windows样本分析之基础静态分析

yong夜 / 2019-09-06 09:11:52 / 浏览数 3369 安全技术 二进制安全 顶(0) 踩(0)

---

title: windows样本分析之基础静态分析
date: 2019-09-01 15:35:19
tags: Windows病毒分析

目标

1.样本鉴定黑白

2.样本初步行为的判断

3.相关信息收集

原理

鉴黑白

特征码检测

检测已知病毒：通常杀毒软件将分析过的病毒中的特征部分提取成相应特征码（文件特征、字符特征、指令特征等）

启发检测

检测未知病毒：检测病毒运行过程中的API调用行为链。

初步型为判断

特征API

不同种类的病毒样本根据其特性总会调用一些特定的API函数

相关信息收集

- 编译时间：可以判断样本的出现的时间
- 文件类型：哪类文件，命令行或者界面或者其他
- 是否有网络行为
- 是否有关联文件
- 壳情况

算法流程

根据常用逆向工具来实现上述原理的检测

鉴黑白

文件特征检测

VirusTotal检测，可以看到是否已经有厂商对其惊醒了黑白判断(SHA-1搜索即可)

文件SHA-1/MD5 Google扫描，看是已有相关检测报告

字符特征检测

- strings/pestdio工具打印字符串。根据一些特征字符串Google搜索，如ip地址、敏感词句、API符号等

加壳/混淆判断

- PEID/DIE工具查看文件是否加壳
- strings判断。如果字符串数量稀少、存在LoadLibray少量API符号，可以对其留意

链接检测

- 运行时链接检测。恶意样本通常采用LoadLibray来运行是链接

样本初步行为判断

pestdio查看导入表的API调用和一些字符串信息，来进行判断

相关信息收集

收集样本相关信息，如果要详细分析，会用到

1. PEStudio查看文件头的时间戳
2. PEStudio查看文件头的文件类型
3. 查看导入表里的API和String表中的网络特征
4. 查看String表中的文件字符串
5. DIE/PEID查壳情况或者string表和api的一些特征

