

# 恶意代码分析与防治技术实验报告

## Lab1

学号：2011937      姓名：姜志凯      专业：信息安全

### 一、实验环境

- 本机 windows10
- Windows xp

### 二、实验工具

- VirusTotal
- PEView
- PEiD
- IDA pro
- linxerUnpacker
- Resource Hacker

### 三、实验内容

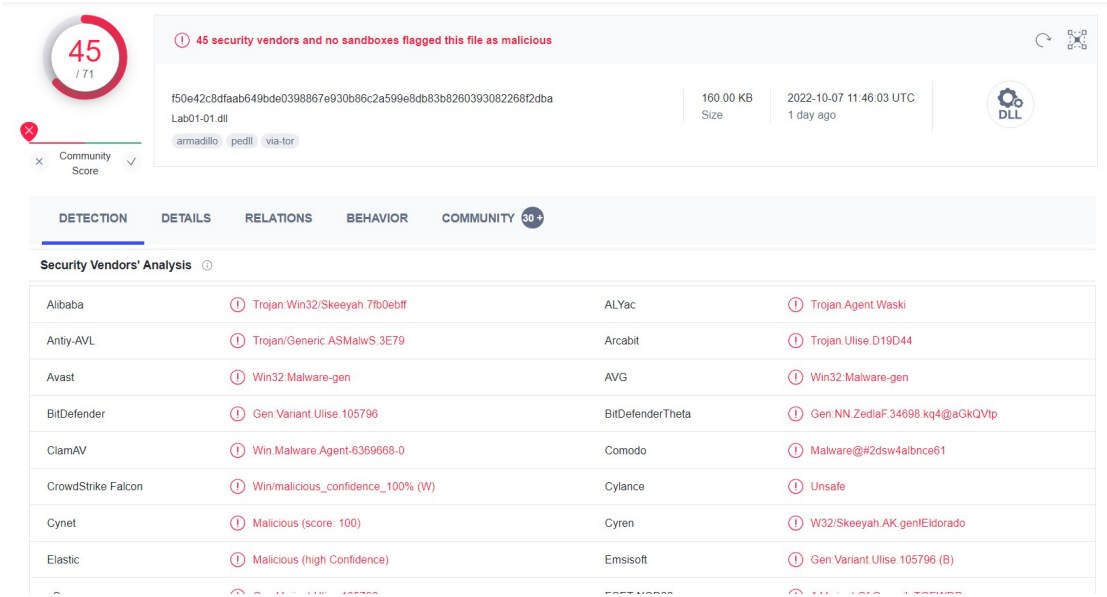
#### Lab1-1

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?

1、将 Lab01-01.dll 上传，得到如下结果：



可见，共 45 个杀毒软件、0 个沙盒将其分析为恶意软件，大概率是恶意软件。

可能包含的恶意软件的特征：

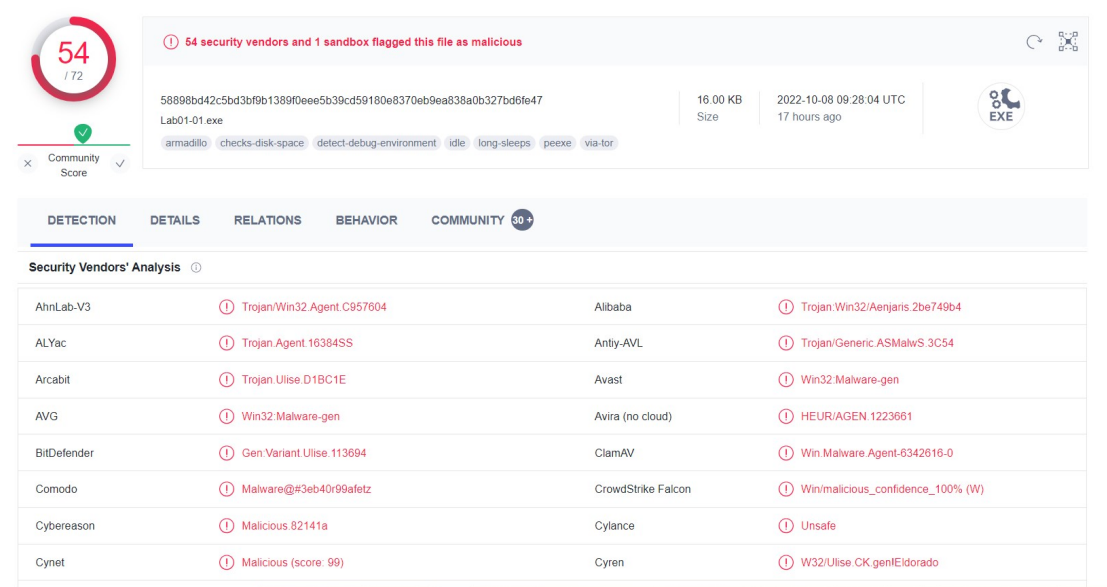
Trojan:Win32/Skeeyah.7fb0ebff：特洛伊微软系统 32 位木马病毒，是一种带有 rootkit 功能的特洛伊病毒，能够修改系统的 winlogon.exe 文件；

