

准备工作

参考：

[熊猫烧香病毒分析 | L-htian](#)

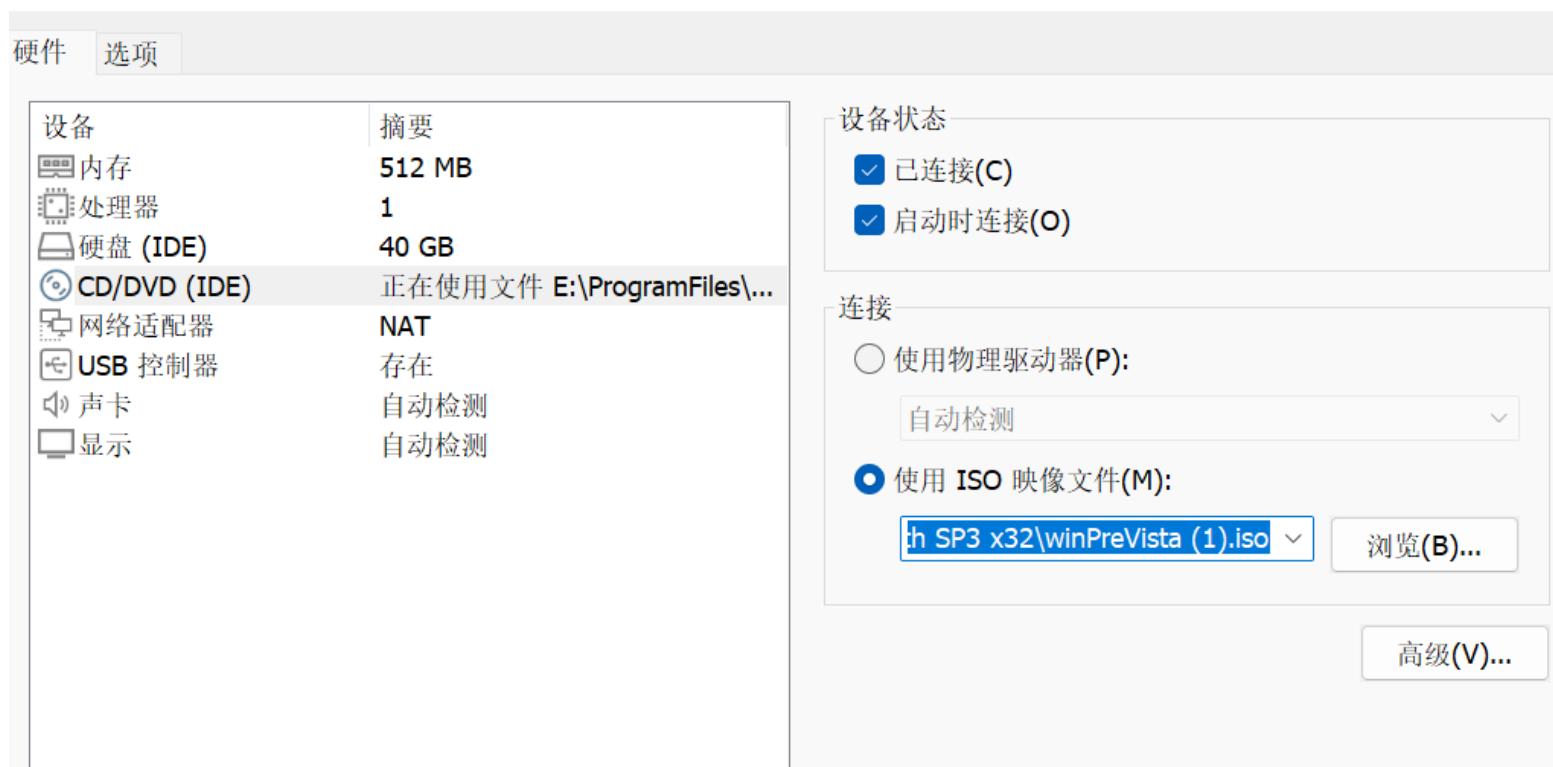
[经典病毒分析——熊猫烧香 - 吾爱破解 - 52pojie.cn](#)

使用的系统是实验3中已经安装的 Windows XP Professional With SP3 x32 (简体中文版)

