windows样本分析之基础静态分析-四

yong夜 / 2019-09-11 09:03:00 / 浏览数 2463 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

一步步实现属于自己的分析流程步骤。

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

感染行为(简单分析)

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1

样本：Lab01-03.exe

鉴黑白

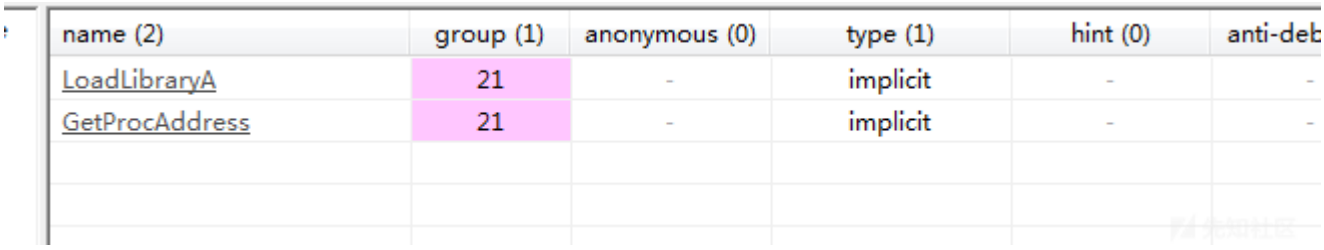
60/69的检测率，确认为病毒样本。

信息收集

信息类型	内容
时间戳	Thu Jan 01 08:00:00 1970
文件类型	32位命令行型可执行文件
壳特征	加壳

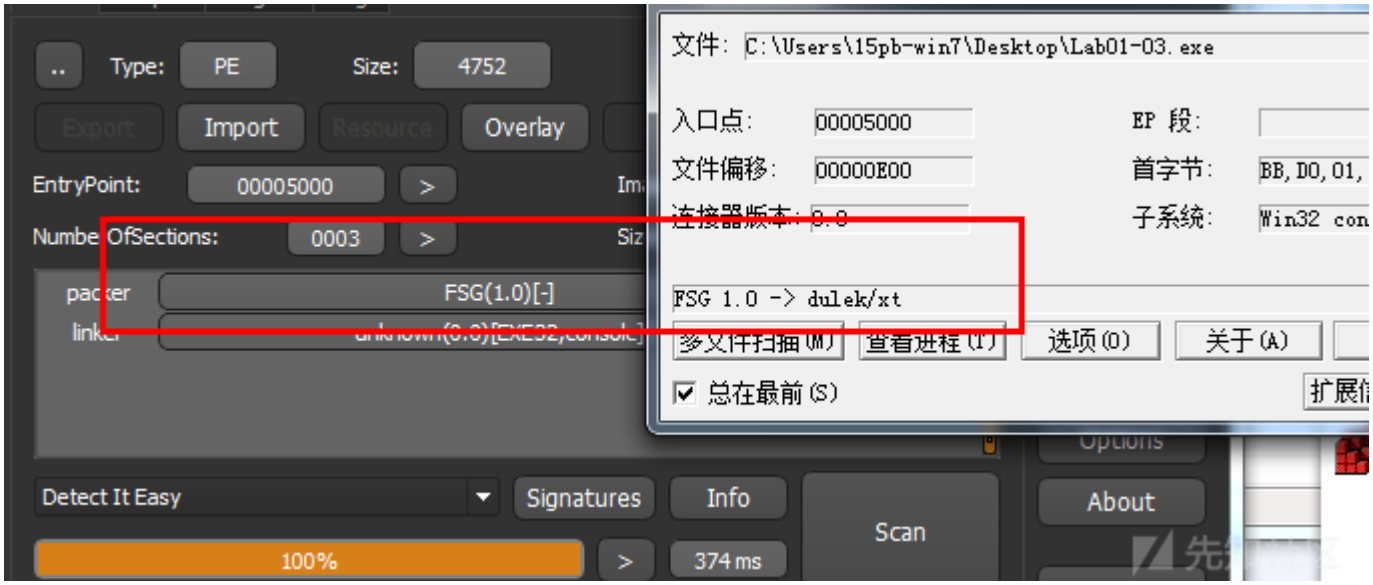
- 壳特征

黑样本+少导入函数=加壳样本



name (2)	group (1)	anonymous (0)	type (1)	hint (0)	anti-deb
LoadLibraryA	21	-	implicit	-	-
GetProcAddress	21	-	implicit	-	-