Win32:Malware-gen：Malware 病毒系列的一个分支，盗号病毒；

Trojan/Generic.ASMalwS.3E79：盗号木马。

等等.....

将 Lab01-01.exe 上传，得到如下结果：



可见，共 54 个杀毒软件、1 个沙盒将其分析为恶意软件，大概率是恶意软件。

可能包含的恶意软件的特征：

Trojan/Win32.Agent.C957604： 下载者木马类；

Trojan.Ulise.D1BC1E： 特洛伊木马。

等等.....

2、根据 details 模块中的 PE 文件信息可以得到编译时间：

**Lab01-01.dll:**

#### Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2010-12-19 16:16:38 UTC
Entry Point	4858
Contained Sections	4

编译时间：2010-12-19 16:16:38 UTC

**Lab01-01.exe:**

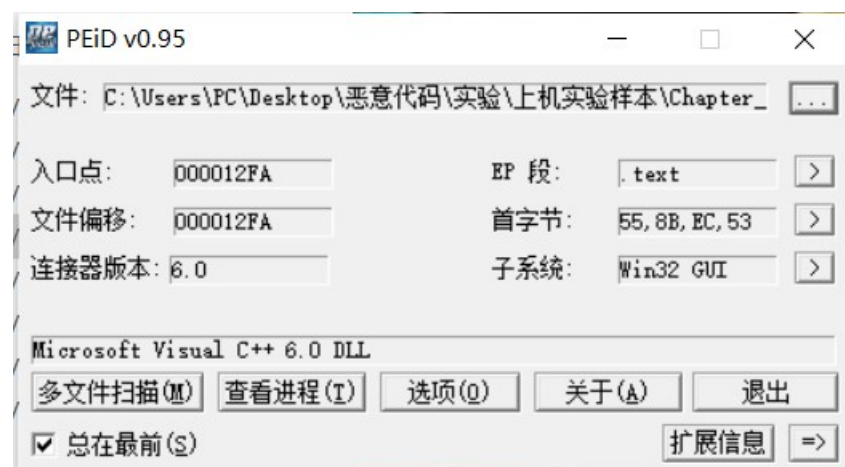
#### Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2010-12-19 16:16:19 UTC
Entry Point	6176
Contained Sections	3

编译时间：2010-12-19 16:16:19 UTC

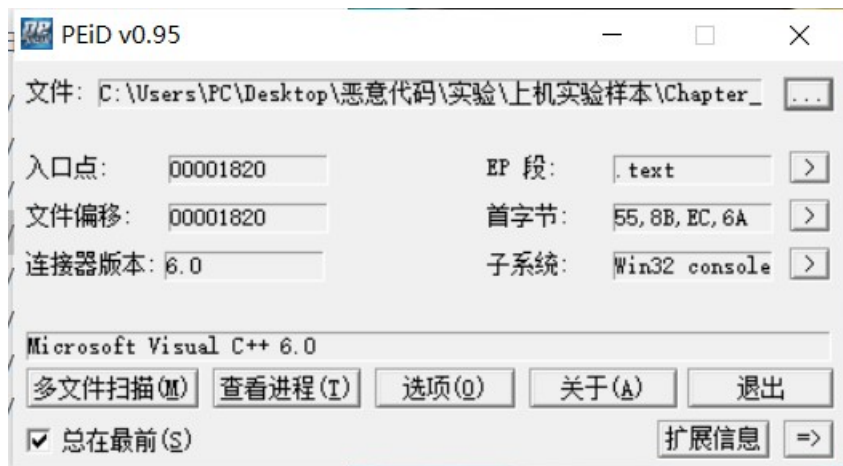
3、使用 PEiD 查看是否有加壳和混淆的迹象

Lab01-01.dll:



