

南开大学

恶意代码分析与防治技术课程实验报告

实验一



学 院 网络空间安全学院
专 业 信息安全
学 号 2213041
姓 名 李雅帆
班 级 信安班

一、实验目的

本实验旨在通过一系列工具和技术，提升对计算机病毒分析与防治的能力。
具体目标包括：

1. 隔离环境分析：掌握在 Windows 虚拟机中安全分析计算机病毒的方法。
2. 加壳与脱壳分析：使用 PEid 工具分析和脱壳文件，同时了解相关的 FGS 知识。
3. 二进制文件分析：学习使用 PView 工具进行深入的二进制文件分析。
4. 函数与字符串分析：通过 IDA Pro 工具分析文件中的字符串和链接函数。
5. 加壳与脱壳操作：在 Linux 和 Windows 环境下使用 upx 工具进行加壳与脱壳。
6. Yara 规则编写：使用 Yara 工具编写规则，对目标文件进行监测。
7. 规则优化与性能监测：优化 Yara 规则并通过 PowerShell 监测其执行速度变化。

二、实验原理

本实验旨在通过静态分析技术对多个恶意文件进行深入分析，以识别其特征、行为和潜在威胁。分析主要分为以下几个部分：

1. 文件上传与病毒检测：使用 VirusTotal 等在线工具可以自动检测文件是否与已知的恶意软件特征匹配，从而判断其潜在风险。
2. 编译时间分析：通过查看文件的元数据，可以确定程序的编译时间，这有助于追踪其发布和更新的历史。
3. 加壳与混淆检测：通过分析文件的结构和导入函数，可以识别是否存在加壳或混淆的迹象。常见的特征包括异常的文件头、未解析的导入函数等。
4. 导入函数分析：静态分析导入函数可以揭示恶意程序的功能。例如，网络通信相关的函数或系统调用可能表明该程序具有后门功能或数据窃取能力。
5. 主机与网络迹象：通过对文件的行为分析，可以识别感染系统的迹象，包括修改的注册表项、创建的进程或网络连接等。基于网络的迹象可通过监控流量和 DNS 请求来识别。

6. 资源分析：恶意文件中可能包含隐藏的资源（如图像、字符串或其他可执行代码），使用工具（如 Resource Hacker）提取和分析这些资源，可以揭示程序的意图或额外的恶意功能。

三、实验过程

I . Lab 1-1

这个实验使用 Lab01-01.exe 和 Lab01-01.dll 文件, 使用本章描述的工具和技术来获取关于这些文件的信息。

问题

1. 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？

58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47

56 / 73
Community Score 12

56/73 security vendors flagged this file as malicious

Size: 16.00 KB | Last Analysis Date: 7 hours ago

Lab01-01.exe

peexe via-tor checks-disk-space armadillo idle detect-debug-environment checks-user-input long-sleeps

Reanalyze Similar More

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.ulise/aenjaris Threat categories trojan Family labels ulise aenjaris kkbov

Security vendors' analysis

AhnLab-V3	Trojan.Win32.Agent.C957604	Alibaba	Trojan.Win32/Aenjaris.2be749b4
ALYac	Trojan.Agent.1638455	Antiy-AVL	Trojan.Win32.TSGeneric
Arcabit	Trojan.Ulise.D1BC1E	Avast	Win32-Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	TR/Agent.kkbov
BitDefender	Gen:Variant.Ulise.113694	Bkav Pro	W32.Common.4C83E082
ClamAV	Win.Malware.Agent-6342616-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.generic	Cylance	Unsafe

f50e42c8dfa6b649bde0398867e930b86c2a599e8db83b8260393082268f2dba

46 / 73
Community Score -108

46/73 security vendors flagged this file as malicious

Size: 160.00 KB | Last Analysis Date: 1 day ago

Lab01-01.dll

pedll idle via-tor armadillo checks-user-input spreader

Reanalyze Similar More

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.skeeyah/doina Threat categories trojan Family labels skeeyah doina waski

Security vendors' analysis

Max size 650MB

Alibaba	Trojan.Win32/Skeeyah.7fb0ebff	ALYac	Trojan.Agent.Waski
Antiy-AVL	Trojan.Win32.BTSGeneric	Arcabit	Trojan.Doina.D12B4A
Avast	Win32:Malware-gen	AVG	Win32-Malware-gen
BitDefender	Gen:Variant.Doina.76618	Bkav Pro	W32.AIDetectMalware
ClamAV	Win.Malware.Agent-6369668-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	DLL.trojan.skeeyah	Cylance	Unsafe
Cynet	Malicious (score: 100)	Deeplnstant	MALICIOUS

Lab01-01.exe 和 Lab01-01.dll 文件都匹配到了反病毒软件特征，被多个软件标记为病毒。

2. 这些文件是什么时候编译的？

History ⓘ	
Creation Time	2010-12-19 16:16:19 UTC
First Seen In The Wild	2012-01-08 02:19:06 UTC
First Submission	2012-02-16 07:31:54 UTC
Last Submission	2024-09-21 15:29:16 UTC
Last Analysis	2024-09-21 07:47:35 UTC
Names ⓘ	
Lab01-01.exe	
Lab 1.exe	
Lab1.exe	
Practical Malware Analysis Lab 01-01.exe_	
Lab01-01 - Copy.exe	
Lab01-01.malz	

