练手之经典病毒熊猫烧香分析(上)

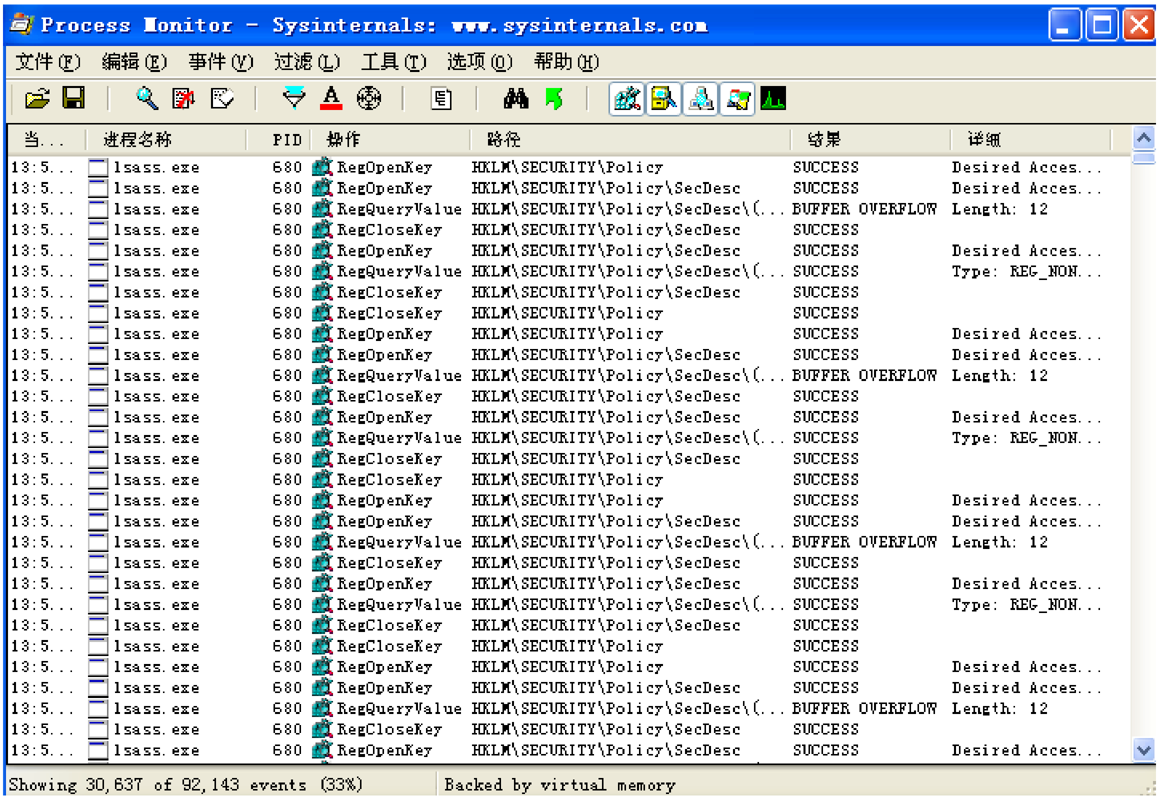
原创

qiye_ 于 2017-08-20 18:50:00 发布 4162 收藏 12

熊猫烧香病毒在当年可是火的一塌糊涂，感染非常迅速，算是病毒史上比较经典的案例。不过已经比较老了，基本上没啥危害，其中的技术也都过时了。作为练手项目，开始对熊猫烧香病毒进行分析。首先准备好病毒样本(看雪论坛有)，VM虚拟机和Xp Sp3系统。样本参数如下:

- 病毒名称：panda.exe
- 文件大小：61952 bytes
- MD5值：3520D3565273E41C9EEB04675D05DCA8
- SHA1值：BB1D8FA7EE4E59844C1FEB7B27A73F9B47D36A0A
- CRC32：23B6DA2A

今天说的主要是行为分析，所以还需要两个软件，一个是Process Monitor v3.10,一个是PCHunter。Process Monitor v3.10是微软提供的，可以监视一个进程对文件，注册表，网络和线程进程操作的工具。