分析得，用 VC++编写的 DLL 文件，入口点、文件偏移等均可知，所以没有加壳和混淆；

Lab01-01.exe:



分析得，用 VC++编写的可执行文件，入口点、文件偏移等均可知，所以没有加壳和混淆。

#### 4、是否有导入函数显示出恶意代码是做什么的

(1) 将 Lab01-01.dll 文件上传到 VT，可以查看输入表函数，发现导入了三个 dll，每个 dll 下有多个 API 函数：

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

• kernel32.dll 是 Windows 9x/Me 中非常重要的 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，当 Windows 启动时，kernel32.dll 就驻留在内存中特定的写保护区域，使别的程序无法占用这个内存区域。

下面出现了创建进程、互斥量以及系统休眠的相关 API 函数：

• msvcrt.dll 是微软在 windows 操作系统中提供的 C 语言运行库执行文件，其中提供了 printf、malloc、strcpy 等 C 语言库函数的具体运行实现，并且为使用 C/C++ (Vc) 编译的程序提供了初始化（如获取命令行参数）以及退出等功能。

下面出现了申请、释放堆块的相关函数：

- ws2\_32.dll 是 Windows Sockets 应用程序接口， 用于支持 Internet 和网络应用程序。

下面的 API 函数主要是用于联网、进行数据传输（send、recv）。

使用 IDA 打开，查看 string:

Address	Length	Type	String
.rdata:1000214E	0000000D	C	KERNEL32.dll
.rdata:1000215C	0000000B	C	WS2_32.dll
.rdata:10002172	0000000B	C	MSVCRT.dll
.data:10026010	00000005	C	exec
.data:10026018	00000006	C	sleep
.data:10026020	00000006	C	hello
.data:10026028	0000000E	C	127.26.152.13
.data:10026038	00000009	C	SADFHUHF

发现一个 ip 地址，可见此恶意软件可能会联网，向外界进行数据传输造成信息泄露。

（2）将 Lab01-01.exe 上传，查看输入表函数，发现两个 dll，对应有几个 API 函数：

Imports		
— KERNEL32.dll		— MSVCRT.dll
	CloseHandle	__getmainargs
	CopyFileA	__p__initenv
	CreateFileA	__p__commode
	CreateFileMappingA	__p__fmode
	FindClose	__set_app_type
	FindFirstFileA	__setusermatherr
	FindNextFileA	_adjust_fdiv
	IsBadReadPtr	_controlfp
	MapViewOfFile	_except_handler3
	UnmapViewOfFile	_exit
		_initterm
		_stricmp
		_XcptFilter
		exit
		malloc

CreateFileA 创建文件，CopyFileA 复制文件，FindFirstFileA、FindNextFileA 查找特定文件，因此该恶意程序可能会搜索文件，与上个 dll 文件配合使用，获得用户指定信息，并发往外界。

使用 IDA 打开，查看 string:



Address	Length	Type	String
.rdata:004021C2	0000000D	C	KERNEL32.dll
.rdata:004021E2	0000000B	C	MSVCRT.dll
.data:00403020	0000000D	C	kernel32.dll
.data:00403030	00000005	C	.exe
.data:00403044	00000005	C	C:\*
.data:0040304C	00000021	C	C:\windows\system32\kerne132.dll
.data:0040307C	0000000D	C	Lab01-01.dll
.data:0040308C	00000021	C	C:\Windows\System32\Kernel32.dll
.data:004030B0	00000027	C	WARNING_THIS_WILL_DESTROY_YOUR_MACHINE

发现一个 kerne132.dll 滥竽充数，阻碍检测。

## 5、受感染系统有什么迹象

基于上一步的分析，猜测，Lab01-01.exe 在运行时可能会注入 Lab01-01.dll、kerne132.dll 文件，可以查找这些文件的特征字符串，比如那个可疑的 ip 地址 127.26.152.13，或者可疑的文件 kerne132.dll，因为它们正常主机上不会出现，如果出现，则证明被感染了。

## 6、受感染系统有什么网络上的迹象

在 Lab01-01.dll 中有 ws2\_32.dll，这个库主要用于网络连接；还有发现的那个 ip 地址，也可以作为网络迹象判断受感染机器。

## 7、这些文件的目的是

后门程序，使用 exe 文件装载 dll 文件运行，读取宿主的文件，获取关键信息，绕过安全机制获得系统访问权，更进一步，通过联网，向目标 ip 发送信息，造成信息泄露。

