windows样本分析之基础静态分析-三

yong夜 / 2019-09-10 08:54:01 / 浏览数 2371 安全技术 二进制安全 顶(0) 踩(0)

目标

1.样本鉴定黑白

2.样本行为粗略判断

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。

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

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

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

1. 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
2. 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
3. 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
4. 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

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. DIE/PEID查壳情况或者string表和api的一些特征

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

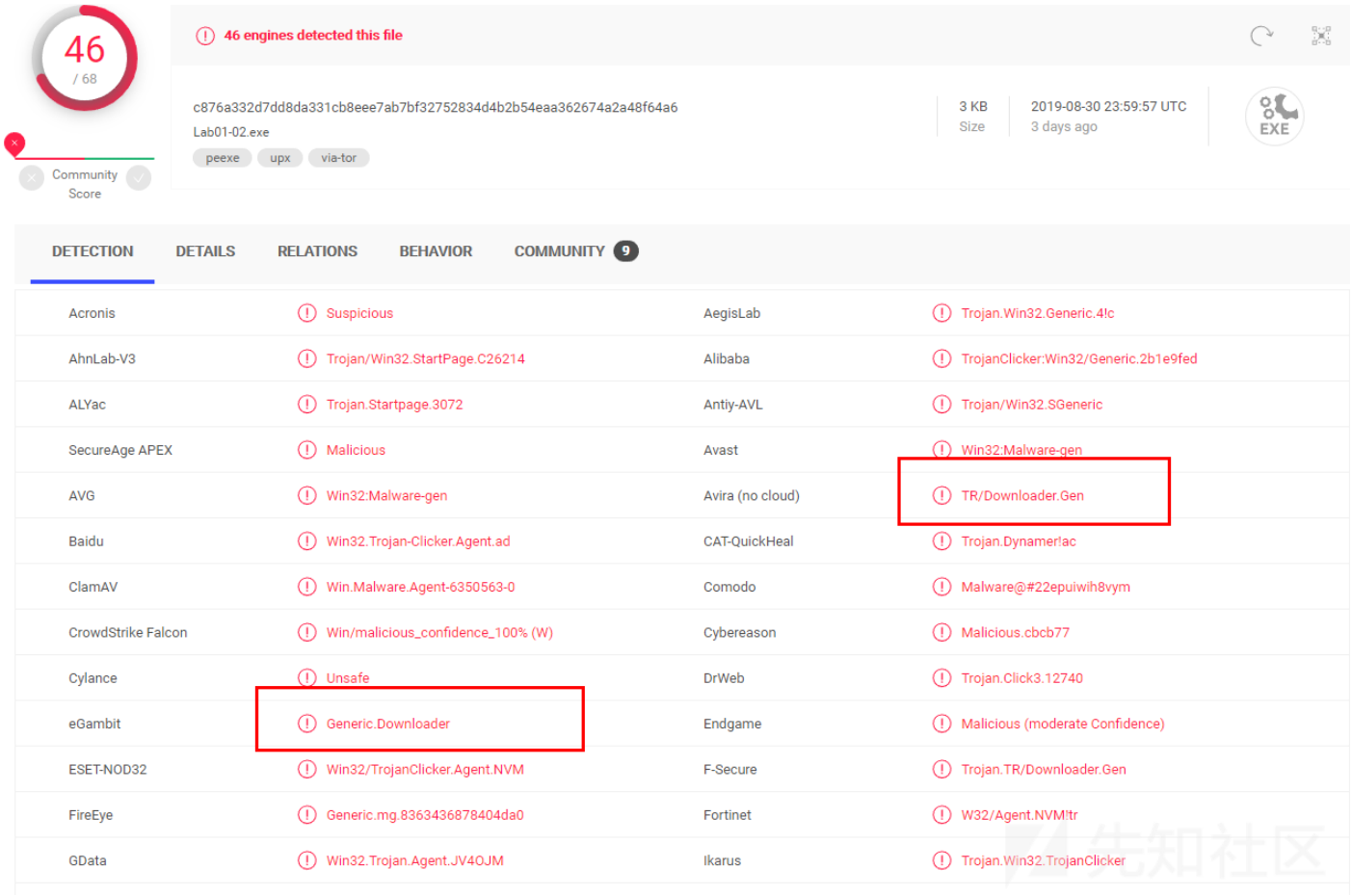