PCHunter则是一个强大的ARK工具，专门对付Rootkit,我主要是想用来挂进病毒进程，发现一些隐藏的文件，和一些启动项。

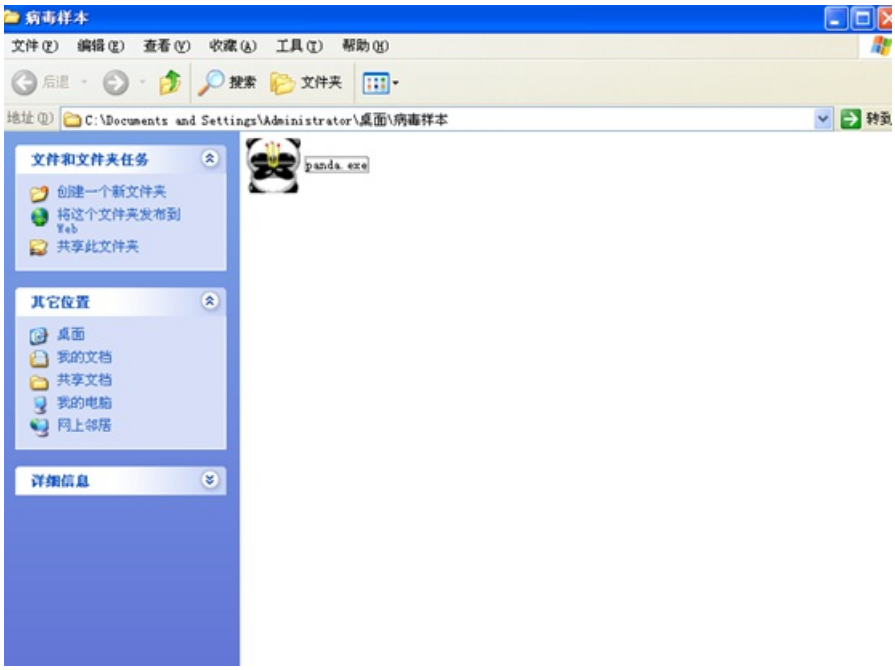
kjuivwwtvxyvbr

进程 | 驱动模块 | 内核 | 内核钩子 | 应用层钩子 | 网络 | 注册表 | 文件 | 启动信息 | 系统杂项 | 电脑体检 | 配置 | 关于

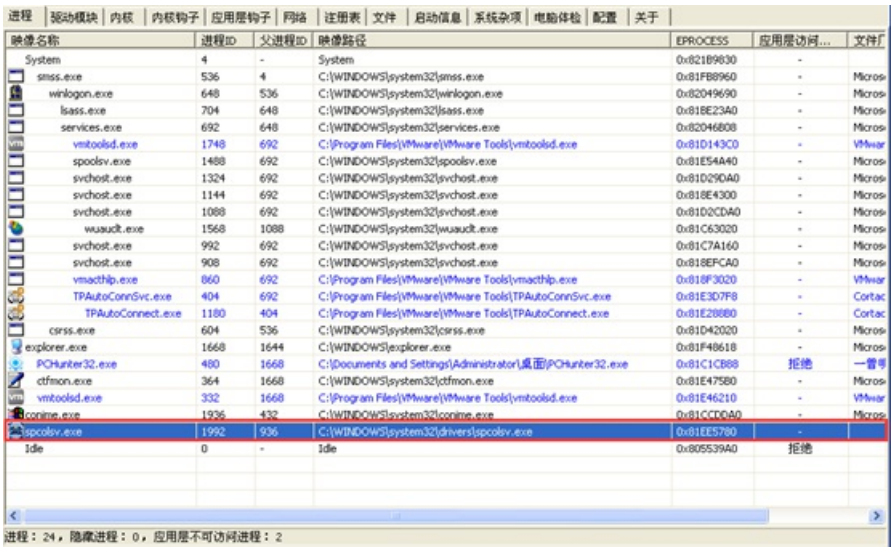
映像名称	进程ID	父进程ID	映像路径	EPROCESS	应用层访问...	文件厂商
System	4	-	System	0x821B9830	-	
smss.exe	536	4	C:\WINDOWS\system32\smss.exe	0x81D705A8	-	Microsoft Corporation
winlogon.exe	624	536	C:\WINDOWS\system32\winlogon.exe	0x81C3A020	-	Microsoft Corporation
wpabaln.exe	1876	624	C:\WINDOWS\system32\wpabaln.exe	0x8181E9F0	-	Microsoft Corporation
lsass.exe	680	624	C:\WINDOWS\system32\lsass.exe	0x81DAE878	-	Microsoft Corporation
services.exe	668	624	C:\WINDOWS\system32\services.exe	0x81BE77B0	-	Microsoft Corporation
vmtoolsd.exe	1800	668	C:\Program Files\VMware\VMware Tools\vmt...	0x81829DA0	-	VMware, Inc.
spoolsv.exe	1596	668	C:\WINDOWS\system32\spoolsv.exe	0x81EAEC10	-	Microsoft Corporation
svchost.exe	1376	668	C:\WINDOWS\system32\svchost.exe	0x820E6020	-	Microsoft Corporation
svchost.exe	1164	668	C:\WINDOWS\system32\svchost.exe	0x81D11020	-	Microsoft Corporation
svchost.exe	1064	668	C:\WINDOWS\system32\svchost.exe	0x81C03B28	-	Microsoft Corporation
wscntfy.exe	1044	1064	C:\WINDOWS\system32\wscntfy.exe	0x81F37228	-	Microsoft Corporation
