电脑操作指南

# 电脑防毒杀毒手册

崔永普　主编

经■济■管■理■出■版■社

# 第三章　病毒的检测及清除

## 1. 怎样手工清除“SQL 服务器”蠕虫病毒



（1）使用服务器网络管理工具把 1433 端口关闭。

（2）用多协议进行通讯。

（3）把运行的 JS 脚本删除：

\ System32 \ Sqlprocess. js

\ System32 \ Sqlexec. js

\ System32 \ Run. js

\ System32 \ Sqldir. js

\ System32 \ Sqlprocess. js

\ System32 \ Sqlexec. js

（4）关闭 GUEST 用户。

（5）删除 cscript. exe 以后恢复。

（6）修复注册表中的键值：在 HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ NetDDE 中删除 ImagePath % COMSPEC% /c start netdde && sqlprocess init

Start2；在 HKEY_LOCAL_MACHINE \ software \ microsoft \ mssqlserver \ client \ connectto 中删除 dsquery dbmssocn。

（7）修改 SA 账号和 GUEST 账号的密码。

（8）使用服务器管理程序删除 XP_CMDSHELL 的扩展存储过程。

## 2. 怎样清除“恶邮差（Worm. Supnot. 78858. c）”病毒

四级恶性蠕虫病毒“恶邮差”的英文名称是“Worm. Supnot. 78858. c”，是蠕虫病毒“Supnot”的最新变种，而且改进了以前版本通过邮件传播方面的性能，手段极其“恶毒”。



“恶邮差”病毒典型破坏行为是能够根据收件箱中的邮件内容自动回复邮件，每封邮件的附件中均携带病毒副本。由于接收者看到的是对已发送邮件的回信，很可能会打开该邮件导致中招。由此邮件服务器可能会在极短时间内不堪重负而崩溃。病毒运行后会搜索本地目录，通过收件箱中的邮件地址向外发送带毒邮件传播自身。病毒会根据收件箱里面的邮件回复带毒邮件给原始发件人，这时的带毒邮件的主题和内容就跟原始邮件有关。

病毒名称：Worm. Supnot. 78858. c。

病毒中文名称：恶邮差。

病毒类型：蠕虫病毒。

病毒长度：78848 字节。

危害级别：中。

传播速度：快。

技术特征：该病毒是蠕虫 Supnot 的最新变种，病毒用 ASPack 压缩，并且改进了以前版本通过邮件传播方面的性能。

病毒运行后会搜索本地文件目录，通过收件箱中的邮件地址向外发送带毒邮件传播自身。病毒激活后会复制自身到系统目录，文件名可能为 winrpc. exe、WinGate. exe、WinRpcsrv. exe、rpcsrv. exe 或 syshelp. exe。病毒可能还会在系统目录生成 1. dll、ily. dll、Task. dll、reg. dll 等文件。病毒还会修改注册表中系统启动项和 txt 文件打开的关联等。

病毒感染 Windows 95/98/Me 的系统后修改 win. ini 文件，在其 Windows 节中添加 run = rpcsrv. exe。病毒会试图生成木马文件（如 1. dll、ily. dll、Task. dll、reg. dll）到系统目录下，会修改注册表，搜寻网络共享目录，监听 10168 端口，允许黑客在被感染的机器上执行不同的动作。

病毒感染 Windows NT/2000/XP 的系统后会复制 ssrv. exe 到系统目录，并修改注册表，启动木马为服务，遍历本地网络，试图登陆其他电脑。

带毒邮件的特征：

可能的附件名：fun. exe、humor. exe、docs. exe、s3msong. exe、midsong. exe、billgt. exe、Card. EXE、SETUP. EXE、searchURL. exe、tamagotxi. exe、hamster. exe、news_doc. exe、PsPGame. exe、joke. exe、images. exe、pics. exe、Roms. exe、Sex. exe、Setup. exe、Source. exe、_SetupB. exe、Pack. exe、LUPdate. exe、Patch. exe、CrkList. exe

病毒会根据收件箱里面的邮件回复带毒邮件给原始发件

人，这时的带毒邮件的主题和内容就跟原始邮件有关。此外，病毒还有可能选择以下主题和内容：

**可能的主题：**Documents、Roms、Pr0n！、Evaluation copy、Help、Beta、Do not release、Last Update、The patch、Cracks！

**可能的邮件正文：**Send me your comments...；Test this ROM！IT ROCKS！；Adult content！！！Use with parental advisory；Test it 30 days for free；I'm going crazy...please try to find the bug！；Send reply if you want to be official beta tester；This is the pack；This is the last cumulative update；I think all will work fine；Check our list and mail your requests！