FSG壳



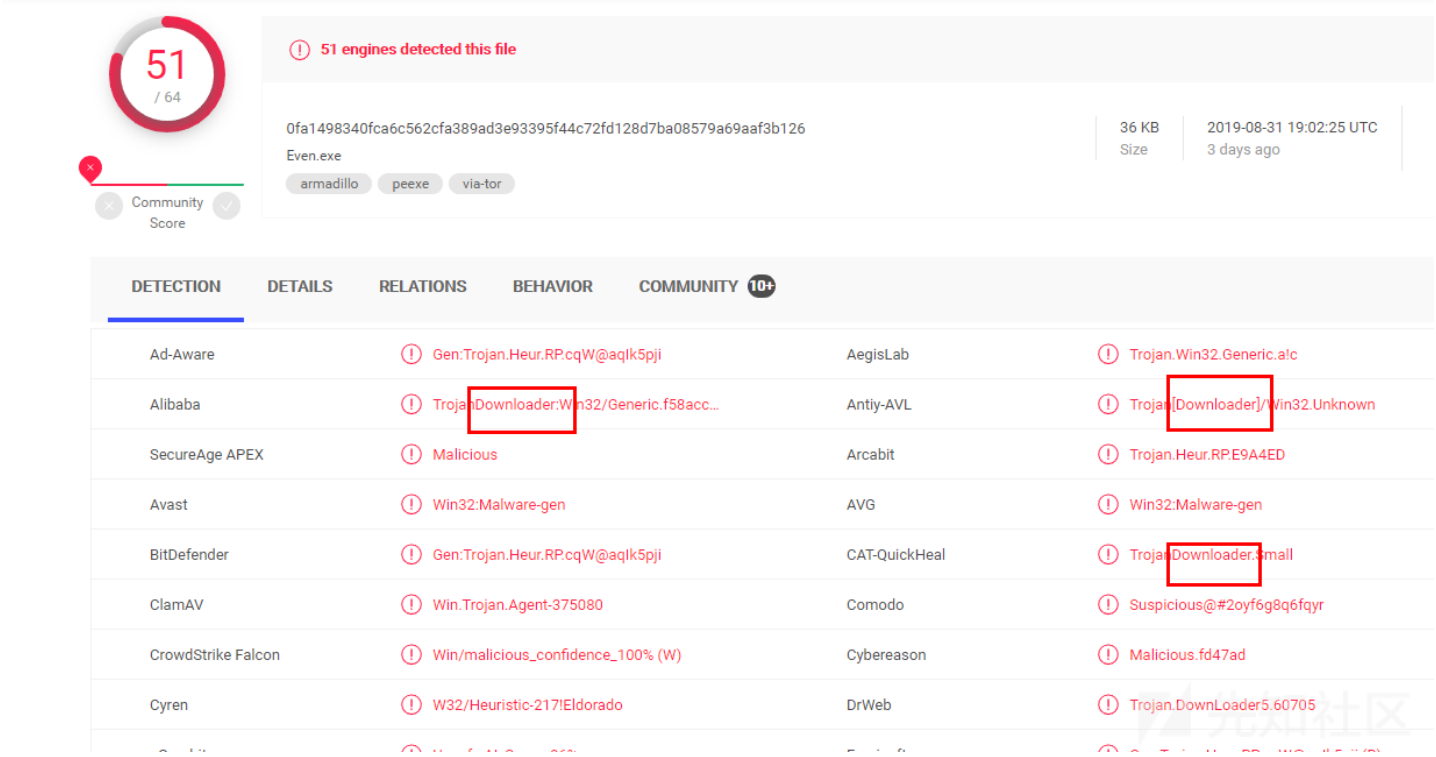
没有找到自动脱FSG1.0的脱壳工具，后面分析暂时中止

实践过程2

样本：Lab01-04.exe

鉴黑白

51/64检出率，判定为病毒样本。并且从病毒名中猜测应该是下载者

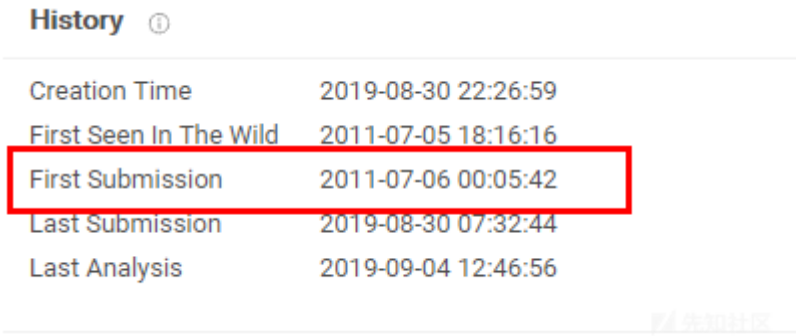