wuauclt.exe	196	1064	C:\WINDOWS\system32\wuauclt.exe	0x81D3E478	-	Microsoft Corporation
alg.exe	1024	668	C:\WINDOWS\system32\alg.exe	0x81DA5558	-	Microsoft Corporation
svchost.exe	948	668	C:\WINDOWS\system32\svchost.exe	0x81F669D8	-	Microsoft Corporation
svchost.exe	856	668	C:\WINDOWS\system32\svchost.exe	0x81F67218	-	Microsoft Corporation
wmiprvse.exe	1336	856	C:\WINDOWS\system32\wbem\wmiprvse.exe	0x8182C020	-	Microsoft Corporation
vmacthlp.exe	840	668	C:\Program Files\VMware\VMware Tools\vma...	0x81F71DA0	-	VMware, Inc.
TPAutoConnSvc.exe	296	668	C:\Program Files\VMware\VMware Tools\TPA...	0x81D7D3B0	-	Cortado AG
TPAutoConnect.exe	1244	296	C:\Program Files\VMware\VMware Tools\TPA...	0x81D6A650	-	Cortado AG
csrss.exe	600	536	C:\WINDOWS\system32\csrss.exe	0x81DAC248	-	Microsoft Corporation
explorer.exe	1568	1548	C:\WINDOWS\explorer.exe	0x8203A020	-	Microsoft Corporation
Procmon.exe	408	1568	C:\Documents and Settings\Administrator\桌...	0x81C27B38	-	Sysinternals - www.sysinte...
PCHunter32.exe	328	1568	C:\Documents and Settings\Administrator\桌...	0x81CB1AC8	拒绝	一普明为（北京）信息...
ctfmon.exe	180	1568	C:\WINDOWS\system32\ctfmon.exe	0x81D22C10	-	Microsoft Corporation
vmtoolsd.exe	136	1568	C:\Program Files\VMware\VMware Tools\vmt...	0x8211B558	-	VMware, Inc.
Idle	0	-	Idle	0x805539A0	拒绝	