**病毒清除方法：**



（1）使用资源管理器查看进程，注意 winrpcsrv. exe、winrpc. exe、wingate. exe、syshelp. exe、rpcsrv. exe、iexplore. exe、winVNC. exe...均为病毒（或由病毒生成的后门软件），甚至其他一切不常见的进程都有可能是病毒，如果不能确定，找一台服务器上的进程来观察（服务器应该不会被感染）。

（2）将程序（后门）的进程结束掉，对于不能结束的进程，可以使用附件中的 pskill. exe 结束掉（命令格式“pskill 进程名”）。

（3）打开“服务”，在服务列表中将没有“描述”服务进行筛选，查找是否有“Browser Telnet”、“Event Thread”“Windows Management Extension”……的服务，依次删掉注册表中的［HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ BRWWTELK ］；

[HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ prom0n. exe]；[HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ Windows anagement Extension]；[HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ Window Remote Service]；[HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Run（Run Services）]；[HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run（Run Services）……**的相关的键值。**

（4）**删掉**[HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ dll_reg]**[**HKEY_CLASSES_ROOT \ Applications \ winrpc. exe]**的键值。**

（5）**修改**[HKEY_CLASSES_ROOT \ txtfile \ shell \ open \ command]**的右侧的默认键值为“** % SystemRoot% \ system32 \ NOTEPAD. EXE % 1 **”。此时，**. txt **的文件无法正常打开，可以点击文本文件的右键，选择其他方式，选择使用** Notepad **即可。**

（6）**删掉系统** system32 **目录下的以下程序（大部分可执行程序的大小都为** 78848 **字节）：**winrpcsrv. exe、winrpc. exe、wingate. exe、syshelp. exe、rpcsrv. exe、iexplore. exe、prom0n. exe**（注意中间的是数字** 0**）**、irftpd. exe、irftpd. dll、iexplore. exe、reg. dll、task. dll、ily. dll、Thdstat. exe、1. dll、winvnc. exe。

（7）**清空“** C：\ Documents and Settings \ Default User**（或** Default Uesr. . WINNT） \ Local Settings \ Temporary Inter-

net Files \ Content. IE5 ”目录下除了“ desktop. ini ”的所有文件，该路径下，发现有一些后门软件。

（8）关闭所有目录的完全共享！这是关闭了该程序通过网络感染的途径。

（9）重新启动电脑，观察是否还有类似进程出现，尤其是 irftpd. exe，这个程序是由上述第 3 步的“ 服务 ”程序自动生成的。

## 3. 怎样清除“红色代码新变种（CodeRed. F）”蠕虫病毒



病毒名称：CodeRed. F。

病毒类型：蠕虫病毒。

受感染的系统：病毒的攻击的对象为安装了 IIS 的 Windows NT/2000 系统，并且仅仅影响没有打微软的 MS01-033 补丁的 IIS 服务器。

病毒特征：“ CodeRed. F ”利用微软 IIS 远程缓冲区溢出漏洞获取系统权限实施攻击，并在这个被感染的 Web 服务器上安装一个后门程序，使得攻击者对被感染系统具有完全的访问权限，因此，一旦遭受感染，网络安全就会受到严重威胁。

“ CodeRed. F ”通过 IIS 服务器的 idq 缓冲区溢出漏洞在 Web 服务器上安装并繁衍，只有没有安装最后的 IIS service pack 的系统才会受影响。

当 Web 服务器受感染后，病毒将执行下面操作：

（1）调用初始化程序，在 IIS Server 服务进程空间中找



到 Kernel32. dll 的基地址。

（2）接着查找 GetProcAddress 的地址。

（3）调用 GetProcAddress，并访问其他 API 的地址，包括：LoadLibrayA、CreateThread、GetSystemTime 等。

然后病毒加载 WS2_32. dll 并调用相关的 TCP/IP 函数，如 socket 等，在从 User32. dll 中调用 ExitWindowsEx 函数以便重新启动系统。

