电脑报总策划

病毒杀除不求人

CCTV病毒栏目主持人 张晓兵
微软信息系统安全讲师 谢 魏

简单实用 即查即杀

- QQ病毒、QQ木马大作战
- 让木马程序无处遁形
- 冲击波、震荡波轻松搞定
- 向网络游戏盗号程序说再见

光盘赠送：

- 瑞星杀毒软件
- 江民杀毒软件
- 金山杀毒软件
- 卡巴斯基反病毒软件
- 各类木马查杀工具、反间谍软件及病毒专杀工具

山东电子音像出版社出版

病毒杀除不求人

CCTV病毒栏目主持人 张晓兵
微软信息系统安全讲师 谢 魏

山东电子音像出版社出版

内容提要

病毒已经成为了危害网络和个人电脑安全的第一大杀手。随着上网用户的不断增加，每一次病毒肆虐所造成的经济损失也不断增加。为此，我们编撰了本书，以便让更多的读者轻松掌握各种计算机病毒的诊断与防治方法。

本书摒弃了同类书中大量阐述理论的写作方法，从实用性出发，以丰富的实例和方法，指导用户自己动手清除各类病毒。

光盘内容：

各类木马查杀工具、反间谍软件及病毒专杀工具

书　　名：病毒杀除不求人
编　　著：张晓兵 谢　魏
责任编辑：李　萍
执行编辑：程晔扬 周　聂
出版单位：山东电子音像出版社
地　　址：济南市胜利大街 39 号
邮政编码：250001
电　　话：(0531)2060055-7616
发　　行：山东电子音像出版社
经　　销：各地新华书店、报刊亭
CD 生产：四川蓥山数码科技有限公司
文本印刷：重庆科情印务有限公司
开本/规格：797 毫米×1092 毫米　1/16　13.5 印张　200 千字
版　　号：ISBN 7-89491-457-6
版次/印次：2005 年 12 月第 1 版　2005 年 12 月第 1 次印刷
定　　价：22.00 元(1CD)

目录

第一章 QQ病毒的查杀

第二章 蠕虫病毒的查杀

第三章 脚本病毒的查杀

目录

目录

第六章 木马的查杀

第七章 间谍软件的查杀

第八章 文件型病毒的查杀

目录

第一章 QQ病毒的查杀

QQ是世界上使用人数最多的即时通讯软件，与此同时各种各样的QQ病毒也在互联网上大规模传播。绝大多数QQ用户都受到过QQ病毒的骚扰。

在这一章中我们主要给各位读者讲述QQ病毒的种类、原理以及如何查杀和防御QQ病毒。

1.1 QQ盗号木马概述

小王兴奋地攥了攥自己的拳头，也难怪他会如此的兴奋，一把年纪了还没找到一个合适的伴侣，终于工夫不负有心人，最近他在QQ上结识了一位漂亮的MM，而且这位MM极有希望成为小王的初恋。终于到了网吧，小王迅速在一台计算机前坐下来，点击QQ图表，输入QQ号码和密码后，登录！但他并没有如愿以偿地登录上去，而是在计算机屏幕上弹出了一个密码输入错误的对话框。小王并没在意，接着重新登录，这次成功了！

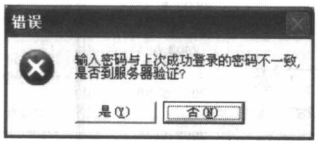

图1-1 QQ密码输入错误

与MM海聊了一晚上，双方约好第二天老时间在QQ上见。次日，小王准时赶到了网吧，打开QQ输入密码后登录，密码不正确！退出继续登录，还是不正确！一连试了十多次，QQ仍然提示密码错误。旁边的一个人告诉他，可能是中了QQ木马，QQ号码已经被人盗走了。小王忽然想起，昨天第一次登录QQ时提示密码不正确，难道那是QQ木马在捣鬼？小王呆呆地望着这熟悉的计算机屏幕欲哭无泪。唉！要是自己早点防御就好了。

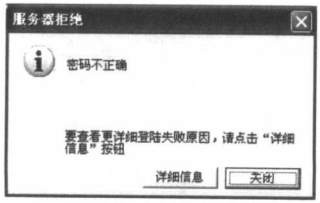

图1-2 QQ密码不正确

QQ 号码虽然只是虚拟账号，但是实际上人们对于一些简单易记或者带有吉祥意义的 QQ 号码也非常感兴趣。比如：一些 5 位数到 7 位数的 QQ 号码，甚至可以兑换现金。加上 QQ 号码的申请存在随机性，因此 QQ 盗号木马应运而生。

