Users\Nirvana\Desktop\samples\上机实验样本\Chapter_1

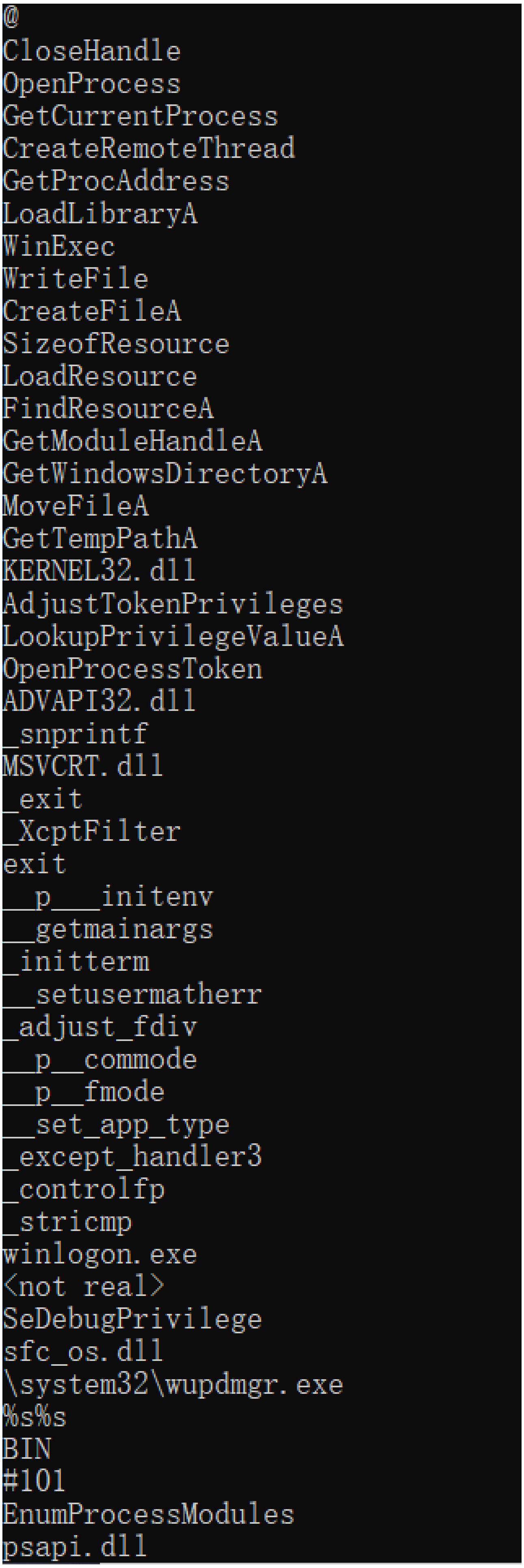
入口点: 000015CF EP 段: .text

文件偏移: 000015CF 首字节: 55,8B,EC,6A

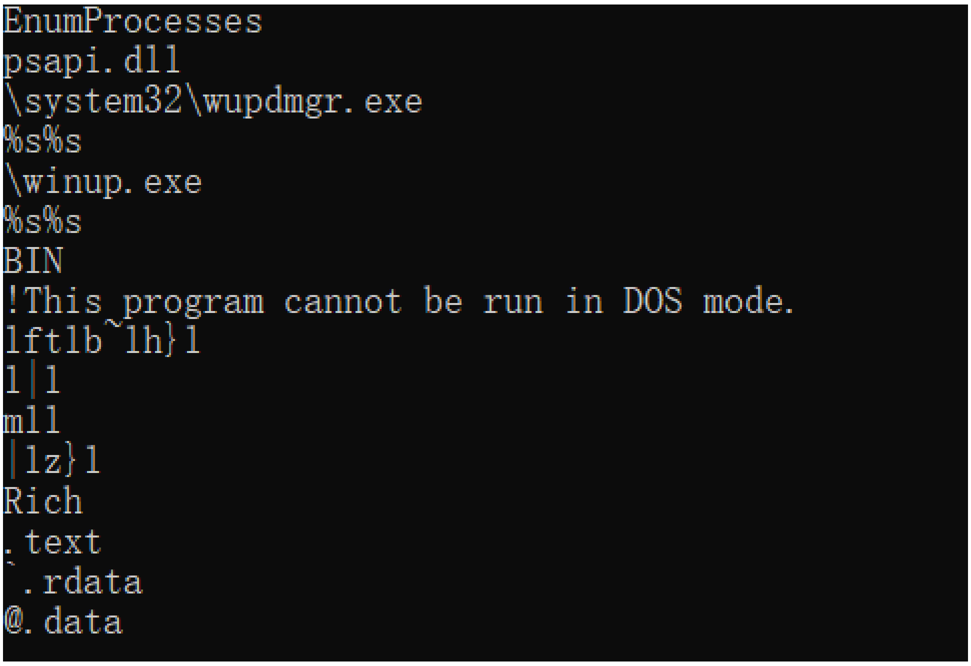
连接器版本: 6.0 子系统: Win32 GUI

Microsoft Visual C++ 6.0

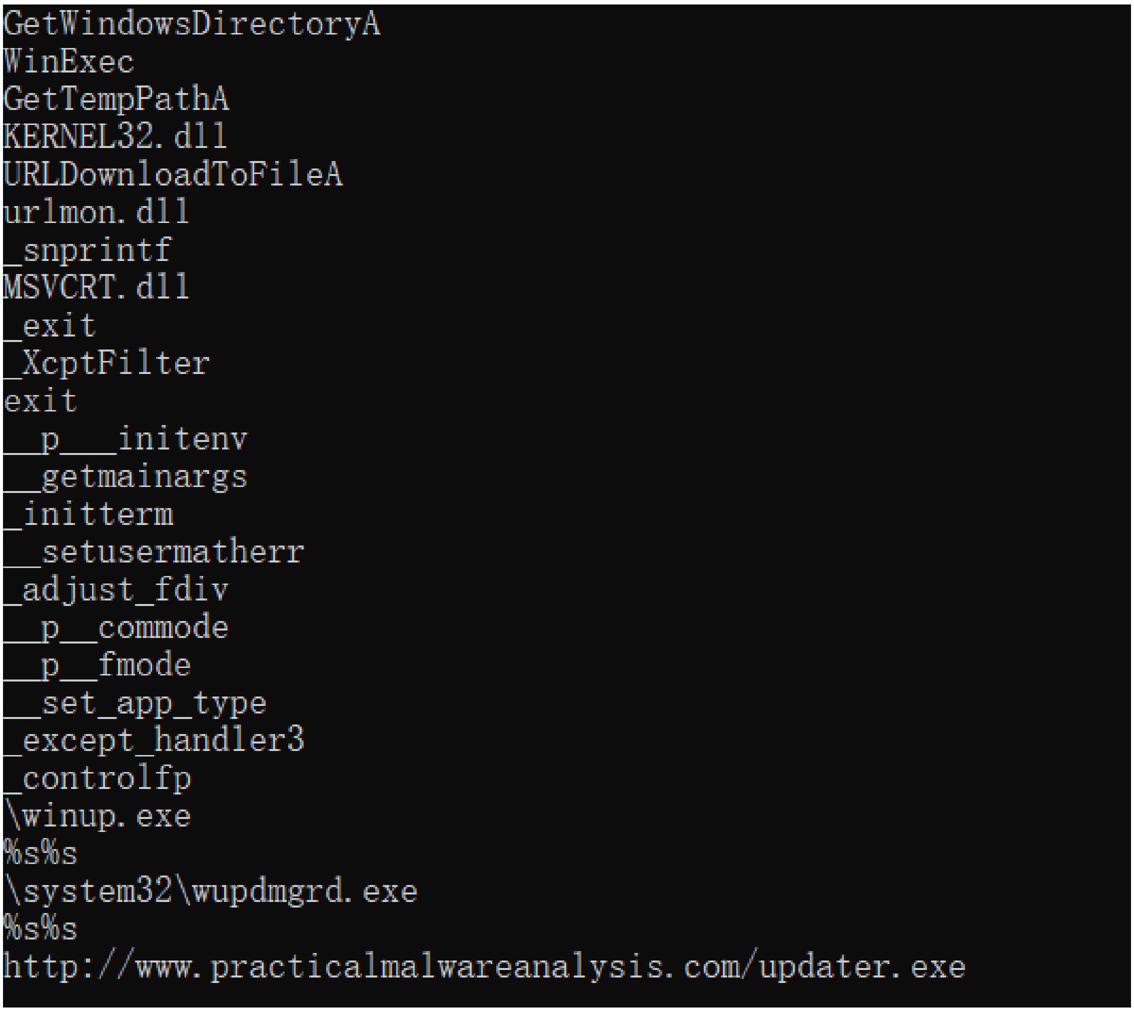
3. 使用strings工具检测



```
@
CloseHandle
OpenProcess
GetCurrentProcess
CreateRemoteThread
GetProcAddress
LoadLibraryA
WinExec
WriteFile
CreateFileA
SizeofResource
LoadResource
FindResourceA
GetModuleHandleA
GetWindowsDirectoryA
MoveFileA
GetTempPathA
KERNEL32.dll
AdjustTokenPrivileges
LookupPrivilegeValueA
OpenProcessToken
ADVAPI32.dll
_snprintf
MSVCRT.dll
_exit
_XcptFilter
exit
__p___initenv
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
__set_app_type
_except_handler3
_controlfp
_stricmp
winlogon.exe
<not real>
SeDebugPrivilege
sfc_os.dll
\system32\wupdmgr.exe
%s%s
BIN
#101
EnumProcessModules
psapi.dll
```

