

目标

- 鉴定黑白(静态分析失败或者不准确的第二步)
- 简单行为分析

原理

监控样本的行为。

手动双击击执行或者输入一些命令参数来运行样本，通过监控工具来抓取样本的行为

通过沙箱监控样本运行的行为

判定样本黑白

- 根据样本行为和衍生物来判断样本的性质

算法流程

1.简单静态分析流程

2.沙箱分析。通过开源在线沙箱或者本地沙箱进行初步行为获取

2.手动分析

实践过程1

Lab03-01.exe

鉴黑白

简单静态分析

假设我们未从VT上判断出文件黑白，我们从他的其他信息和行为中找线索

字符串检测

HTTP请求

根据CONNECT %s:%i HTTP/1.0\r\n\r\n和www.practicalmalwareanalysis.com字符特征，可以判断样本访问该站点

程序自启动

SOFTWARE\Classes\http\shell\open\commandV，http协议的默认处理程序，一旦进行http协议请求，就执行该程序

Software\Microsoft\Active Setup\Installed Components\，检测是否为安装的组件如果没有则进行启动该程序

SOFTWARE\Microsoft\Windows\CurrentVersion\Run开机自启动选项

隐藏自身






vmx32to64.exe，伪装成正常程序

其他

SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders，将程序放入开始菜单

ascii	40	-	x	-	This program cannot be run in DOS mode.
ascii	30	-	x	-	CONNECT %s:%i HTTP/1.0\r\n\r\n
ascii	41	-	x	-	SOFTWARE\Classes\http\shell\open\commandV
ascii	53	-	x	-	Software\Microsoft\Active Setup\Installed Components\
ascii	33	-	x	-	www.practicalmalwareanalysis.com
ascii	13	-	x	-	vmx32to64.exe
ascii	45	-	x	-	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
ascii	64	-	x	-	SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
ascii	11	-	-	2	ExitProcess
ascii	4	-	-	-	Rich
ascii	5	-	-	-	.text
ascii	6	-	-	-	data

- 加壳/混淆判断

- indicators (3/11)
- ▶ virustotal (offline)
- ▶ dos-header (64 bytes)
- **▶ dos-stub (112 bytes)**
- ▶ file-header (Jan.2008)
- ▶ optional-header (GUI)
-  directories (2)
- ▶ sections (92.86%)
- ▶ libraries (count)
- **▶ imports (count)**
-  exports (n/a)
-  tls-callbacks (n/a)
-  resources (n/a)
- abc strings (count)
-  debug (n/a)

PEiD扫描得出壳类型:PEncrypt 3.1 Final -> junkcode

小结

原因：

简答行为分析

可以从VT上的BEHAVIOR选项中看到沙箱跑出的数据

← → ↻ <https://www.virustotal.com/gui/file/eb84360ca4e33b8bb60df47ab5ce962501ef3420bc7aab90655fd507d2ffcedd/behavior/Lastline>

应用 Google Analysis TOOLS Query Information 赛题 安全资讯 TOOLS 开发 安全 360企业安全 Cyber 样本源 MachineLear

eb84360ca4e33b8bb60df47ab5ce962501ef3420bc7aab90655fd507d2ffcedd

68
/ 70

Community Score

68 engines detected this file

eb84360ca4e33b8bb60df47ab5ce962501ef3420bc7aab90655fd507d2ffcedd
Lab03-01.exe
peexe via-tor

7 KB
Size

2019
8 hou

DETECTION DETAILS RELATIONS **BEHAVIOR** COMMUNITY 10+

Lastline

Network Communication

主机感染行为

主要设置了开机自启动的注册表键值

- 还有疑似隐藏自己到C:\Users\Olivia\AppData\Local\Temp\KeJsFBhovilbosu8hR1K.exe这里的可能
- 互斥量WinVMX32来防止程序多开

Registry Keys Set

+ HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN

开机自启动注册表

Process And Service Actions

Processes Created

C:\DOCUME~1\Miller\LOCALS~1\Temp\Lab03-01.exe
C:\Users\Olivia\AppData\Local\Temp\KeJsFBhovilbosu8hR1K.exe

Shell Commands

C:\DOCUME~1\Miller\LOCALS~1\Temp\Lab03-01.exe
C:\Users\Olivia\AppData\Local\Temp\KeJsFBhovilbosu8hR1K.exe

Processes Tree

1316 - C:\DOCUME~1\Miller\LOCALS~1\Temp\Lab03-01.exe
1612 - C:\Users\Olivia\AppData\Local\Temp\KeJsFBhovilbosu8hR1K.exe