为了和主机之间互传文件，需要安装vmwaretools。

[【vmware】vmware中手动安装vmwaretools_vmware tools 不再随旧版客户机操作系统的 vmware workstation 一起提供-CSDN博客](#)

注意光驱中最好只能有winPreVista.iso这一个CD/DVD，否则可能造成冲突，无法在虚拟机的我的电脑中看到安装助手



[熊猫烧香样本\[52pojie\].zip - 蓝奏云](#) 解压密码：52pojie

下载后将vir后缀改为exe即可

在虚拟机中设置共享文件夹，将所需文件放入

硬件 选项

设置	摘要
常规	Windows XP Professional With SP3 x32
电源	
共享文件夹	已启用
快照	
自动保护	已禁用
客户机隔离	
访问控制	未加密
VMware Tools	关闭时间同步
VNC 连接	已禁用
设备视图	
自动登录	已禁用
高级	默认/默认

文件夹共享

⚠ 共享文件夹会将您的文件显示给虚拟机中的程序。这可能为您的计算机和数据带来风险。请仅在您信任虚拟机使用您的数据时启用共享文件夹。

- 已禁用(D)
 总是启用(E)
 在下次关机或挂起前一直启用(U)

在 Windows 客户机中映射为网络驱动器(M)

文件夹(F)

名称	主机路径
5. 342-13	C:\Users\肖羽\Desktop\期...

[添加\(A\)...](#)

[移除\(R\)](#)

[属性\(P\)](#)



VMware Tools (D:)

网络驱动器



'vmware-host' 上的
Shared Folders (Z:)

复制到桌面上，即可看到。

本次分析的病毒样本：

↑ 主页 ×

Win7 x64_52pojie ×

Windows XP Professional ... ×

xiongmao 属性



常规

兼容性

摘要



xiongmao



xiongmao

文件类型： 应用程序

描述： xiongmao

位置： C:\Documents and Settings\xiaoyu\桌面

大小： 29.2 KB (30,001 字节)

占用空间： 32.0 KB (32,768 字节)

创建时间： 2024年12月23日, 1:19:03

修改时间： 2024年12月23日, 1:16:26

访问时间： 2024年12月23日, 1:19:03

属性： 只读 (R) 隐藏 (H)

对虚拟机进行断网操作，并用VMWare拍摄快照，作为安全状态的存档。防火墙也要关闭。



快照创建时间:2024/12/23 1:21:10

名称(N): **safe**

描述(D): 安全状态



拍摄快照(T)...

保留(K)

克隆(O)...

删除(E)

显示自动保护快照(S)

转到(G)

自动保护(A)...

关闭(C)

帮助

已选择 1 个快照

运行病毒

运行病毒后，任务管理器无法打开，会快速闪退。

使用cmd查看进程，可以看到可疑的spo0lsv.exe程序，即为该病毒

命令提示符

System	4	Console	0	296 K
smss.exe	460	Console	0	404 K
csrss.exe	596	Console	0	5,668 K
winlogon.exe	620	Console	0	4,604 K
services.exe	664	Console	0	3,456 K
lsass.exe	676	Console	0	6,172 K
vmacthlp.exe	832	Console	0	2,620 K
svchost.exe	844	Console	0	4,896 K
svchost.exe	928	Console	0	4,336 K
svchost.exe	1024	Console	0	17,920 K
svchost.exe	1076	Console	0	3,116 K
svchost.exe	1128	Console	0	4,528 K
explorer.exe	1500	Console	0	18,532 K
spoolsv.exe	1580	Console	0	4,600 K
vmtoolsd.exe	1696	Console	0	12,960 K
ctfmon.exe	1704	Console	0	3,956 K
UGAuthService.exe	184	Console	0	9,136 K
vmtoolsd.exe	272	Console	0	14,524 K
wmiprvse.exe	1068	Console	0	8,308 K
conime.exe	1412	Console	0	3,200 K
spo0lsv.exe	1184	Console	0	4,668 K
cmd.exe	2616	Console	0	2,776 K
tasklist.exe	2716	Console	0	4,548 K