信息收集

信息类型	内容
时间戳	Sat Aug 31 06:26:59 2019
文件类型	32位GUI型可执行文件
壳特征	未加壳

- 时间戳

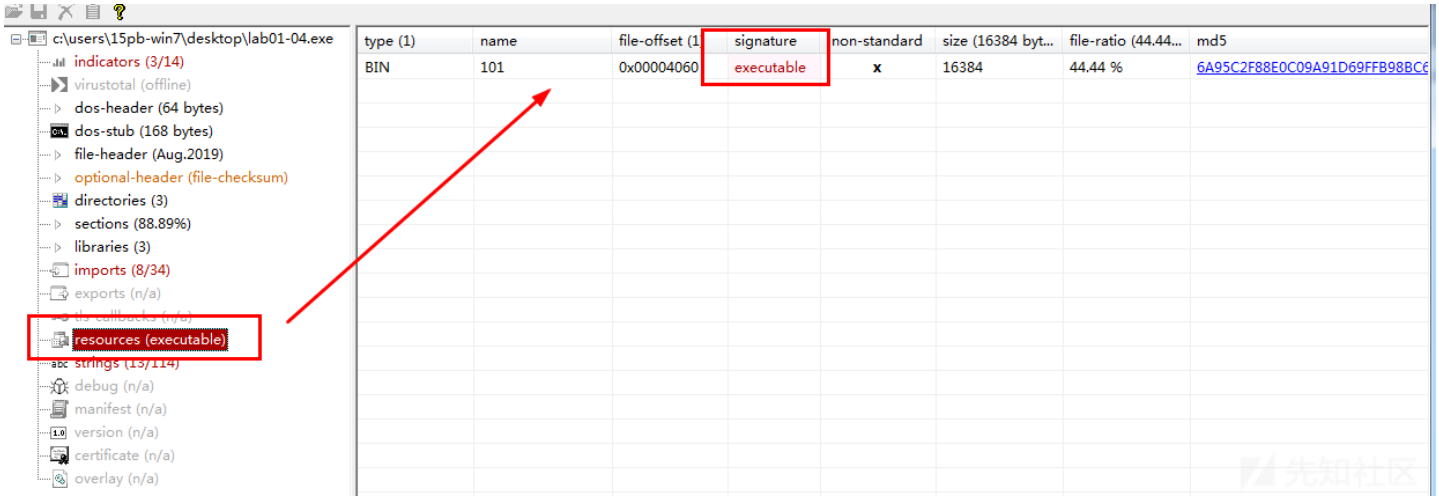
样本在VT首次上传时间为2011年，所以这个时间戳是伪造的



感染行为(简单分析)