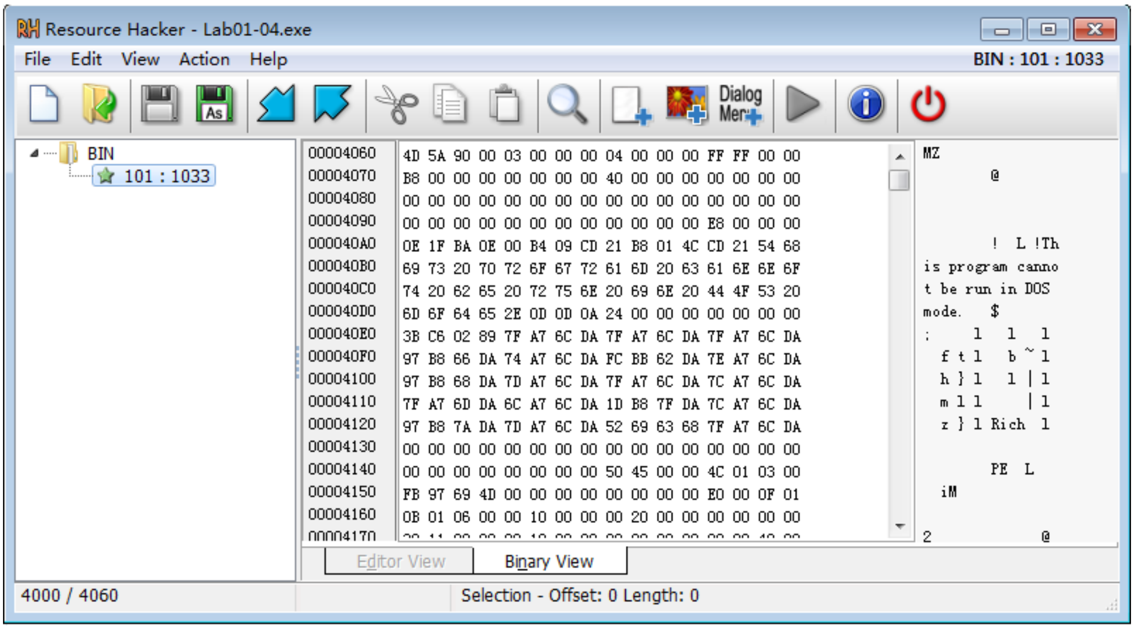


```
EnumProcesses
psapi.dll
\system32\wupdmgr.exe
%s%s
\winup.exe
%s%s
BIN
!This program cannot be run in DOS mode.
1ftlb~1h}1
1|1
m11
|1z}1
Rich
.text
`.rdata
@.data
```



```
GetWindowsDirectoryA
WinExec
GetTempPathA
KERNEL32.dll
URLDownloadToFileA
urlmon.dll
_snprintf
MSVCRT.dll
_exit
_XcptFilter
exit
__p___initenv
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
__set_app_type
_except_handler3
_controlfp
\winup.exe
%s%s
\system32\wupdmgrd.exe
%s%s
http://www.practicalmalwareanalysis.com/updater.exe
```

