微软认证辅导:这病毒真牛(死了也要盗号)Microsoft认证考试
 病毒类型：下载类病毒、闪存类病毒 病毒目的：入侵系统，下载盗号病毒 小编点睛：病毒为何叫死牛？听圈内的朋友戏说，是因为它死了都要“ 牛 ”，不入侵你电脑誓不罢休，多种途径强行闯入，是一个人见人烦的恶性病毒，会下载各种盗号病毒，目标直指用户的各种账号和密码。 上周PDF漏洞爆发，由于漏洞官方补丁未能及时推出，不能自动更新，被许多病毒盯上，其中就有死牛病毒（截至到发稿，官方自动升级补丁还没有推出）。死牛病毒是一个专门下载盗号病毒、关闭杀毒软件的恶性病毒。“ 黑榜 ”一周收录了与死牛病毒相关的挂马网页57个，而且还有逐渐增多的趋势。 这样一个恶性病毒会给用户造成什么后果呢？这就要从它下载的盗号病毒说起，它可以下载网游、网银、QQ等多个类型的盗号病毒。假想一下，如果它下载的是盗取网银的盗号病毒，当你在网上银行输入账号和密码的时候，电脑中的盗号病毒就秘密地盗取了你的这些重要信息，你账号中的资金就可能会展出一对“ 黑色的翅膀 ”，不翼而飞了。 许多朋友看了上期的文章，也安装了临时的PDF漏洞补丁，这下应该没有事情了吧？其实你安装了临时补丁，并也不意味着安全了。死牛病毒还有一招“ 杀手锏 ”，利用最新的MSO9-002漏洞，一个当前非常受黑客青睐的挂马漏洞，进行挂马传播。如果你没有打上MSO9-002漏洞补丁，还是逃不过死牛病毒的“ 魔掌 ”。 如果你长期关注安全版，这下漏洞补丁早应该打上了，但别以为这样死牛

病毒就进不来了。平时用闪存吧！如果你电脑没有关闭自动播放功能，这个功能默认是开启的，死牛病毒就会通过闪存进入你的电脑。 病毒原理：死牛病毒进入系统以后，会将自身文件释放到临时目录，接着再加载到系统内存中。病毒进程往往以 SafeSys（23）.exe的形式出现，其中括号中的数字是随机生成的。病毒主文件SafeSys.exe会复制到所有磁盘的根目录里面。之后，死牛病毒将破坏系统的注册表，生成kvnad、stiva等服务，用来自启动。最后它就会利用ARP攻击对局域网进行破坏，下载其他盗号木马。 克制病毒方案 第一步：断开系统的网络连接。运行进程管理工具Wsyscheck（下载地址：http://www.shudoo.com/bzsoft），选中被标成红色的SafeSys（23）.exe进程以及那些粉紫红色的系统进程，然后点击右键选择“ 选择结束的进程 ”即可。需要说明的是，这时系统桌面将会消失，但并不影响后面的操作。 第二步：点击Wsyscheck中的“ 服务管理 ”，选中红色的病毒启动服务HidServ、iwwsfvufqiqg、kvnad、stiva，点击右键选择“ 删除选中的服务 ”即可。另外再点击“ 安全检查→活动文件 ”标签，选择除ctfmon.exe以及驱动程序以外的所有选项，点击右键选择“ 修复所选项 ”即可。 第三步：运行“ 文件删除终结者 ”，将System32、IE浏览器目录、磁盘根目录、以及临时目录中的病毒文件，通过鼠标拖放到程序的文件列表里面，点击右键选择“ 立即重启执行删除 ”即可。再点击“ 安全检查→常规检查 ”标签，选择“ 禁用程序管理 ”列表中的所有内容，点击右键选择“ 允许程序运行 ”就可以解除映像劫持。 第四步：重新启动系统，然后调出系统修复工具SREng（下载地址：http://download.cpcw.com/soft/260/260765.html），点击

“ 系统修复→高级修复 ” 标签，再点击 “ 自动修复 ” 即可恢复被病毒破坏的系统。 最后打开杀毒软件（例如《金山毒霸》， 下载地址：http://www.duba.net/download/index.shtml）,升级病毒库到最新版本，再进行全盘查杀，彻底未打补丁这段时间可能已经乘虚而入的病毒。 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