

---

## 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

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

### 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. 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.dll

鉴黑白

33/68的检出率，是黑样本

33 / 68

Community Score

33 engines detected this file

f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba

Lab01-01.dll

armadillo pedli via-tor

160 KB

Size

2019-09-01 14:47:44 UTC

21 hours ago

DLL

| DETECTION | DETAILS                       | RELATIONS        | COMMUNITY 10+            |
|-----------|-------------------------------|------------------|--------------------------|
| Acronis   | Suspicious                    | AegisLab         | Trojan.Win32.Generic.4tc |
| Alibaba   | Trojan:Win32/Generic.1594ec0f | ALYac            | Trojan.Agent.Waski       |
| Antiy-AVL | Trojan/Win32.BTSGeneric       | Avast            | Win32.Malware-gen        |
| AVG       | Win32.Malware-gen             | Avira (no cloud) | TR/Dldr.Waski.163840.1   |

样本初步行为判断

导入表

可以看到一下函数，出现了网络通信、开启进程等操作

- CreateMutexA\OpenMutexA，创建打开互斥体，防止进程多开
- socket、send、connect、recv等函数，进行网络socket通信，有可能是发送数据、接收命令，很明显的后门通信行为
- createProcessA，创建进程。

indicators (5/15)  
virusotal (offline)  
dos-header (64 bytes)  
dos-stub (160 bytes)  
file-header (Dec.2010)  
optional-header (file-checksum)  
directories (invalid)  
sections (97.50%)  
libraries (1/3)  
imports (11/20)  
exports (n/a)  
tls-callbacks (n/a)  
resources (n/a)  
strings (count)  
debug (n/a)  
manifest (n/a)  
version (n/a)  
certificate (n/a)  
overlay (n/a)

|                  |   |   |          |   |   |   |   |              |
|------------------|---|---|----------|---|---|---|---|--------------|
| CreateMutexA     | 7 | - | implicit | - | - | - | - | kernel32.dll |
| OpenMutexA       | 7 | - | implicit | - | - | - | - | kernel32.dll |
| malloc           | 5 | - | implicit | - | - | - | - | msvcrt.dll   |
| 23 (socket)      | 3 | x | implicit | x | - | - | - | ws2_32.dll   |
| 115 (WSAStartup) | 3 | x | implicit | x | - | - | - | ws2_32.dll   |
| 11 (inet_addr)   | 3 | x | implicit | x | - | - | - | ws2_32.dll   |
| 4 (connect)      | 3 | x | implicit | x | - | - | - | ws2_32.dll   |
| 19 (send)        | 3 | x | implicit | x | - | - | - | ws2_32.dll   |
| 22 (shutdown)    | 3 | x | implicit | x | - | - | - | ws2_32.dll   |
| 16 (recv)        | 3 | x | implicit | x | - | - | - | ws2_32.dll   |
| 3 (closesocket)  | 3 | x | implicit | x | - | - | - | ws2_32.dll   |
| 116 (WSACleanup) | 3 | x | implicit | x | - | - | - | ws2_32.dll   |
| 9 (htons)        | 3 | x | implicit | x | - | - | - | ws2_32.dll   |
| Sleep            | 2 | - | implicit | - | - | - | - | kernel32.dll |
| CreateProcessA   | 2 | - | implicit | x | - | - | - | kernel32.dll |
| CloseHandle      | - | - | implicit | - | - | - | - | kernel32.dll |
| _adjust_fdiv     | - | - | implicit | - | - | - | - | msvcrt.dll   |
| _initterm        | - | - | implicit | - | - | - | - | msvcrt.dll   |
| free             | - | - | implicit | - | - | - | - | msvcrt.dll   |
| strncmp          | - | - | implicit | - | - | - | - | msvcrt.dll   |