## Lab1-2

### 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?

1、上传到 VT，得到

54  
/ 72

54 security vendors and no sandboxes flagged this file as malicious

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6  
Lab01-02.exe

3.00 KB  
Size

2022-10-09 04:06:47 UTC  
2 hours ago

EXE

Community Score

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

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY

Security Vendors' Analysis

AhnLab-V3	Trojan/Win32.StartPage.C28214	Alibaba	TrojanClicker.Win32/Generic.1ba980f
ALYac	Trojan.Startpage.3072	Antiy-AVL	Trojan/Generic.ASMalwS.330C
Arcabit	Trojan.Ser.Ulisse.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.Ulisse.216
BitDefenderTheta	Gen.NN.ZexaF.34698.amGfaWi/867f	ClamAV	Win/Malware.Agent-6350563-0
Comodo	Malware@#22epuiwih8vym	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.878404	Cylance	Unsafe

54 个安全供应商、0 个沙盒分析为恶意程序，大概率是恶意程序。

## 2、是否加壳或混淆

导入到 PEiD



由于查壳入口点 EP 段为 UPX1，说明源程序被压缩为 UPX0 和 UPX1 两个节，而且“什么都没找到”，都说明了有壳。

下面利用 [linxerUnpacker](#) 进行脱壳



已知壳脱壳均失败，由脱壳信息可知，该壳为未知壳，所以点击未知壳脱壳，成功！



说明：本机用 linxerUnpacker 脱壳一直失败，放到 xp 虚拟机中，脱壳成功！（我分析可能是本机版本太高，安全防护机制比较完善，将 linxerUnpacked 视为不安全的软件，未知壳脱壳时直接阻止进程）

将脱壳后的程序再次放入 PEiD 中，得到





3、是否有导入函数显示程序是干什么的

使用 IDA，可以查看导入函数

Address	Ordinal	Name	Library
00000000...		CreateServiceA	ADVAPI32
00000000...		StartServiceCtrlDispatcherA	ADVAPI32
00000000...		OpenSCManagerA	ADVAPI32
00000000...		SystemTimeToFileTime	KERNEL32
00000000...		GetModuleFileNameA	KERNEL32
00000000...		CreateWaitableTimerA	KERNEL32
00000000...		ExitProcess	KERNEL32
00000000...		OpenMutexA	KERNEL32
00000000...		SetWaitableTimer	KERNEL32
00000000...		WaitForSingleObject	KERNEL32
00000000...		CreateMutexA	KERNEL32
00000000...		CreateThread	KERNEL32
00000000...		_exit	MSVCRT
00000000...		_XcptFilter	MSVCRT
00000000...		exit	MSVCRT
00000000...		__p__initenv	MSVCRT
00000000...		__getmainargs	MSVCRT
00000000...		_initterm	MSVCRT
00000000...		_setusermatherr	MSVCRT
00000000...		_adjust_fdiv	MSVCRT
00000000...		__p__commode	MSVCRT
00000000...		__p__fmode	MSVCRT
00000000...		__set_app_type	MSVCRT
00000000...		_except_handler3	MSVCRT
00000000...		_controlfp	MSVCRT
00000000...		InternetOpenUrlA	WININET
00000000...		InternetOpenA	WININET