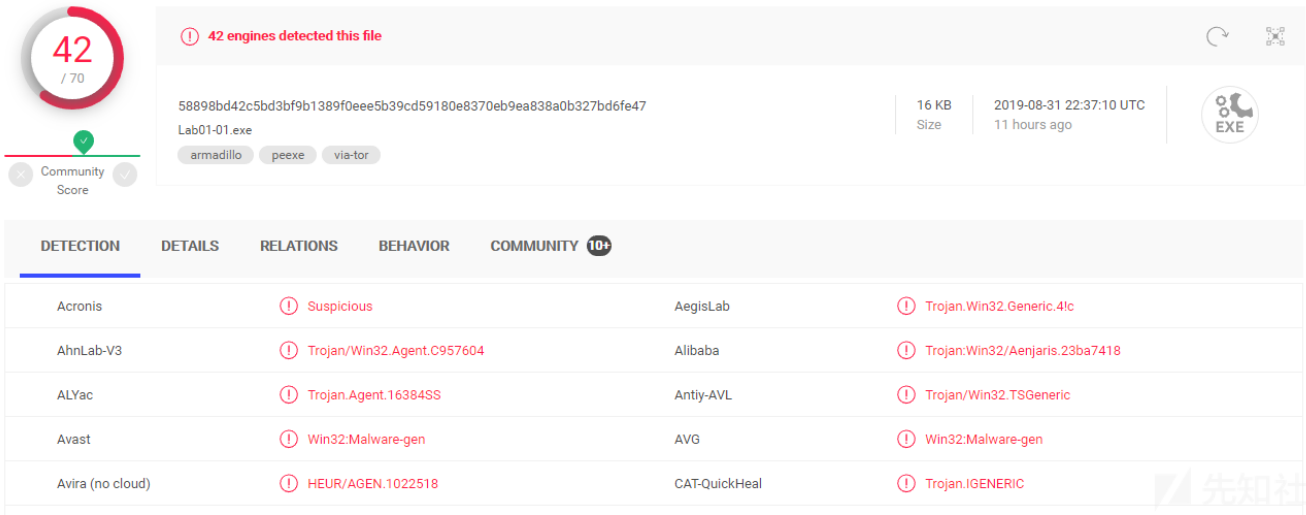
实践过程

样本：Lab01-01.exe

鉴黑白

- VT(virusTotal)扫描。

42/70的检出率，可以确认是病毒。后面几个检测就可以放到后面，收集样本信息的地方了



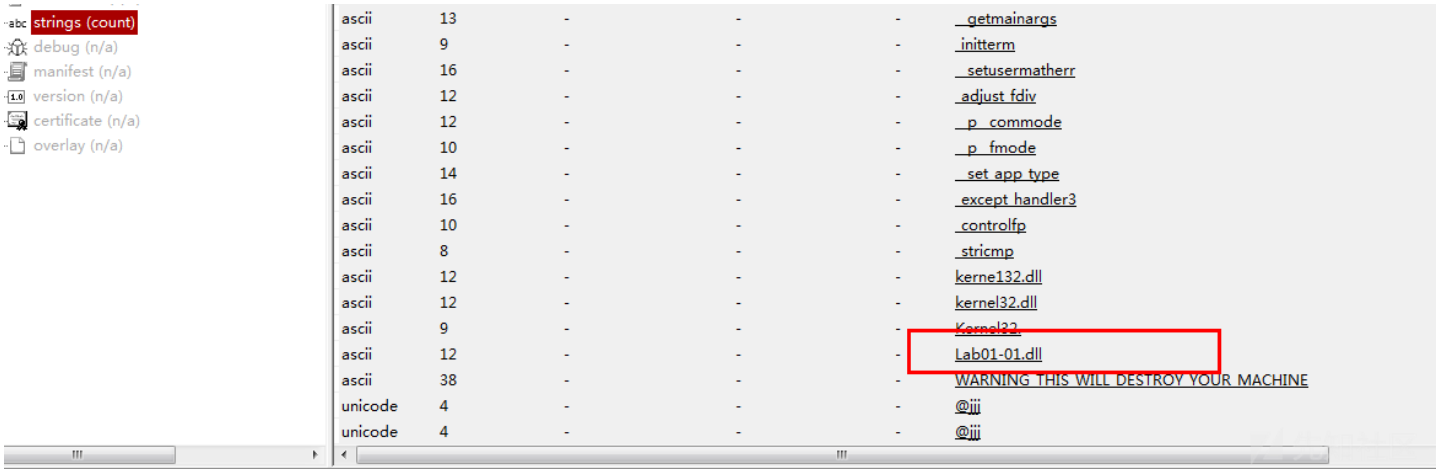
样本初步行为判断

从导入表方法中的信息，可以看出，`FindFirstFileA`■`FindNexFileA`很可能遍历文件，然后又copy文件，一般勒索会有遍历的操作，但是VT扫描后并没有Ransom这样

接着在strings表内发现`C:\*`■`.exe`这类字段，可以合理判断，可能实在c盘遍历exe文件

type (2)	size (b...	blacklist (9)	hint (5)	group (2)	value (69)
ascii	40	-	x	-	!This program cannot be run in DOS mode.
ascii	4	-	x	-	.exe
ascii	4	x	x	-	C:*
ascii	32	x	x	-	C:\windows\system32\kerne132.dll
ascii	32	x	x	-	C:\Windows\System32\Kernel32.dll
ascii	15	x	-	6	UnmapViewOfFile
ascii	13	x	-	6	MapViewOfFile
ascii	17	x	-	6	CreateFileMapping
ascii	10	-	-	6	CreateFile
ascii	9	x	-	6	FindClose
ascii	12	x	-	6	FindNextFile
ascii	13	x	-	6	FindFirstFile
ascii	8	-	-	6	CopyFile
ascii	12	-	-	5	IsBadReadPtr
ascii	6	-	-	5	malloc
ascii	5	-	-	-	Richm
ascii	5	-	-	-	.text
ascii	7	-	-	-	`.rdata
ascii	6	-	-	-	@.data
ascii	4	-	-	-	UVWj

接着查看字符串表，看见一个明显不是系统dll的Lab01-01.dll文件，但出现一个警示语，毁坏机器的提示，结合前面遍历复制文件，难道是要复制文件占满磁盘、资源之类的



下面这个是被我忽略了的一个细节，两个DLL很像，但仔细看会发现其中一个是kernel132.dll，他将字母换成数字来混淆视线，所以根据上面出现的dll，合理推想是可能是

ascii	4	-	x	-	.exe
ascii	4	x	x	-	C:*
ascii	32	x	x	-	C:\windows\system32\kerne132.dll
ascii	32	x	x	-	C:\Windows\System32\Kernel32.dll
ascii	15	x	-	6	UnmapViewOfFile