Synchronization Mechanisms & Signals

Mutexes Created

WinVMX32
Local\SM0:1612:168:WilStaging_02

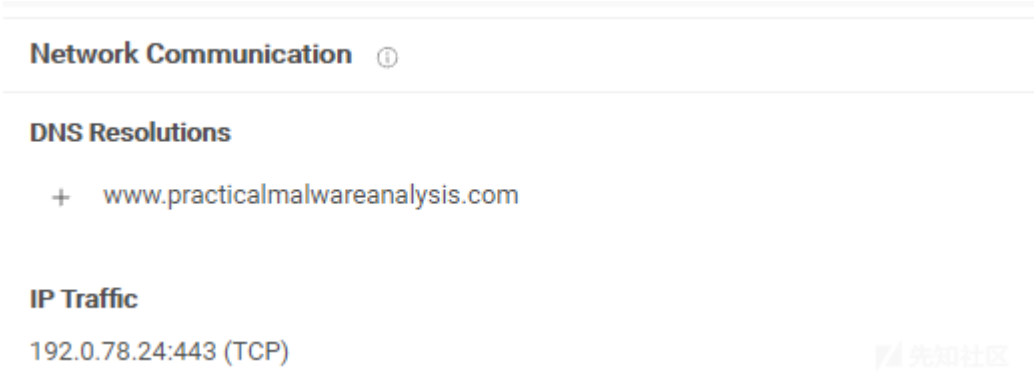
Mutexes Opened

Local\ShimViewer

Modules Loaded

可能是隐藏自身程序到临时目录

网络感染行为



小结

因为程序在分析机上未能正常运行，所以只能根据在线沙箱以前的分析数据和简单静态分析进行总结。

- 1.添加开机自启动来运行自身
- 2.修改文件名和存放目录来隐藏自己
- 3.跟远程服务器通信

实践过程2

Lab03-04.exe

直接进入行为分析

简单行为分析

沙箱分析

通过VT上的瑞星沙箱，和HyBrid沙箱

主机感染行为

- 删除文件
- 修改Internet选项，添加信任站点

Files Opened

\\?\MountPointManager
\\?\NUL
C:\

Files Deleted

C:\analyse\1556503968.847145_1a7b9e56-b39c-4347-836a-bef81ab95538
C:\analyse\155650~1.847

删除文件

Registry Actions

Registry Keys Set

- + HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect
- + HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet

添加可信任站点

Process And Service Actions

Processes Created

C:\Windows\System32\cmd.exe

创建cmd进程执行删除文件操作

Shell Commands

"C:\Windows\System32\cmd.exe" /c del c:\analyse\155650~1.847 >> NUL

\\?\C:\Windows\system32\conhost.exe



网络感染行为

- C2通信(88.221.52.75)
- 网页访问 (216.58.205.238)

Contacted Hosts

Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
216.58.205.238	80 TCP	-	United States
88.221.52.75	49167 TCP	-	European Union