共有 4 个 dll，每个 dll 下有几个函数

Kernel32 和 msvcrt.dll 为基本的库

WININET 库，为网络编程接口，InternetOpenA、InternetOpenUrlA 为打开应用程序和一个资源；

ADVAPI32.dll 下的三个 API 函数有创建服务的作用。

所以程序可能会联网并创建服务。

4、哪些迹象判断主机被此程序感染

还是进入 IDA，查看 string，看是否有特征

Address	Length	Type	String
UPX0:00403010	0000000B	C	MalService
UPX0:0040301C	0000000B	C	Malservice
UPX0:00403028	00000007	C	HGL345
UPX0:00403030	00000023	C	http://www.malwareanalysisbook.com
UPX0:00403054	00000016	C	Internet Explorer 8.0
UPX2:00406098	0000000D	C	KERNEL32.DLL
UPX2:004060A5	0000000D	C	ADVAPI32.dll
UPX2:004060B2	0000000B	C	MSVCRT.dll
UPX2:004060BD	0000000C	C	WININET.dll
UPX2:004060CA	0000000D	C	LoadLibraryA
UPX2:004060D8	0000000F	C	GetProcAddress
UPX2:004060E8	0000000F	C	VirtualProtect
UPX2:004060F8	0000000D	C	VirtualAlloc
UPX2:00406106	0000000C	C	VirtualFree
UPX2:00406114	0000000C	C	ExitProcess
UPX2:00406122	0000000F	C	CreateServiceA
UPX2:00406132	00000005	C	exit
UPX2:00406138	0000000E	C	InternetOpenA
.linxer:004070...	0000000B	C	MSVCRT.dll
.linxer:004071...	0000000C	C	WININET.dll
.linxer:004071...	0000000D	C	KERNEL32.DLL
.linxer:004072...	0000000D	C	ADVAPI32.dll

一些个正常主机不会出现的字符串，如 MalService 或者那个奇怪的网址，否可以判断主机是否被感染。

## Lab1-3

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?

1、上传，得到

65  
/ 71

65 security vendors and no sandboxes flagged this file as malicious

7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff40f050f0aec  
Lab01-03.exe  
4.64 KB  
Size  
2022-10-03 09:09:08 UTC  
5 days ago  
EXE  
detect-debug-environment direct-cpu-clock-access fsg long-sleeps overlay peexe runtime-modules via-tor

Community Score

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY 90+

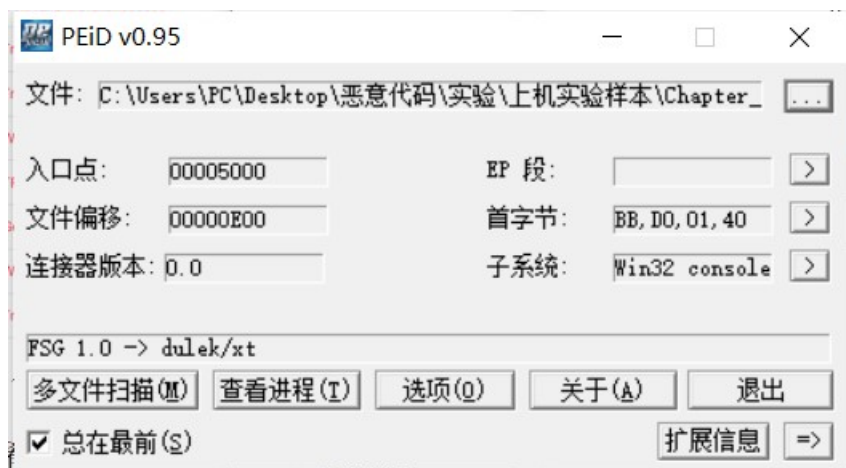
Security Vendors' Analysis

Ad-Aware	Gen.Variant.Graftor.968808	AhnLab-V3	Trojan.Win.Generic.R427327
Alibaba	TrojanClicker.Win32/Tnega.3bb840a6	ALYac	Gen.Variant.Graftor.968808
Antiy-AVL	Trojan.Generic.ASMalwS.330C	Arcabit	Trojan.Graftor.DEC868
Avast	Win32.Malware-gen	AVG	Win32.Malware-gen
Avira (no cloud)	TR/Clicker.knmor	Baidu	Win32.Trojan-Clicker.Agent.z
BitDefender	Gen.Variant.Graftor.968808	BitDefenderTheta	Gen.NN.ZexaF.34698.ambdaODILcf
Bkav Pro	W32.AIDetect.malware1	ClamAV	Win.Malware.Emoney.9937593-0
Comodo	TrojWare.Win32.Trojan.Inor.B_10@1qra8i	CrowdStrike Falcon	Win/malicious_confidence_100% (W)