小结

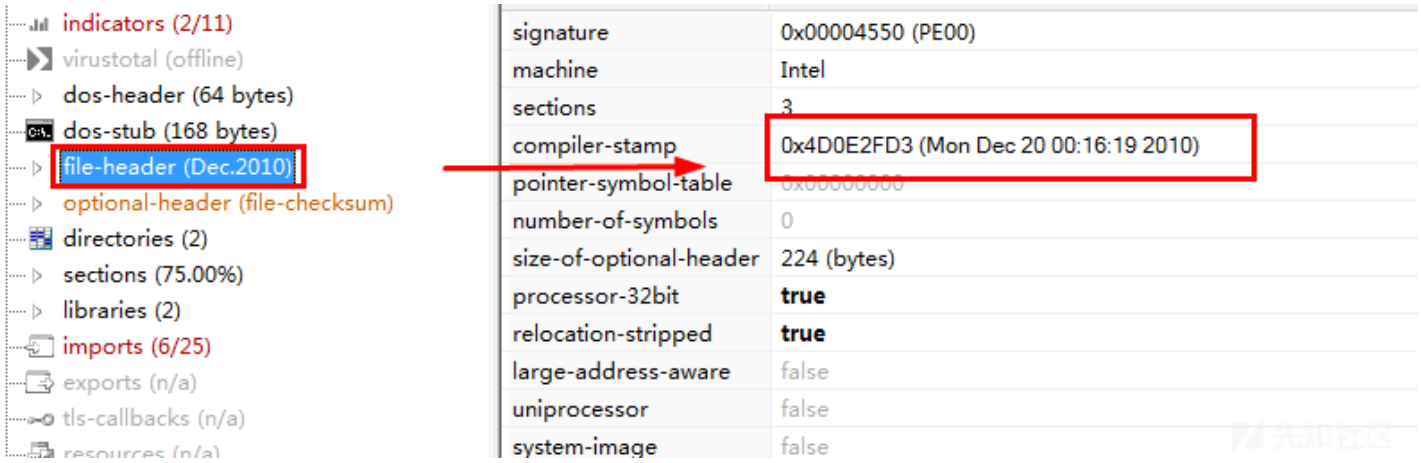
有文件遍历和复制文件的操作，和一个非系统Dll文件，有可能是将这个文件复制到哪里，虽然这里没有看见加载这个dll的操作，但是可以合理怀疑会有其他没发现的行为来