实践过程

样本：Lab01-02.exe

鉴黑白

46/68的检出率，确定为病毒。

并且根据检测结果有可能是下载者



信息收集

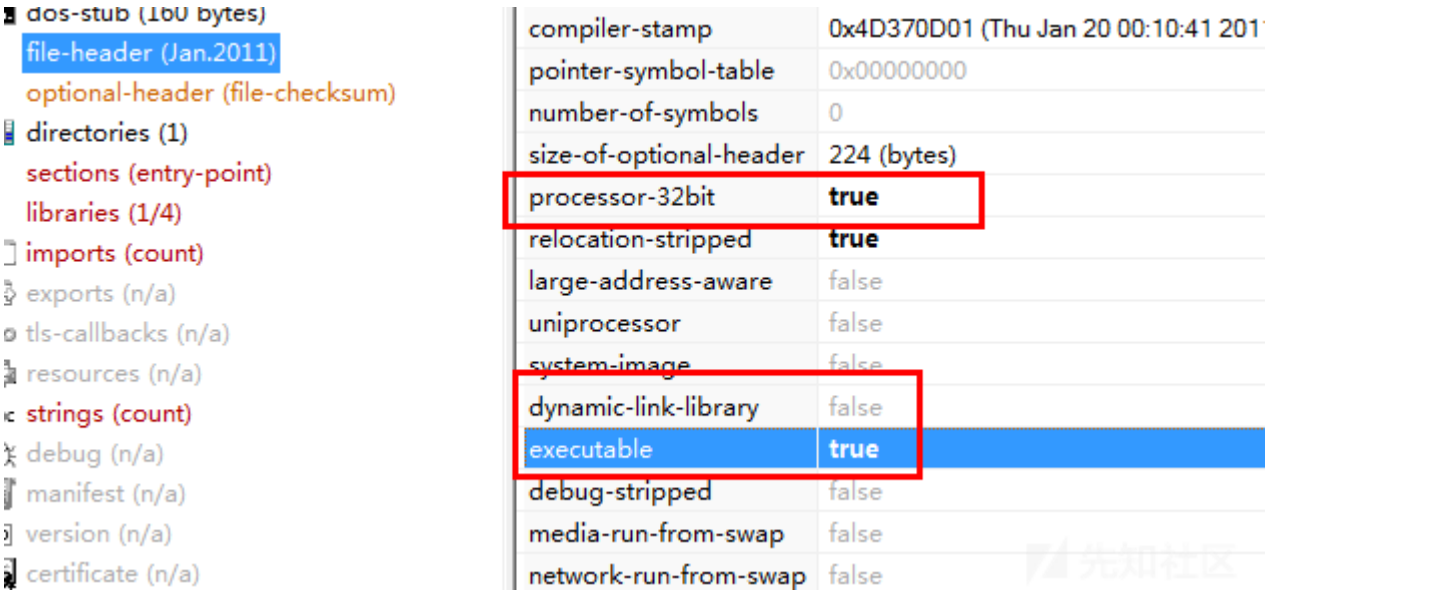
- 时间戳

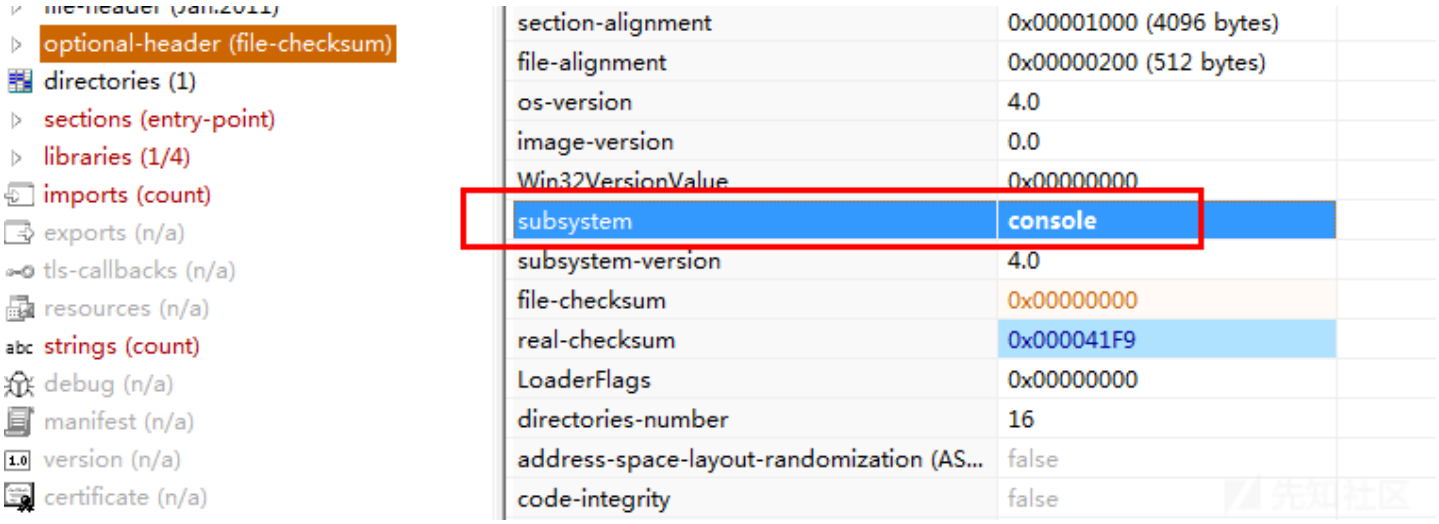
老样本了

```
Thu Jan 20 00:10:41 2011
```

- 文件类型

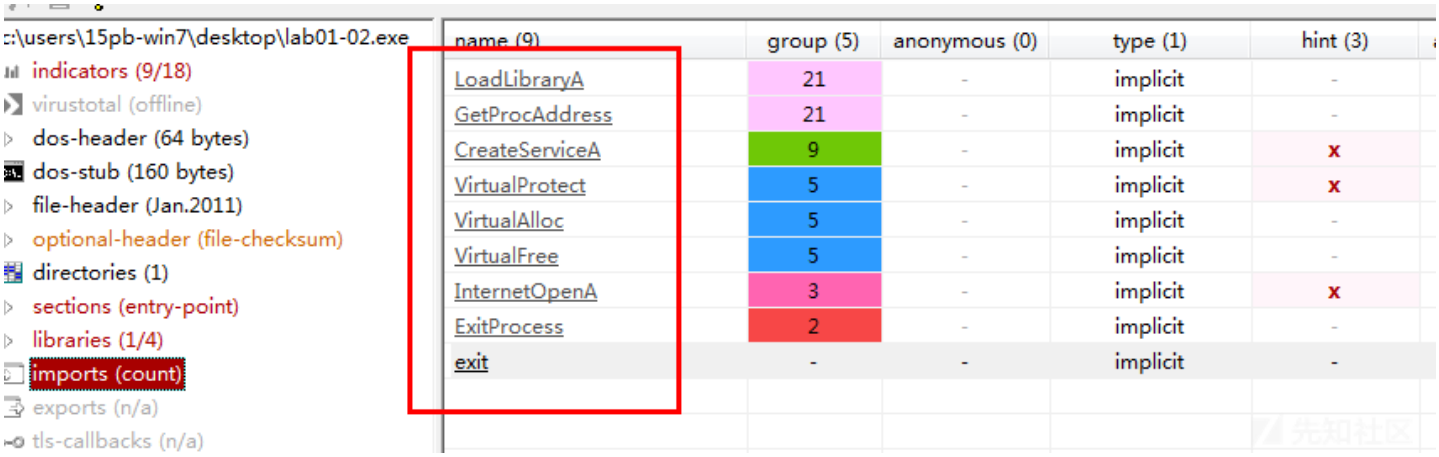
32位命令行型可执行文件





- 壳信息

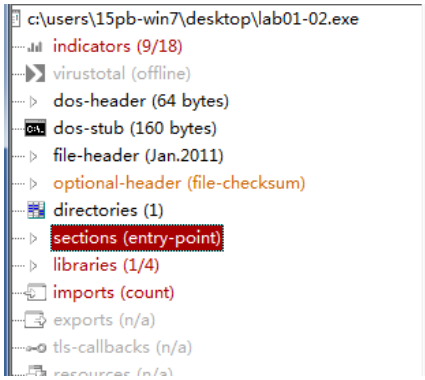
导入函数很少，有LoadLibray函数，而主机感染类函数和网络感染函数，应该是加壳了