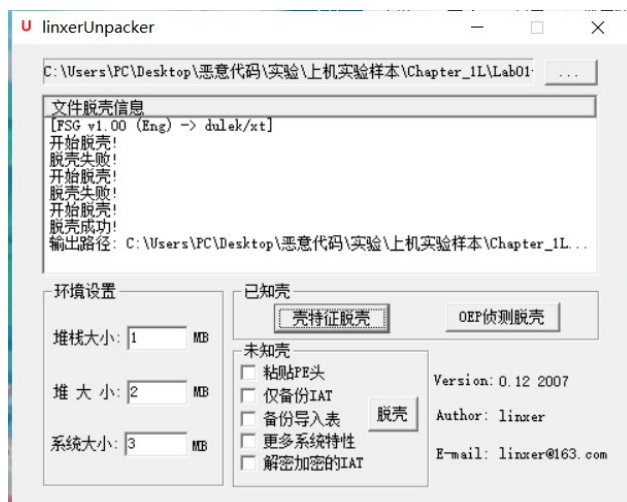
65 个安全供应商、0 个沙盒分析为恶意软件，大概率为恶意软件。

2、是否有壳或者混淆

放入 PEiD



发现，EP 段为空，下边显示 FSG，有明显的壳特征，直接用 linxerUnpacked 的壳特征脱壳



脱壳后的放入 PEiD 查看



3、是否有导入函数显示程序的作用

将脱壳后的文件传到 VT 上，得到 imports

— MSVCRT.dll		
Imports		_except_handler3
		__p__fmode
		_adjust_fdiv
		__p__commode
		__setusermatherr
		__p__initenv
		exit
		_XcptFilter
		__getmainargs
		_initterm
— ole32.dll		— OLEAUT32.dll
	OleUninitialize	SysFreeString
	CoCreateInstance	VariantInit
	OleInitialize	SysAllocString
		_controlfp
		_exit
		__set_app_type

Msvcrt 为基本的 C 语言库

ole.dll 文件是链接和嵌入在应用程序中的对象的过程文件。它是用于编写和整合来自不同应用程序的数据在 Windows 作业系统的骨干部分。

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），并启用一些特别用于 OLE 技术的额外功能。



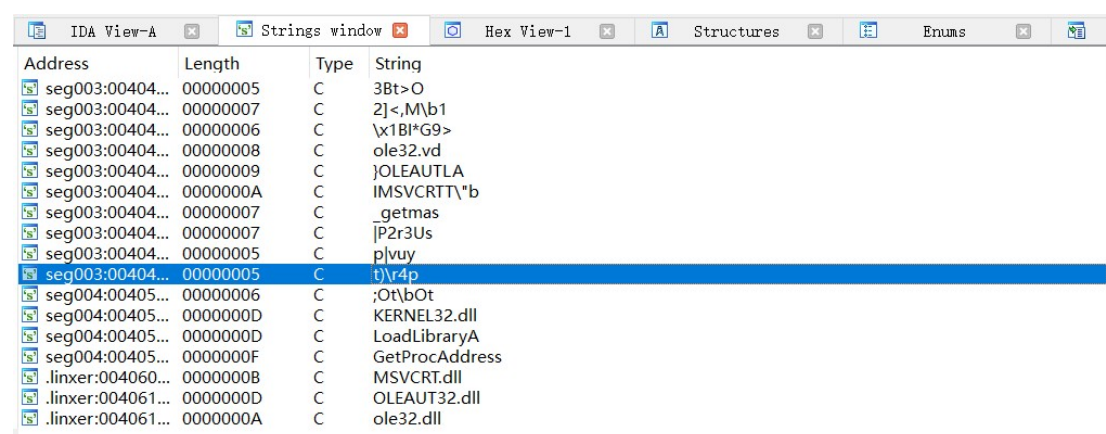
CoCreateInstance, 函数名。用指定的类标识符创建一个 Com 对象,用指定的类标识符创建一个未初始化的对象。当在本机中只创建一个对象时,可以调用 CoCreateInstance;在远程系统中创建一个对象时,可以调用 CoCreateInstanceEx;创建多个同一 CLSID 的对象时,可以参考 CoGetClassObject 函数。

如果在应用程序关闭时调用 OleUninitialize , 作为最后一个 COM 库调用,如果单元是使用对 OleInitialize 的调用初始化的。OleUninitialize 在内部调用 CoUninitialize 函数以关闭 OLE 组件对象 (COM) 库。

所以程序可能会链接或嵌入别的程序,是某些 dll 文件不可用。

#### 4、是否有主机或者网络迹象判断被感染

打开 IDA, 查看 string



Address	Length	Type	String
seg003:00404...	00000005	C	3Bt>O
seg003:00404...	00000007	C	2]<,M\b1
seg003:00404...	00000006	C	\x1Bl*G9>
seg003:00404...	00000008	C	ole32.vd
seg003:00404...	00000009	C	}OLEAUTLA
seg003:00404...	0000000A	C	IMSVCR7T\b
seg003:00404...	00000007	C	_getmas
seg003:00404...	00000007	C	P2r3Us
seg003:00404...	00000005	C	p vuy
seg003:00404...	00000005	C	t\r4p
seg004:00405...	00000006	C	;Ot\bOt
seg004:00405...	0000000D	C	KERNEL32.dll
seg004:00405...	0000000D	C	LoadLibraryA
seg004:00405...	0000000F	C	GetProcAddress
.linxer:004060...	0000000B	C	MSVCRT.dll
.linxer:004061...	0000000D	C	OLEAUT32.dll
.linxer:004061...	0000000A	C	ole32.dll

一些特殊字符串,如 IMSVCRTT 等,有网址的话也可以作为依据。

## Lab1-4

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?