进程： 27， 隐藏进程： 0， 应用层不可访问进程： 2

首先我们在XP Sp3虚拟机中打开Process Monitor，然后运行panda.exe病毒，这时候就开始监听熊猫烧香的一举一动。



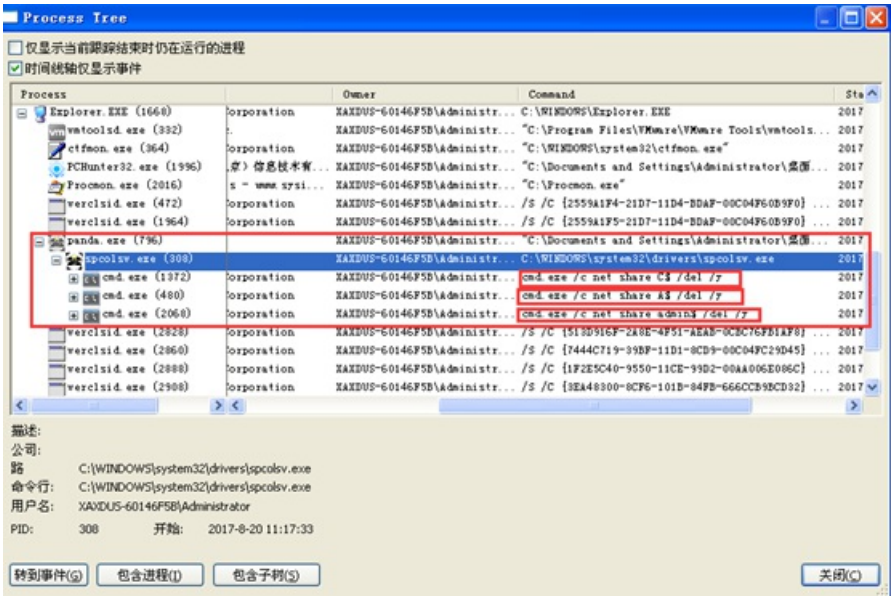
大约运行两分钟后，我们使用PCHunter将病毒进程挂起，停止他的工作。此时你会发现进程名称不是panda.exe,而是spcolsv.exe,右键将他挂起再说。



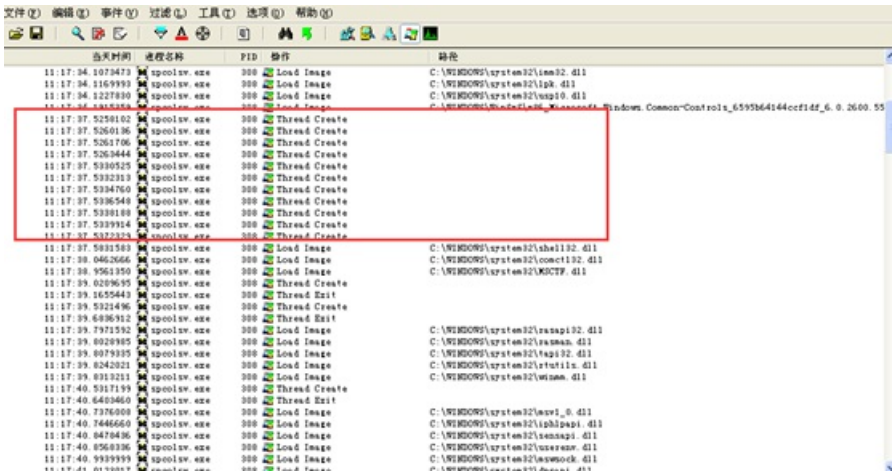
挂起之后，将Process Monitor中的监听数据进行保存，然后我们就可以进行离线分析了。Process Monitor的强大之处在于过滤器，因为Process Monitor监听的是所有的进程，数据量太大。下面我们从进程线程，文件，注册表和网络四个方面来分析一下病毒的行为。