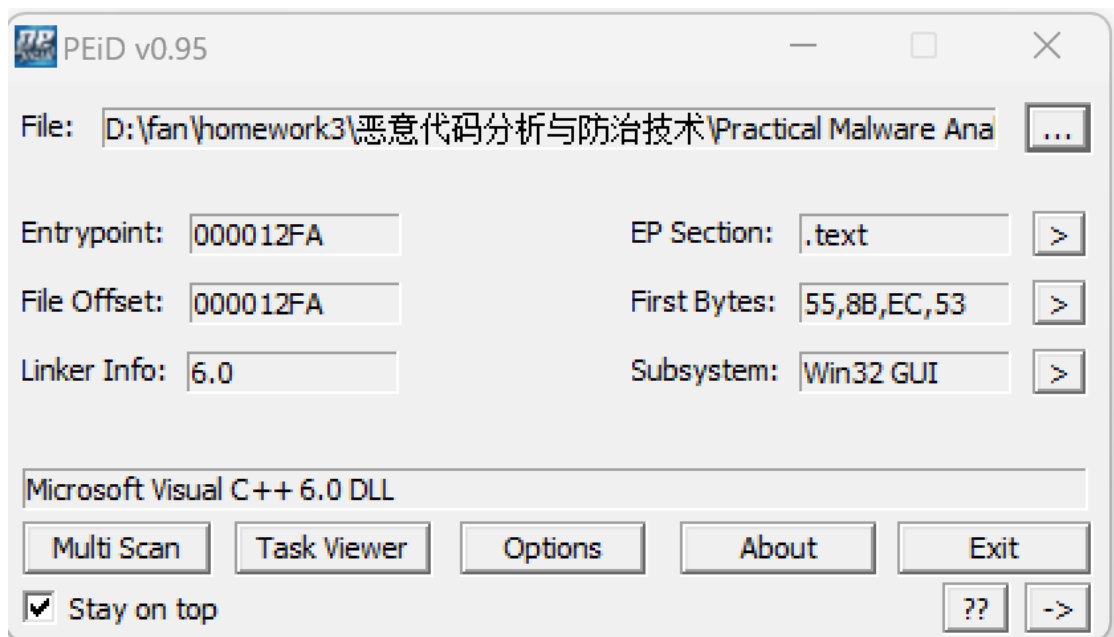
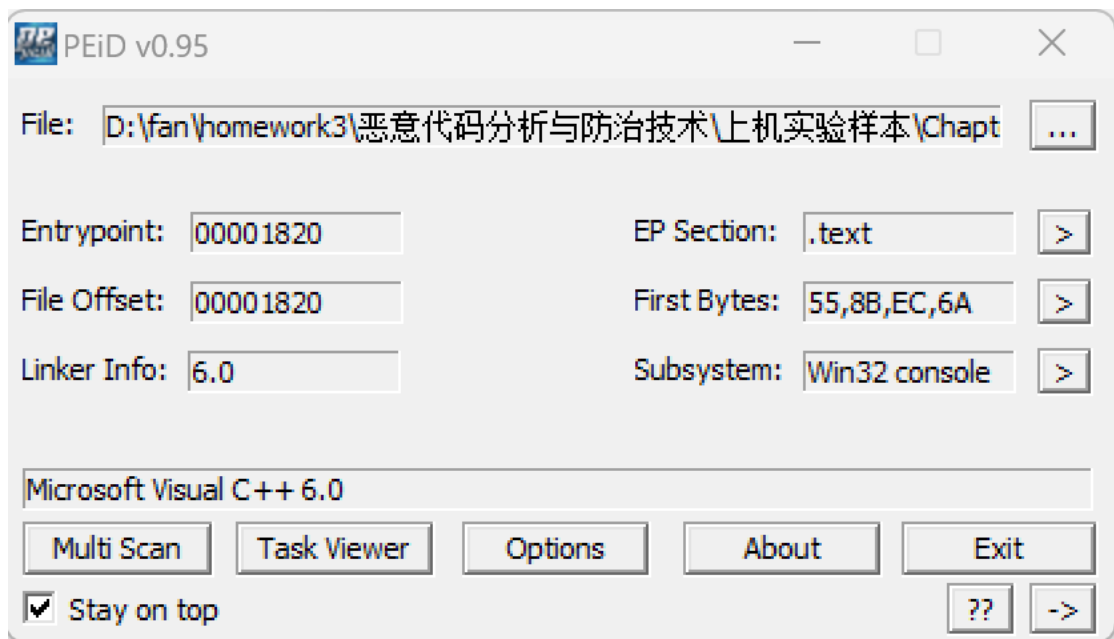
History ⓘ	
Creation Time	2010-12-19 16:16:38 UTC
First Seen In The Wild	2010-12-19 09:16:38 UTC
First Submission	2011-07-04 19:57:48 UTC
Last Submission	2024-09-21 15:29:08 UTC
Last Analysis	2024-09-20 08:26:09 UTC
Names ⓘ	
Lab01-01.dll	
Lab 2.dll	
Lab1.dll	
Practical Malware Analysis Lab 01-01.dll_	
Lab07-03.dll	

Lab01-01.exe 的编译时间为 2010-12-19 16:16:19; Lab01-01.dll 的编译时间为 2010-12-19 16:16:38。

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

使用 PEiD 进行查壳操作, 得到的结果如下:

可知 Lab01-01.exe 和 lab01-01.dll 都是没有加壳的文件。



4. 是否有导入函数显示出了这个恶意代码是做什么的?如果是, 是哪些导入函数?

(1) Lab01-01.exe

使用 `pestudio` 查看文件的导入表, 得到的结果如下:

pestudio 9.53 - Malware Initial Assessment - www.winitor.com - [d:\fan\homework3\恶意代码分析与防治技术\chapter_1\lab01-01.exe]

file settings about

d:\fan\homework3\恶意代码分析与防治技术\lab01-01.exe

indicators (imports > flag)

footprints (7)

virusotal (error)

dos-header (64 bytes)

rich-header (Visual Studio)

file-header (Intel-386)

optional-header (console)

directories (2)

sections (3)

libraries (2)

imports (flag)

exports (n/a)

thread-local-storage (n/a)

.NET (n/a)

resources (n/a)

strings (151)

debug (n/a)

manifest (n/a)

version (n/a)

certificate (n/a)

overlay (n/a)

imports (25)	flag (4)	callback (0)	first-thunk-original (L...	first-thunk (IAT)	hint	group (2)
malloc	-	-	0x000021D0	0x000021D0	657 (0x0291)	memory
UnmapViewOfFile	x	-	0x00002132	0x00002132	688 (0x02B0)	file
MapViewOfFile	x	-	0x00002154	0x00002154	470 (0x01D6)	file
CreateFileMappingA	-	-	0x00002164	0x00002164	53 (0x0035)	file
CreateFileA	-	-	0x0000217A	0x0000217A	52 (0x0034)	file
FindClose	-	-	0x00002188	0x00002188	144 (0x0090)	file
FindNextFileA	x	-	0x00002194	0x00002194	157 (0x009D)	file
FindFirstFileA	x	-	0x000021A4	0x000021A4	148 (0x0094)	file
CopyFileA	-	-	0x000021B6	0x000021B6	40 (0x0028)	file
CloseHandle	-	-	0x00002124	0x00002124	27 (0x001B)	-
IsBadReadPtr	-	-	0x00002144	0x00002144	437 (0x01B5)	-
exit	-	-	0x000021DA	0x000021DA	585 (0x0249)	-
_exit	-	-	0x000021EE	0x000021EE	211 (0x00D3)	-
XcptFilter	-	-	0x000021F6	0x000021F6	72 (0x0048)	-
_p_initenv	-	-	0x00002204	0x00002204	100 (0x0064)	-
_getmainargs	-	-	0x00002214	0x00002214	88 (0x0058)	-
_initterm	-	-	0x00002224	0x00002224	271 (0x010F)	-
_setusermatherr	-	-	0x00002230	0x00002230	131 (0x0083)	-
_adjust_fdiv	-	-	0x00002244	0x00002244	157 (0x009D)	-
_p_commode	-	-	0x00002254	0x00002254	106 (0x006A)	-
_p_fmode	-	-	0x00002264	0x00002264	111 (0x006F)	-
_set_app_type	-	-	0x00002272	0x00002272	129 (0x0081)	-
_except_handler3	-	-	0x00002284	0x00002284	202 (0x00CA)	-
_controlfp	-	-	0x00002298	0x00002298	183 (0x00B7)	-

sha256: 58898BD42C5BD3BF9B1389F0EE5B39CD59180E8370EB9EA838A0B327BD6FE4' cpu: 32-bit file-type: executable subsystem: console entry-point: 0x00001