1、上传，得到

62  
172

Community Score

62 security vendors and 1 sandbox flagged this file as malicious

0fa1498340fca6c562cfa389ad3e93395f44c72fd128d7ba08579a69aaf3b126

36.00 KB  
Size

2022-09-29 20:54:10 UTC  
9 days ago

EXE

armadillo idle peexe via-tor

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 30

Security Vendors' Analysis

Ad-Aware	Gen.Variant.Cerbu.64782	Alibaba	TrojanDownloader.Win32/DownLdr.080f...
ALYac	Gen.Variant.Cerbu.64782	Antiy-AVL	Trojan.Generic.ASMalwS.3304
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
Bkav Pro	W32.AIDetect.malware2	ClamAV	Win.Trojan.Agent-375080
Comodo	Malware@#2oyf6g8q6fgyr	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.f447ad	Cylance	Unsafe

62 个安全供应商和 1 个沙盒分析为恶意软件，大概率恶意。

2、有没有加壳或者混淆

放入 PEiD 中

PEiD v0.95

文件: C:\Users\PC\Desktop\恶意代码\实验\上机实验样本\Chapter\_...

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

多文件扫描(M)

查看进程(T)

选项(O)

关于(A)

退出

☒ 总在最前(S)

扩展信息 =>

如图，未加壳。

3、编译时间

传到 VT 上，details 模块，PE 文件信息查看

Header	
Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2019-08-30 22:26:59 UTC
Entry Point	5583
Contained Sections	4

编译时间：2019-08-30 22:26:59

#### 4、是否有导入函数可以判断程序功能

Imports		— KERNEL32.dll	— MSVCRT.dll
— ADVAPI32.dll	AdjustTokenPrivileges	CloseHandle	__getmainargs
	LookupPrivilegeValueA	CreateFileA	__p__initenv
	OpenProcessToken	CreateRemoteThread	__p__commode
		FindResourceA	__p__fmode
		GetCurrentProcess	__set_app_type
		GetModuleHandleA	__setusermatherr
		GetProcAddress	_adjust_fdiv
		GetTempPathA	_controlfp
		GetWindowsDirectoryA	_except_handler3
		LoadLibraryA	_exit
		LoadResource	_initterm
		MoveFileA	_snprintf
		OpenProcess	_stricmp
		SizeofResource	_XcptFilter
		WinExec	exit
		WriteFile	