其实只要明白 QQ 盗号木马的原理，你就会发现这个东西也不是很神秘。如果某一台计算机中了 QQ 盗号木马，那么它就会潜伏在计算机中等待用户输入 QQ 号码和密码。一旦用户登录 QQ，QQ 盗号木马就会截取用户的 QQ 号码和密码，然后将它们发送到一个指定的邮箱中，至此你的 QQ 号码已经凶多吉少了。就是原理如此简单的 QQ 木马，不知道让多少用户丢失了自己心爱的QQ 号。

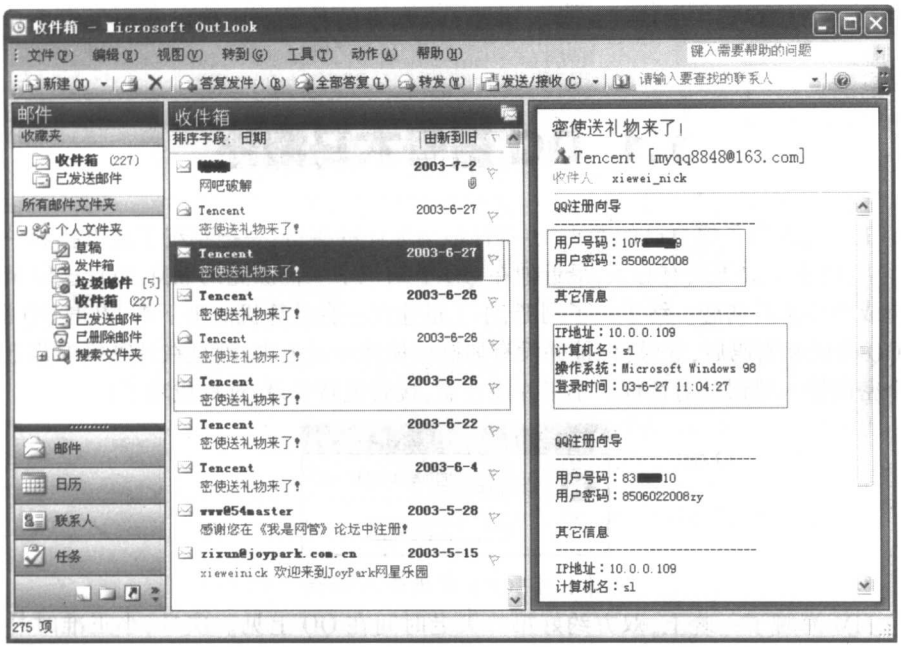

图 1-3 盗取 QQ 号码的邮件

1.2 QQ盗号木马查杀实例

1.2.1 QQ密码轻松盗查杀实例

QQ密码轻松盗是一款最典型的QQ盗号木马工具，也是国内目前使用最为广泛的QQ盗号木马。很多用户的QQ号码丢失，大多都是QQ密码轻松盗所为。因此，了解如何查杀QQ密码轻松盗对每一位用户的QQ安全至关重要。

如果用户的计算机中了QQ密码轻松盗，计算机并不会出现非常明显的变化，这也让QQ密码轻松盗更具隐蔽性。那么如何有效地查杀QQ密码轻松盗呢？

工具清除

由于QQ密码轻松盗的盛行，所以现在市场上的主流杀毒软件都能够对QQ密码轻松盗进行查杀。如果用户不怕麻烦的话，建议大家在每次开机后，都对系统进行一次全面的病毒扫描，再登录我们的QQ，这样就能保证万无一失。