C:\Documents and Settings\xiaoyu>

CH



命令提示符



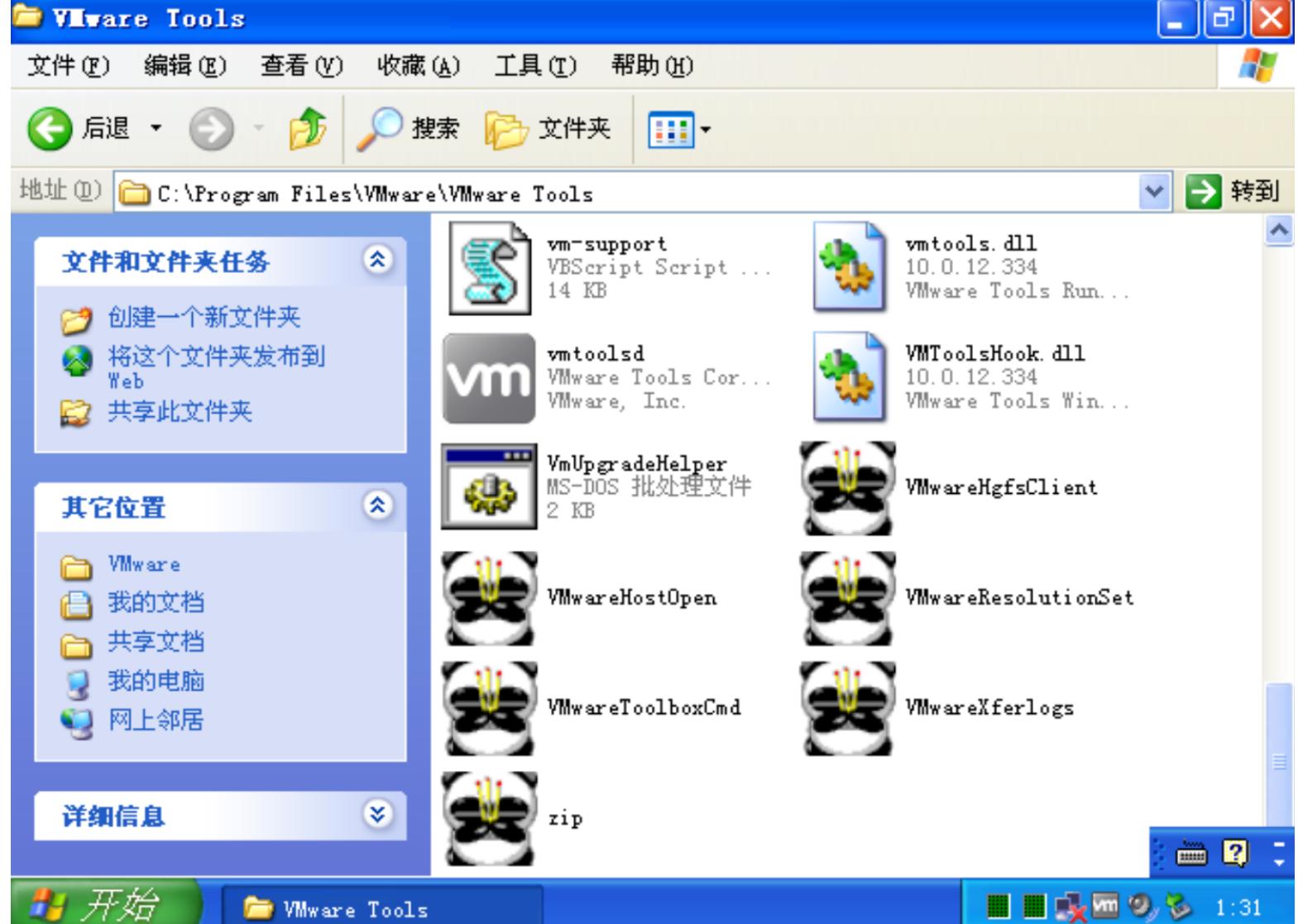
1:28

“熊猫烧香”不但能感染系统中exe , com , pif , src , html , asp等文件，他还能中止大量的反病毒软件进程并且会删除扩展名为gho的文件。该文件一般是系统备份工具GHOST的备份文件，使用户的系统备份文件丢失。