由 kernel32 中的 API 函数可以发现，有 WriteFile 可能关于文件的读写、FindResourceA 涉及资源的查找；

advapi32.dll 是一个高级 API 应用程序接口服务库的一部分，包含的函数与对象的安全性，注册表的操控以及事件日志有关；

因此，该程序可能会改变权限来读取或写入特定文件，造成攻击。

#### 5、是否有主机或网络上的迹象可以判断被感染的主机

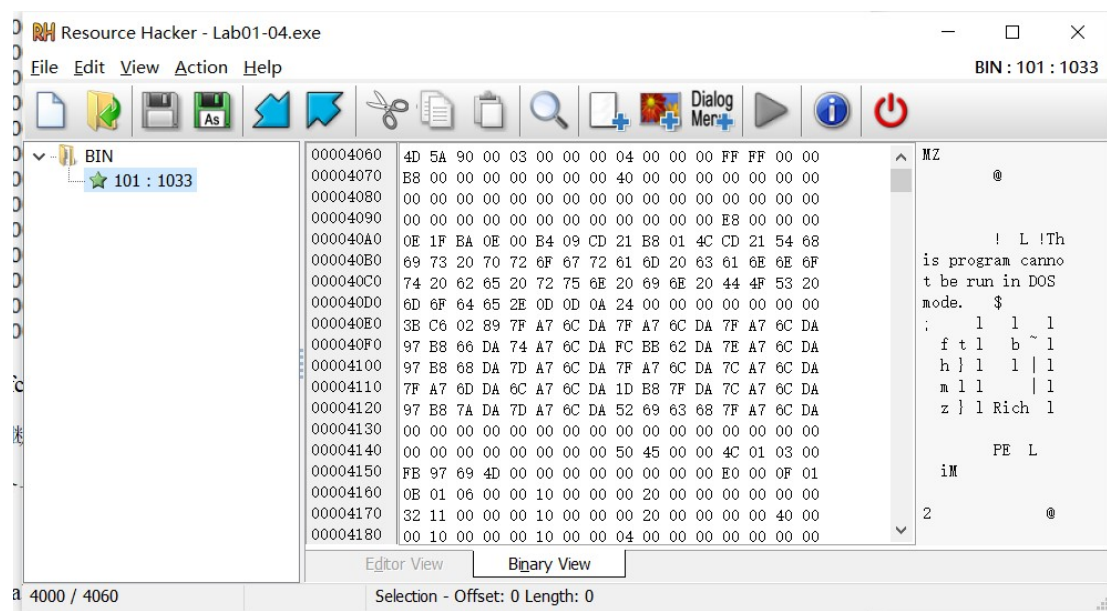
进入 IDA，查看 string

Address	Length	Type	String
.rdata:0040228E	0000000D	C	KERNEL32.dll
.rdata:004022E0	0000000D	C	ADVAPI32.dll
.rdata:004022FA	0000000B	C	MSVCRT.dll
.data:0040302C	00000011	C	SeDebugPrivilege
.data:00403040	0000000B	C	sfc_os.dll
.data:0040304C	00000016	C	\\system32\\wupdmgr.exe
.data:00403064	00000005	C	%s%s
.data:00403070	00000005	C	#101
.data:00403078	00000013	C	EnumProcessModules
.data:0040308C	0000000A	C	psapi.dll
.data:00403098	00000013	C	GetModuleBaseNameA
.data:004030AC	0000000A	C	psapi.dll
.data:004030B8	0000000E	C	EnumProcesses
.data:004030C8	0000000A	C	psapi.dll
.data:004030D4	00000016	C	\\system32\\wupdmgr.exe
.data:004030EC	00000005	C	%s%s
.data:004030F4	0000000B	C	\\winup.exe
.data:00403100	00000005	C	%s%s

好多奇怪的 dll 文件，如 sfc\_os.dll、psapi.dll 等，还有好多奇怪的 exe 文件，如 wupdmgr.exe、winup.exe，可作为特征判断是否被感染。

6、文件的资源段中还包含一个资源，使用 Resource Hacker 工具来检测，并提取资源，能发现什么

用 Resource Hacker 打开 Lab01-04.exe，检测资源



将资源文件保存，放入 IDA 中查看 string

Address	Length	Type	String
seg000:00000...	00000015	C	GetWindowsDirectoryA
seg000:00000...	00000008	C	WinExec
seg000:00000...	0000000D	C	GetTempPathA
seg000:00000...	0000000E	C	wnloadToFileA
seg000:00000...	00000016	C	system32\\wupdmgrd.exe
seg000:00000...	00000032	C	tp://www.practicalmalwareanalysis.com/updater.exe

可以发现 wupdmgrd.exe 和一个网址。

## 四、 实验心得

通过本次实验，熟悉了恶意代码分析的大致流程：

- 通过 VirusTotal，查看各种杀毒软件对一个恶意程序的分析结果，并分析综合判断是否为恶意软件，还可以查看文件的综合信息：各种 hash 值、时间戳、PE 文件结构、将此程序判定为恶意程序的沙盒的分析结果等；
- 利用 PEView 查看 PE 文件结构；
- 利用 PEiD 工具检查程序是否加壳；
- 利用 linuxerUnpacker 工具进行脱壳；
- 利用 IDA pro 查看输入表信息，通过导入的 API 函数分析程序功能；
- 通过 IDA pro 查看程序的 string，寻找程序的特征，利用特征判断主机是否被感染；
- 通过 Resource Hacker 查找并提取文件的资源段，进行下一步的分析。

许多工作可以用多种工具实现，比如查看输入表，既可以通过 VT 查看，也可以通过 IDA 查看，选择自己习惯的方式即可。

本次实验，掌握了各种小工具的使用，分析恶意代码的能力显著提高。