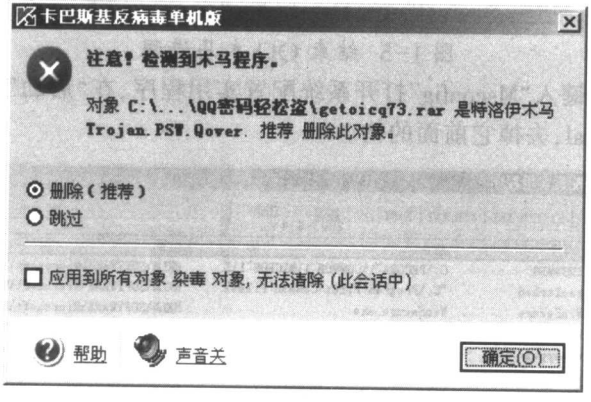

图 1-4 杀毒软件清除QQ木马

手工清除

在网吧或者机房上网时，很多计算机上没有单独的杀毒软件供用户使用，QQ号码在这个时候极其容易被盗，所以学会手工清除QQ密码轻松盗也是用户必须掌握的技能。

首先按“Ctrl+Shift+Del”组合键打开任务管理器，查看任务管理器中的进程。QQ密码轻松盗的进程名称为Interal.exe，如果用户发现任务管理器中存在这个进程，那么一定要毫不犹豫地将它结束掉。

图 1-5 结束 QQ 木马进程

然后在运行中键入“Msconfig”打开系统配置实用程序,在“启动”中找到 QQ 密码轻松盗的启动项 Interal,去掉它前面的钩。

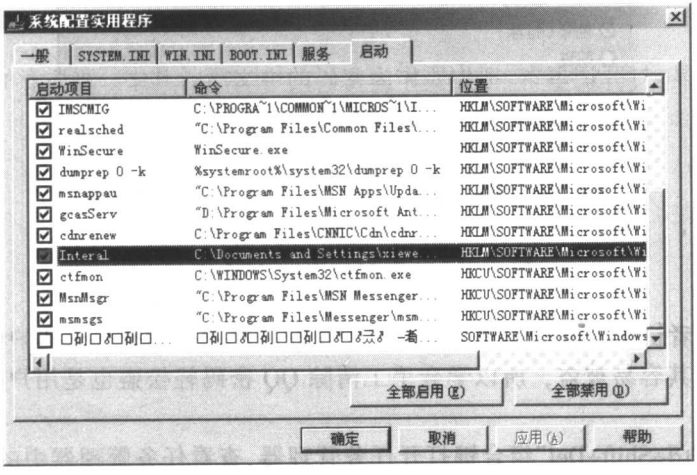

图 1-6 删除 QQ 木马启动项

最后在系统中搜索 Interal.exe 文件,将搜索出的文件一一删除,重新启动计算机即可将 QQ 密码轻松盗完全清除。

小知识：

所谓的QQ盗号木马其实就是一个键盘记录器，它只能死板地记录下用户输入的字母和数字。如果你巧妙地在QQ登录时改变QQ密码的输入顺序，那么QQ木马就只会记录下一个错误的密码。

具体方法是：假设你的QQ密码是123456，可以先输入456，然后把光标移到4前面再输入123，这样你输入的密码依然是123456，但在QQ木马看来你输入的就是456123了，一字之差，谬之千里。这是最简单也是最有效的对付QQ木马的方法。

