

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:

38
/ 67

38 security vendors flagged this file as malicious

f50e42c8dfa6b49bde0398867e930b86c2a599e8db83b8260393082268f2dba
Lab01-01.dll

160.00 KB
Size

2021-09-16 05:30:25 UTC
1 day ago

armadillo pedli via-tor

DETECTION	DETAILS	RELATIONS	COMMUNITY
Alibaba	Trojan.Win32/Generic.6956aaeb	ALYac	Trojan.Agent.Waski
Antiy-AVL	Trojan/Generic.ASMalwS.2055E8D	SecureAge APEX	Malicious
Arcabit	Trojan.Ulisse.D19D44	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	BitDefender	Gen:Variant.Ulisse.105796
BitDefenderTheta	Gen:NN.ZedlaF.34142.kq4@aGkQVtp	ClamAV	Win.Malware.Agent-6369668-0
Comodo	Malware@#2dsw4albnc61	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)
Cyren	W32/Skeeyah.AK.gen/Eldorado	Elastic	Malicious (high Confidence)
Emsisoft	Gen:Variant.Ulisse.105796 (B)	eScan	Gen:Variant.Ulisse.105796
ESET-NOD32	A Variant Of Generic.TGEWDD	FireEye	Generic.mg.290934c61de9176a
Fortinet	PossibleThreat	GData	Gen:Variant.Ulisse.105796
Gridinsoft	Trojan.Win32.Agent.dg	Ikarus	Trojan.SuspectCRC
Lionic	Trojan.Win32.Ulisse.4lc	MAX	Malware (ai Score=96)
McAfee	GenericRXFO-RTI290934C6IDE9	McAfee-GW-Edition	GenericRXFO-RTI290934C6IDE9
Microsoft	Trojan.Win32/Skeeyah.AIMTB	NANO-Antivirus	Trojan.Win32.Waski.dtkvsp
SentinelOne (Static ML)	Static AI - Suspicious PE	Sophos	Mal/Generic-R
Symantec	MLAttribute.HighConfidence	TrendMicro	TROJ_GEN.R002COPHF20
TrendMicro-HouseCall	TROJ_GEN.R002COPHF20	VIPRE	Trojan.Win32.GenericIBT
Webroot	W32.Gen.BT	Zillya	Adware.InstallCore.Win32.1036

Lab01-01.exe:

45

167

45 security vendors flagged this file as malicious

58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47

Lab01-01.exe

16.00 KB

Size

2021-09-17 08:40:26 UTC

10 minutes ago

EXE

Community Score

armadillo

checks-disk-space

detect-debug-environment

long-sleeps

peexe

via-tor

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
AhnLab-V3		Trojan.Win32.Agent.C957604	Alibaba	Trojan.Win32/Aenjaris.94b5660f
ALYac		Trojan.Agent.1638455	AntiV-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	WinMalicious_confidence_100% (W)
Cylance		Unsafe	Cynet	Malicious (score: 99)
Cyren		W32/Ulise.CK.gen/Eldorado	Elastic	Malicious (high Confidence)
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.WOMtr	GData	Gen:Variant.Ulise.113694
Gridinsoft		Trojan.Win32.Agent.dg	Ikarus	Trojan.Rogue
K7AntiVirus		Trojan (004b6b551)	K7GW	Trojan (004b6b551)
Lionic		Trojan.Win32.Ulise.41c	Malwarebytes	Trojan.SystemKiller
McAfee		RDN/Generic.afz	McAfee-GW-Edition	RDN/Generic.afz
Microsoft		Trojan.Win32/Aenjaris.CTibit	NANO-Antivirus	Trojan.Win32.Generic.fhvmhd
Palo Alto Networks		Generic.ml	Sophos	Mal/Generic-R
Symantec		ML.Attribute.HighConfidence	Tencent	Malware.Win32.Gencirc.11caa00a
TrendMicro		TROJ_GEN.R002C0DID20	TrendMicro-HouseCall	TROJ_GEN.R002C0DID20
VBA32		Trojan.Tiggre	VIPRE	Trojan.Win32.GenericBT
Webroot		W32/Malware.Gen	Yandex	Trojan.GenAsalcGc9XwKYsAs
Zillya		Downloader.Amonetize.Win32.3112	Acronis (Static ML)	Undetected
Ad-Aware		Undetected	Baidu	Undetected

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:

PE Explorer - C:\Documents and Settings\Administrator\桌面\上机实验样本\Chapter_11\Lab01-01.dll

文件(F)

视图(V)

工具(T)

帮助(H)

HEADERS INFO

入口点地址:

100012FA

实际映像校验和:

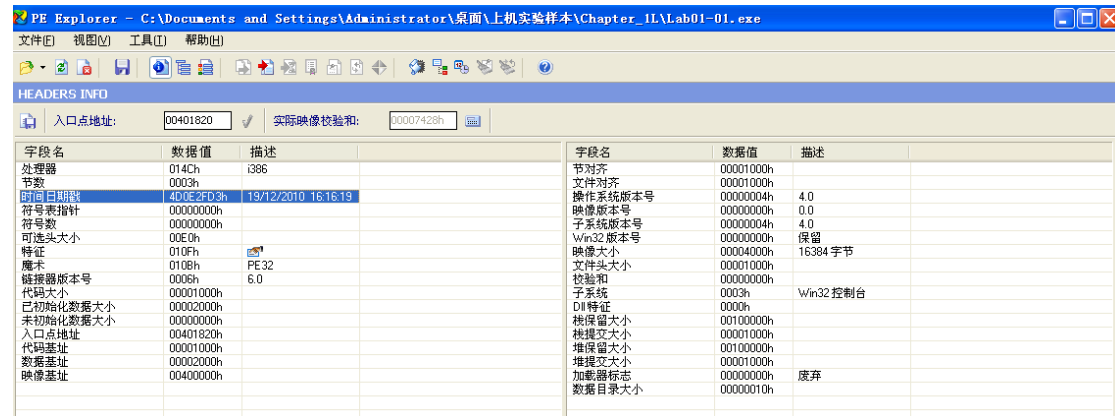
000327BEh

字段名	数据值	描述
机器数	014C	1386
节数	0004h	
时间日期戳	4D0E2FE6h	19/12/2010 16:16:38
符号表指针	00000000h	
符号表	00000000h	
可选头大小	00E0h	
特征	210Eh	
魔术	0108h	PE 32
链接器版本号	0008h	6.0
代码大小	00001000h	
已初始化数据大小	00026000h	
未初始化数据大小	00000000h	
入口点地址	100012FAh	
代码基址	00001000h	
数据基址	00002000h	
映像基址	10000000h	

字段名	数据值	描述
节对齐	00001000h	
文件对齐	00001000h	
操作系统版本号	00000004h	4.0
映像版本号	00000000h	0.0
子系统版本号	00000004h	4.0
Win32 版本号	00000000h	保留
映像大小	00028000h	163840 字节
文件头大小	00001000h	
校验和	00000000h	
子系统	0002h	Win32 GUI
Dll 特征	0000h	
栈保留大小	00100000h	
堆保留大小	00001000h	
堆保留大小	00100000h	
堆保留大小	00001000h	
堆保留大小	00000000h	
加载器标志	00000000h	废弃
数据目录大小	00000010h	

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

Lab01-01.exe:

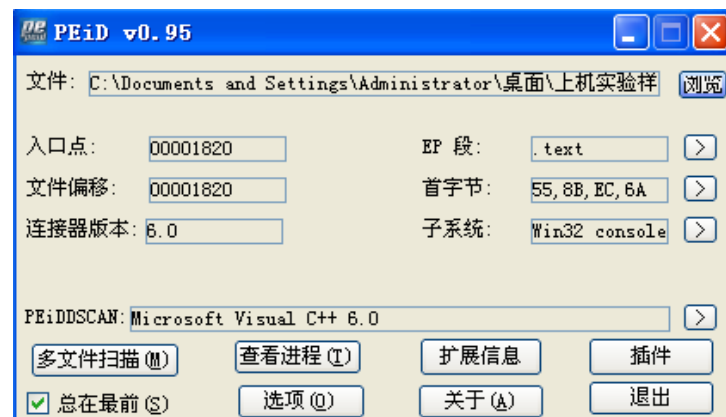


Compilation Timestamp 2010-12-19 16:16:19

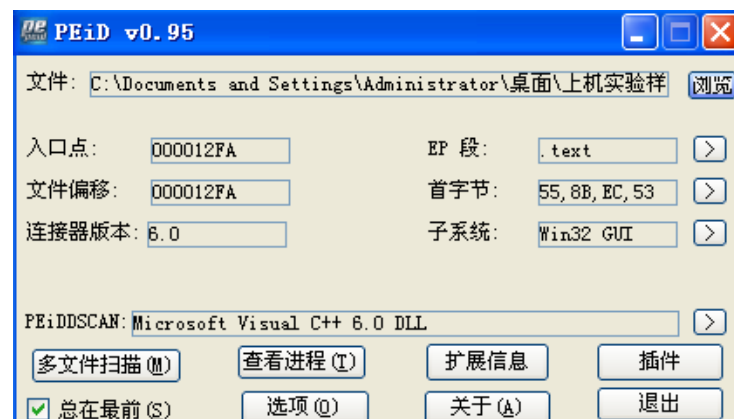
Q3: 这两个文件中是否存在迹象说明它们是否被加壳或混淆？如果是，这些迹象在哪里？

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：

模块	文件时间戳	连接时间戳	文件大小	属性	连接校验和	校验和	CPU	子系统	符号	优先基址	实际基址	虚拟大小	装载顺序	文件版本	产品版本	映像版本
KERNEL32.DLL	2008-04-14 20:00	2008-04-14 10:13	1,150,464	A	0x00122A2B	0x00122A2B	x86	Console	CV	0x7C800000	Unknown	0x0011E000	未载入	5.1.2600.5512	5.1.2600.5512	5.1
LAB01-01.EXE	2012-01-08 2:19	2010-12-20 0:16	16,384	A	0x00000000	0x00007428	x86	Console	None	0x00400000	Unknown	0x00004000	未载入	N/A	N/A	0.0
MSVCRT.DLL	2008-04-14 20:00	2008-04-14 10:15	343,040	A	0x0006101F	0x0006101F	x86	GUI	CV	0x77B20000	Unknown	0x00058000	未载入	7.0.2600.5512	6.1.8638.5512	5.1
NTDLL.DLL	2008-04-14 20:00	2008-04-14 10:13	589,312	A	0x00097CB7	0x00097CB7	x86	Console	CV	0x7C900000	Unknown	0x00093000	未载入	5.1.2600.5512	5.1.2600.5512	5.1

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, 可以帮助你在这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 kernel32.dll 以及 Lab01-01.dll 文件。所以如果在主机上找到了 kernel32.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