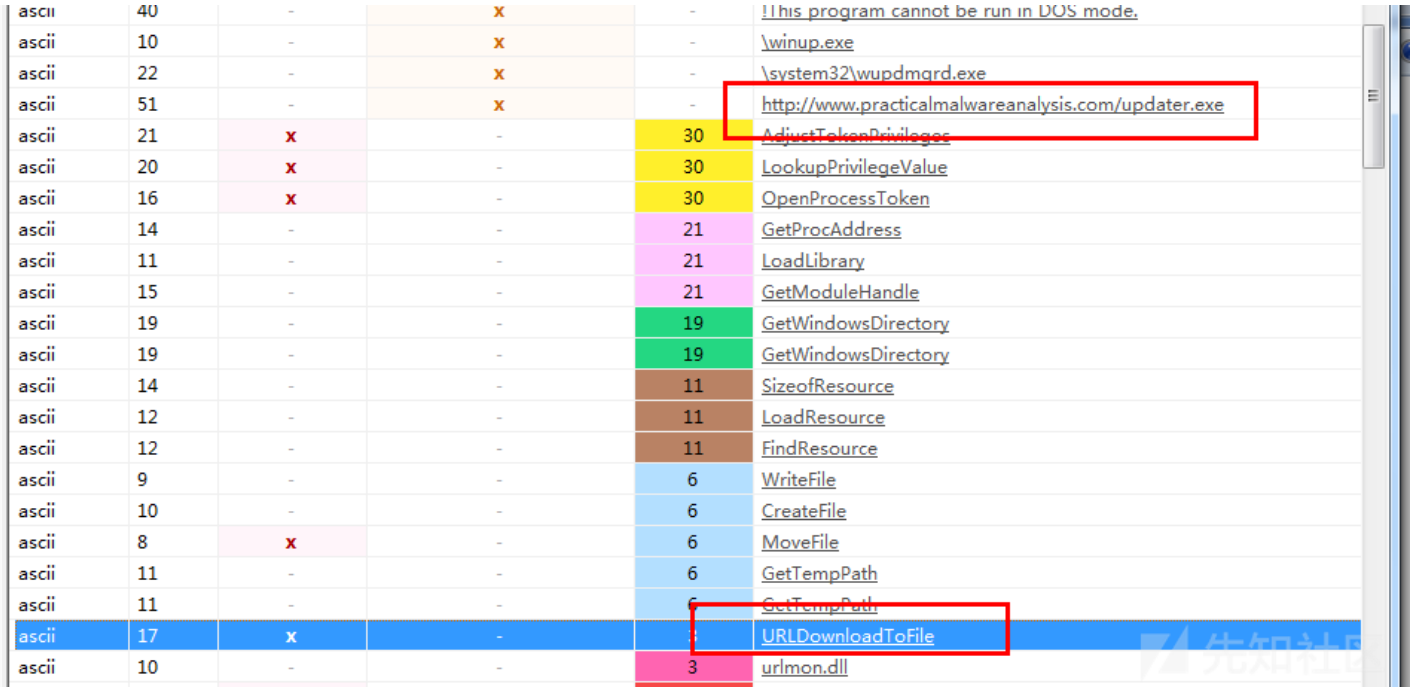
1. 资源加载

`FindResourceA`■`LoadResource` API函数结合资源节中的exe文件，应该是加载恶意模块，对这个衍生物文件简单分析放在后面

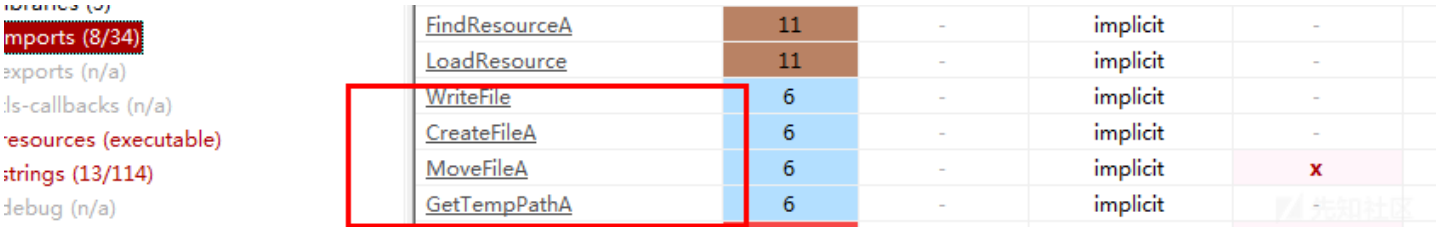


1. 远程下载样本、隐藏样本

远程下载样本



将下载后的样本隐藏于临时目录或者系统目录



-	!This program cannot be run in DOS mode.
-	winlogon.exe
-	SeDebugPrivilege
-	\system32\wupdmgr.exe
-	\system32\wupdmgr.exe
-	\winup.exe
-	!This program cannot be run in DOS mode.
-	\winup.exe
-	\system32\wupdmgrd.exe
-	http://www.practicalmalwareanalysis.com/updater.exe
30	AdjustTokenPrivileges
30	LookupPrivilegeValue
30	OpenProcessToken
21	GetProcAddress
21	LoadLibrary
21	GetModuleHandle
19	GetWindowsDirectory

有可能隐藏当前样本于临时目录或系统目录

-	6	GetTempPath
-	3	URLDownloadToFile
-	3	urlmon.dll
-	2	OpenProcess
-	2	GetCurrentProcess
-	2	CreateRemoteThread
-	2	WinExec
-	2	EnumProcessModules
-	2	psapi.dll
-	2	GetModuleBaseName
-	2	psapi.dll
-	2	EnumProcesses
-	2	psapi.dll

1. 程序启动

`WinExec`用该API来启动程序下载来的程序或者资源中的程序

1. 远程线程注入

有可能想将加载恶意DLL，但是暂时未看见陌生的DLL字符，这个观点有待进一步分析

ascii	40	-	x	-	!This program cannot be run in DOS mode.
