

WinXP中震荡波后应采取的措施 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/454/2021_2022_WinXP_E4_B8_AD_E9_9C_c100_454528.htm

如果您使用的是 Microsoft Windows XP 或 Windows XP Service Pack 1 (SP1) 并且您的计算机感染了震荡波蠕虫病毒，则可以采取这些措施来更新您的软件、移除蠕虫病毒并使您免于以后再被感染。

第1步：断开 Internet 连接 为了避免出现更多问题，请断开 Internet 连接：

宽带连接用户：确定连接外置 DSL 或网线调制解调器的网线位置，然后从调制解调器或电话线插孔将该网线拔下。

拨号连接用户：确定连接计算机内置调制解调器与电话线插孔的网线位置，然后从电话线插孔或从计算机将该网线拔下。

第2步：终止关机周期 此蠕虫会导致 LSASS.EXE 停止响应，此程序使操作系统在 60 秒钟后强行关机。如果您的计算机开始关机，请按照这些步骤中断可能处于运行状态的任意系统关机进程。在屏幕底部的任务栏上单击“开始”，然后单击“运行”。键入“cmd”，然后单击“确定”。在命令提示符下，键入“shutdown.exe -a”，然后按 ENTER。

第3步：减轻漏洞隐患 您可以通过创建日志文件来暂时消除令蠕虫病毒可通过其侵入计算机的漏洞。创建日志文件 在屏幕底部的任务栏上单击“开始”，然后单击“运行”。键入“cmd”，然后单击“确定”。在命令提示符下键入“echo dcpromo >%systemroot%\debug\dcpromo.log”，然后按 ENTER。将日志文件设置为只读属性 在命令提示符下键入“attrib R %systemroot%\debug\dcpromo.log”，然后按 ENTER。

第4步：改善系统性能 如果您的计算机反应迟缓或者 Internet 连接

速度过慢，则说明蠕虫病毒可能已经在您的局域网连接内扩散。这会使您无法下载并安装所需的软件更新。要改善系统性能：按 CTRL ALT DELETE，然后单击“任务管理器”。对于以下可能列出的每个任务，单击并选中该任务，然后单击“结束任务”按钮，将其结束。任意以_up.exe 结尾的任务（例如 12345_up.exe）。任意以avserve开头的任务（例如 avserve.exe）。任意以avserve2开头的任务（例如 avserve2.exe）。任意以skynetave开头的任务（例如 skynetave.exe）。hkey.exe msiwin84.exe wmiprvsw.exe 注意：切勿结束 wmiprvse.exe 任务；这是一个合法的系统任务。

第5步：启用防火墙 防火墙是一个软件或硬件，能够在计算机和 Internet 之间构筑一道保护屏障。如果您的计算机已感染病毒，防火墙将有助于限制蠕虫的影响。Windows XP 包含 Internet 连接防火墙 (ICF)。要打开 ICF：在屏幕底部的任务栏上单击“开始”，然后单击“控制面板”。单击“网络与 Internet 连接”。（如果未显示“网络与 Internet 连接”，请单击“控制面板”窗口左侧“控制面板”中的“切换到分类视图”。）单击“网络连接”。右键单击用于连接至 Internet 的拨号、LAN 或高速 Internet 连接，然后单击快捷菜单中的“属性”。在“Internet 连接防火墙”的“高级”选项卡上，选择“保护我的计算机和网络”，然后单击“确定”。现在，您便已开始启用 Windows XP 防火墙。

第6步：重新连接 Internet 将网线（参阅第1步）重新接回计算机、电话线插孔或调制解调器。

第7步：安装所需的更新 要使以后您的计算机不受此蠕虫病毒的感染，您必须下载并安装安全更新 835732，安全更新下载。

第8步：检查并移除震荡波蠕虫 在完成安装更新

并重新启动计算机后，转到网页上的“ What You Should Know About the Sasser Worm and Its Variants ”（对于震荡波蠕虫及其变体您应该了解的信息）。使用震荡波蠕虫移除工具搜索您的硬盘并移除 Sasser.A、Sasser.B、Sasser.C 和 Sasser.D。（微软）

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