被感染的用户系统中所有.exe可执行文件全部被改成熊猫烧香的模样。

熊猫烧香病毒对系统中所有除了盘符为A , B的磁盘类型为DRIVE_REMOTE , DRIVE_FIXED的磁盘进行文件遍历感染

可以看见，C盘中毒后被感染的可执行文件都会变成“熊猫烧香”的图标



分析病毒行为

使用exeinfo查看病毒的信息，可以看出这个程序带了FSG 2.0的壳。

文件(E): xiongmao.vir

程序入口:	00000154	oo	<	入口区段:	
文件偏移:	00000154			入口首字节:	87 25 F4 D2 41 0
连接器版本:	0.00			子系统:	Windows GUI
文件大小:	00007531h	<	NET	叠加数据:	NO 00000000

Image is 32bit executable RES/OVL : 6 / 0 % 1987

FSG v2.0 F[ast] S[mall] G[ood] - www.xtreeme.prv.pl

初步信息 - 帮助提示 - 脱壳信息 0 ms.

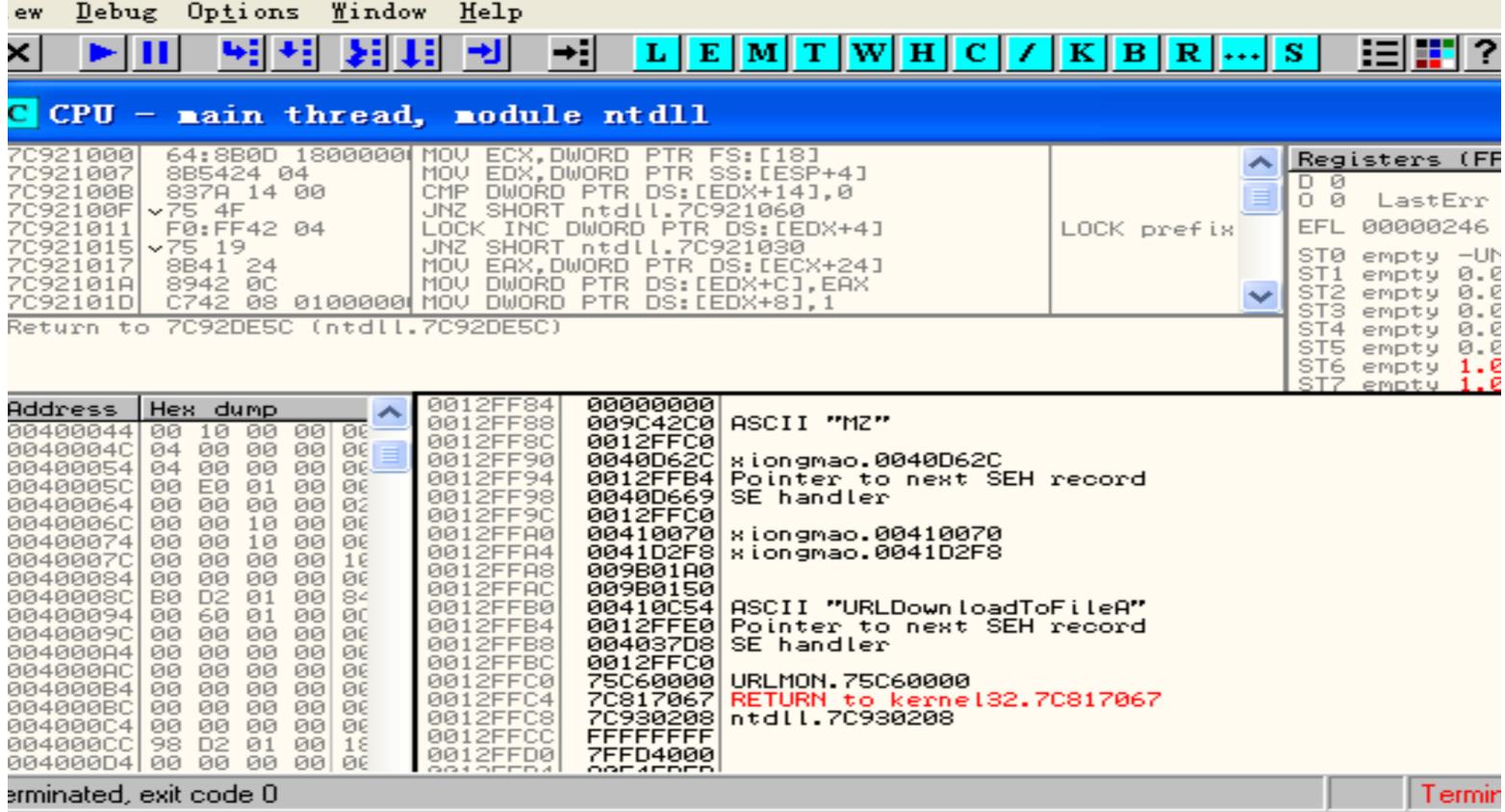
Big sec. 02 [] , try UnFSG2.0.exe - by "Eedy31 with Radasm IDE" (no www)