ascii	12	-	x	-	winlogon.exe
ascii	16	-	x	-	SeDebugPrivilege
ascii	21	-	x	-	\system32\wupdmgr.exe
ascii	21	-	x	-	\system32\wupdmgr.exe
ascii	10	-	x	-	\winup.exe
ascii	40	-	x	-	!This program cannot be run in DOS mode.
ascii	10	-	x	-	\winup.exe
ascii	22	-	x	-	\system32\wupdmgrd.exe
ascii	51	-	x	-	http://www.practicalmalwareanalysis.com/updater.exe
ascii	21	x	-	30	AdjustTokenPrivileges
ascii	20	x	-	30	LookupPrivilegeValue
ascii	16	x	-	30	OpenProcessToken
ascii	14	-	-	21	GetProcAddress
ascii	11	-	-	21	LoadLibrary
ascii	15	-	-	21	GetModuleHandle
ascii	19	-	-	19	GetWindowsDirectory
ascii	19	-	-	19	GetWindowsDirectory
ascii	14	-	-	11	SizeofResource
ascii	12	-	-	11	LoadResource
ascii	12	-	-	11	FindResource
ascii	9	-	-	6	WriteFile
ascii	10	-	-	6	CreateFile
ascii	8	x	-	6	MoveFile
ascii	11	-	-	6	GetTempPath
ascii	11	-	-	6	GetTempPath
ascii	17	x	-	3	URLDownloadToFile
ascii	10	-	-	3	urlmon.dll
ascii	11	x	-	2	OpenProcess
ascii	17	x	-	2	GetCurrentProcess
ascii	18	x	-	2	CreateRemoteThread
ascii	7	x	-	2	WinExec
ascii	18	x	-	2	EnumProcessModules
ascii	9	-	-	2	psapi.dll