病毒的主线程检查两个标识：

①“29A”，这个用来控制随蠕虫病毒的后门木马的安装。

② 另一个是“CodeRedll”，如果该信号存在，那么蠕虫病毒将进入无限制的休眠。

病毒的主线程还会检查系统的默认语言，如果默认语言是中文（繁体中文或者简体中文），就会创建 600 个新的扫描线程，否则就创建 300 个扫描线程，这些线程根据随机产生的 IP 地址扫描新的主机，并试图感染。在这些扫描线程创建时，病毒的主线程复制 Cmd. exe 到以下地方：



C：\ Inetpub \ Scripts \ Root. exe

D：\ Inetpub \ Scripts \ Root. exe

C：\ Progra ~ 1 \ Common ~ 1 \ System \ MSADC \ Root. exe

D：\ Progra ~ 1 \ Common ~ 1 \ System \ MSADC \ Root. exe

病毒在主机中安装的后门会在注册表中添加下面内容：HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ W3SVC \ Parameters \ Virtual Roots。

通过该修改，并将用户组设置为 217，那么，黑客就可以通过 Web 服务器用 HTTP 的 GET 请求在服务器上执行 scripts/root. exe 程序。

病毒的主线程会在中文系统上休眠 48 小时，而其他系统则休眠 24 小时。但是，那些扫描线程仍然继续运行，并试图去感染其他电脑主机。当病毒的主线程重新苏醒时，会重新启动主机。同时，所有的线程会检查是否是 10 月或者以后，以及年份大于 34951，如果是，那么系统就被重新启动。

该病毒复制的 cmd. exe 程序到 IIS 的默认可执行目录下，那么，就允许进行远程控制。同时它也会设置 C：\ Explorer. exe 和 D：\ Explorer. exe 属性为隐藏、系统文件和只读文件。



主机被感染 24 小时或者 48 小时后，系统会被重新启动，相同的主机可能被重复感染，除非安装了最新的补丁。如果月份是 10 月或者以后，以及年份大于 34951，那么系统也会被重新启动。当系统重新启动后，木马就在系统执行 Explorer. exe 时运行起来。C：\ Explorer. exe 木马先休眠几分钟，然后重新设置键值并“确认”。

注意：当电脑重新启动后，内存中原本驻留的蠕虫病毒就不存在了，那么，它将不会重新去感染其他主机，除非该主机又被重新感染。

木马会修改注册表：HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Windows NT \ CurrentVersion \ Winlogon 并将 SFCDisable 设置为 0xFFFFFF9D，这个修改会禁止系统文件检查保护（SFC）。

**注意：如果在运行** Microsoft FrontPage **或者其他** Web **编辑程序，**IIS **可能会被重新安装。**

**清除方法：**

① **杀掉木马的进程。在进程管理器中，可以看见两个** Exploere. exe **进程，其中一个是合法的，另一个则是木马进程。要确认哪个是木马进程，请在查看——选择列中选择上线程数。这时你可以看见只有** 1 **个线程的** Exploere. exe **进程，这个就是木马的进程。请终止该进程的运行。**

② **删除** Exploere. exe **文件。这些文件有隐藏、系统文件和只读文件属性。请运行** cmd. exe**，并执行下面的命令：**

```
cd c:\
attrib -h -s -r explorer. exe
del explorer. exe
cd d:\
attrib -h -s -r explorer. exe
del explorer. exe
```

③ **删除下面的文件（可能存在）：**

C：\ Inetpub \ Scripts \ Root. exe

D：\ Inetpub \ Scripts \ Root. exe

C：\ Progra ~ 1 \ Common ~ 1 \ System \ MSADC \ Root. exe

D：\ Progra ~ 1 \ Common ~ 1 \ System \ MSADC \ Root. exe

④ **在** IIS **管理器中，删除** C、D **或者其他驱动器根的虚拟目录。**

⑤ **删除注册表的相关项。**

在注册表的下面位置：HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ W3SVC \ Parameters \ Virtual Roots 中，删除其中的键为/C 和/D 的内容，双击/MSADC 和/Scripts，删除其中的数字 217，并修改为 201。

在注册表的下面位置：HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Windows NT \ CurrentVersion \ WinLogon 双击键 SFCDisable，修改其中的内容为 0。

⑥ 重新启动电脑系统，清除内存中的蠕虫病毒。为避免被病毒感染，请用户到以下链接下载微软针对该漏洞的安全补丁：

MS01-033 patch（http：//www. microsoft. com/technet/security/bulletin/MS01-033. asp）



MS01-044patch （http：//www. microsoft. com/technet/treeview/default. asp？url =/technet/security/bulletin/MS01-044. asp）