> icon"/>

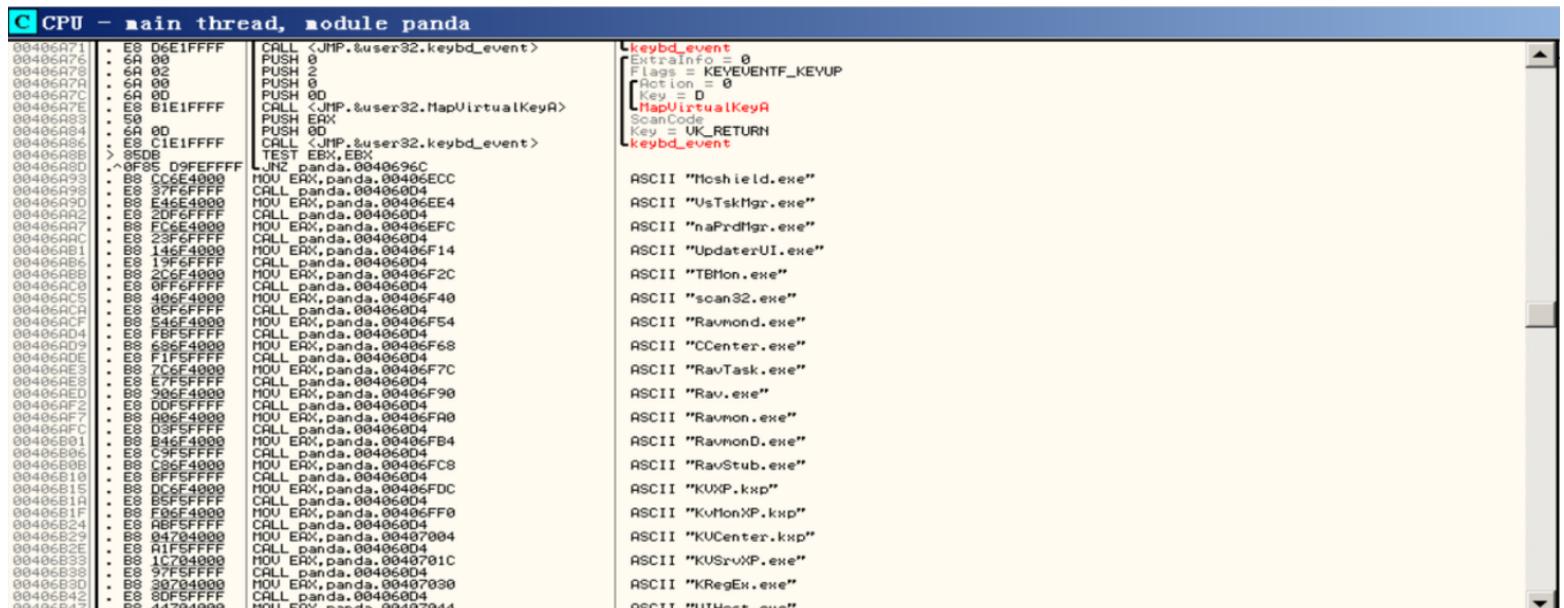
使用Ollydbg对病毒进行分析。

可以发现病毒自我复制到C:\Windows\System32\driver，并启动spo0lsv.exe

0012FB84	00000000	
0012FB88	00000000	
0012FB8C	009B0380	ASCII "C:\WINDOWS\system32\"
0012FB90	009B03A4	ASCII "C:\WINDOWS\system32\drivers\spo0lsv.exe"
0012FB94	009B0340	
0012FB98	009B02E8	ASCII "C:\WINDOWS\system32\"
0012FB9C	009B030C	ASCII "C:\WINDOWS\system32\drivers\spo0lsv.exe"
0012FBAC	009B0290	ASCII "C:\WINDOWS\system32\"
0012FBAA	009B02B4	ASCII "C:\WINDOWS\system32\drivers\spo0lsv.exe"
0012FBAB	009CB880	ASCII "C:\WINDOWS\system32\"
0012FBAC	009CB8A4	ASCII "C:\WINDOWS\system32\drivers\spo0lsv.exe"
0012FBBA	009CB8D8	ASCII "C:\WINDOWS\SYSTEM32\DRIVERS\SPO0LSV.EXE"
0012FBBC	009CB800	
0012FBBD	009CB840	
0012FBBC	00000000	
0012FBCC	009B0250	
0012FBCC	00000000	
0012FBCC	00000000	
0012FBCC	00000000	



病毒会尝试关闭各种防火墙和杀毒软件



在每个目录下创建Desktop.ini，保存被感染的时间

00408BEF	. E8 24B4FFFF	CALL panda.00404018	
00408BF4	. v 0F84 38030000	JE panda.00408F32	
00408BFA	. FF75 FC	PUSH DWORD PTR SS:[EBP-4]	
00408BFD	. FFB5 A8FEFFFF	PUSH DWORD PTR SS:[EBP-158]	