小结

主机行为

加载资源中的模块

- 隐藏以及执行该样本或者远程样本

远程DLL注入

网络行为

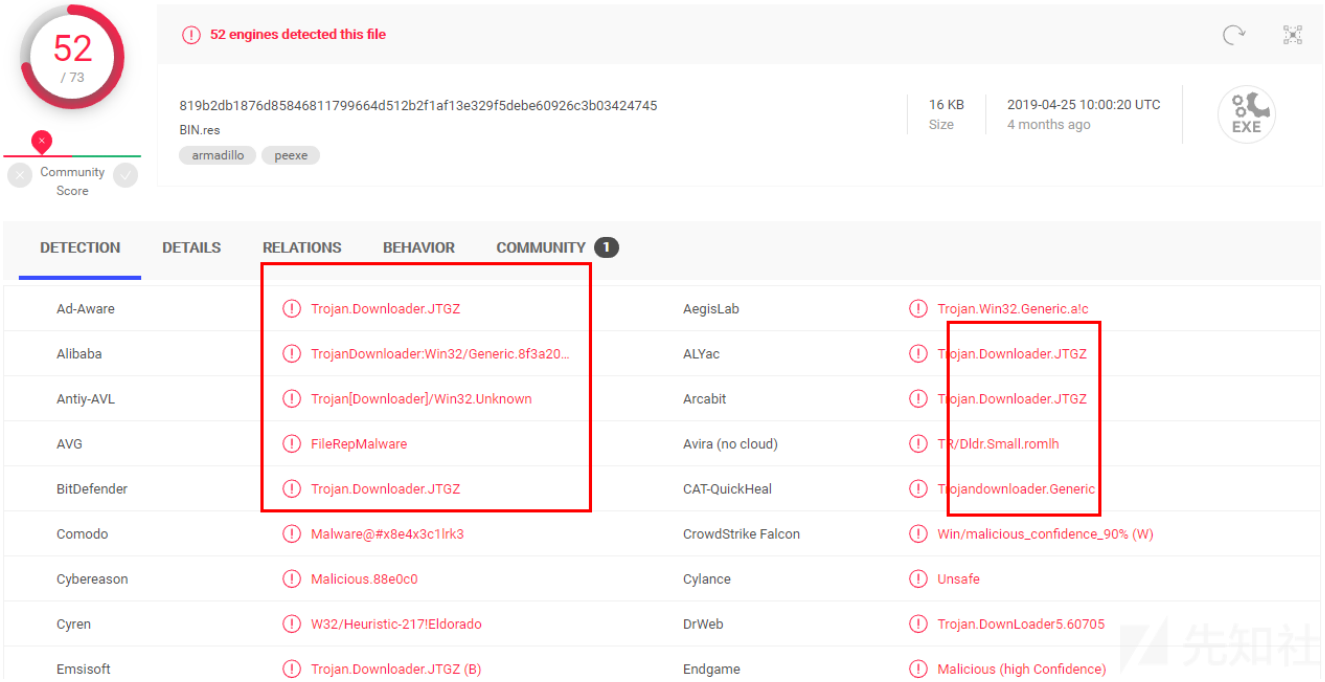
远程从http://www.practicalmalwareanalysis.com/updater.exe下载恶意样本

衍生物1

资源dump下的文件：resource.bin

鉴黑白

52/73检出率，判定为病毒样本 ,根据家族名可以看出又是一个下载者



信息收集

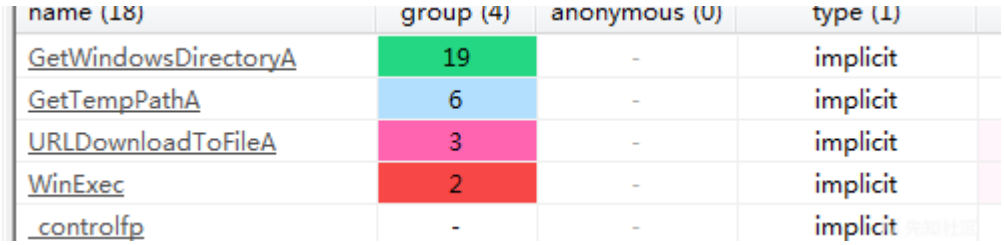
信息类型	内容
时间戳	Sun Feb 27 08:16:59 2011
文件类型	32位GUI型可执行文件
壳特征	未加壳