注：微软的 Service Pack 3 已经包含了该补丁。

## 4. 怎样判断和清除“红色代码（CodeRed）”、“红色代码 II（CodeRed2）”病毒

病毒类型：蠕虫病毒。

病毒传播途径及发作描述：“CodeRed”采用了一种叫做“缓存区溢出”的黑客技术，利用网络上使用微软 IIS 系统的服务器来进行病毒的传播。这个蠕虫病毒使用服务器的端口 80 进行传播，而这个端口正是 Web 服务器与浏览器进行信息交流的渠道。“CodeRed”主要有如下特征：入侵 IIS



服务器，“ CodeRed ”会将 WWW 英文站点改写为“ Hello！Welcome to www. Worm. com！Hacked by Chinese！”与其他病毒不同的是，“ CodeRed ”并不将病毒信息写入被攻击服务器的硬盘，它只是驻留在被攻击服务器的内存中，并借助这个服务器的网络连接攻击其他的服务器。

“ 红色代码 2 ”是“ 红色代码 ”的改良版，病毒作者对病毒体做了很多优化，同样可以对“ 红色代码 ”病毒可攻击的联网电脑发动进攻，但与“ 红色代码 ”不同的是，这种新变种不仅仅只对英文系统发动攻击，而是攻击任何语言的系统。而且这种病毒还可以在遭到攻击的机器上植入“ 特洛伊木马 ”，使得被攻击的机器“ 后门大开 ”。“ 红色代码 2 ”拥有极强的可扩充性，通过程序自行完成木马植入工作，使得病毒作者可以通过改进此程序来达到不同的破坏目的。当机器日期大于 2002 年 10 月时，病毒将强行重启电脑。



判断你的系统是否已被感染方法：

① 如果系统已被“ CodeRed ”蠕虫病毒感染，主页将无法正常显示，而被代之以“ Hacked by ××× （已遭××人入侵）”的提示信息。

② 如果您的服务器被更新的“ CodeRed II （红色代码 II）”蠕虫病毒感染，将在硬盘上发现 C：/Inetpub/scripts/root. exe 文件（如果除了 C 盘外还使用其他硬盘，则应对它们一并执行检测）。

防杀方法：

① 开启杀毒软件中的实时防病毒功能，可以防止病毒的感染。

②“红色代码”专杀工具——DubaqCodeRed2，文件大小为94.5K，适用平台为Windows 9X/Me/2000/NT，下载地址为http：//www.iduba.net/download/other/DubaqCodeRed2.exe。

## 5. 怎样清除‘QQ爱情森林（Trojan. Sckiss）”病毒

（1）“爱情森林”病毒。8月25日，金山反病毒应急处理中心截获到首个“爱情森林”病毒，在随后几天里，金山公司的反病毒监测网又截获其数个变种。据统计，该木马病毒已衍生出5个变种，这一系列病毒都是利用QQ软件的聊天机制向用户发送恶意网页链接，诱导用户点击以达到快速传播自己的目的。有的变种还会盗取用户的QQ密码。目前已有不少用户受此病毒危害。



病毒名称：Trojan. sckiss. 176643。

病毒类型：木马病毒。

感染长度：176643字节。

危害级别：低。

传播速度：慢。

病毒特征：该木马病毒原始文件名为hack. exe，用Delphi编写，并用UPX进行了压缩。木马病毒被运行后会：

①复制自身到Windows操作系统的system目录（通常为windowssystem）下，并改名为Explorer. exe。由于它和Windows目录下的Explorer文件同名，因此会迷惑用户，使用户误认为这是一个正常的系统文件。



②　修改注册表，在HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionRun下添加键值 Explorer = “% windowssystem% Explorer. exe”，使木马病毒可以在开机后自动运行（其中% windowssystem% 为 Windows 的系统目录）。

③该木马病毒还会在站点 http：//orchid. diy. 163. com/ 下载文件 update. exe，并执行下载下来的程序，进行其他的破坏活动。

（2）“爱情森林变种一”。

病毒名称：Trojan. Sckiss. 178752。

病毒类型：木马病毒。

感染长度：178752 字节。

危害级别：高。

传播速度：中。

病毒特征：该病毒运行后会：

①复制两个自己的复制到 Windows 的系统目录（Win9X 通常为 Windowssystem，WinNt 通常为 WinNtsystem32）下，并分别更名为 rundll. exe 和 sysedit32. exe。