00408C03	. 68 C0914000	PUSH panda.004091C0	
00408C08	. 8D85 DCDFFFFF	LEA EAX,DWORD PTR SS:[EBP-224]	
00408C0E	. BA 03000000	MOV EDX,3	
00408C13	. E8 74B3FFFF	CALL panda.00403F8C	
00408C18	. 8B85 DCDFFFFF	MOV EAX,DWORD PTR SS:[EBP-224]	
00408C1E	. E8 81CBFFFF	CALL panda.004057A4	
00408C23	. 84C0	TEST AL,AL	
00408C25	. v 0F84 D7010000	JE panda.00408E02	
00408C2B	. FF75 FC	PUSH DWORD PTR SS:[EBP-4]	
00408C2E	. FFB5 A8FEFFFF	PUSH DWORD PTR SS:[EBP-158]	
00408C34	. 68 C0914000	PUSH panda.004091C0	
00408C39	. 8D85 D8FDFFFF	LEA EAX,DWORD PTR SS:[EBP-228]	
00408C3F	. BA 03000000	MOV EDX,3	
00408C44	. E8 43B3FFFF	CALL panda.00403F8C	
00408C49	. 8B85 D8FDFFFF	MOV EAX,DWORD PTR SS:[EBP-228]	
00408C4F	. 8D55 F8	LEA EDX,DWORD PTR SS:[EBP-8]	
00408C52	. E8 89ECFFFF	CALL panda.004078E0	
00408C57	. 8D85 8CFEFFFF	LEA EAX,DWORD PTR SS:[EBP-174]	
00408C5D	. 50	PUSH EAX	
00408C5E	. E8 01BFFFFFF	CALL <JMP.&kernel32.GetLocalTime>	
00408C63	. 8D95 D4FDFFFF	LEA EDX,DWORD PTR SS:[EBP-22C]	
00408C69	. 0FB785 8CFEFF	MOUZX EAX,WORD PTR SS:[EBP-174]	

ASCII "\Desktop_.ini"

ASCII "\Desktop_.ini"