行为暂时分析到这，下面分析这个dll文件和文件操作的相关行为来继续进行分析工作

相关信息收集

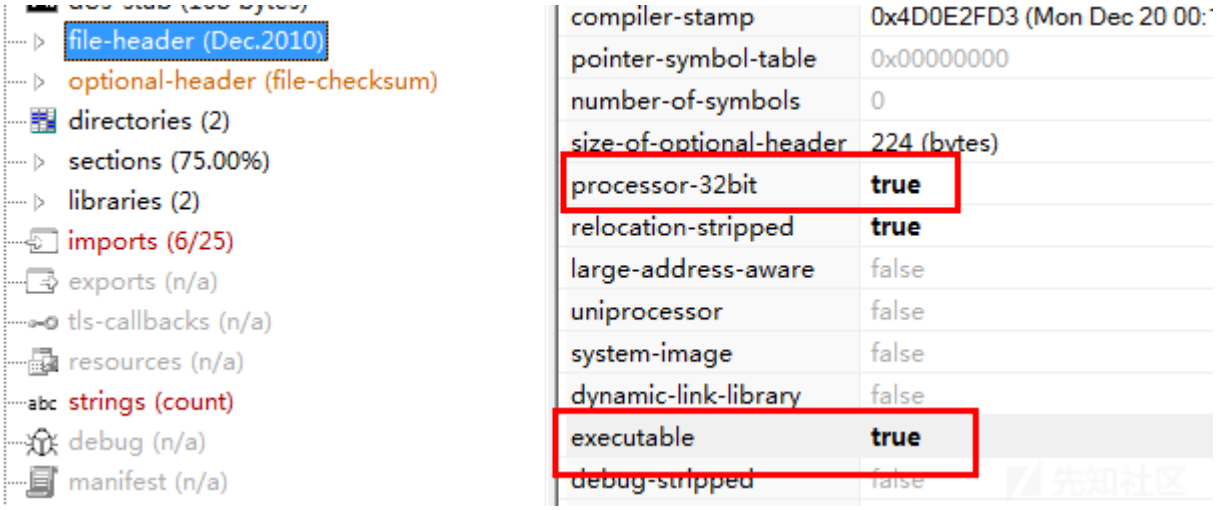
- 编译时间

2010年，年代久远的老样本



- 文件类型

32位可执行文件



- 导入表和String表

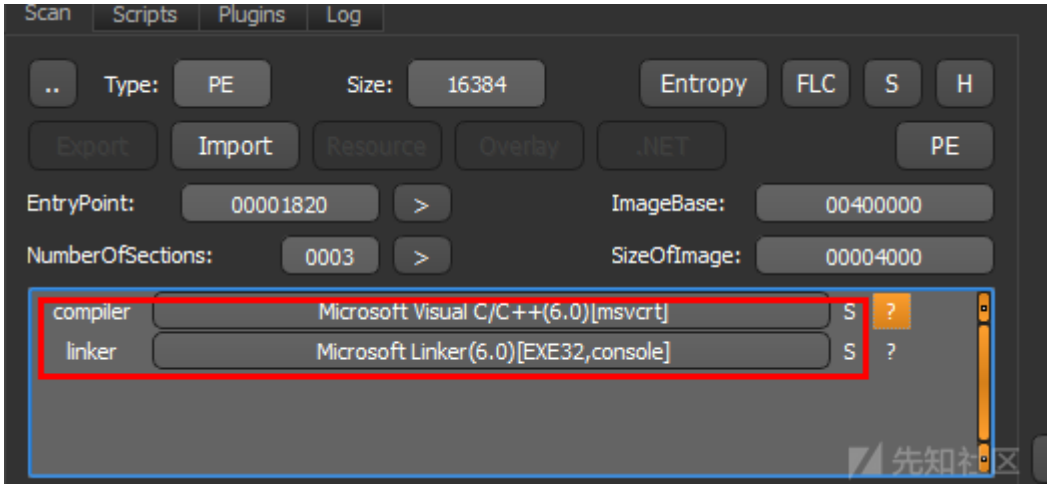
未有网络特征

- string表内字符串

有一句警示语，意思破坏机器行为，但并未发现相关API，或者说根据之前分析，疑似想占满磁盘、资源等无聊行为

- 壳信息

查壳工具未查出相关特征



导入表中函数和字符串表的字符还是挺多的，并未出现LoadLibray等脱壳API，排除加壳行为

ior	name (25)	group (2)	anonymous (0)	type (1)	hint (6)	anti-debug (0)	undocumented (0)	deprecated (2)	lib
	UnmapViewOfFile	6	-	implicit	x	-	-	-	ke
	MapViewOfFile	6	-	implicit	x	-	-	-	ke
	CreateFileMappingA	6	-	implicit	x	-	-	-	ke
	CreateFileA	6	-	implicit	-	-	-	-	ke
	FindClose	6	-	implicit	x	-	-	-	ke
	FindNextFileA	6	-	implicit	x	-	-	-	ke
	FindFirstFileA	6	-	implicit	x	-	-	-	ke
	CopyFileA	6	-	implicit	-	-	-	-	ke
	IsBadReadPtr	5	-	implicit	-	-	-	x	ke
	malloc	5	-	implicit	-	-	-	-	m
	CloseHandle	-	-	implicit	-	-	-	-	ke
	exit	-	-	implicit	-	-	-	-	m
	_exit	-	-	implicit	-	-	-	-	m
	_XcptFilter	-	-	implicit	-	-	-	-	m
	__p__initenv	-	-	implicit	-	-	-	-	m
	__getmainargs	-	-	implicit	-	-	-	-	m
	_initterm	-	-	implicit	-	-	-	-	m
	__setusermatherr	-	-	implicit	-	-	-	-	m
	_adjust_fdiv	-	-	implicit	-	-	-	-	m
	__p__commode	-	-	implicit	-	-	-	-	m
	__p__fmode	-	-	implicit	-	-	-	-	m
	__set_app_type	-	-	implicit	-	-	-	-	m
	_except_handler3	-	-	implicit	-	-	-	-	m
	_controlfp	-	-	implicit	-	-	-	x	m
	_stricmp	-	-	implicit	-	-	-	-	m

小结

本exe文件暂时静态分析完毕，后面需要结合dll文件来综合进行下面的分析

参考

【1】恶意样本分析实战