②　修改注册表，在HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionRun下添加键值 internet = “% windowssystem% rundll. exe”，使木马病毒在开机后自动运行（其中% windowssystem% 为 Windows 的系统目录）。

③　修改注册表，修改HKEY_CLASSES_ROOTtxtfileshellopencommand 的默认键值

为% windowssystem% sysedit32. exe，关联记事本，使用户打开 txt 文件时木马病毒能获得运行机会。

④ 该木马病毒会通过 QQ 程序向其他的 QQ 用户发送“ http：//sckiss. yeah. net，你快去看看 ”的消息，诱导用户浏览含有恶意代码的网页。

⑤ 该木马病毒还会尝试盗取 QQ 用户的密码并将其发送至指定的邮箱。有趣的是，由于病毒作者使用了一个组件来发送邮件，因此当木马病毒执行发送邮件的操作时，该组件可能会弹出两个对话框，其中一个的内容为“ 220 welcome to coremail system （With Anti-Spam）2. 1 ”，另外一个对话框为“ Cannot open file.  mima. txt ”。

（3）“ 爱情森林变种二 ”。



病毒名称：Trojan. ScKiss. 126996。

病毒类型：木马病毒。

感染长度：126996 字节。

危害级别：中。

传播速度：中。

病毒特征：该木马病毒被包装在一个名为 s. eml 的邮件中，并且利用了 Iframe 漏洞。当没有打补丁的用户浏览含有该邮件的网页时，邮件中的木马病毒（Hack. exe）就会自动运行。

木马病毒运行后会：

① 复制自身到 Windows 系统目录（通常为 windowssystem）下，改名为 Explorer. exe。由于它和 Windows 目录下的 Explorer 文件同名，因此会使用户误认为这是一个正常的系统文件。

②　修改注册表，在HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionRun下添加键值Internet = “% windowssystem% Explorer. exe”，使木马病毒可以在开机后自动运行。（其中% windowssystem% 为 Windows 的系统目录）

③ 该木马病毒会通过 QQ 的“发送消息”窗口给 QQ 用户的网友发送如下信息“http：//ajim. delphibbs. com 去看看，很好看的”，当用户点击该网址浏览时，木马病毒就会被再次激活，从而使该木马病毒通过 QQ 聊天工具不断地传播自己。

（4）“爱情森林变种三”。

病毒名称：Trojan. Sckiss. 198702。

病毒类型：木马病毒。

感染长度：198702 字节。

危害级别：高。

传播速度：中。

病毒特征：该病毒运行后会：

① 复制两个自己的复制到 Windows 的系统目录（Win9X 通常为 windowssystem，WinNt 通常为 winntsystem32）下，并分别更名为 rundll. exe 和 sysedit32. exe。

②　修改注册表，在HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionRun下添加键值 intarnet = “% windowssystem% rundll. exe”，使木马病毒在开机后自动运行。（其中% windowssystem% 为 Windows 的系统目录）

③ 修改注册表，修改 HKEY_CLASSES_ROOTtxtfileshellopencommand 的默认键值为% windowssystem% sysedit32. exe，关联记事本，使用户打开 txt 文件时木马病毒能获得运行机会。

④ 修改注册表，修改 IE 浏览器的默认页、开始页和起始页。

⑤ 该木马病毒会通过 QQ 程序向其他 QQ 用户发送“ http：//ontimer. spedia. net，你快去看看 ”的消息，诱导用户浏览含有恶意代码的网页。

⑥ 该木马病毒还会尝试盗取 QQ 用户的密码并将其发送至指定的邮箱。

(5)“ 爱情森林变种四 ”。



病毒名称：Trojan. sckiss. 7695。

病毒类型：木马病毒。

感染长度：7695 字节。

危害级别：低。

传播速度：慢。

病毒特征：该木马病毒用 Delphi 编写，并用 UPX 进行了压缩，但该病毒需要在用户的机器上安装了 Delphi 的动态库才能运行。该病毒具有同“ 爱情森林 ”的第一个版本相同的特征，因此，极有可能是病毒作者对“ 爱情森林 ”的第一个版本重新编译后生成的。木马病毒被运行后会：

① 复制自身到 Windows 操作系统的 system 目录（通常为 windowssystem） 下，并改名为 Explorer. exe。由于它和 Windows 目录下的 Explorer 文件同名，因此会迷惑用户，使用户误认为这是一个正常的系统文件。