- 时间戳

根据VT上传时间，宿主样本的上传时间和这个时间戳比较相近，所以这个时间戳应该是问价你的编译时间

感染行为(简单分析)

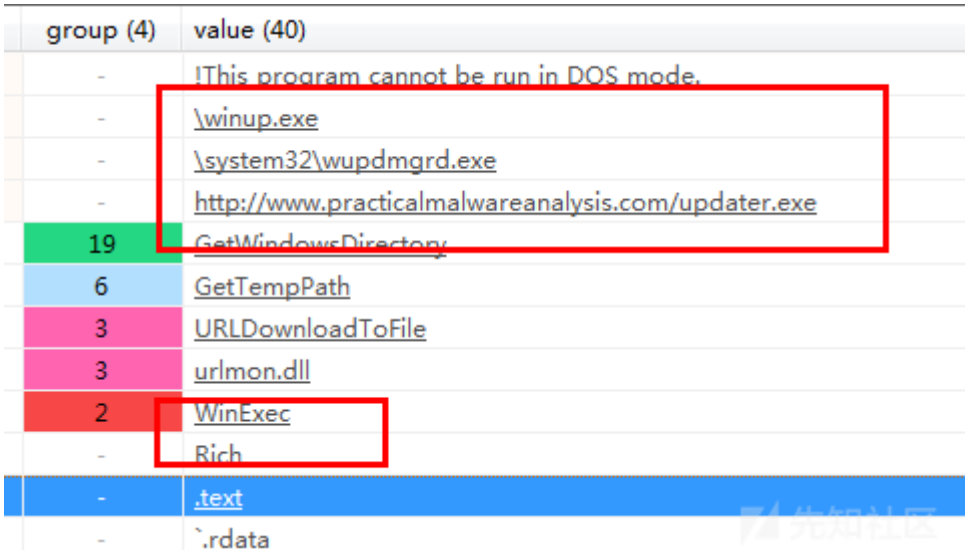
从API可以得出，是远程下载并执行的操作



name (18)	group (4)	anonymous (0)	type (1)
GetWindowsDirectoryA	19	-	implicit
GetTempPathA	6	-	implicit
URLDownloadToFileA	3	-	implicit
WinExec	2	-	implicit
_controlfp	-	-	implicit

从字符串信息中可以看出具体从http://www.practicalmalwareanalysis.com/updater.exe下载，并执行该文件。

并且又出现了`\winup.exe■\system32\wupdmgrd.exe`文件，暂时没有相关API作为依据，无法判断



group (4)	value (40)
-	!This program cannot be run in DOS mode.
-	\winup.exe
-	\system32\wupdmgrd.exe
-	http://www.practicalmalwareanalysis.com/updater.exe
19	GetWindowsDirectory
6	GetTempPath
3	URLDownloadToFile
3	urlmon.dll
2	WinExec
-	Rich
-	.text
-	`.rdata

