

新蠕虫W32.Mocon专门窃取用户击键记录计算机等级考试

PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/580/2021\\_2022\\_\\_E6\\_96\\_B0\\_E8\\_A0\\_95\\_E8\\_99\\_ABW\\_c98\\_580458.htm](https://www.100test.com/kao_ti2020/580/2021_2022__E6_96_B0_E8_A0_95_E8_99_ABW_c98_580458.htm)

蠕虫W32.Mocon专门窃取用户击键记录，通过主动拷贝自身至移动存储设备中进行传播。病毒名称：W32.Mocon 病毒类型：蠕虫 受影响的操作系统：Windows 95/98/2000/Me/XP/Vista/NT、Windows Server 2003 病毒分析：浏览网页，上网聊天，网络购物等已成为很多计算机用户的常规活动。用户需要输入网址、用户名和密码登陆网站；如果需要进行网上交易，用户还需输入自己的银行账户和密码等信息。这些都是攻击者认为有利可图的信息，因此，盗取这类信息的病毒也就层出不穷。赛门铁克安全响应中心最新监测到一个专门窃取用户击键记录的蠕虫W32.Mocon。一旦感染成功，W32.Mocon会将自己拷贝到C盘根目录下，伪装成系统文件，并更名为cssrs.exe。同时创建autorun.inf，使得用户在每次打开C盘时蠕虫都会自动运行。蠕虫将这两个文件设置为隐藏属性，以避免被用户发现。另外，W32.Mocon还会创建注册表键值以实现开机自动启动。W32.Mocon的最大安全威胁在于它会试图记录和窃取用户的键盘击键记录，如用户的账号和密码等，并将窃取的保密信息发送到指定的恶意服务器。W32.Mocon主要通过主动拷贝自身至移动存储设备中进行传播，以进一步感染其它计算机。诺顿安全专家建议：1.诺顿安全软件独有的“身份防护”功能，协助用户自动登录网站和填写表单，以防止窃听击键记录程序窃取您的保密信息。2.配置诺顿安全软件的“智能双向防火墙”功能，阻止不明应用程序访问网络，令被

窃取的用户信息无法传输。 3.及时安装操作系统的安全更新，并禁用可移动存储设备的“自动运行”功能。 4.没有安装安全软件的用户可以下载诺顿360（3.0版）、诺顿网络安全特警2009或诺顿防病毒2009试用版对病毒进行查杀。 5.使用诺顿2006版本及之后产品的现有用户，可以免费将产品升级至诺顿2009版本。

**赛门铁克中国安全响应中心简介** 赛门铁克中国安全响应中心于2008年2月成立于成都，与位于全球各地的安全响应中心共同协作，针对当前威胁和安全风险进行监控分析，主动识别并分析新型威胁，并将作为中国互联网安全威胁现状的窗口，为本地以及全球用户提供更为强大的覆盖力度，从容应对新型威胁。

2009年上半年全国计算机等级考试参考答案请进入计算机考试论坛 2009年全国计算机等级考试报名信息汇总 2009年NCRE考试有新变化 2009年全国计算机等级考试大纲 2009年上半年全国计算机二级考试试题及答案 2009年上半年全国计算机等级考试试题答案汇总 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](http://www.100test.com)