图 1-7 变换QQ密码的输入顺序

具体方法是：打开记事本，把你要作为密码的中文写入其中。要注意的是：每个字占两个字符，QQ最大支持16位字符，所以你的中文密码不能超过8个字。

小提示：

由于QQ木马只是一个简单的字母与数字记录器，因此它无法记录下中文密码。如果我们用中文作为QQ的密码，那么将会让QQ木马无计可施。

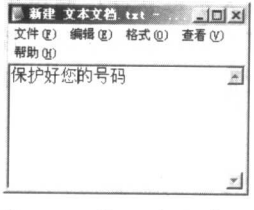

图 1-8 输入中文密码

在设置 QQ 密码的时候,把记事本里的中文密码粘贴进去。这样在你下次登录输入密码时就可以输入你设置的中文口令了。输入密码的方法依然是使用粘贴方式。

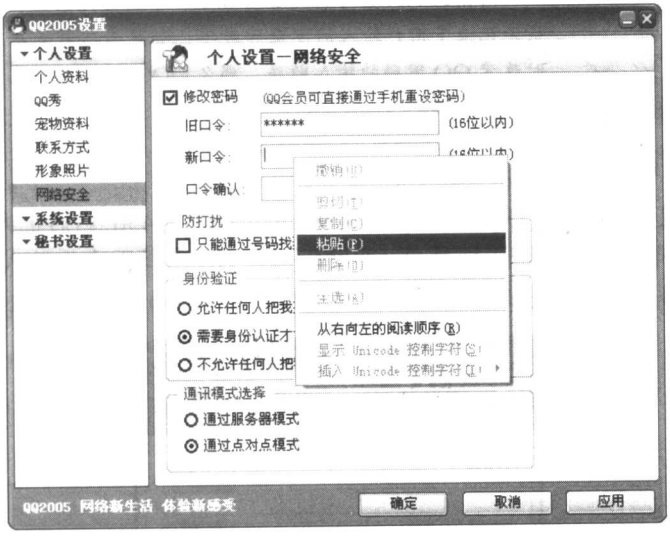

图 1-9 使用中文密码

1.2.2 好友号好好盗查杀实例

好友号好好盗是一款较为独特的 QQ 盗号木马工具，因为它主要利用了用户的心理,使用者将一张很有诱惑力的图片和 QQ 盗号木马捆绑在一起,然后把它发送给自己的 QQ 好友。如果受害用户运行了这个文件,那么用户的 QQ 将立即死掉,当受害用户在重新登录 QQ 的时候,藏在图片中的 QQ盗号木马将自动记录下用户的 QQ 号码和密码,受害用户一旦成功登录QQ，那么他的 QQ 将自动地发一个 QQ 消息给好友号好好盗的使用者,而这个消息的内容就是受害用户的 QQ 号码及密码。

一个看似如此厉害的 QQ 盗号木马,我们用什么方法清除它呢?

工具清除

由于该盗号木马的特殊性,各大杀毒软件厂商也早早地将它列为了病毒。所以用户在使用 QQ 时,一定要记住随时打开杀毒软件实时监控,这样即使用户不小心接收了好友号好好盗的木马文件,病毒实时监控也能发觉,并及时将它清除。

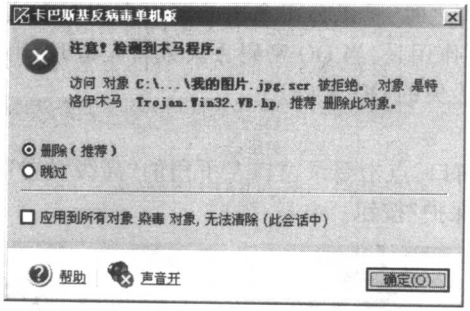

图 1-10 杀毒软件清除好友号好好盗

手工清除

如果用户在没有杀毒软件的情况下不慎运行了好友号好好盗的木马文件，那么千万不要慌乱。首先，用户需要做的是千万不要登录自己的 QQ，这样就可以避免 QQ 盗号木马对用户 QQ 号码和密码的记录。然后打开任务管理器，在进程中有一个名称为“我的图片.jpg.scr”的进程，将它结束，最后删除病毒图片即可将好友号好好盗清除。

小提示：

好友号好好盗只是一个运行程序，并且没有修改系统注册表和启动项，所以只须将它的进程结束即可将它停止。

图 1-11 结束木马进程

在 QQ 木马泛滥成灾之时,腾讯公司拿出的第一个应对方法就是为 QQ 申请密码保护。QQ 密码保护的主要作用是,当 QQ 密码丢失或者忘记时,用户可以通过事先设置好的密码保护口令找回你丢失的 QQ 号码。

1.申请密码保护

首先打开 QQ 登录窗口,点击登录窗口左下角的“高级设置”按钮,然后点击“其他选项”菜单中的“申请密码保护”按钮。

图 1-12 申请 QQ 密码保护按钮

此时会自动弹出腾讯 QQ 密码保护申请网站,按照网站的要求,首先填入你的 QQ 号码、密码以及附加码,然后点击“下一步”按钮。

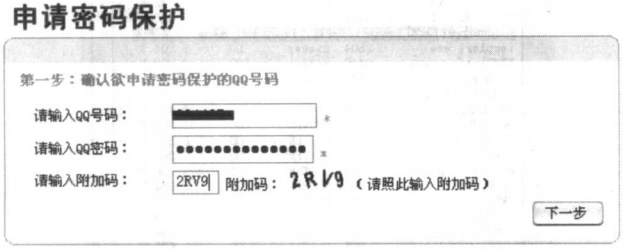

图 1-13 填入 QQ 号码申请密码保护

接下来再按要求填入你的有效证件号码、密码提示问题和密码提示答案等。密码提示问题和密码提示答案这个步骤尤为关键，请大家一定要牢牢地记住你的密码提示答案,否则密码保护就不起任何作用了。继续点击“下一步”按钮。另外,切忌不可使用很容