1.进程线程

由于我们发现进程名改变了，所以先看一下Process Monitor中的进程树，了解一下进程和线程的变化。

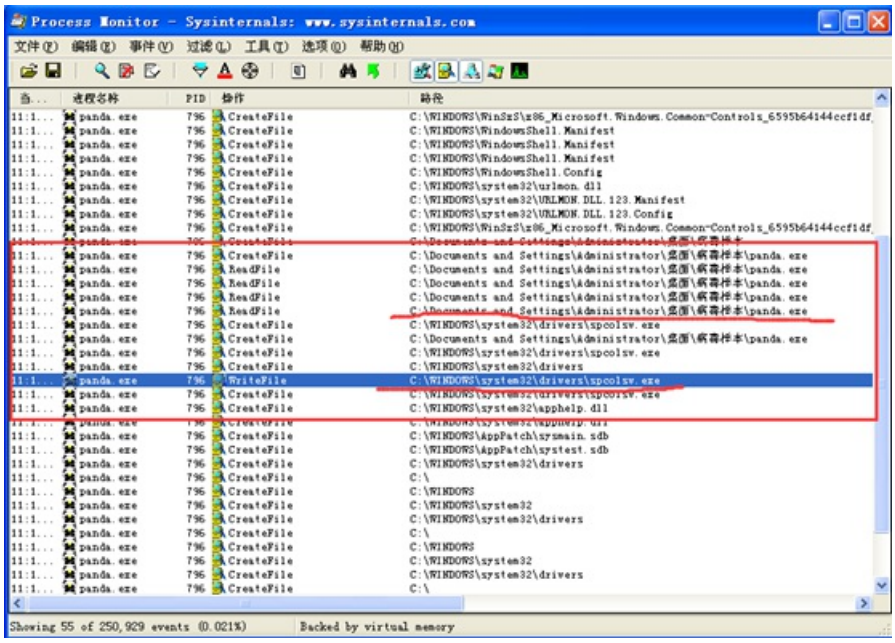


在上图的红框中，我们发现panda.exe启动了spcolsv.exe进程，然后spcolsv.exe有启动了三个cmd，执行的命令为：cmd.exe /c net share C$ /del /y ， cmd.exe /c net share A$ /del /y，cmd.exe /c net share admin$ /del /y ，这些cmd的命令主要是用来删除默认共享。下面我们看一下线程的情况，spcolsv.exe启动了很多的线程，来执行一些操作。

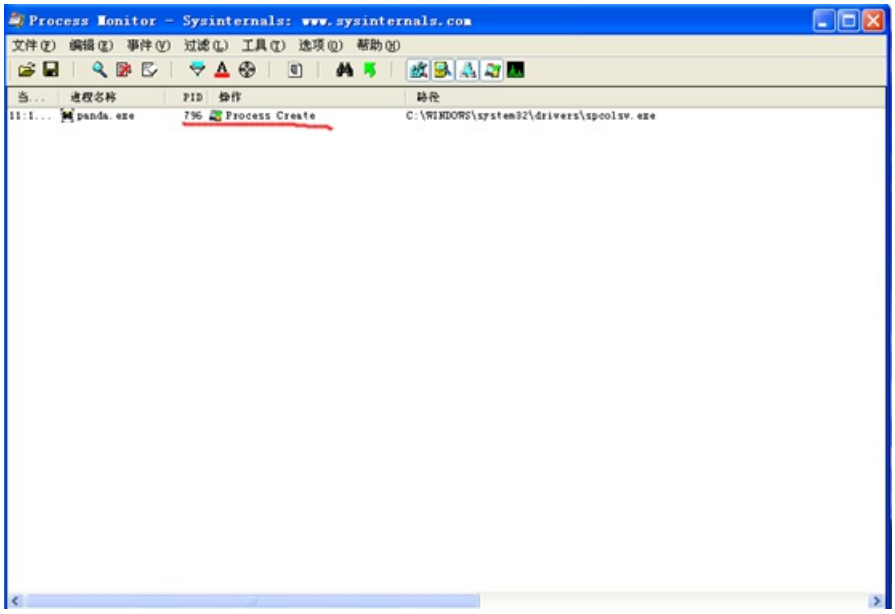


2.文件

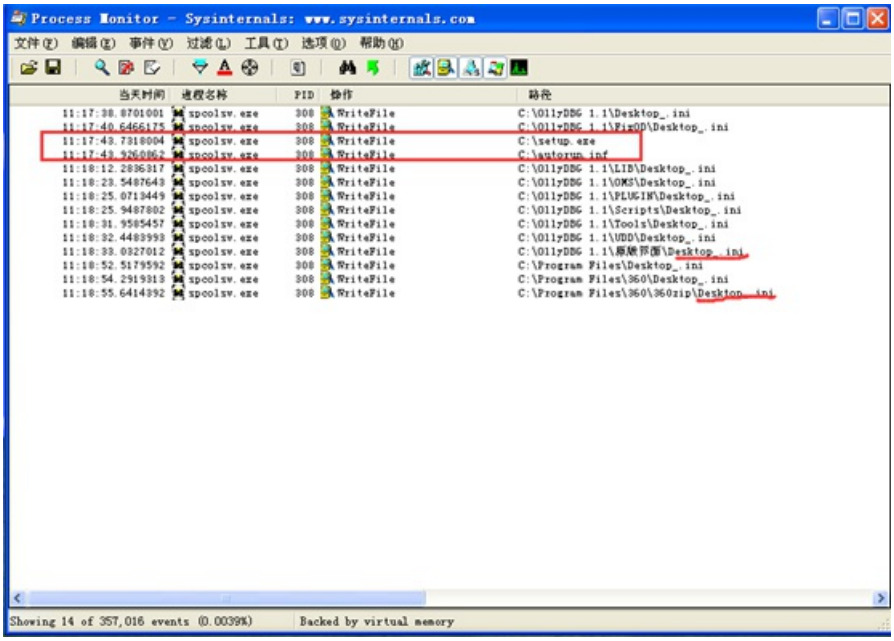
首先看一下spcolsv.exe进程从哪来的，过滤一下panda.exe的文件操作。