4. 使用resource hacker工具查看



```
00004060  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00   MZ
00004070  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00           @
00004080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004090  00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00
000040A0  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68           !  L !Th
000040B0  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F   is program canno
000040C0  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20   t be run in DOS
000040D0  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00   mode.    $
000040E0  3B C6 02 89 7F A7 6C DA 7F A7 6C DA 7F A7 6C DA   ;      l   l   l
000040F0  97 B8 66 DA 74 A7 6C DA FC BB 62 DA 7E A7 6C DA     f t l   b ~ l
00004100  97 B8 68 DA 7D A7 6C DA 7F A7 6C DA 7C A7 6C DA     h } l   l | l
00004110  7F A7 6D DA 6C A7 6C DA 1D B8 7F DA 7C A7 6C DA     m l l     | l
00004120  97 B8 7A DA 7D A7 6C DA 52 69 63 68 7F A7 6C DA     z } l Rich  l
00004130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004140  00 00 00 00 00 00 00 00 50 45 00 00 4C 01 03 00           PE  L
00004150  FB 97 69 4D 00 00 00 00 00 00 00 00 E0 00 0F 01     iM
00004160  0B 01 06 00 00 10 00 00 00 20 00 00 00 00 00 00
00004170                                                    2           @
```

问题回答

Q1

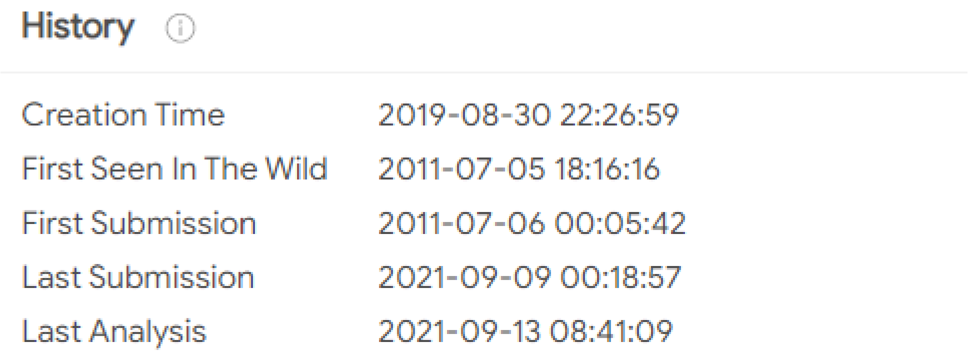
从VirusTotal的报告可以看出，有56家杀毒公司检测出此文件为病毒

Q2

从两个工具的检测结果来看，此样本应当是没有进行加壳

Q3

VirusTotal的报告如下：



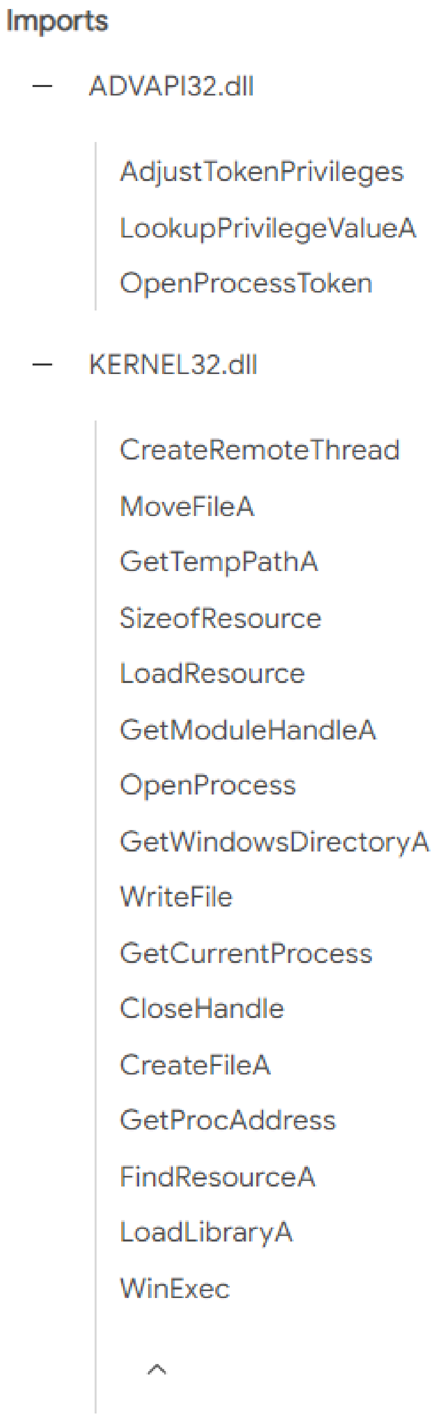
History

Creation Time	2019-08-30 22:26:59
First Seen In The Wild	2011-07-05 18:16:16
First Submission	2011-07-06 00:05:42
Last Submission	2021-09-09 00:18:57
Last Analysis	2021-09-13 08:41:09

可以看出，文件的创建时间应该是在2019-08-30

Q4

VirusTotal的报告如下：



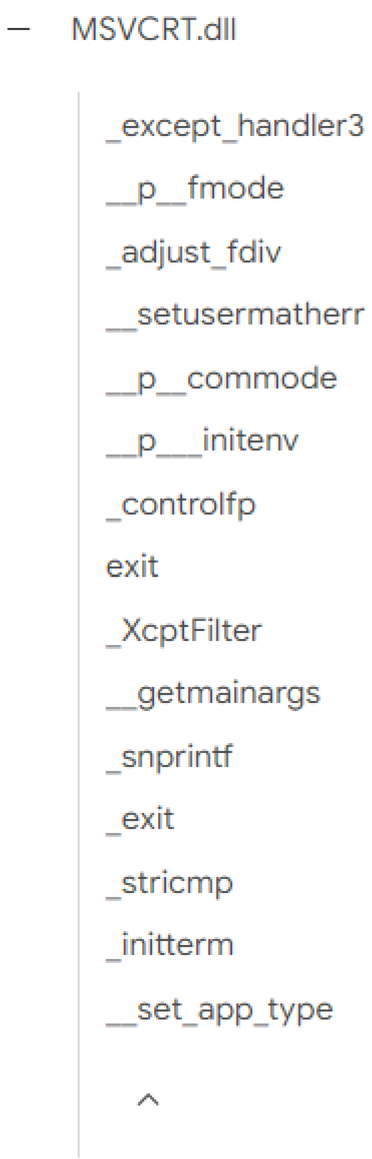
Imports

— ADVAPI32.dll

- AdjustTokenPrivileges
- LookupPrivilegeValueA
- OpenProcessToken

— KERNEL32.dll

- CreateRemoteThread
- MoveFileA
- GetTempPathA
- SizeofResource
- LoadResource
- GetModuleHandleA
- OpenProcess
- GetWindowsDirectoryA
- WriteFile
- GetCurrentProcess
- CloseHandle
- CreateFileA
- GetProcAddress
- FindResourceA
- LoadLibraryA
- WinExec



