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：Trojan.DL.Win32.MyDown.che 分析与其清除

作者：smallyou93

样本来自：http://ttttu.com.cn/qq.css

瑞星：Trojan.DL.Win32.MyDown.che

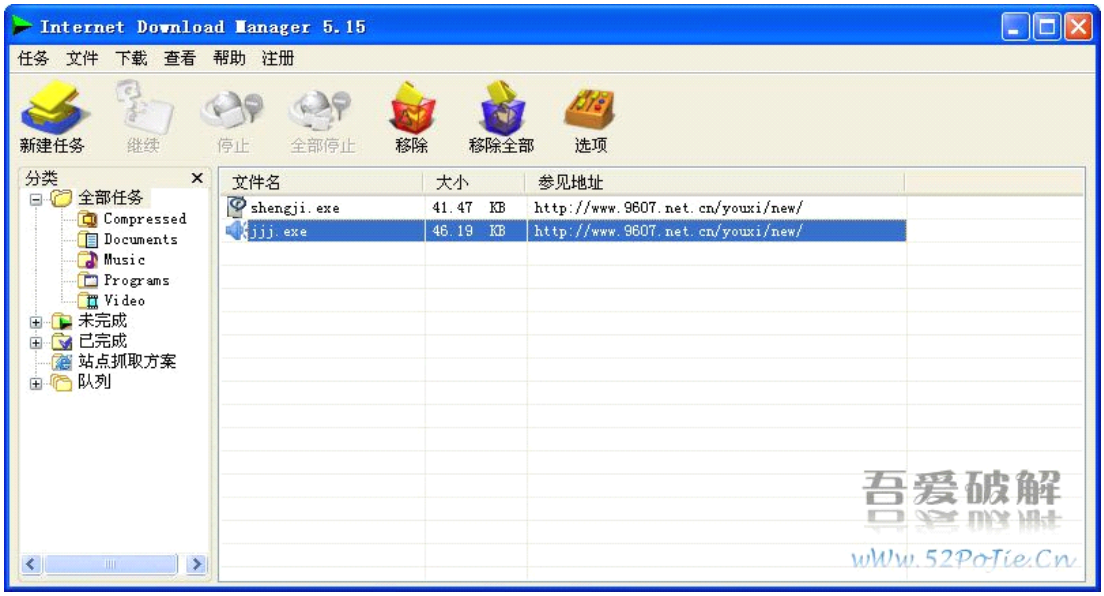
P.S：本文作者水平有限，若有错误，请指正..

释放文件
%windir%\system\jjxzwzjy******.exe
%windir%\system\jjxzbjcj32dl.dll
%ALLUSERSPROFILE%\jjjydf16.in
%ALLUSERSPROFILE%\jjdf32.inii

写入注册表
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\run]
"dlmcjjcefc"="C:\\WINDOWS\\system\\jjxzwzjy090329.exe"

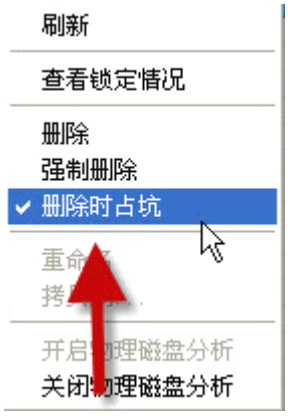
调出 iexplore.exe 联网下载病毒：
http://www.9607.net.cn/youxi/new/shengji.exe
http://www.9607.net.cn/youxi/new/jjj.exe

都给偶的 IDM 拦截了



调出 cmd 删除自身

清除方法：
下载 XUeTr
文件→C:\WINDOWS\SYSTEM
找到病毒后（排序下文件的创建时间）
右键，勾选



然后“强制删除”jjxzwzjy******.exe 和 jjxzbjcj32dl.dll

注册表
→HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\run
删除病毒的启动项