CopyFileA 和 CreateFileA 的存在表明该恶意代码可能会复制自身到其他位置或创建新的恶意文件，以增强传播能力。

FindFirstFileA、FindNextFileA 和 FindClose 用于遍历文件系统，这表明它能够寻找特定目标文件，可能用于数据窃取或攻击。

CreateFileMappingA 和 MapViewOfFile 显示其可能在内存中直接操作文件，提高执行效率，减少被检测的风险。

CloseHandle 用于管理资源，表明该程序旨在保持稳定性并避免资源泄漏。

_except_handler3**的存在暗示该恶意代码具有处理异常的能力，以应对运行时错误，进一步提升其隐蔽性和生存能力。

这些导入函数表明 Lab01-01.exe 可能涉及文件传播、数据窃取和系统控制等恶意活动。

(2) Lab01-01.dll

使用 pestudio 查看文件的导入表，得到的结果如下：

pestudio 9.53 - Malware Initial Assessment - www.winitor.com - [d:\fan\homework3\恶意代码分析与防治技术\practical malware analysis labs\binarycollection\chapter_1\lab01-01.dll]

file settings about

d:\fan\homework3\恶意代码分析与防治技术\p

- indicators (strings > URL)
- footprints (8)
 - virusotal (error)
 - dos-header (64 bytes)
 - dos-stub (160 bytes)
 - rich-header (Visual Studio)
 - file-header (Intel-386)
 - optional-header (GUI)
 - directories (3)
 - sections (4)
 - libraries (flag)
 - imports (flag)**
 - exports (n/a)
 - thread-local-storage (n/a)
 - .NET (n/a)
 - resources (n/a)
 - strings (count)
 - debug (n/a)
 - manifest (n/a)
 - version (n/a)
 - certificate (n/a)
 - overlay (n/a)

imports (20)	flag (11)	callback (0)	first-thunk-original (L...	first-thunk (IAT)	hint	group (4)
CreateMutexA	-	-	0x00002130	0x00002130	63 (0x003F)	synchronization
OpenMutexA	-	-	0x00002140	0x00002140	493 (0x01ED)	synchronization
23 (socket)	x	-	0x80000017	0x80000017	0 (0x0000)	network
115 (WSAStartup)	x	-	0x80000073	0x80000073	0 (0x0000)	network
11 (inet_addr)	x	-	0x80000008	0x80000008	0 (0x0000)	network
4 (connect)	x	-	0x80000004	0x80000004	0 (0x0000)	network
19 (send)	x	-	0x80000013	0x80000013	0 (0x0000)	network
22 (shutdown)	x	-	0x80000016	0x80000016	0 (0x0000)	network
16 (recv)	x	-	0x80000010	0x80000010	0 (0x0000)	network
3 (closesocket)	x	-	0x80000003	0x80000003	0 (0x0000)	network
116 (WSACleanup)	x	-	0x80000074	0x80000074	0 (0x0000)	network
9 (hton)	x	-	0x80000009	0x80000009	0 (0x0000)	network
malloc	-	-	0x00002192	0x00002192	657 (0x0291)	memory
Sleep	-	-	0x00002116	0x00002116	662 (0x0296)	execution
CreateProcessA	x	-	0x0000211E	0x0000211E	68 (0x0044)	execution
CloseHandle	-	-	0x00002108	0x00002108	27 (0x001B)	-
_adjust_fdiv	-	-	0x0000219C	0x0000219C	157 (0x009D)	-
_initterm	-	-	0x00002186	0x00002186	271 (0x010F)	-
free	-	-	0x0000217E	0x0000217E	606 (0x025E)	-
strncmp	-	-	0x00002168	0x00002168	704 (0x02C0)	-

sha256: F50E42C8DFAAB6498DE0398867E930B86C2A599E8DB83B8260393082268F2DB1 cpu: 32-bit file-type: dynamic-link-library subsystem: GUI entry-point: 0x00001

CreateMutexA 和 OpenMutexA 的存在表明该恶意代码可能试图在系统中创建或访问互斥量，以确保自身的单一实例运行，防止重复感染。

CreateProcessA 用于创建新进程，这暗示该代码可能用来启动其他恶意程序或实现进一步的攻击行为。

网络相关的函数如 socket、connect、send 和 recv 表明该恶意代码可能具有网络通信能力，能够与远程服务器建立连接，发送和接收数据，这可能用于数据泄露或指令接收。

