吾爱破解论坛

[LCG]

[LSG]

立足软件安全和病毒分析最前端，丰富的技术版块交相辉映，由无数加密解密及反病毒爱好者共同维护，留给世界一抹值得百年回眸的惊艳，沉淀百年来计算机应用之精华与优雅，信息线条与生活质感淡定交融，任岁月流转，低调而奢华的技术交流与研究却是亘古不变。

标题：卡饭上的马 分析

作者：smallyou93

样本来源：http://bbs.52pojie.cn/thread-23199-1-1.html

1.调用 CMD 执行以下命令：
cmd /c sc config ekrn start= disabled
cmd.exe /c taskkill.exe /im ekrn.exe /f

明显针对 Nod....

2.释放文件%SystemRoot%\System32\killdll.dll

反复写入该文件并加载
%SystemRoot%\System32\rundll32.exe %SystemRoot%\System32\killdll.dll testall

篡改驱动
%SystemRoot%\System32\Drivers\aec.SYS
%SystemRoot%\System32\Drivers\AsyncMac.sys

加载，恢复 SSDT

添加 IFEO，挟持多种安软

删除启动项
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

最后删除自身

3.释放文件%SystemRoot%\??????_xeex.exe

下载木马群。。。。
http://wgg.6d2n.com/01/fz.txt

1:http://u8.d7n9.com/sb/ok.exe
1:http://u2.d7n9.com/la/L1.exe
1:http://u2.d7n9.com/la/L3.exe
1:http://u2.d7n9.com/la/L4.exe
1:http://u2.d7n9.com/la/L5.exe
1:http://u2.d7n9.com/la/L6.exe
1:http://u2.d7n9.com/la/L7.exe
1:http://u3.d7n9.com/lm/S10.exe
1:http://u3.d7n9.com/lm/S1.exe
1:http://u3.d7n9.com/lm/S8.exe
1:http://u3.d7n9.com/lm/S2.exe
1:http://u3.d7n9.com/lm/S12.exe
1:http://u3.d7n9.com/lm/S14.exe

1:http://u3.d7n9.com/lm/S01.exe
1:http://u2.d7n9.com/lm/M5.exe
1:http://u2.d7n9.com/lm/M39.exe
1:http://u2.d7n9.com/lm/M25.exe
1:http://u2.d7n9.com/lm/M4.exe
1:http://u2.d7n9.com/lm/M35.exe
1:http://u2.d7n9.com/lm/M33.exe
1:http://u2.d7n9.com/lm/M01.exe
1:http://u3.d7n9.com/lm/S15.exe
1:http://u3.d7n9.com/lm/S16.exe
1:http://u3.d7n9.com/lm/S21.exe
1:http://u2.d7n9.com/lm/M37.exe
1:http://u2.d7n9.com/lm/M15.exe
1:http://u2.d7n9.com/lm/M24.exe
1:http://u2.d7n9.com/lm/M38.exe
1:http://u2.d7n9.com/lm/M23.exe
1:http://u2.d7n9.com/lm/M02.exe
1:http://u3.d7n9.com/lm/S13.exe
1:http://u3.d7n9.com/lm/S17.exe
1:http://u3.d7n9.com/lm/S20.exe
1:http://u3.d7n9.com/lm/S21.exe
1:http://u3.d7n9.com/lm/S11.exe
1:http://u7.d7n9.com/cj/1a.exe
1:http://u9.d7n9.com/cj/a2.exe
1:http://u9.d7n9.com/cj/a10.exe
1:http://u9.d7n9.com/cj/a6.exe
1:http://u7.d7n9.com/cj/a9.exe
1:http://u7.d7n9.com/cj/csj.exe
1:http://u0.d7n9.com/cj/a8.exe
1:http://u8.d7n9.com/sb/01.exe
1:http://u0.d7n9.com/cj/sb1.exe

4.释放文件%SystemRoot%\System32\Drivers\pcidump.sys
安装驱动并加载恢复 SSDT

_uok.bat（可能是随机名）
删除自身
:Repeat
del "C:\DOCUME~1\SMALLY~1\桌面\Actvev.exe"
if exist "C:\DOCUME~1\SMALLY~1\桌面\Actvev.exe" goto Repeat
rmdir C:\DOCUME~1\SMALLY~1\桌面
del "C:\DOCUME~1\SMALLY~1\LOCALS~1\Temp_uok.bat"

篡改驱动
%SystemRoot%\System32\Drivers\aec.SYS
%SystemRoot%\System32\Drivers\AsyncMac.sys

加载，恢复 SSDT

启动进程%SystemRoot%\??????_xeex.exe

%SystemRoot%\System32\Drivers\pcidump.sys
安装驱动并加载恢复 SSDT

关键是驱动，如果看守好 drivers 目录的话，这病毒就没戏了