易回答的提问和答案,否则提问就没有意义了。

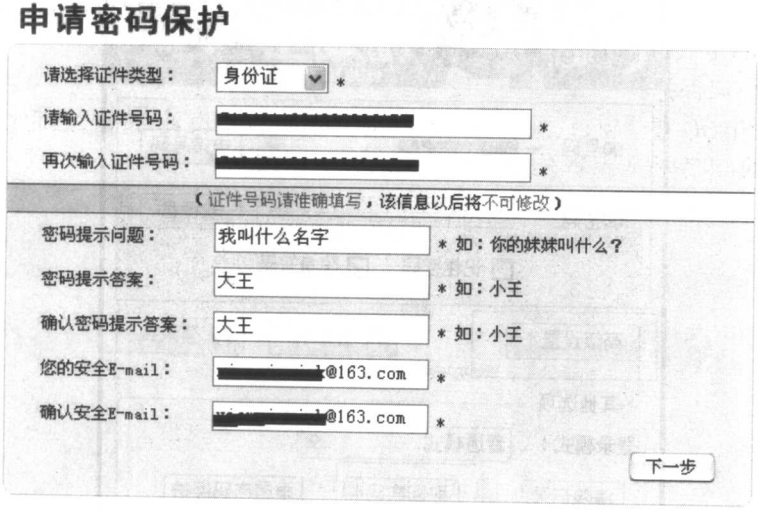

图 1-14 申请密码保护第二步

当出现“恭喜您成功申请密码保护服务”的对话框时,你的QQ 密码保护已经申请成功了。

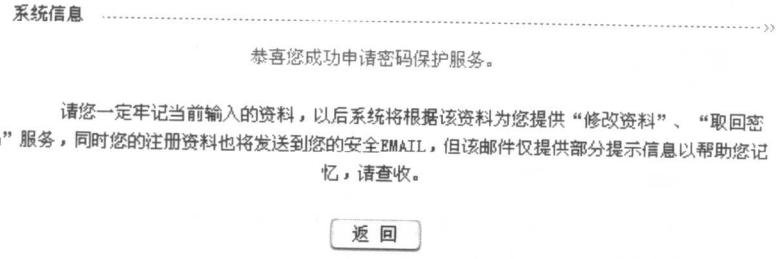

图 1-15 QQ 密码保护申请成功

2.利用密码保护找回 QQ 号码

申请过 QQ 密码保护的 QQ 号码,我们又该如何利用它去找回我们的 QQ 号呢？方法很简单。首先,打开 QQ 登录窗口,然后点击登录窗口左下角的“高级设置”按钮,这次我们应该选择“取回密码”按钮。

图 1-16 利用密码保护找回 QQ

此时会自动弹出腾讯 QQ 密码保护申请网站。首先填入你丢失的 QQ 号码和附加码，然后点击“下一步”按钮。

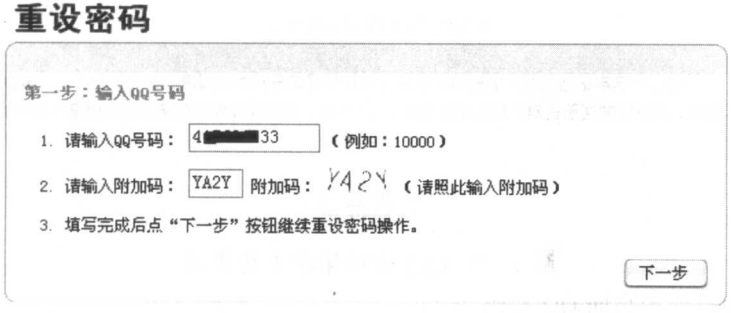

图 1-17 输入自己被盗的 QQ 号码

这时就进入了找回你的 QQ 号码最关键的一步。首先回答你在 QQ 密码保护中所设置的问题，然后在“请选择您需要取回的密码类型”中选择“QQ 密码”，最后选择取回方式，推荐大家选择第一个选项“将邮件发送到默认的 Email 信箱”。如果你忘记了申请密码保护时填入的邮箱地址，可以选择第二个选项。完成之后继续点击“下一步”按钮。