pLocaltim
GetLocalTime

被感染的文件类型

00409BC2	. 50	PUSH EAX	
00409BC3	. 8D95 70FDFFFF	LEA EDX,DWORD PTR SS:[EBP-290]	
00409BC9	. B8 38A14000	MOU EAX,panda.0040A138	
00409BCE	. E8 59B7FFFFFF	CALL panda.0040532C	
00409BD3	. 8B95 70FDFFFF	MOU EDX,DWORD PTR SS:[EBP-290]	
00409BD9	. 58	POP EAX	
00409BDA	. E8 39A4FFFF	CALL panda.00404018	
00409BDF	. v 75 1F	JNZ SHORT panda.00409C00	
00409BE1	. 8D85 6CFDFFFF	LEA EAX,DWORD PTR SS:[EBP-294]	
00409BE7	. 8B8D A8FEFFFF	MOV ECX,DWORD PTR SS:[EBP-158]	
00409BED	. 8B55 FC	MOV EDX,DWORD PTR SS:[EBP-4]	
00409BF0	. E8 23A3FFFF	CALL panda.00403F18	
00409BF5	. 8B85 6CFDFFFF	MOV EAX,DWORD PTR SS:[EBP-294]	
00409BFB	. E8 F4DEFFFF	CALL panda.00407AF4	
00409C00	> 8D95 64FDFFFF	LEA EDX,DWORD PTR SS:[EBP-29C]	
00409C06	. 8B85 A8FEFFFF	MOV EAX,DWORD PTR SS:[EBP-158]	
00409C0C	. E8 47B8FFFFFF	CALL panda.00405458	
00409C11	. 8B85 64FDFFFF	MOV EAX,DWORD PTR SS:[EBP-29C]	
00409C17	. 8D95 68FDFFFF	LEA EDX,DWORD PTR SS:[EBP-298]	
00409C1D	. E8 0AB7FFFFFF	CALL panda.0040532C	
00409C22	. 8B85 68FDFFFF	MOU EAX,DWORD PTR SS:[EBP-298]	
00409C28	. 50	PUSH EAX	
00409C29	. 8D95 60FDFFFF	LEA EDX,DWORD PTR SS:[EBP-2A0]	
00409C2F	. B8 44A14000	MOU EAX,panda.0040A144	
00409C34	. E8 F3B6FFFFFF	CALL panda.0040532C	
00409C39	. 8B95 60FDFFFF	MOU EDX,DWORD PTR SS:[EBP-2A0]	
00409C3F	. 58	POP EAX	
00409C40	. E8 D3A3FFFF	CALL panda.00404018	
00409C45	. v 75 1F	JNZ SHORT panda.00409C66	
00409C47	. 8D85 5CFDFFFF	LEA EAX,DWORD PTR SS:[EBP-2A4]	
00409C4D	. 8B8D A8FEFFFF	MOV ECX,DWORD PTR SS:[EBP-158]	
00409C53	. 8B55 FC	MOV EDX,DWORD PTR SS:[EBP-4]	
00409C56	. E8 BDA2FFFF	CALL panda.00403F18	
00409C5B	. 8B85 5CFDFFFF	MOV EAX,DWORD PTR SS:[EBP-2A4]	
00409C61	. E8 8EDEFFFF	CALL panda.00407AF4	
00409C66	> 8D95 54FDFFFF	LEA EDX,DWORD PTR SS:[EBP-2AC]	
00409C6C	. 8B85 A8FEFFFF	MOV EAX,DWORD PTR SS:[EBP-158]	
00409C72	. E8 E1B7FFFFFF	CALL panda.00405458	
00409C77	. 8B85 54FDFFFF	MOU EAX,DWORD PTR SS:[EBP-2AC]	
00409C7D	. 8D95 58FDFFFF	LEA EDX,DWORD PTR SS:[EBP-2A8]	
00409C83	. E8 A4B6FFFFFF	CALL panda.0040532C	
00409C88	. 8B85 58FDFFFF	MOU EAX,DWORD PTR SS:[EBP-2A8]	
00409C8E	. 50	PUSH EAX	
00409C8F	. 8D95 50FDFFFF	LEA EDX,DWORD PTR SS:[EBP-2B0]	
00409C95	. B8 54A14000	MOU EAX,panda.0040A154	
00409C9A	. E8 8DB6FFFFFF	CALL panda.0040532C	
00409C9F	. 8B95 50FDFFFF	MOU EDX,DWORD PTR SS:[EBP-2B0]	
00409CA5	. 58	POP EAX	
00409CA6	. E8 60A3FFFF	CALL panda.00404018	
00409CAB	. v 75 1F	JNZ SHORT panda.00409CCC	
00409CAD	. 8D85 4CFDFFFF	LEA EAX,DWORD PTR SS:[EBP-2B4]	
00409CB3	. 8B8D A8FEFFFF	MOV ECX,DWORD PTR SS:[EBP-158]	
00409CB9	. 8B55 FC	MOV EDX,DWORD PTR SS:[EBP-4]	
00409CCR	. F8 57A2FFFFFF	CALL panda.00403F18	

ASCII "htm"

ASCII "html"

ASCII "asp"