小结

- 主机行为

执行远程下载的样本

- 网络行为

远程下载样本

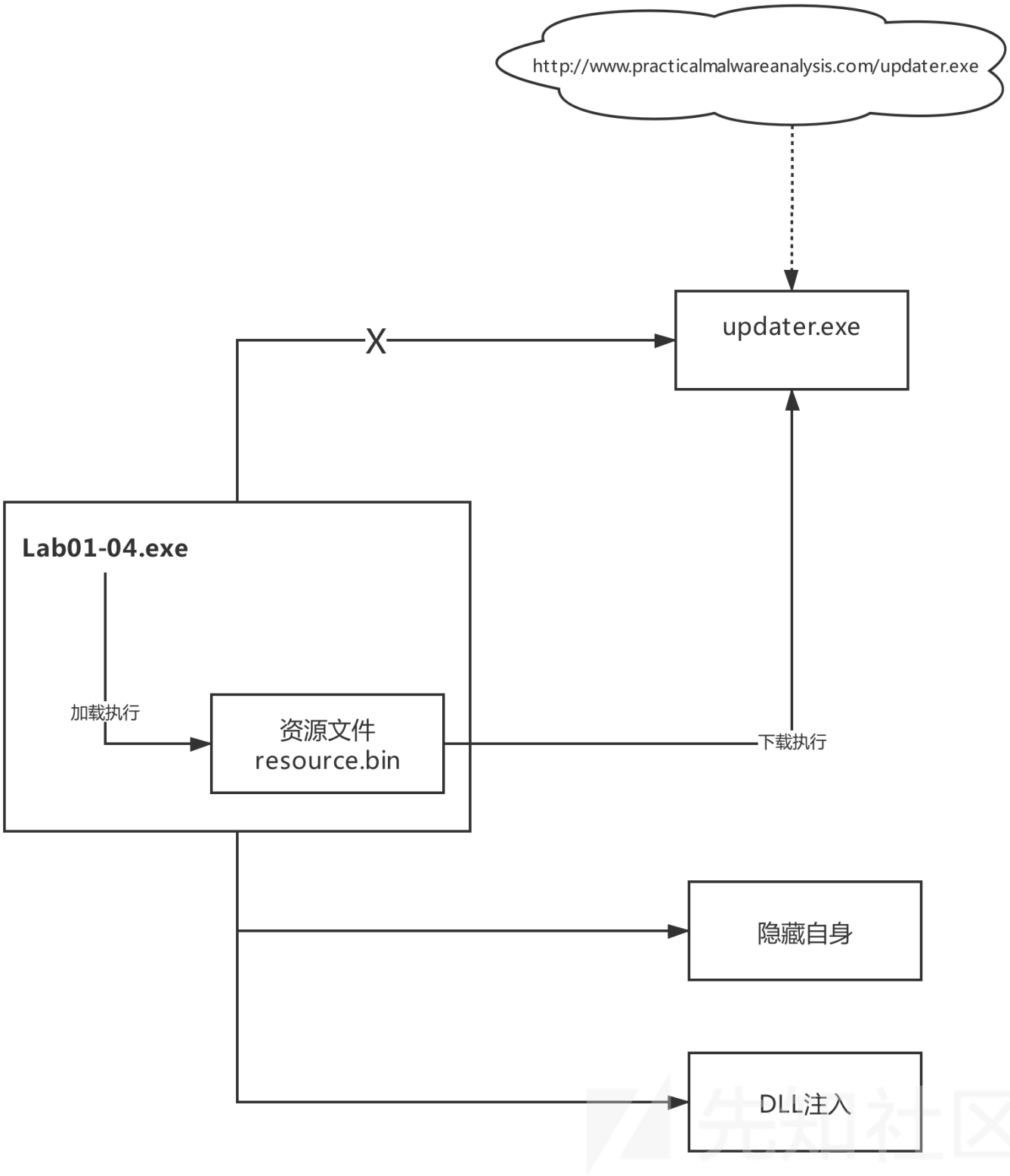
衍生物2

updater.exe文件，因网址实效，未能下载进行分析

小结

大致可能有如下恶意行为。

这里有个遗漏点，在Lab01-04.exe的导入表中没有相关网络操作API，我以为是运行时链接或者动态链接可以隐藏相关API调用，但是根据答案解释应该是因为资源中的模块
需要学习的地方还很多



点击收藏 | 0 关注 | 1

上一篇：phar相关安全知识总结 下一篇：通过修改源代码达到菜刀无特征链接

1. 0 条回复

- 动动手指，沙发就是你的了！

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