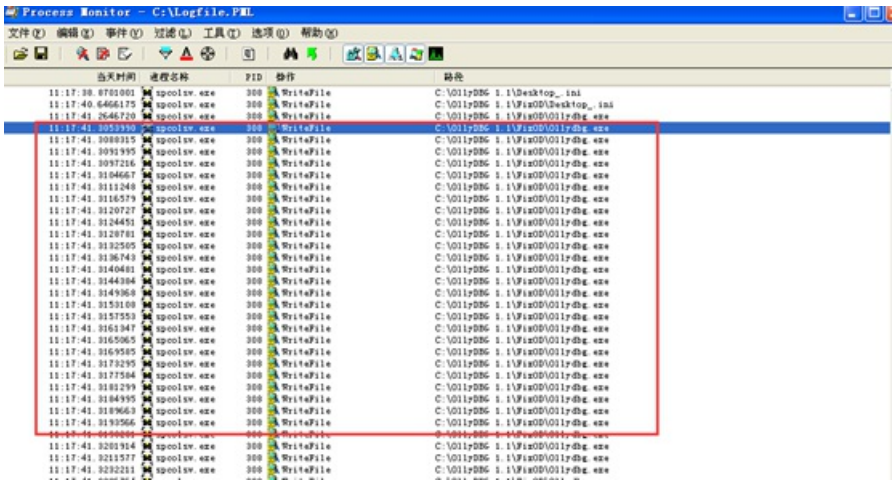
可以看到panda.exe从自身分离出spcolsv.exe，然后将文件写到C:\WINDOWS\system\driver 文件夹下。然后panda.exe将spcolsv.exe启动起来。



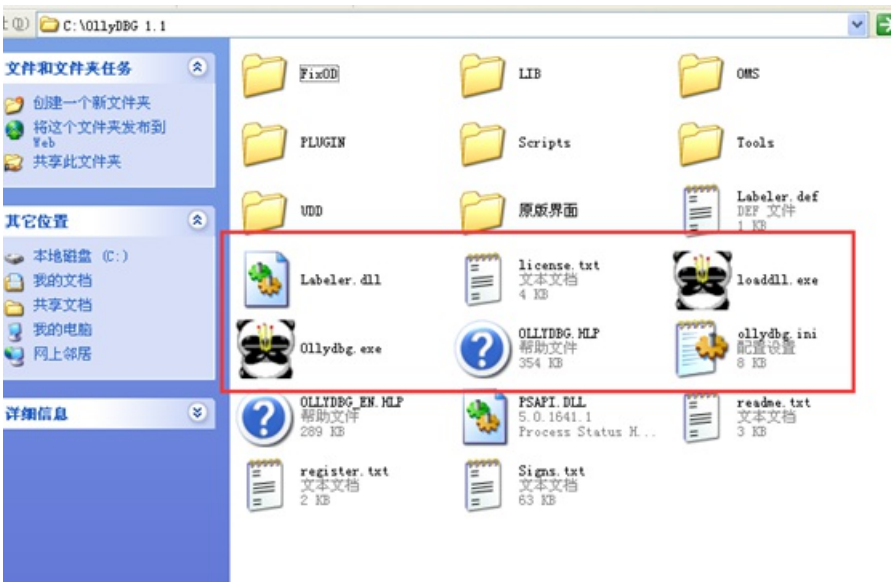
spcolsv.exe启动起来开始进行真正的感染工作，在每个盘的根目录下复制出自身，命名为setup.exe，并生成autorun.inf文件。autorun.inf的作用是当用户打开盘符的时候，会自动运行setup.exe，实现持久性运行。同时在整个盘的每个文件夹下创建Desktop_.ini文件。