模块	文件时间戳	连接时间戳	文件大小	属性	连接校验和	校验和	CPU	子系统	符号	优先基址	实际基址	虚拟大小	装载顺序	文件版本	产品版本	映像版本
KERNEL32.DLL	2008-04-14 20:00	2008-04-14 10:13	1,150,464	A	0x00122A2B	0x00122A2B	x86	Console	CV	0x7C800000	Unknown	0x0011E000	未载入	5.1.2600.5512	5.1.2600.5512	5.1
ADVAPI32.DLL	2008-04-14 20:00	2008-04-14 10:12	674,816	A	0x000A5F75	0x000A5F75	x86	Console	CV	0x77DA0000	Unknown	0x000A8000	未载入	5.1.2600.5512	5.1.2600.5512	5.1
KERNEL32.DLL	2008-04-14 20:00	2008-04-14 10:13	1,150,464	A	0x00122A2B	0x00122A2B	x86	Console	CV	0x7C800000	Unknown	0x0011E000	未载入	5.1.2600.5512	5.1.2600.5512	5.1
LAB01-01.DLL	2010-12-19 11:16	2010-12-20 0:16	163,840	A	0x00000000	0x000327B8	x86	GUI	None	0x10000000	Unknown	0x00028000	未载入	N/A	N/A	0.0
MSVCRT.DLL	2008-04-14 20:00	2008-04-14 10:15	343,040	A	0x0006101F	0x0006101F	x86	GUI	CV	0x77B20000	Unknown	0x00058000	未载入	7.0.2600.5512	6.1.8638.5512	5.1
NTDLL.DLL	2008-04-14 20:00	2008-04-14 10:13	589,312	A	0x00097CB7	0x00097CB7	x86	Console	CV	0x7C900000	Unknown	0x00093000	未载入	5.1.2600.5512	5.1.2600.5512	5.1

警告: 由于在延迟加载依赖模块中丢失导入函数, 至少有一个模块具有不能解析的导入。

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:

PEView - C:\Documents and Settings\Administrator\桌面\上机实验样本\Chapter_11\Lab01-01.dll

文件(F) 视图(V) 前往(G) 帮助(H)

	pFile	Raw Data	Value
Lab01-01.dll			
IMAGE_DOS_HEADER	00026000	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
MS-DOS Stub Program	00026010	65 78 65 63 00 00 00 00 73 6C 65 65 70 00 00 00	exec.....sleep...
IMAGE_NT_HEADERS	00026020	68 65 6C 6C 6F 00 00 00 31 32 37 2E 32 36 2E 31	hello...127.26.1
IMAGE_SECTION_HEADER	00026030	35 32 2E 31 33 00 00 00 53 41 44 46 48 55 48 46	52.13...SADFHUHF
IMAGE_SECTION_HEADER	00026040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
IMAGE_SECTION_HEADER	00026050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
IMAGE_SECTION_HEADER	00026060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
SECTION .text	00026070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
SECTION .rdata	00026080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
SECTION .data	00026090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
SECTION .reloc	000260A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

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

42
/ 59

42 security vendors flagged this file as malicious

c876a332d7dd8da31cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6
Lab01-02.exe
3.00 KB
Size
2021-09-15 09:03:44 UTC
2 days ago
EXE

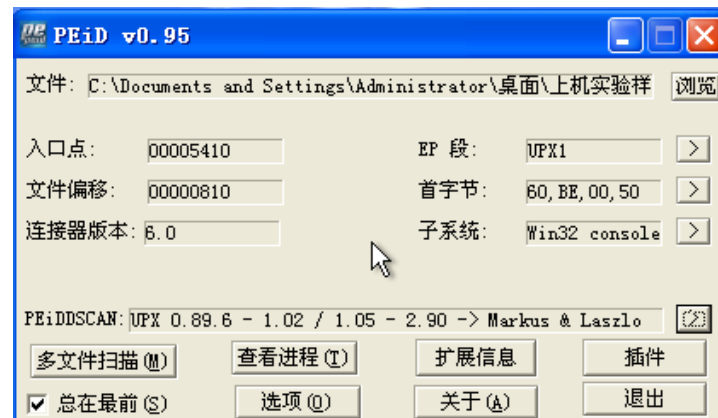
checks-disk-space detect-debug-environment long-sleeps peexe upx via-tor

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
AhnLab-V3	Trojan.Win32.StartPage.C26214	Alibaba	Trojan.Clicker.Win32/Generic.tbaf980f	
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	BitDefender Theta	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.DJ.C.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/Trojan.Clicker.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.Trojan.Clicker	Jiangmin	Trojan.Generic.fxlq	
Kingsoft	Win32.Malware.Heur_Generic.A.(kcloud)	Lionic	Trojan.Win32.Zbot.IsXA	
Malwarebytes	Trojan.Agent.UPX	MAX	Malware (ai Score=100)	
McAfee	Generic.ait	NANO-Antivirus	Trojan.Win32.Click3.laupgs	
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.AgentISYJ1YtE/ZV4	Zillya	Trojan.Agent.Win32.1288291	

Q2:

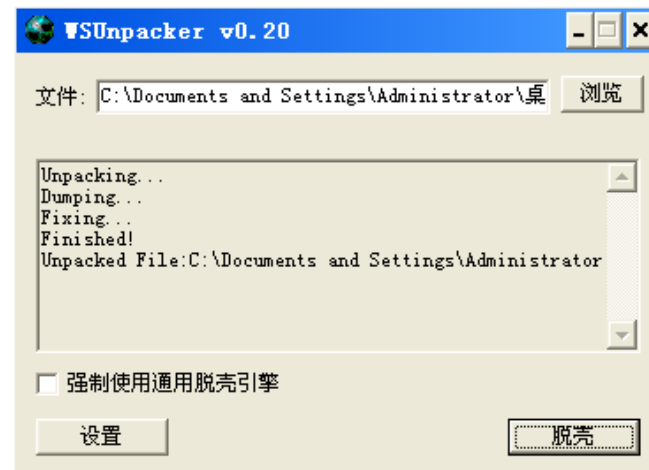
探索是否有加壳

用 peid 探测如下图

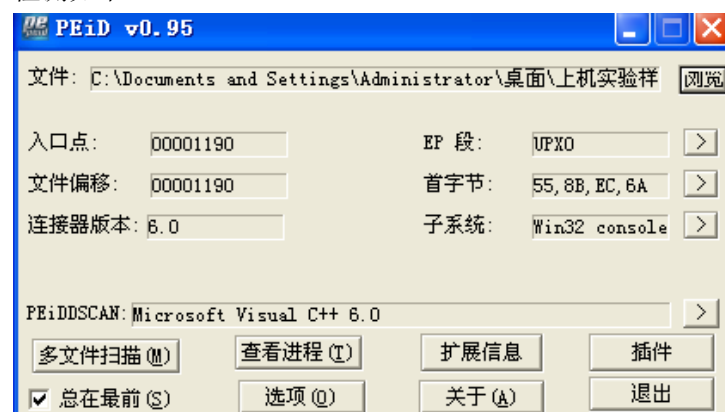


Upx 加壳

使用 wsunpacker 脱壳

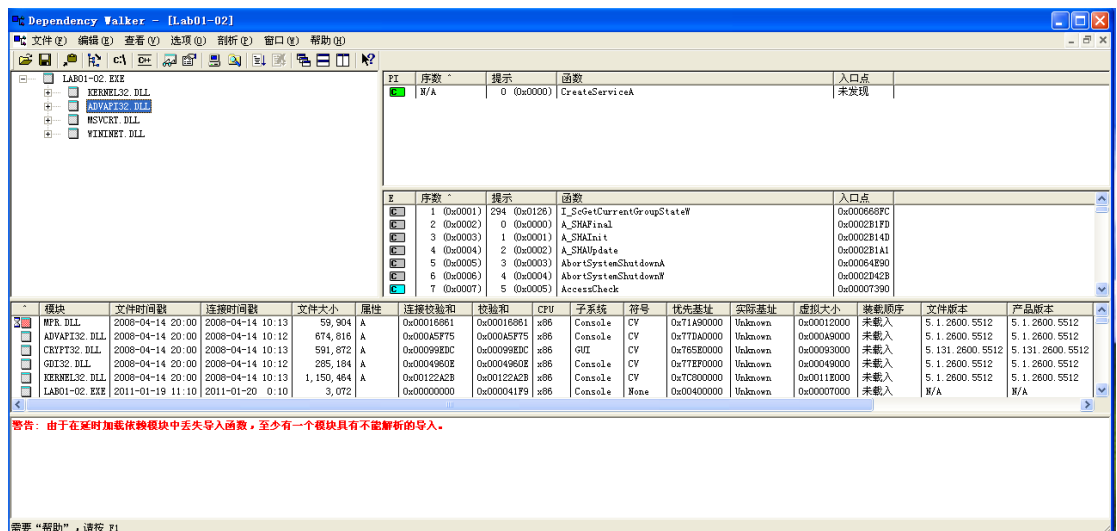


检测如下:



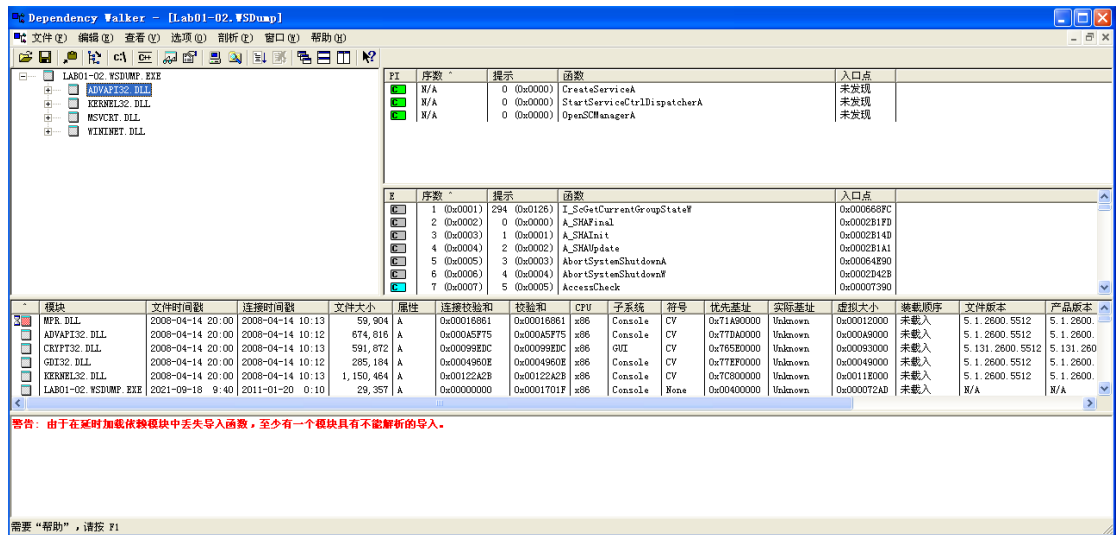
Q3:

脱壳前:



需要“帮助”，请按 F1

脱壳后：



需要“帮助”，请按 F1

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：

Address	Length	Type	String
UPX0:0040...	00000018	C	3个字节...FF%ld @
UPX0:0040...	0000000B	C	MalService
UPX0:0040...	0000000B	C	MalService
UPX0:0040...	00000007	C	HGL345
UPX0:0040...	00000023	C	http://www.malwareanalysisbook.com
UPX0:0040...	00000016	C	Internet Explorer 8.0
.demoscene...	0000001F	C	WSUnpacker v2.0 - by demoscene
.demoscene...	0000000D	C	ADVAPI32.dll
.demoscene...	0000000D	C	kernel32.dll
.demoscene...	0000000B	C	MSVCRT.dll
.demoscene...	0000000C	C	WININET.dll

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:

59

1.67

7983a58293924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec

Lab01-03.exe

4.64 KB

Size

2021-09-13 08:35:03 UTC

4 days ago

EXE

detect-debug-environment

direct-cpu-clock-access

fsg

long-sleeps

overlay

peexe

runtime-modules

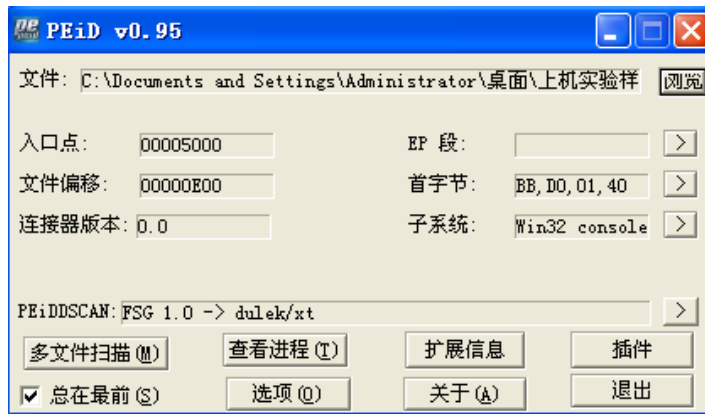
via-tor

Community Score

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	<div>Gen:Variant.Zusy.389663</div>	AhnLab-V3	<div>Trojan/Win.Generic.R427327</div>	
Alibaba	<div>Trojan.Clicker:Win32/Agentb.3bb840a6</div>	ALYac	<div>Gen:Variant.Zusy.389663</div>	
Antiy-AVL	<div>Trojan/Generic.ASMalwS.CDDF32</div>	Arcabit	<div>Trojan.Zusy.D5F21F</div>	
Avast	<div>Win32:Malware-gen</div>	AVG	<div>Win32:Malware-gen</div>	
Avira (no cloud)	<div>TR/Clicker.knmor</div>	Baidu	<div>Win32:Trojan-Clicker.Agent.z</div>	
BitDefender	<div>Gen:Variant.Zusy.389663</div>	BitDefender Theta	<div>Gen:NN.ZexaF.34142.ambdaODfLcf</div>	
CAT-QuickHeal	<div>Trojan.Agentb</div>	Comodo	<div>TrojWare.Win32.Trojan.Inor.B_10@1qra8l</div>	
CrowdStrike Falcon	<div>WinMalicious_confidence_100% (W)</div>	Cylance	<div>Unsafe</div>	
Cynet	<div>Malicious (score: 100)</div>	Cyren	<div>W32/SuspPack.DH.genEldorado</div>	
DrWeb	<div>Trojan.Click2.16518</div>	Elastic	<div>Malicious (high Confidence)</div>	
Emsisoft	<div>Gen:Variant.Zusy.389663 (B)</div>	eScan	<div>Gen:Variant.Zusy.389663</div>	
ESET-NOD32	<div>Win32/TrojanClicker.Agent.NVN</div>	F-Secure	<div>Trojan.TR/Clicker.knmor</div>	
FireEye	<div>Generic.mg.9c5c27494c28ed0b</div>	Fortinet	<div>W32/WebDown.E76Atr</div>	
GData	<div>Gen:Variant.Zusy.389663</div>	Gridinsoft	<div>Trojan.Win32.Agent.ns</div>	
Ikarus	<div>Trojan.Win32.Genome</div>	Jiangmin	<div>Trojan/Genome.bmbp</div>	
K7AntiVirus	<div>Spyware (0055e3f61)</div>	K7GW	<div>Spyware (0055e3f61)</div>	
Kaspersky	<div>Trojan.Win32.Agentb.bquu</div>	Kingsoft	<div>Win32.Troj.Genome.(kcloud)</div>	
Lionic	<div>Trojan.Multi.Generic.IVbD</div>	Malwarebytes	<div>Trojan.Agent.MWL</div>	
MAX	<div>Malware (ai Score=100)</div>	MaxSecure	<div>Trojan.Malware.300983.susgen</div>	
McAfee	<div>GenericRXAA-FA19C5C27494C28</div>	McAfee-GW-Edition	<div>GenericRXOH-BSI90a6EED29B66</div>	
Microsoft	<div>Trojan:Win32/Tnega1MSR</div>	NANO-Antivirus	<div>Trojan.Win32.Inor.getjo</div>	
Palo Alto Networks	<div>Generic.ml</div>	Rising	<div>Trojan.Proxy.Win32.Small.gs (CLASSIC)</div>	
SentinelOne (Static ML)	<div>Static AI - Malicious PE</div>	Sophos	<div>Mal/Generic-R + Mal/Packer</div>	

Q2:

使用 peid 探测是否加壳

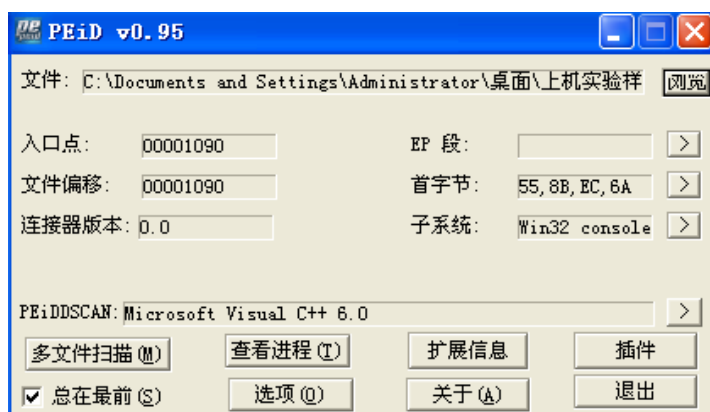


使用 FSG 加壳

Wsunpacker 脱壳:

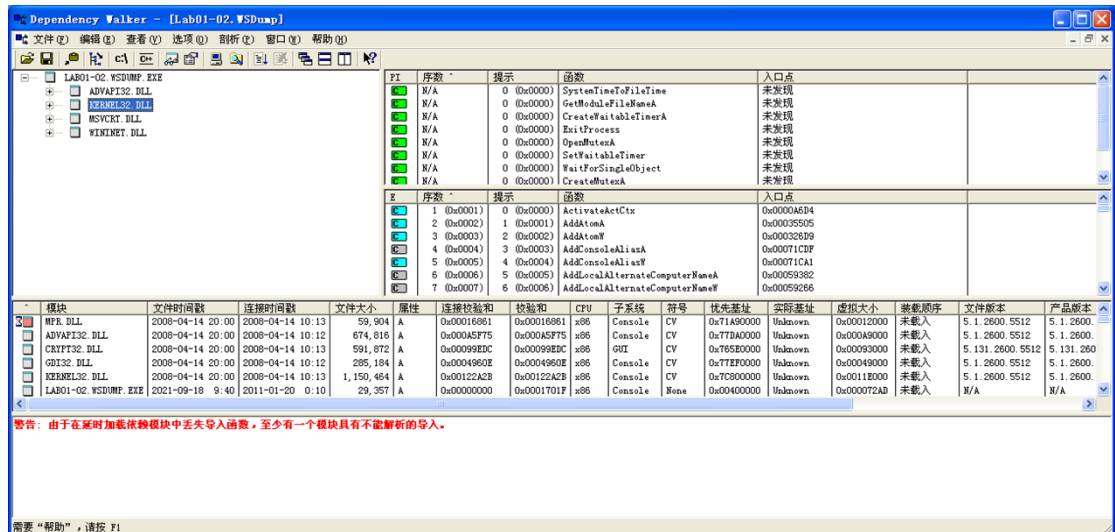
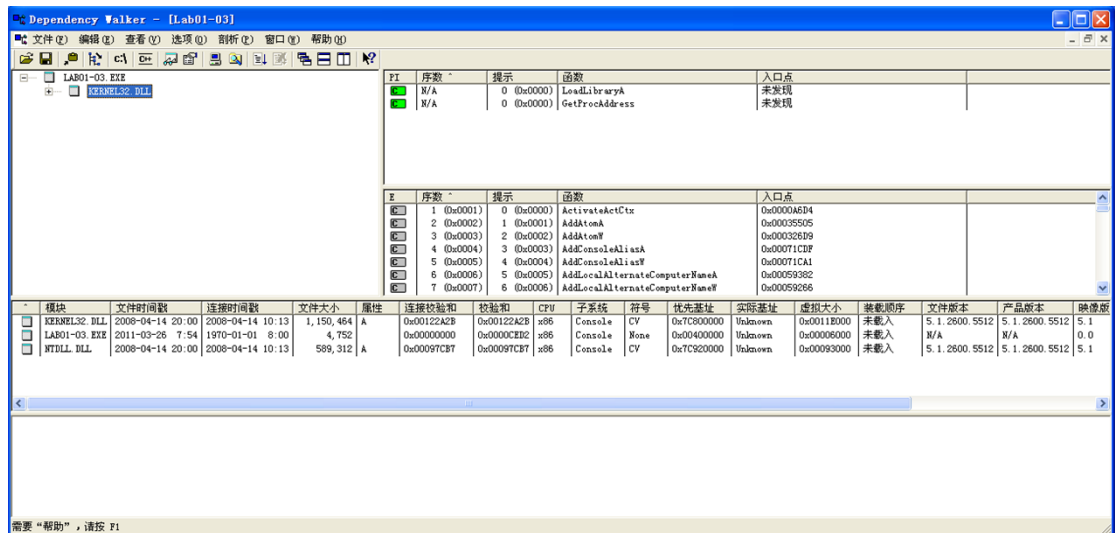


再次检测:



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(&rcIsid, 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？

56
/ 69

Community Score

56 security vendors and 1 sandbox flagged this file as malicious

Ofa1498340fca5c562cfa389ad3e93395f44c72fd128d7ba08579a69aaf3b126

Lab01-04.exe

armadillo peexe via-tor

36.00 KB

Size

2021-09-18 00:06:26 UTC

3 days ago

EXE

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	① Gen:Variant.Cerbu.64782	Alibaba	① TrojanDownloader:Win32/Downldr.83a3e...	
ALYac	① Gen:Variant.Cerbu.64782	Antiy-AVL	① TrojanGeneric.ASMalwS.856815	
SecureAge APEX	① Malicious	Avast	① Win32:DropperX-gen [Drp]	
AVG	① Win32:DropperX-gen [Drp]	Avira (no cloud)	① TR/Dldr.Small.romlh	
BitDefender	① Gen:Variant.Cerbu.64782	BitDefenderTheta	① Ai:Packer.691D1B71F	
ClamAV	① Win.Trojan.Agent-375080	Comodo	① Malware@#2oyf6g8q6fyqr	
CrowdStrike Falcon	① Win/malicious_confidence_100% (W)	Cybereason	① Malicious.f447ad	
Cylance	① Unsafe	Cynet	① Malicious (score: 100)	
Cyren	① W32/Heuristic-217EIdorado	DrWeb	① Trojan.Downloader5.60705	
eGambit	① Unsafe.AI_Score_89%	Elastic	① Malicious (high Confidence)	
Emsisoft	① Gen:Variant.Cerbu.64782 (B)	eScan	① Gen:Variant.Cerbu.64782	
ESET-NOD32	① Win32/TrojanDownloader.Small.BFX	FireEye	① Generic.mg.625ac05fd47adc3c	
Fortinet	① W32/Generic.AC.345C6Ftr	GData	① Gen:Variant.Cerbu.64782	
Gridinsoft	① Trojan.Win32.Agent.dg	Ikarus	① Backdoor.Win32.SuspectCRC	
Jiangmin	① Trojan/Invader.cph	K7AntiVirus	① Trojan-Downloader (0055e3da1)	
K7GW	① Trojan-Downloader (0055e3da1)	Kaspersky	① HEUR:Trojan-Downloader.Win32.Generic	
Lionic	① Trojan.Win32.Cerbu.41c	Malwarebytes	① Malware.AI.1254955992	
MAX	① Malware (ai Score=96)	MaxSecure	① Trojan.Malware.23478.susgen	
McAfee	① GenericRXEW-DZi625AC05FD47A	McAfee-GW-Edition	① BehavesLike.Win32.Downloader.nz	