字符串中出现经典壳UPX的字样，并且一般这个壳都会有自己独特的段，确认进行了UPX加壳

type (1)	size (b...	blacklist (6)	hint (1)	group (5)	value (47)
ascii	40	-	x	-	!This program cannot be run in DOS mode.
ascii	11	-	-	21	LoadLibrary
ascii	14	-	-	21	GetProcAddress
ascii	13	x	-	9	CreateService
ascii	14	x	-	5	VirtualProtect
ascii	12	-	-	5	VirtualAlloc
ascii	11	-	-	5	VirtualFree
ascii	11	-	-	3	WININET.dll
ascii	12	x	-	3	InternetOpen
ascii	11	-	-	2	ExitProcess
ascii	4	-	-	-	Rich
ascii	4	x	-	-	UPX0
ascii	4	x	-	-	UPX1
ascii	4	x	-	-	UPX2
ascii	4	-	-	-	3.04
ascii	4	-	-	-	UPX!
ascii	4	-	-	-	a\`Y
ascii	4	-	-	-	(23h
ascii	10	-	-	-	MalService
ascii	7	-	-	-	sHGL345
ascii	8	-	-	-	http://w

先知社区



property	value	value	value
name	UPX0	UPX1	UPX2
md5	n/a	AD0F236C2B34F1031486...	F998D25F473E69CC89BF4...
entropy	n/a	7.067	2.798
file-ratio (66.67%)	n/a	50.00 %	16.67 %
raw-address	0x00000400	0x00000400	0x00000A00
raw-size (2048 bytes)	0x00000000 (0 bytes)	0x00000600 (1536 bytes)	0x00000200 (512 bytes)
virtual-address	0x00401000	0x00405000	0x00406000
virtual-size (24576 bytes)	0x00004000 (16384 bytes)	0x00001000 (4096 bytes)	0x00001000 (4096 bytes)
entry-point	-	0x00005410	-
writable	x	x	x
executable	x	x	-
shareable	-	-	-

既然是UPX，那么就可以直接用网上的脱壳器直接脱壳得到原始EXE文件，然后直接进入行为的初步判断

样本初步行为判断

- 主机行为

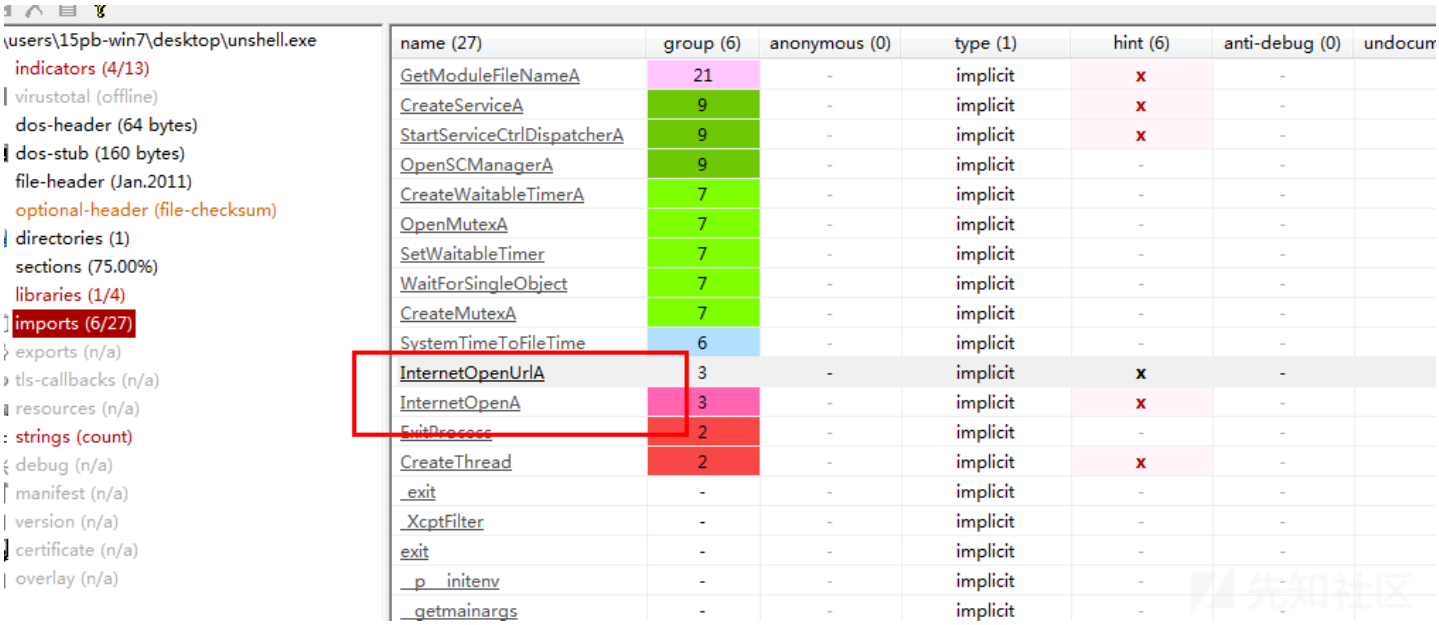
有创建服务的API，字符串种有铭感字段`MalService`，可能是服务名称，可能主要做一些长期驻留的目的