运行一会后开始感染exe文件，从下图可以看到对我电脑中的Ollydbg.exe进行了写入操作。



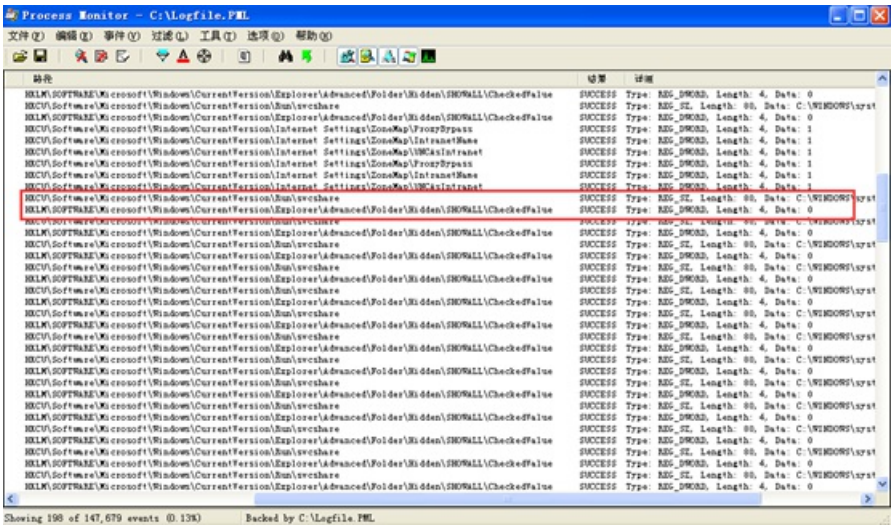
感染的结果变成了下图的样子。



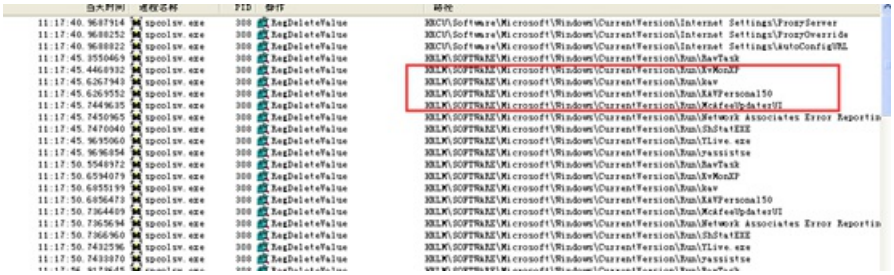
3.注册表

病毒对注册表的操作主要干了两件事情，第一件事是加入自启动，在HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run键项中添加svcshare。同时通过设置

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL 中的CheckedValue的键值设置为0，进行文件隐藏，防止用户查看释放的病毒。这个过程是隔一段时间就会进行一次。

