

实战新型U盘病毒 干掉“文件夹模仿者” Microsoft认证考试
PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/644/2021_2022__E5_AE_9E_E6_88_98_E6_96_B0_E5_c100_644561.htm 如果你发现U盘被杀毒软件报毒，杀毒后资料全部“失踪”，你会想到是病毒隐藏了正常的文件夹吗？近来，一类名为“文件夹模仿者”的U盘病毒正在疯狂传播，侵袭对象包括U盘、移动硬盘、数码相机存储卡、手机存储卡等各种移动设备。为此，国内唯一的“双核”杀毒软件360杀毒专门针对“文件夹模仿者”实施清剿，不光要把病毒杀掉，还能恢复U盘等移动设备中的正常文件，把珍贵的资料从病毒魔爪中拯救出来。据了解，“文件夹模仿者”主要通过U盘等移动设备进行传播，它会将U盘中的正常文件及文件夹隐藏，然后把自己伪装为被隐藏的文件/文件夹。同时，它还会把自己的图标改为文件夹图标或常见软件图标（如图片、视频等）。中招用户如果缺乏警惕，双击了病毒文件后，病毒就会立刻运行起来，把数十种木马病毒一股脑下载到和U盘相连接的电脑里，从而利用U盘在不同电脑间造成病毒的交叉感染。针对“文件夹模仿者”的恶行，“双核”360杀毒软件特别增强了对这类病毒的防护和查杀：在开启360杀毒“实时防护”功能的情况下，当用户把U盘等移动设备插入电脑时，如果U盘中存在同名的隐藏文件，360杀毒会立刻发出警告，并建议用户扫描U盘等移动设备。在“双核”的360云查杀引擎和杀毒引擎扫描下，“文件夹模仿者”自然会被轻松清除，被隐藏的文件和文件夹也会被360杀毒自动恢复到正常状态。即使用户电脑处于断网状态，云查杀引擎无法联网工作，360杀毒也会对“文件夹模仿

者”的可疑文件添加“.360”后缀，确保其不能运行。接下来，我们通过实测的方式看看“双核”360杀毒如何清除“文件夹模仿者”病毒。首先，在没有安装360杀毒的电脑中看看带有“文件夹模仿者”病毒的U盘。在不显示隐藏文件的情况下，带毒U盘看起来没有任何异状。我们依次点开“工具”-“文件夹选项”，让电脑把隐藏的文件和文件夹也显示出来，并且显示出文件类型的扩展名，结果让人大吃一惊。原来，真正的文件夹被病毒隐藏起来，摆在用户面前的是病毒的exe文件！很显然，如果用户缺乏警惕，一旦用鼠标双击了“图片收藏”或是“我的文档”，木马病毒将从U盘侵入电脑。接下来，我们在装有“双核”360杀毒软件的电脑中插入这个带毒U盘，病毒的伪装伎俩竟被瞬间揭穿。点击“扫描”后，即便“文件夹模仿者”病毒经过免杀处理，“双核”360杀毒也能够通过它的行为特征进行彻底查杀。经过360杀毒的紧急处理，善于伪装的文件夹模仿者病毒被一举干掉，被病毒隐藏起来的“图片收藏”和“我的文档”则被拯救出来，自动恢复到用户面前。有了这样的机制，用户保存在U盘等移动设备中的资料当然不会轻易丢失。100Test 下载频道开通，各类考试题目直接下载。详细请访问

www.100test.com