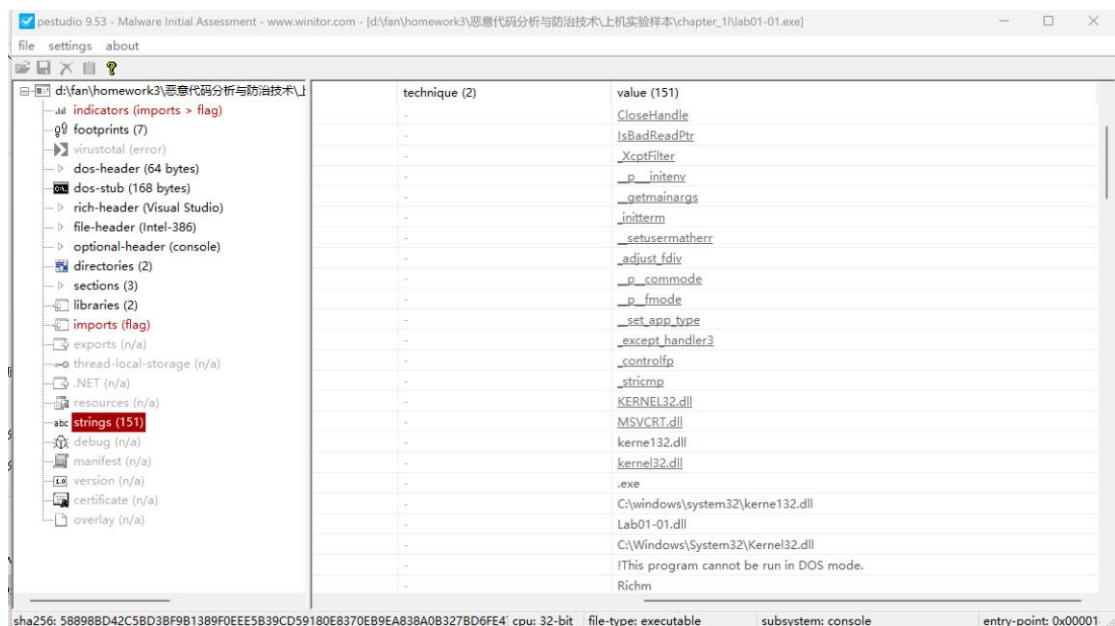
Sleep 函数可能用于延迟执行，增加检测难度。

内存管理函数如 malloc、free 和 strncmp 暗示其进行动态内存分配和字符串比较，以便处理数据。

这些导入函数显示 Lab01-01.dll 可能涉及进程管理、网络通信和数据处理等恶意活动。

5. 是否有任何其他文件或基于主机的迹象，让你可以在受感染系统上查找？

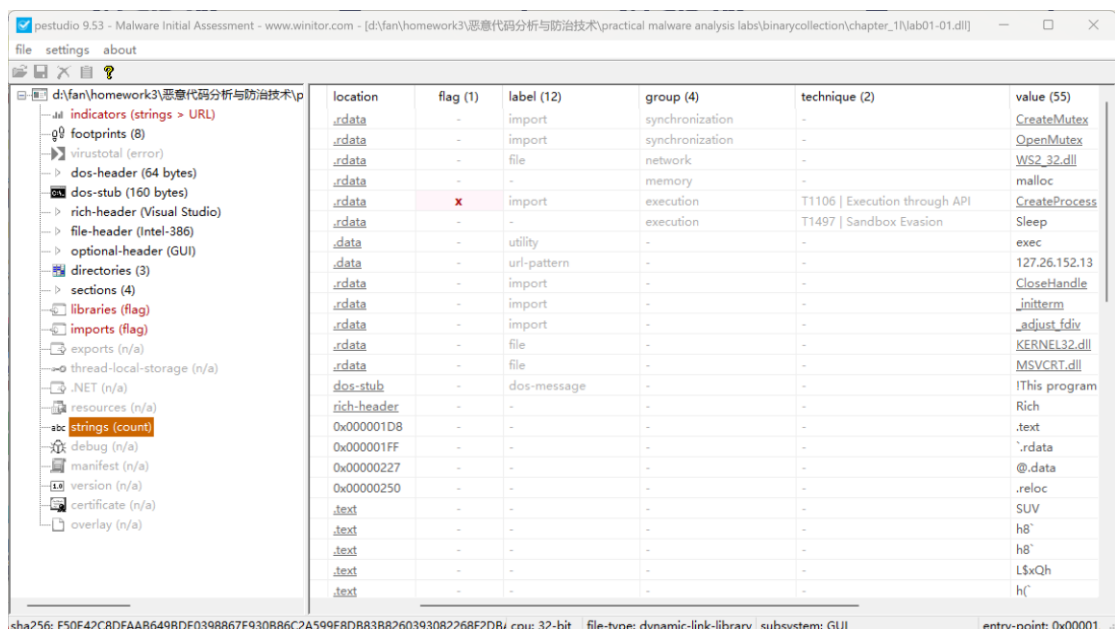
使用 pestudio 查看 Lab01-01.exe 中的字符串，得到的结果如下：



发现其中 kernel32.dll 中的 ‘1’ 被替换成了数字 ‘1’，可能为了将.dll 文件伪装成 kernel32.dll。可以在主机上搜索“kernel32.dll”来发现受感染的迹象，如果发现.dll 文件说明被感染。

6. 是否有基于网络的迹象,可以用来发现受感染机器上的这个恶意代码?

使用 pestudio 查看 Lab01-01.dll 中的字符串,得到的结果如下:



该文件包含 Sleep 和 exec 等 Windows 命令，并且 127.26.152.13 是一个 IP 地址，可能表明该程序作为后门与该 IP 进行交互，控制受感染的机器

并执行越权命令。该恶意代码有网络行为，将访问该 IP 地址，监视相关网络访问行为，可以发现受感染机器上的这个恶意代码。

7. 你猜这些文件的目的是什么？

Lab01-01.dll 文件可能是一个后门。后门是恶意代码将自身安装到一台计算机来允许攻击者访问。后门程序通常让攻击者只需很少认证甚至无需认证，便可连接到远程计算机上，并可以在本地系统执行命令。

Lab01-01.exe 文件是用来安装与运行 DLL 文件的。

II. Lab 1-2

分析 Lab01-02.exe 文件。

问题

1. 将 Lab01-02.exe 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？

57 / 72
Community Score -171

57/72 security vendors flagged this file as malicious

Reanalyze Similar More

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6
Lab01-02.exe
Size 3.00 KB
Last Analysis Date 2 days ago
EXE

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

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.ulise/trojanclicker Threat categories trojan downloader Family labels ulise trojanclicker click3

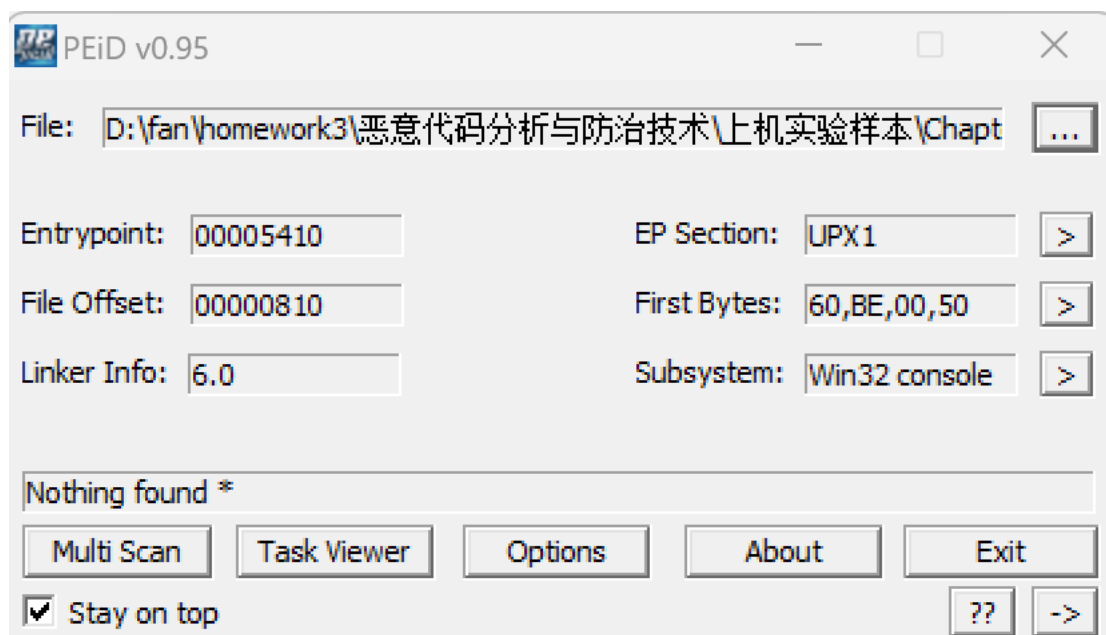
Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win32.StartPage.C26214	Alibaba	TrojanClicker:Win32/Generic.47e7b5e4
ALYac	Trojan.Startpage.3072	Antiy-AVL	Trojan/Win32.SGeneric
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
Bkav Pro	W32.AI DetectMalware	ClamAV	Win.Malware.Agent-6350563-0
CrowdStrike Falcon	Win/malicious_confidence_100%_000	CTX	Exe.trojan.generic

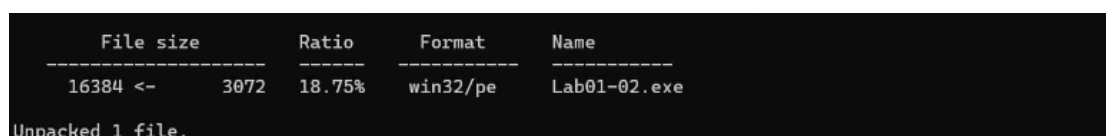
由图中可以看出，Lab01-02.exe 文件匹配到了反病毒软件特征，被多个软件标记为病毒。

2. 是否有这个文件被加壳或混淆的任何迹象?如果是这样,这些迹象是什么?如果该文件被加壳,请进行脱壳,如果可能的话。

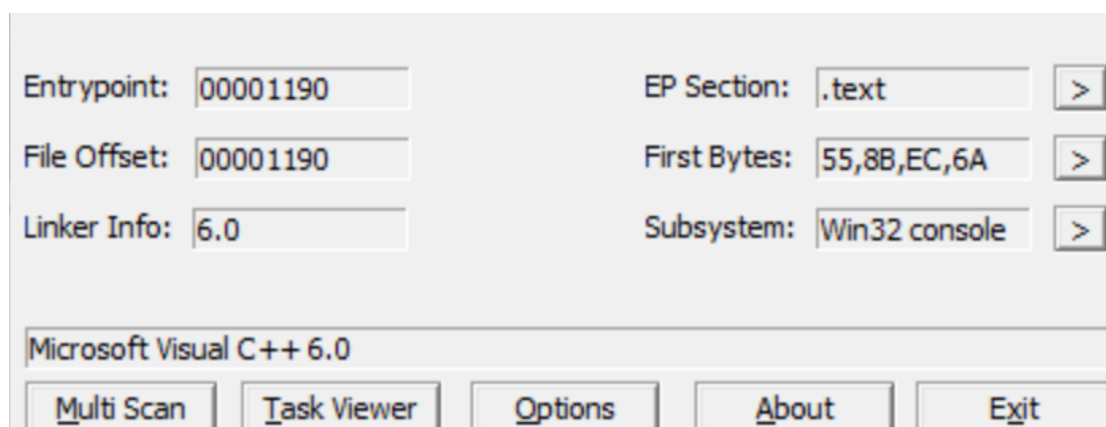
使用 PEiD 进行查壳操作,得到的结果如下:



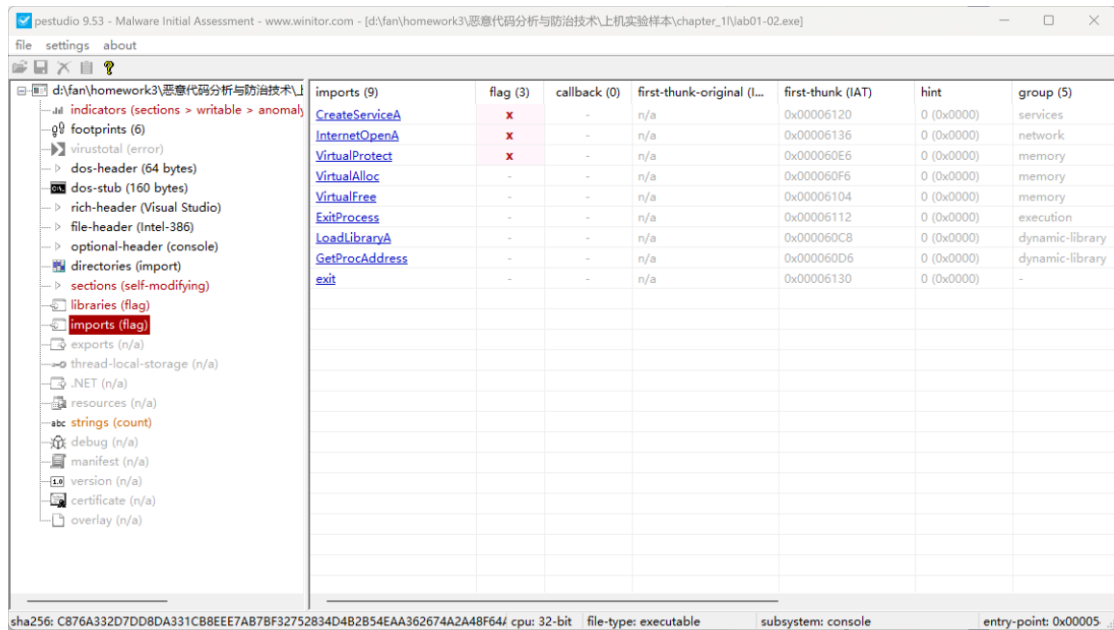
该文件被加了壳,执行 upx -d 命令脱壳成功,脱壳成功。



对脱壳后的文件重新查壳,结果如下,发现脱壳成功。



3. 有没有任何导入函数能够暗示出这个程序的功能?如果是,是哪些导入函数,它们会告诉你什么?



VirtualAlloc 和 VirtualFree 用于动态内存分配和释放，可能表明程序会分配内存以存储恶意代码或数据。

VirtualProtect 则允许改变内存页的保护属性，可能用于执行自我修改的代码，常见于病毒和木马。

GetProcAddress 和 LoadLibraryA 的组合暗示程序可能动态加载其他 DLL，这使得程序能够在运行时扩展其功能，可能用于隐蔽地引入额外的恶意组件。

CreateServiceA 的存在则指向程序可能创建一个 Windows 服务，通常用于确保程序在系统启动时自动运行，从而提高其持久性和隐蔽性。

最后，InternetOpenA 显示了网络能力，意味着程序可能会进行数据传输，发送或接收命令。

这些导入函数共同实现一个可能具有恶意目的的程序，涉及内存操控、持久性和网络交互。

4. 哪些基于主机或基于网络的迹象可以被用来确定被这个恶意代码所感染的机器？

用 IDApro 打开 Lab01-02.exe，查看字符串，有一些可疑字符串和可疑网址。

Address	Ordinal	Name	Library
00402000		OpenProcessToken	ADVAPI32
00402004		LookupPrivilegeValueA	ADVAPI32
00402008		AdjustTokenPrivileges	ADVAPI32
00402010		GetProcAddress	KERNEL32
00402014		LoadLibraryA	KERNEL32
00402018		WinExec	KERNEL32
0040201C		WriteFile	KERNEL32
00402020		CreateFileA	KERNEL32
00402024		SizeofResource	KERNEL32
00402028		CreateRemoteThread	KERNEL32
0040202C		FindResourceA	KERNEL32
00402030		GetModuleHandleA	KERNEL32
00402034		GetWindowsDirectoryA	KERNEL32
00402038		MoveFileA	KERNEL32
0040203C		GetTempPathA	KERNEL32
00402040		GetCurrentProcess	KERNEL32
00402044		OpenProcess	KERNEL32
00402048		CloseHandle	KERNEL32
0040204C		LoadResource	KERNEL32
00402054		_snprintf	MSVCRT
00402058		exit	MSVCRT

III. Lab 1-3

分析 Lab01-03.exe 文件。

问题

1. 将 Lab01-03.exe 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？

Max size 650MB

7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec

66/73 security vendors flagged this file as malicious

Reanalyze Similar More

7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec

Size 4.64 KB

Last Analysis Date 4 hours ago

Lab01-03.exe

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

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.graftor/genome

Threat categories trojan spyware

Family labels grafter genome trojanclicker

Security vendors' analysis

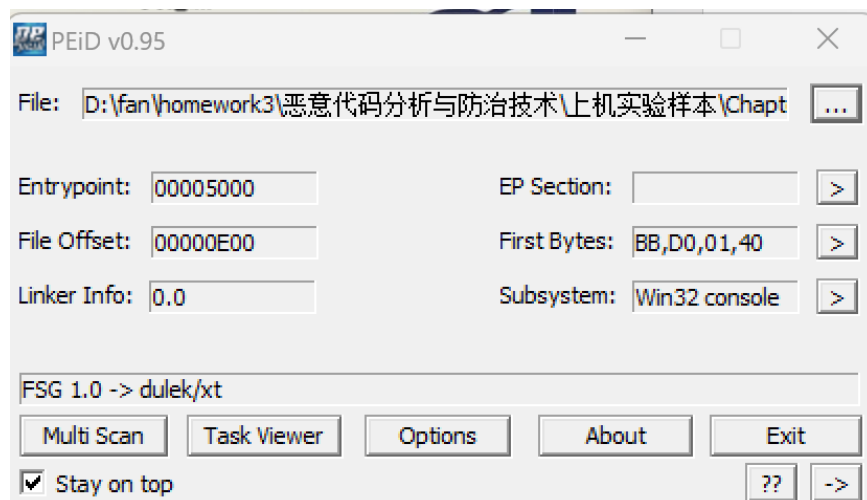
Do you want to automate checks?