name (27)	group (6)	anonymous (6)	type (1)	hint (6)
GetModuleFileNameA	21	-	implicit	x
CreateServiceA	9	-	implicit	x
StartServiceCtrlDispatcherA	9	-	implicit	x
OpenSCManagerA	9	-	implicit	-
CreateWaitableTimerA	7	-	implicit	-
OpenMutexA	7	-	implicit	-
SetWaitableTimer	7	-	implicit	-
WaitForSingleObject	7	-	implicit	-
CreateMutexA	7	-	implicit	-
SystemTimeToFileTime	6	-	implicit	-
InternetOpenUrlA	3	-	implicit	x

	10	-	-	-	__p__fmode
	14	-	-	-	__set_app_type
	16	-	-	-	_except_handler3
	10	-	-	-	_controlfp
	10	-	-	-	MalService
	10	-	-	-	Malservice
	6	-	-	-	HGL345
	21	-	-	-	Internet Explorer 8.0

- 网络行为

选中区域很明显的网络访问请求，接着下面字符串信息可以知道可能对http://www.malwareanalysisbook.com链接有访问请求



name (27)	group (6)	anonymous (0)	type (1)	hint (6)	anti-debug (0)	undocum
GetModuleFileNameA	21	-	implicit	x	-	
CreateServiceA	9	-	implicit	x	-	
StartServiceCtrlDispatcherA	9	-	implicit	x	-	
OpenSCManagerA	9	-	implicit	-	-	
CreateWaitableTimerA	7	-	implicit	-	-	
OpenMutexA	7	-	implicit	-	-	
SetWaitableTimer	7	-	implicit	-	-	
WaitForSingleObject	7	-	implicit	-	-	
CreateMutexA	7	-	implicit	-	-	
SystemTimeToFileTime	6	-	implicit	-	-	
InternetOpenUrlA	3	-	implicit	x	-	
InternetOpenA	3	-	implicit	x	-	
ExitProcess	2	-	implicit	-	-	
CreateThread	2	-	implicit	x	-	
_exit	-	-	implicit	-	-	
_XcptFilter	-	-	implicit	-	-	
exit	-	-	implicit	-	-	
__p__initenv	-	-	implicit	-	-	
__getmainargs	-	-	implicit	-	-	

pe (2)	size (b...	blacklist (6)	hint (2)	group (6)	value (56)
ascii	40	-	x	-	!This program cannot be run in DOS mode.
ascii	34	-	x	-	http://www.malwareanalysisbook.com
ascii	17	x	-	21	GetModuleFileName
ascii	13	x	-	9	CreateService

小结

分析流程做了调整，鉴定黑板完成后，如果是黑样本，做简单分析的话，先做信息收集，然后根据信息对样本有个大致概念，后简单分析前的准备，接着开始简单分析。

这个样本主要进行了加壳隐藏，可能会有创建服务来进行长期的网络访问活动或其他的，具体可能会对http://www.malwareanalysisbook.com进行访问，具体情况需要后面

点击收藏 | 0 关注 | 1
上一篇：BurpSuite插件 - Au... 下一篇：从某cmsV4.1.0 sql注入...
1. 0 条回复
- 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

目录