手动分析

- 样本自删除

手动执行后，样本消失，根据沙箱检测出的删除命令，排除样本移动到其他目录的可能

Time	Process Name	PID	Operation	Path
21:5...	Lab03-04.exe	3192	CreateFile	C:\Windows\Prefetch\LAB03-04.EXE-D06517BB.pf
21:5...	Lab03-04.exe	3192	QueryStandardInformationFile	C:\Windows\Prefetch\LAB03-04.EXE-D06517BB.pf
21:5...	Lab03-04.exe	3192	ReadFile	C:\Windows\Prefetch\LAB03-04.EXE-D06517BB.pf
21:5...	Lab03-04.exe	3192	CloseFile	C:\Windows\Prefetch\LAB03-04.EXE-D06517BB.pf
21:5...	Lab03-04.exe	3192	CreateFile	C:
21:5...	Lab03-04.exe	3192	QueryInformationVolume	C:
21:5...	Lab03-04.exe	3192	FileSystemControl	C:
21:5...	Lab03-04.exe	3192	CreateFile	C:\ProgramData
21:5...	Lab03-04.exe	3192	SetBasicInformationFile	C:\ProgramData
21:5...	Lab03-04.exe	3192	QueryFileInternalInformati...	C:\ProgramData
21:5...	Lab03-04.exe	3192	FileSystemControl	C:\ProgramData
21:5...	Lab03-04.exe	3192	CloseFile	C:\ProgramData
21:5...	Lab03-04.exe	3192	CreateFile	C:\ProgramData\Microsoft
21:5...	Lab03-04.exe	3192	SetBasicInformationFile	C:\ProgramData\Microsoft
21:5...	Lab03-04.exe	3192	QueryFileInternalInformati...	C:\ProgramData\Microsoft
21:5...	Lab03-04.exe	3192	FileSystemControl	C:\ProgramData\Microsoft
21:5...	Lab03-04.exe	3192	CloseFile	C:\ProgramData\Microsoft
21:5...	Lab03-04.exe	3192	CreateFile	C:\ProgramData\Microsoft\Windows
21:5...	Lab03-04.exe	3192	SetBasicInformationFile	C:\ProgramData\Microsoft\Windows
21:5...	Lab03-04.exe	3192	QueryFileInternalInformati...	C:\ProgramData\Microsoft\Windows
21:5...	Lab03-04.exe	3192	FileSystemControl	C:\ProgramData\Microsoft\Windows
21:5...	Lab03-04.exe	3192	CloseFile	C:\ProgramData\Microsoft\Windows
21:5...	Lab03-04.exe	3192	CreateFile	C:\ProgramData\Microsoft\Windows\Caches
21:5...	Lab03-04.exe	3192	SetBasicInformationFile	C:\ProgramData\Microsoft\Windows\Caches
21:5...	Lab03-04.exe	3192	QueryFileInternalInformati...	C:\ProgramData\Microsoft\Windows\Caches
21:5...	Lab03-04.exe	3192	FileSystemControl	C:\ProgramData\Microsoft\Windows\Caches
21:5...	Lab03-04.exe	3192	CloseFile	C:\ProgramData\Microsoft\Windows\Caches
21:5...	Lab03-04.exe	3192	CreateFile	C:\Users
21:5...	Lab03-04.exe	3192	SetBasicInformationFile	C:\Users
21:5...	Lab03-04.exe	3192	QueryFileInternalInformati...	C:\Users
21:5...	Lab03-04.exe	3192	FileSystemControl	C:\Users
21:5...	Lab03-04.exe	3192	CloseFile	C:\Users
21:5...	Lab03-04.exe	3192	CreateFile	C:\Users\15pb-win7
21:5...	Lab03-04.exe	3192	SetBasicInformationFile	C:\Users\15pb-win7
21:5...	Lab03-04.exe	3192	QueryFileInternalInformati...	C:\Users\15pb-win7
21:5...	Lab03-04.exe	3192	FileSystemControl	C:\Users\15pb-win7
21:5...	Lab03-04.exe	3192	CloseFile	C:\Users\15pb-win7
21:5...	Lab03-04.exe	3192	CreateFile	C:\Users\15pb-win7\AppData
21:5...	Lab03-04.exe	3192	SetBasicInformationFile	C:\Users\15pb-win7\AppData
21:5...	Lab03-04.exe	3192	QueryFileInternalInformati...	C:\Users\15pb-win7\AppData
21:5...	Lab03-04.exe	3192	FileSystemControl	C:\Users\15pb-win7\AppData
21:5...	Lab03-04.exe	3192	CloseFile	C:\Users\15pb-win7\AppData
21:5...	Lab03-04.exe	3192	CreateFile	C:\Users\15pb-win7\AppData\Local
21:5...	Lab03-04.exe	3192	SetBasicInformationFile	C:\Users\15pb-win7\AppData\Local
21:5...	Lab03-04.exe	3192	QueryFileInternalInformati...	C:\Users\15pb-win7\AppData\Local
21:5...	Lab03-04.exe	3192	FileSystemControl	C:\Users\15pb-win7\AppData\Local

根据沙箱的数据，可以在Process Monitor中进程监控里看见cmd进程的创建来执行自删除指令

Event	Process	Stack
Date:	2019/9/7 21:54:58.4643112	
Thread:	2024	
Class:	Process	
Operation:	Process Create	
Result:	SUCCESS	
Path:	C:\Windows\System32\cmd.exe	
Duration:	0.0000000	
PID:	2228	
Command line:	"C:\Windows\System32\cmd.exe" /c del C:\Users\15PB-W~1\Desktop\Lab03-04.exe >> NUL	

- 添加站点信任

设置好过滤条件可以抓到对站点信任注册表键值的修改

Time	Process Name	PID	Operation	Path	Result	Detail
1:5...	Lab03-04.exe	3192	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS	Type: REG_DWORD, Leng...
1:5...	Lab03-04.exe	3192	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG_DWORD, Leng...
1:5...	Lab03-04.exe	3192	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS	Type: REG_DWORD, Leng...
1:5...	Lab03-04.exe	3192	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG_DWORD, Leng...

小结

简单的行为分析，只抓取到了部分的行为，如：

- 设置注册表键值，实现Internet可信站点修改
- 创建cmd进程实现自删除

其余的网络行为是未触发的

点击收藏 | 0 关注 | 1

[上一篇：记一次简单的Win Server渗透](#) [下一篇：bugbounty: 利用JSON...](#)

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](#)