AhnLab-V3	Trojan.Win.Generic.R427327	Alibaba	TrojanClicker.Win32/Tnega.79c6a6fb
ALYac	Gen:Variant.Grafter.968808	Antiy-AVL	Trojan.Win32.SGeneric
Arcabit	Trojan.Grafter.DEC868	Avast	Win32:Evo-gen [Trj]
AVG	Win32:Evo-gen [Trj]	Avira (no cloud)	TR/Clicker.lhuqy
Baidu	Win32.Trojan-Clicker.Agent.z	BitDefender	Gen:Variant.Grafter.968808
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Malware.Emoneg-9937593-0
CrowdStrike Falcon	Win/malicious-confidence-100% (W)	CTX	Exe.trojan.generic

由图中可以看出，Lab01-03.exe 文件匹配到了反病毒软件特征，被多个软件标记为病毒。

2. 是否有这个文件被加壳或混淆的任何迹象?如果是这样,这些迹象是什么?如果该文件被加壳,请进行脱壳,如果可能的话。

使用 PEiD 进行查壳操作,得到的结果如下:



由图中可以看出,文件被加壳,该文件加的是 FSG1.0 的壳,使用 linxerUnpacker 进行脱壳,结果如下:



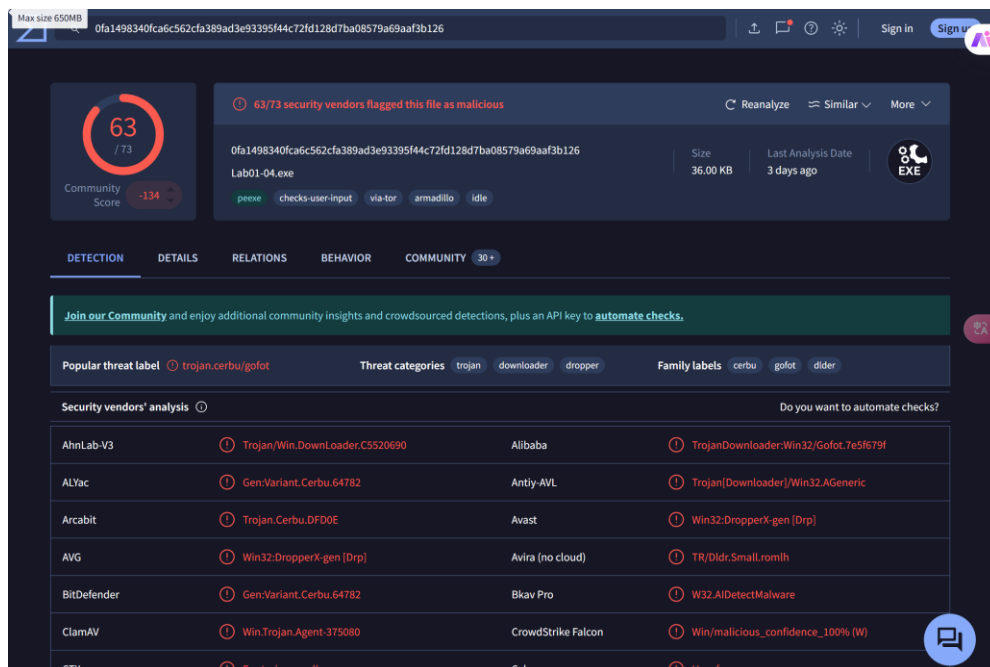
3. 有没有任何导入函数能够暗示出这个程序的功能?如果是,是哪些导入函数,它们会告诉你什么?

使用 pestudio 查看脱壳后的文件的导入表,结果如下:

分析 Lab01-04.exe 文件。

问题

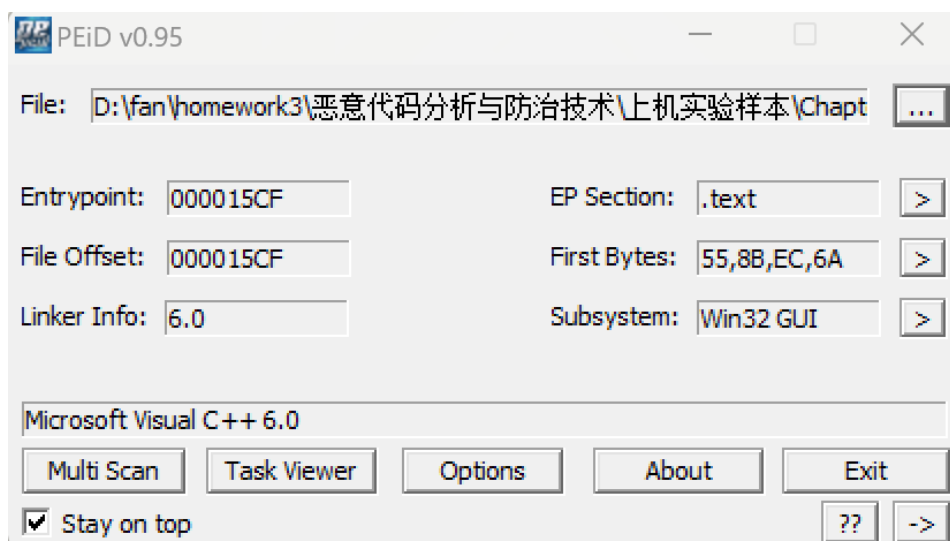
1. 将 Lab01-04.exe 文件上传至 <http://www.VirusTotal.com/> 进行分析并查看报告。文件匹配到了已有的反病毒软件特征吗？



由图中可以看出，Lab01-04.exe 文件匹配到了反病毒软件特征，被多个软件标记为病毒。

2. 是否有这个文件被加壳或混淆的任何迹象？如果是这样，这些迹象是什么？如果该文件被加壳，请进行脱壳，如果可能的话。

使用 PEiD 进行查壳操作，得到的结果如下，从该图中可以看出，该文件并没有被加壳。

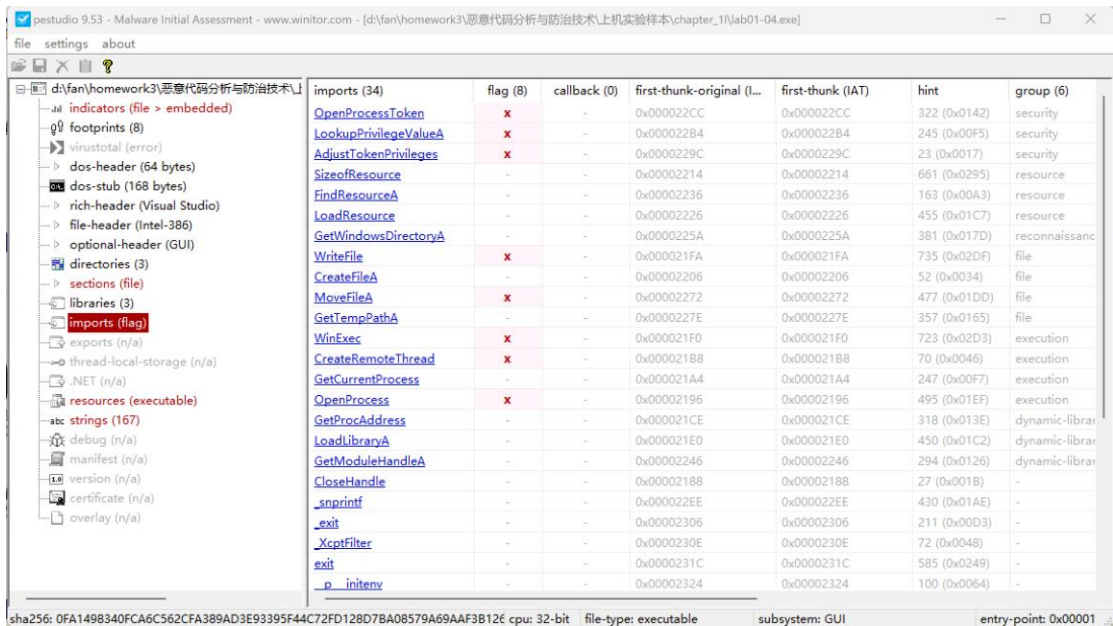


3. 这个文件是什么时候被编译的？

History ①	
Creation Time	2019-08-30 22:26:59 UTC
First Seen In The Wild	2011-07-05 18:16:16 UTC
First Submission	2011-07-06 00:05:42 UTC
Last Submission	2024-09-22 14:12:16 UTC
Last Analysis	2024-09-19 05:59:24 UTC
Names ①	
Lab01-04.exe	
Lab03-01.exe	
Lab 5.exe	

