找出木马背后的黑手 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/181/2021_2022__E6_89_BE_E5_87_BA_E6_9C_A8_E9_c101_181844.htm 当你发现自己的爱机中了木马时一定很气愤，很想知道是谁把马放在你的爱机里。这里先简单解释一下原理，然后去找出马的主人吧! 现在很多木马都有发IP信件的功能，“ 冰河 ”就是其中的佼佼者，也是国内用得最多的木马。它能把你的动态IP，电脑里的隐藏密码和个人信息等在受害密码和个人信息等在受害者不知道的情况下记录下来并发到指定的E-mail信箱。我们就利用它发的IP信是明文信息的特点(现在好像还没有哪个木马发的IP信有进行过加密的)，用sniffer类软件把它记录下来。这样我们就能知道对你用过木马那人的E-mail了。所以我们不要立即把爱机里的木马清除掉(不入虎穴焉得虎子)，因为我们还要靠它找出它的主人呢! 首先去下载必要的工具，http://www.xfocus.org/htm1/data/tools/winsniff.zip(在DOS下运行)或HTTP://www.guanqian.com/starkun/tools/other/mpsnif01013.zip(在windos下运行)。两个不同环境下运行的工具各有所长。 一、DOS下winsniff的用法 在c盘创建一个winsniff目录，把包解压，解压后它里面有七个文件。 打开一个MS-DOS窗口(“ 点击开始--程序--MS-DOS方式 ”)进入winsniff目录(在MSDOS方式下输入cd\winsniff,跟着按车键)。接着输入winsniff/1，按回车，检查拨号适配器的编号(这里检查结果为0)。 输入winsniff/a 0 /a mail.txt,按回车，这时显示，其中的“ 0 ”是表示你的拨号适配器即modem的编号，当你还装有其它网络设

备(如:局域网网卡)时它就不一定是0 了，那时就要因应不同的需要而改变，“ mail.txt ”是表示记录文件的名字，可以任意取名字。 接着就是拨号上网或与网络连接(局域网的用户)，等着winsniff帮你截获信息吧。 当你看到显示，出现“ [mail] ”时请按“ ctrl c ”键结束程序，这时你就可以用笔记本打开“ mail.txt ”文件看看里面的信息了，是不是很惊讶呢，你的密码什么的都给记录下来了!记录文件中的“ TO: ”后面显示的E-mail地址就是木马主人的E-mail地址了，跟阆想怎么利用这E- mail地址对付那可恶的人就你自已喜欢了，呵呵。但不要玩过火了!这软件的优点是比较稳定不容易出错.缺点就是操作烦琐，适合具备一点DOS操作经验的人用，但我个人比较喜欢用它，因为稳定! 二、Windows下masnif的使用 在c盘创建一个mpsnif目录，把它解压，解压后有四个文件。通过双击MPSnif文件运行软件，它的工作界面如图4所示。 首先要对它进行一下设置，点击一下设置，点击一下“ setup ”按钮就会出现所示对话框，“ Dicectory(目录) ”后原来填的是“ c:\ ”，把它改为“ C:\mpsnif\ ”，而“ DNS ”可以忽略，点击“ OK ”按钮后它会再出现一个对话框，忽略它点击“ 确定 ”即可。然后把软件关掉再重新启动，这时刚才的设置就生效了。 选择要监视的设备，一般是选“ 拨号适配器 ”(如果你还装了其它网络设备，并且要对它进行监视才选你要监视的设备)。还要选择要监视的协议，单击“ TCP ports ”选中“ Smtp(25) ”，使它的前面有个钩。 这时可以点击“ Start ”按钮使软件开始工作，按着要做的就是拨号上网或与网络连接(局域网的用户)，等着MPsnif帮你截获信息。我们也可以去干别的事，这时MPSnif会显示很多数据记录。 等下到网后再

到“ C:mpsnif ”目录中查找并打开文件名为XXX_XXX_XXX_XXX$XXX-XXX_XXX_XXX_XXX $25_XXXXXXX的文件(其中$XXXX为你在发信出去时在本机打开的承受机端口，而它前面的XXX_XXX_XXX_XXX是你该次上网的IP地址.$25为邮件服务器打开的S M T P 端口，它前面的XXXXXX为该邮件的大小)，在文件里“ TO: ”后面的E-mail地址就是木马主人的E-mail地址了。这软件的优点是操作较为简单方便，容易使用，功能比上面那个强(还有很多别的监视功能，有兴趣的可以自己研究。).缺点是不够稳定，常提示你程序出错(可能是它还是测试版的原因吧，或是我的系统出了问题)，但不会影响到它的拦截数据的功能，它适合那些对电脑了解不深的人应用。 三、使用注意事项 1.运行这两个软件时都必须要在拨号上网或与网络连接前就运行，因为这样才能肯定拦截到木马所发出的IP信. 2.在运行这两个软件时不要作任何收发邮件的工作，因为这样会影响到拦截数据的准确性，给你造成“ 误报 ”的可能性. 3.这两个软件者不是百分之百的不会出问题，有时可能会拦截不到，请多试一两次提高准确率. 4.我们知道木马主人的E-mail后，记得把爱机里的木马给清除了，这样才能彻底的杜绝其他人对你爱机进行的木马侵扰. 5.在给木马主人的惩罚时请适可而止，不要过火了，到时候造成别的人严重损失时理亏就会变成你了. 6.这两个软件都会牵涉到一些别的安全问题，请不要用来做