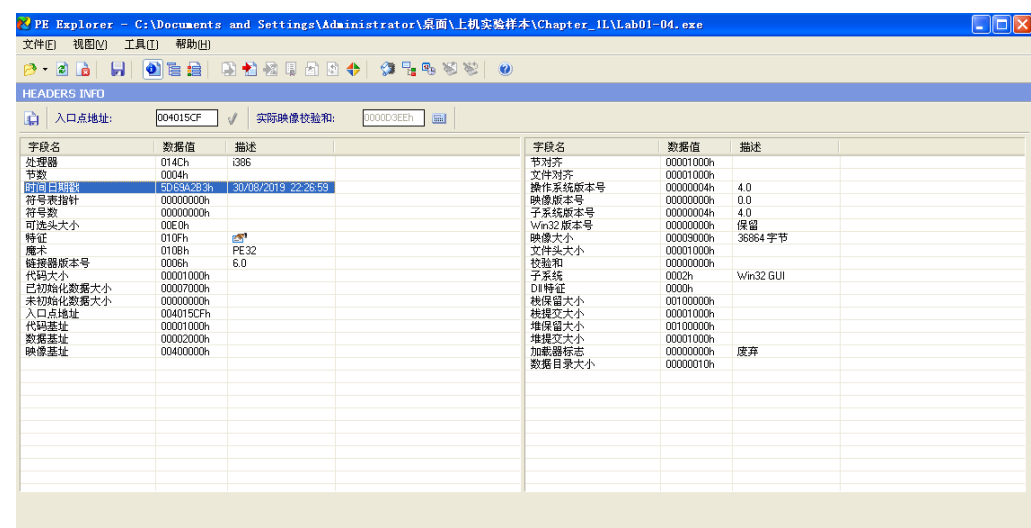
Q2:

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

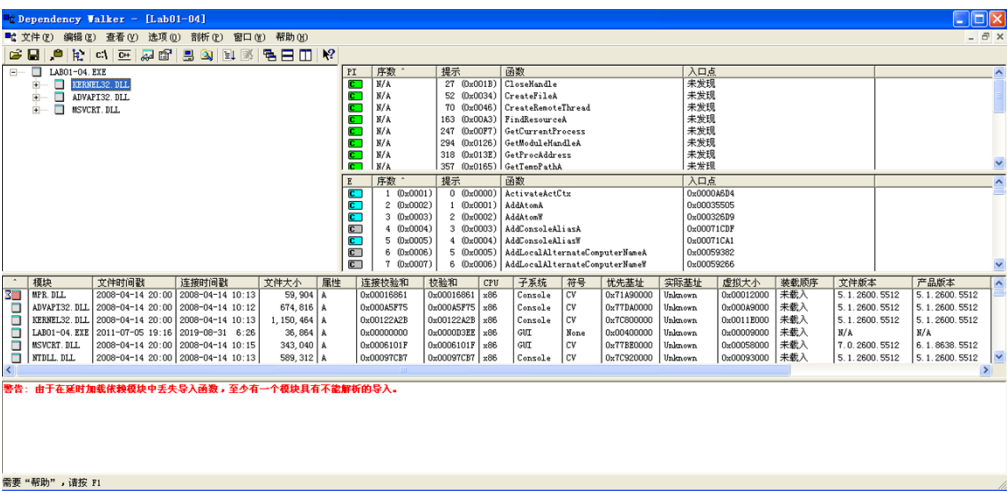
Q3:

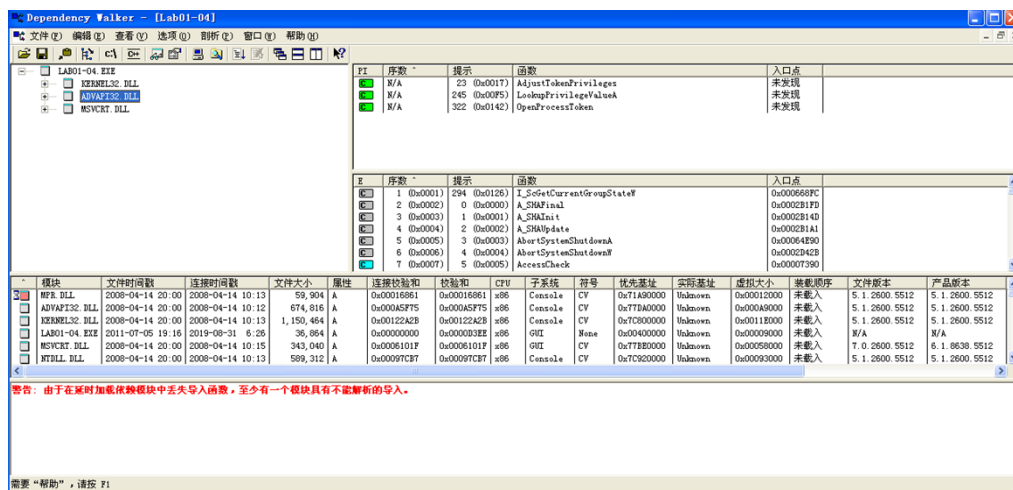


使用 PE Explorer 查看样例代码编时间 2019/08/30 22:26:59

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

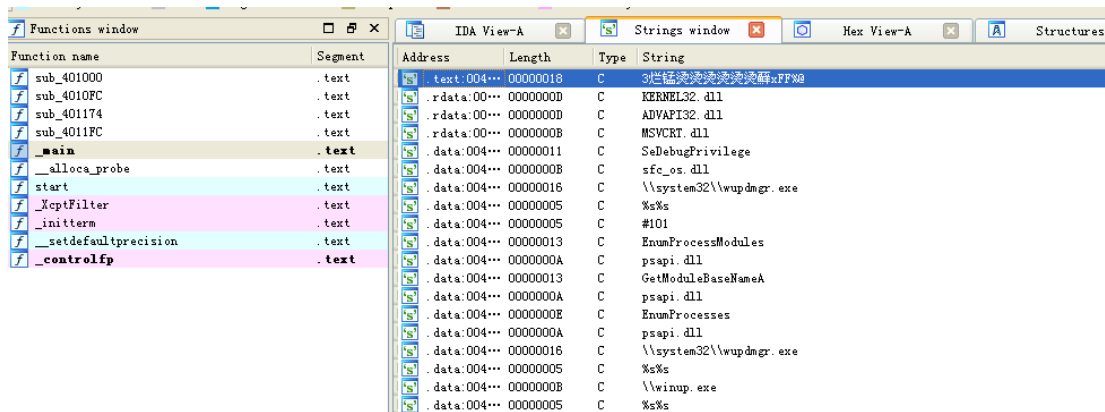
ADVAPI32.DLL 中的一些关键导入函数:

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, 加载到全局存储器后运行程序。

Q5:

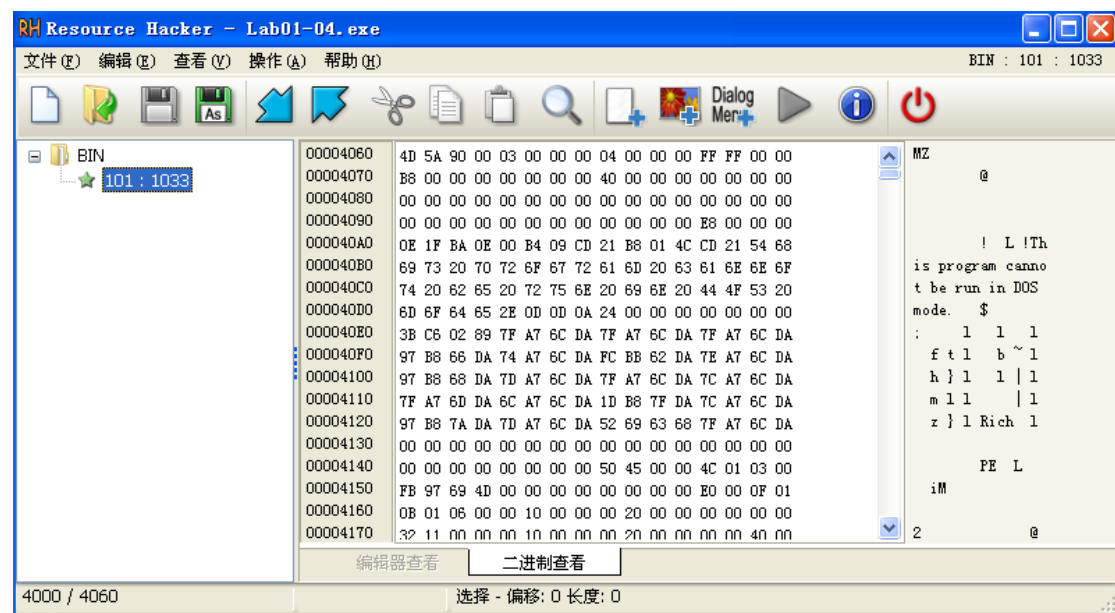
用 ida 打开该文件, 得到字符串如下:



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

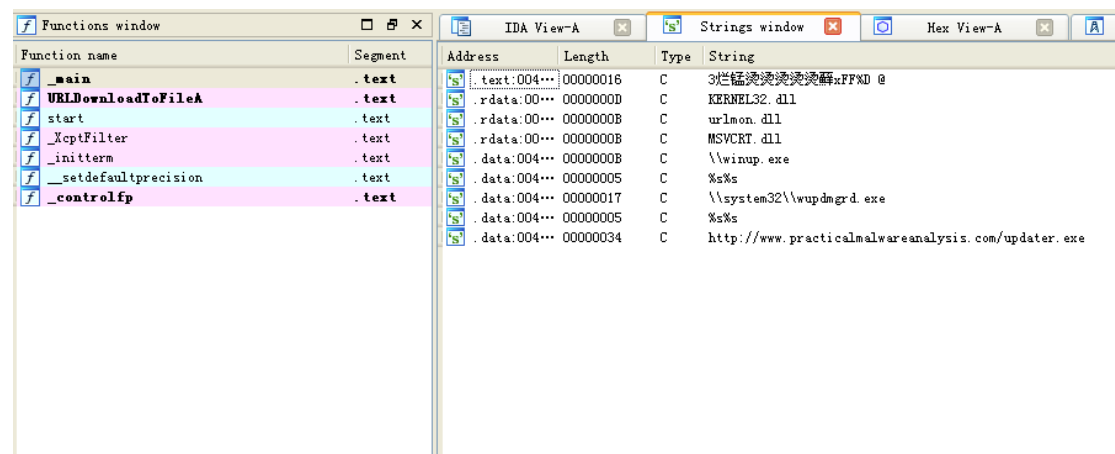
Q6:

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