该文件的编译时间为 2019 年 8 月 30 日 22:26:59。

4. 有没有任何导入函数能够暗示出这个程序的功能？如果是，是哪些导入函数，它们会告诉你什么？



imports (34)	flag (8)	callback (0)	first-thunk-original (l...	first-thunk (IAT)	hint	group (6)
OpenProcessToken	x	-	0x000022CC	0x000022CC	322 (0x0142)	security
LookupPrivilegeValueA	x	-	0x000022B4	0x000022B4	245 (0x00F5)	security
AdjustTokenPrivileges	x	-	0x0000229C	0x0000229C	23 (0x0017)	security
SizeofResource	-	-	0x00002214	0x00002214	661 (0x0295)	resource
FindResourceA	-	-	0x00002236	0x00002236	163 (0x00A3)	resource
LoadResource	-	-	0x00002226	0x00002226	455 (0x01C7)	resource
GetWindowsDirectoryA	-	-	0x0000225A	0x0000225A	381 (0x017D)	reconnaissance
WriteFile	x	-	0x000021FA	0x000021FA	735 (0x02DF)	file
CreateFileA	-	-	0x00002206	0x00002206	52 (0x0034)	file
MoveFileA	x	-	0x00002272	0x00002272	477 (0x01DD)	file
GetTempPathA	-	-	0x0000227E	0x0000227E	357 (0x0165)	file
WinExec	x	-	0x000021F0	0x000021F0	723 (0x02D3)	execution
CreateRemoteThread	x	-	0x000021B8	0x000021B8	70 (0x0046)	execution
GetCurrentProcess	-	-	0x000021A4	0x000021A4	247 (0x00F7)	execution
OpenProcess	x	-	0x00002196	0x00002196	495 (0x01EF)	execution
GetProcAddress	-	-	0x000021CE	0x000021CE	318 (0x013E)	dynamic-library
LoadLibraryA	-	-	0x000021E0	0x000021E0	450 (0x01C2)	dynamic-library
GetModuleHandleA	-	-	0x00002246	0x00002246	294 (0x0126)	dynamic-library
CloseHandle	-	-	0x00002188	0x00002188	27 (0x001B)	-
_snprintf	-	-	0x000022EE	0x000022EE	430 (0x01AE)	-
_exit	-	-	0x00002306	0x00002306	211 (0x00D3)	-
_XcptFilter	-	-	0x0000230E	0x0000230E	72 (0x0048)	-
exit	-	-	0x0000231C	0x0000231C	585 (0x0249)	-
_p_initenv	-	-	0x00002324	0x00002324	100 (0x0064)	-

从 Advapi32.dll 中导入的函数：OpenProcessToken 用来打开与进程相关联的访问令牌；LookupPrivilegeValueA 查看系统权限的特权值并返回到一个 LUID 结构体里；AdjustTokenPrivileges 用于启用或禁止指定的访问令牌的特权。

从 Kernel32.dll 中导入的函数：GetProcAddress、LoadLibraryA 用于加载函数；WinExec 用于运行 exe 文件；File 相关的几个函数能够创建、

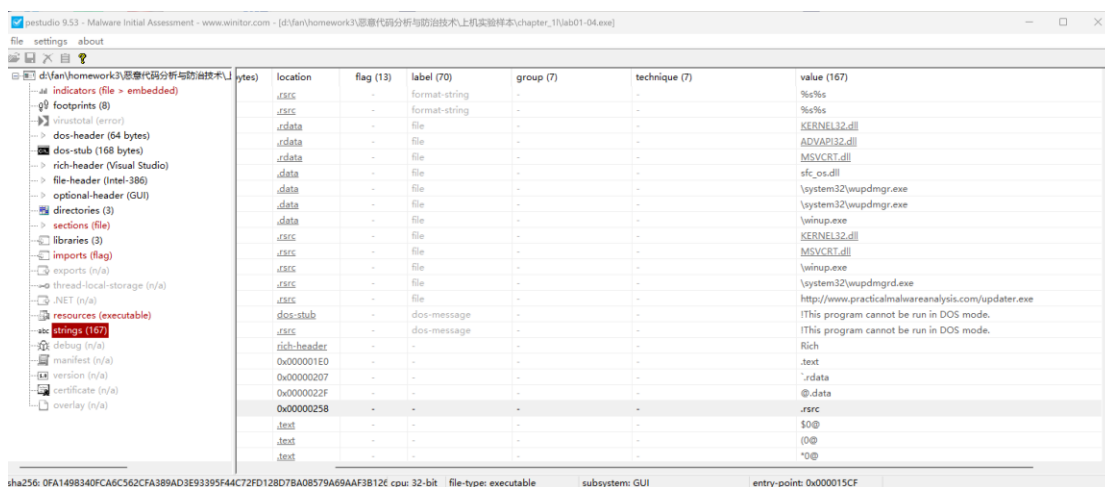
移动、写文件；Resource 相关的几个函数应该是对资源节中的资源进行一些操作；GetTempPathA 获取用户的临时文件夹的路径；

GetWindowsDirectory 用来获取 Windows 目录的完整路径名；OpenProcess 打开本地进程对象；GetCurrentProcess 获取当前进程的一个伪句柄；

CreateRemoteThread 能够创建一个在其他进程空间中运行的线程。

我推测该文件可以下载其他的恶意代码来对主机进行感染。

5. 有哪些基于主机或基于网络的迹象, 可以被用来确定被这个恶意代码所感染的机器?