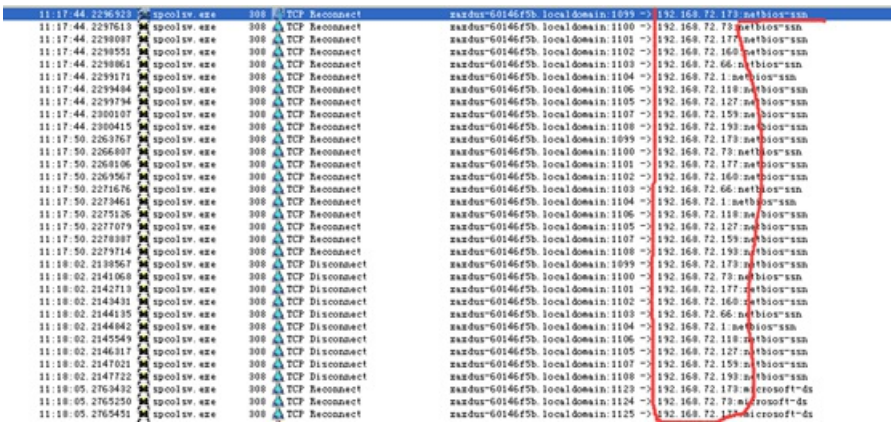


第二件事是删除杀软的自启动项，其中包括卡巴斯基，迈克菲McAfee等杀软。



4.网络

从目前的分析来看，病毒将不断扫描局域网默认共享。用来在局域网 中传播。

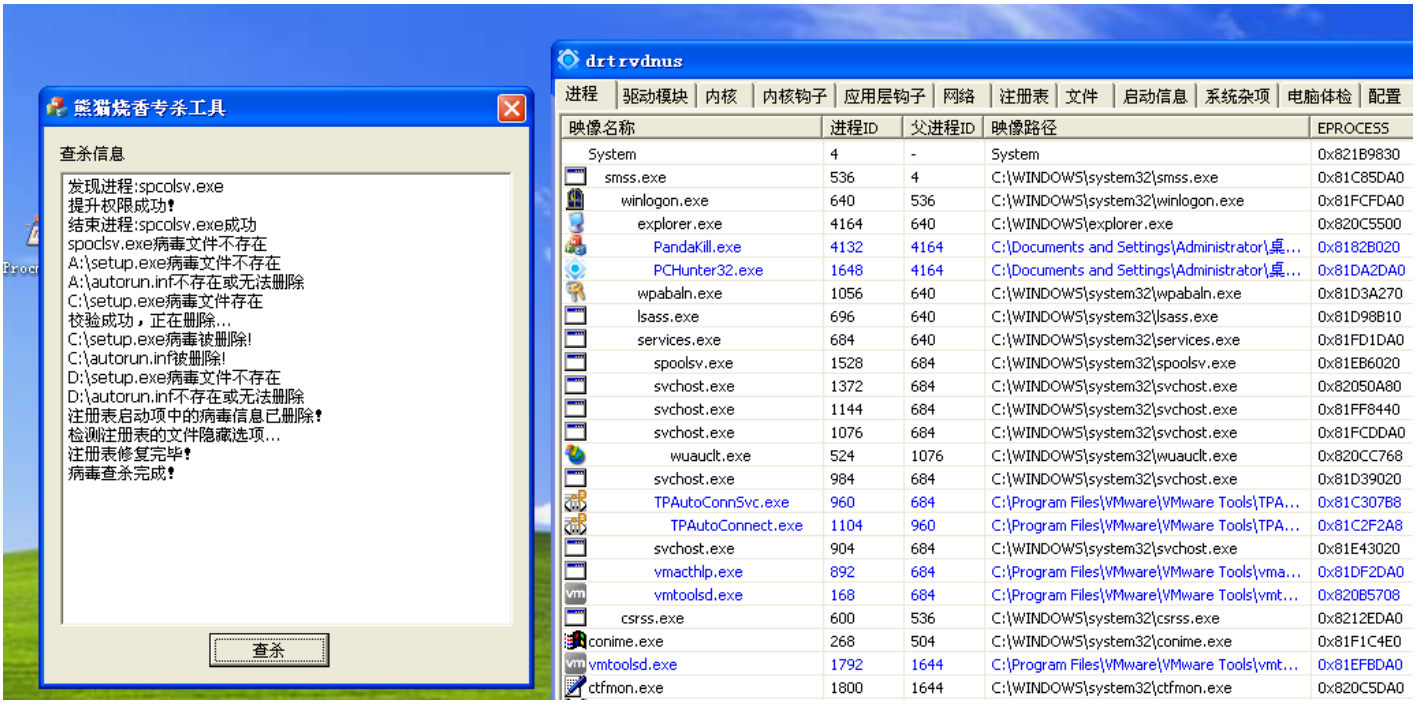


5.编写简单的专杀工具

无论是手动杀毒还是自动杀毒，通过病毒的行为，我们主要从以下方面来杀死病毒：

1. 结束 spcolsv.exe和setup.exe进程
2. 删除spcolsv.exe，setup.exe，autorun.inf和Desktop_.ini文件
3. 删除HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run键项中的svcshare，将HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL中的CheckedValue设置为1

最后使用MFC编写了一个熊猫专杀工具(Desktop_.ini暂时没删除)，部分代码参考 姜晔的技术专栏。



6.总结

通过行为监控的方式完成了对熊猫烧香病毒的查杀，不过还不够彻底。那些被感染的exe文件,我们还没有恢复，如果想要进一步的研究，下一节我们对病毒进行逆向，看它是如何感染的。

7.再续

我新书**《Python爬虫开发与项目实战》**出版了。 这本书包括基础篇，中级篇和深入篇三个部分，不仅适合零基础的朋友入门，也适合有一定基础的爬虫爱好者进阶，如果**你不会分布式爬虫，不会千万级数据的去重，不会怎么突破反爬虫，不会分析js的加密**，这本书会给你惊喜。如果大家对这本书感兴趣的话，可以看一下 **试读样章**。