— MSVCRT.dll

_except_handler3
__p__fmode
_adjust_fdiv
__setusermatherr
__p__commode
__p___initenv
_controlfp
exit
_XcptFilter
__getmainargs
_snprintf
_exit
_stricmp
_initterm
__set_app_type

可以看出，该程序使用了`ADVAPI32.dll`、`KERNEL32.dll`和`MSVCRT.dll`

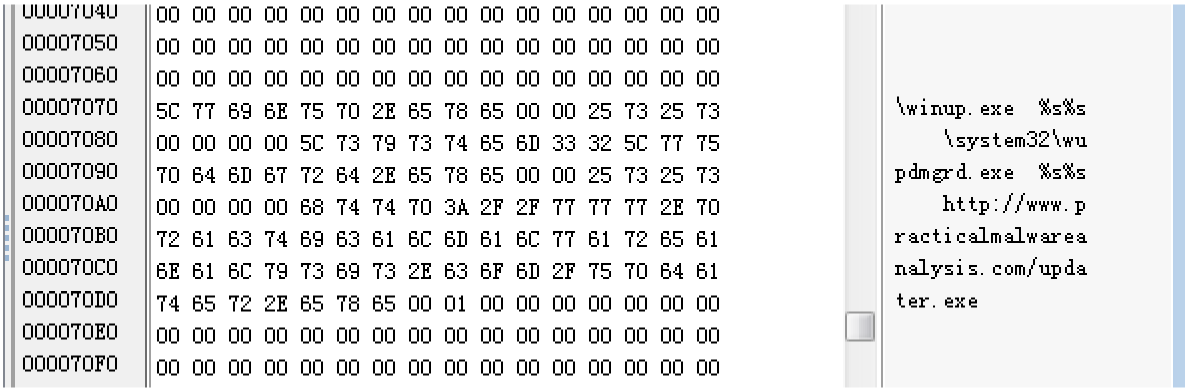
从`OpenProcess`、`GetProcAddress`、`CreateFileA`、`WriteFile`、`LoadResource`等函数可以看出该程序可以创建进程、读写文件、加载资源，猜测会进行远程的资源加载

Q5

根据strings中的检测结果，可以看见此样本可能会访问一个网址：http://www.practicalmalwareanalysis.com/updater.exe，同时还有`URLDownloadToFileA`这个函数的调用，由此可以将文件下载当做特征进行检测

Q6

在resource hacker中有这样一段：



```
00007040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00007050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00007060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00007070  5C 77 69 6E 75 70 2E 65 78 65 00 00 25 73 25 73    \winup.exe  %s%s
00007080  00 00 00 00 5C 73 79 73 74 65 6D 33 32 5C 77 75        \system32\wu
00007090  70 64 6D 67 72 64 2E 65 78 65 00 00 25 73 25 73    pdmgrd.exe  %s%s
000070A0  00 00 00 00 68 74 74 70 3A 2F 2F 77 77 77 2E 70        http://www.p
000070B0  72 61 63 74 69 63 61 6C 6D 61 6C 77 61 72 65 61    racticalmalwarea
000070C0  6E 61 6C 79 73 69 73 2E 63 6F 6D 2F 75 70 64 61    nalysis.com/upda
000070D0  74 65 72 2E 65 78 65 00 01 00 00 00 00 00 00 00    ter.exe
000070E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000070F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

可以看见这里也显示出了之前Q5中strings工具找到的网站。也就是说，在程序进行使用时，不是必须要将所有的信息都自己手敲出来，而是可以通过类似于include的方式，将外部资源进行导入，利用外部资源的一些信息、代码等执行，达到自己程度的目的。同时在对某个样本进行分析时，不单单需要分析源码或者反汇编里的代码，同时还需要注意到其引用的资源等，有时可能源文件是没有什么问题的，但是他加了一句对某个资源的调用，就会产生恶意行为。