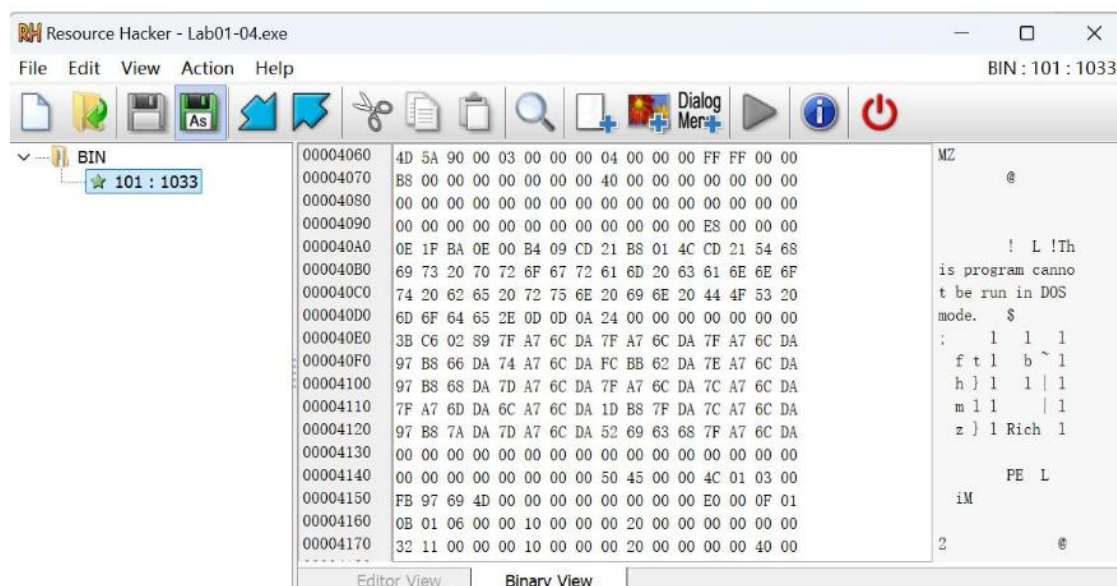
wupdmgr.exe 是系统自动升级程序, 不过病毒木马也经常将自己伪装成这两个 exe 来运行, 但最让人注意的还是 “\winup.exe”, winup.exe 并不是 Windows 系统会自带的 exe 文件, 而是至今仍被广泛使用的 infector 病毒技术的被感染文件。因此可以猜测: 该恶意代码的资源节中存放了 winup.exe。

导入函数 URLDownloadToFileA 和一个网址 “hxxp://www.practicalmalwareanalysis.com/updater.exe” 意味着这个资源节中的 exe 文件将从该网址下载 updater.exe, 那么理论上来说, “\system32\wupdmgrd.exe” 应该就是将改文件下载后存放的路径。

如果电脑中出现了 winup.exe、在 C:\Windows\system32 文件夹下出现了 wupdmgrd.exe, 则该机器被恶意代码所感染; 监视网络行为, 如果有向 “hxxp://www.practicalmalwareanalysis.com/updater.exe” 发送请求, 则该机器被恶意代码所感染。

6. 这个文件在资源段中包含一个资源。使用 Resource Hacker 工具来检查资源，然后抽取资源。从资源中你能发现什么吗？

打开 Resource Hacker，将 Lab01-04.exe 拖入。



导入表信息、可疑字符串信息和我们使用 strings.exe 查看 Lab01-04，从查看结果可以推测出该 exe 文件被从恶意代码导出后应名为 winup.exe，被运行后将从上述网站请求下载 updater.exe，将其更名为 wupdmgrd.exe、放在 C:\Windows\system32\目录下后执行。

V. Yara 检测

结合之前的分析，可将几个文件的特征写成 yara 检测规则，编写的 yara 规则可以匹配各个病毒文件的特征，从而检测病毒文件。

```
private rule IsPE
{
    condition:
        uint16(0) == 0x5A4D and
        uint32(uint32(0x3C)) == 0x00004550
}

rule one_exe
{
    strings:
        $s1 = "kerne132.dll"
        $s2 = "C:\\windows\\system32\\kerne132.dll"
```

```

        condition:
            IsPE and ($s1 or $s2)
    }
rule one_dll
{
    strings:
        $s1 = "Sleep"
        $s2 = "exec"
        $s3 = "127.26.152.13"
    condition:
        IsPE and ($s1 or $s2) and $s3
}

rule two
{
    strings:
        $s1 = "MalService"
        $s2 = "HGL345"
        $s3 = {68 74 74 70 3A 2F 2F 77 FF B7 BF DD 00 2E 6D 1E 77 61 72 65 61
                6E 07 79 73 69 73 62 6F 6F 6B 2E 63 6F FF DB DB 6F 6D}
    condition:
        IsPE and ($s1 or $s2) and $s3
}

rule three
{
    strings:
        $s1 = "_getmas"
        $s2 = "ole32.vd"
        $s3 = "}OLEAUTL"
    condition:
        IsPE and ($s1 or $s2) and $s3
}

rule four
{
    strings:
        $s1 = "\\system32\\wupdmgrd.exe"
        $s2 = "http://www.practicalmalwareanalysis.com/updater.exe"
    condition:
        IsPE and ($s1 or $s2)
}

```

VI. 使用 Windows Defender Antivirus 进行扫描

```
one_exe .\Lab01-01.exe
two .\Lab01-02.exe
three .\Lab01-03.exe
one_dll .\Lab01-01.dll
four .\Lab01-04.exe
```

VI. 使用 Windows Defender Antivirus 进行扫描

```
P5 C:\Program Files\Windows Defender> .\MpCmdRun.exe -Scan -ScanType 3 -File "D:\download\Practical Malware Analysis Labs\BinaryCollection\Chapter_11" -DisableRemediation
Scan starting...
Scan finished.
Scanning D:\download\Practical Malware Analysis Labs\BinaryCollection\Chapter_11 found 5 threats.

=====LIST OF DETECTED THREATS=====
----- Threat information -----
Threat       : Trojan:Win32/Skeeyah.A!MTB
Resources    : 1 total
file         : D:\download\Practical Malware Analysis Labs\BinaryCollection\Chapter_11\Lab01-01.dll
-----
----- Threat information -----
Threat       : TrojanDownloader:Win32/Small!MSR
Resources    : 1 total
file         : D:\download\Practical Malware Analysis Labs\BinaryCollection\Chapter_11\Lab01-04.exe
-----
----- Threat information -----
Threat       : Trojan:Win32/Graftor.GPA!MTB
Resources    : 1 total
file         : D:\download\Practical Malware Analysis Labs\BinaryCollection\Chapter_11\Lab01-03.exe
-----
----- Threat information -----
Threat       : Trojan:Win32/Clicker.GPA!MTB
Resources    : 2 total
file         : D:\download\Practical Malware Analysis Labs\BinaryCollection\Chapter_11\Lab01-02.exe->(UPX)
containerfile : D:\download\Practical Malware Analysis Labs\BinaryCollection\Chapter_11\Lab01-02.exe
-----
----- Threat information -----
Threat       : Trojan:Win32/Aenjaris.CT!bit
Resources    : 1 total
file         : D:\download\Practical Malware Analysis Labs\BinaryCollection\Chapter_11\Lab01-01.exe
-----
```

四、实验结论及心得体会

1. 通过与 VirusTotal 的结合分析，我认识到多种反病毒工具的联合使用能够提高恶意软件检测的准确性，有助于全面评估安全风险。这为未来的安全防护工作提供了新的思路。
2. 优化 Yara 规则方面，我意识到可以通过使用正则表达式和元数据来提高匹配的灵活性和效率。此外，精确定义字符串类型和添加具有辨别力的字符串可以有效减少误报和提高检测准确性。
3. 通过本次实验，我深入分析了多个恶意程序，实践了静态分析技术，使用了 P Eview、ExeinfoPE、PEiD 等工具，提升了对 PE 文件结构的理解。结合 Yara 规则的编写和验证，我发现它们在检测恶意行为方面极具有效性。
4. 使用 VirusTotal 和 Microsoft Defender 进行恶意代码分析，使我更加熟悉了实时检测和分析的方法。这些经验不仅增强了我对恶意软件的理解，也为未来的安全工作奠定了基础。