病毒伪装假冒软件注册机传播计算机等级考试 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__E7_97_85_E6_AF_92_E4_BC_AA_E8_c98_644362.htm 江民反病毒中心监测到，越来越多的病毒开始巧妙使用伪装术，伪装成一些知名软件，达到混淆用户视线逃避查杀的目的。 在江民反病毒中心近日截获的病毒中，“ 克隆先生 ”变种cmo和“ 蝎子王 ”变种p均属于此类伪装病毒。“ 克隆先生 ”变种cmo运行后，自我复制到被感染计算机系统的“ %SystemRoot%＼system32＼ ”文件夹下，并重命名为“ Zip Monsta.exe ”，图标与WINZIP十分相似。“ 克隆先生 ”变种cmo运行后，关闭名为“ Windows Task Manager ”和“ Registry Editor ”的窗口，自我复制到“ C:＼My Shared Folder＼ ”目录下并命名为“ Winzip keygen.exe ”(WINZIP注册机)、“ Norton keygen.exe ”(诺顿注册机)、“ Nero 6 keygen.exe ”(NERO刻录软件注册机)等，试图通过一些P2P网络资源共享软件进行传播。“ 克隆先生 ”变种cmo运行后，会搜索并删除受感染计算机上的所有名为“ *.zip* ”、“ *.rar* ”和“ *.tar* ”的文件。“ 克隆先生 ”变种cmo会通过在被感染计算机系统注册表启动项中添加新键“ Zip Monsta ”的方式来实现木马开机自动运行。 Backdoor/Shift.p“ 蝎子王 ”变种p运行后，则会自我复制到被感染计算机系统的“ %SystemRoot%＼system32＼ ”文件夹下，并重命名为“ wscsvc.exe ”。“ 蝎子王 ”变种p会在被感染计算机的后台遍历当前系统中所有正在运行的进程，一旦发现指定的安全软件便会尝试结束这些安全软件的进程，从而达到自我保护的目的。将自身注册为系统服务运行，不断尝

试与控制端(地址为：yc.puj*wang.com:8101)进行连接，如果连接成功，通过端口监听、数据包交换，接受攻击者发来的指令执行相应的恶意操作，可能对受感染计算机进行进程管理、文件操作、服务管理、连接指定地址下载其他恶意程序等，给用户的计算机安全、个人隐私、甚至是商业机密造成不同程度的损失。病毒会在被感染计算机中注册名为“ syswscsvc ”的系统服务，实现后门开机自启动，服务名称显示为“ Windows Security Center ”(微软Windows安全中心)。江民反病毒专家提醒用户，在遇到此类经过伪装的病毒时，不要被病毒表面现象迷惑，使用带有主动防御“ 沙盒技术 ”和启发式扫描功能的正版杀毒软件进行查杀，相信杀毒软件的判断结果，不给病毒有任何逃避的机会。江民杀毒软件KV2009“ 沙盒技术 ”可以使此类病毒脱去伪装，通过病毒行为准确识别病毒体，确保用户电脑免遭病毒侵害。江民反病毒专家还建议用户，务必去正规网站下载正版软件，慎用网上的各种注册机，以免遭到此类伪装成软件注册机的病毒“ 暗算 ”。 