字符串表

出了刚才分析的行为，这里出现了：

- IP地址，可以Google或VT查一下，可以查到相关信息
- exec，命令执行的字段，结合上面网络通信，可能是接收命令并执行的后门操作

| type (1) | size (b... | blacklist (1) | hint (3) | group (4) | value (36)                               |
|----------|------------|---------------|----------|-----------|--|
| ascii    | 40         | -             | x        | -         | !This program cannot be run in DOS mode. |
| ascii    | 4          | -             | x        | -         | exec                                     |
| ascii    | 13         | -             | x        | -         | 127.26.152.13                            |
| ascii    | 11         | -             | -        | 7         | CreateMutex                              |
| ascii    | 9          | -             | -        | 7         | OpenMutex                                |
| ascii    | 6          | -             | -        | 5         | malloc                                   |
| ascii    | 10         | -             | -        | 3         | WS2_32.dll                               |
| ascii    | 5          | -             | -        | 2         | Sleep                                    |
| ascii    | 13         | x             | -        | 2         | CreateProcess                            |
| ascii    | 5          | -             | -        | 2         | sleep                                    |
| ascii    | 4          | -             | -        | -         | Rich                                     |
| ascii    | 5          | -             | -        | -         | .text                                    |

小结

- 1.初步判断该dll有后门操作，接收127.26.152.13地址的命令，并执行
- 2.进程创建，暂时不清楚

相关信息收集

- 编译时间

这里的小技巧是，根据两个文件编译时间也可以推测是一个代码包的文件，可以用来大概区分是作者自己编写的代码还是调用开源的或其他的

Mon Dec 20 00:16:38 2010

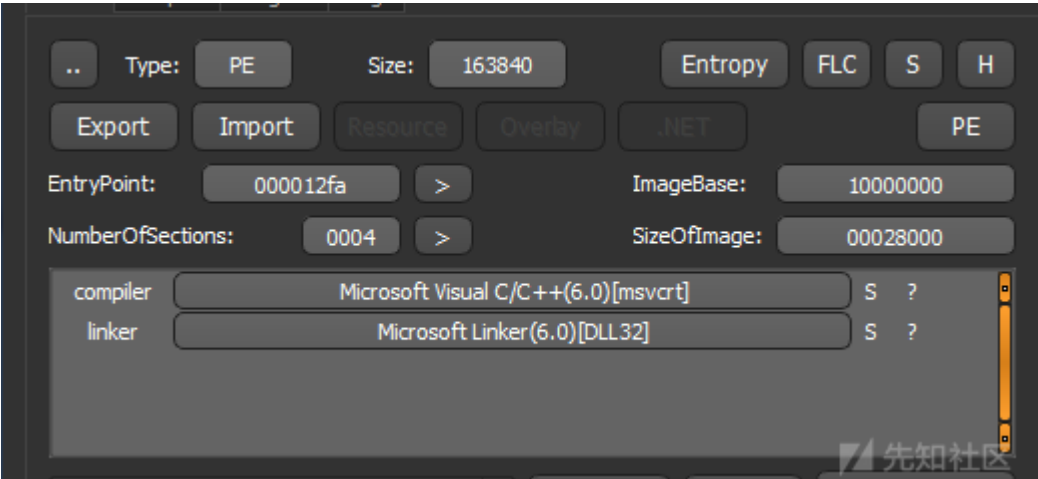
- 文件类型

DLL动态链接库

- 壳信息

从上面导入表的函数可以看出，是没加壳的，要不然就不会暴露网络操作的API了

当然也可以用工具在下个实锤



小结

大致从socket通信函数可以看出后门操作，初步断定是个可能是后门DLL。

前面的exe应该是用来启动和隐藏该DLL的，这里没有看出的是createProcess和sleep函数也是明显的后门常用的API，后面可以写个demo版后门巩固相关API调用

点击收藏 | 0 关注 | 1

[上一篇：利用USB外设实现命令注入](#) [下一篇：Playing with Wind...](#)

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

---

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)