Book
远望图书

边看书、边下载、边使用，轻松打造无忧电脑

电脑无毒

一看就能懂，每个人都可以成为电脑安全高手

一身轻

- 你的股票账号是否安全？
- 你是否经常受到流氓软件的骚扰？
- 你的游戏账号是否被盗取过？
- 你是否收到过含有格式化硬盘的病毒邮件？
- 你是否知道杀毒软件并不能彻底保护电脑？
- 你是否被盗取过网上银行卡号？
- 你的QQ消息是否被人偷看过？
- 你是否在看视频时中过病毒？
- 你是否打开过带病毒的办公文档？
- 你是否知道下载时的陷阱？

本书中实例相关软件下载
网站互动

重庆大学出版社
http://www.cqup.com.cn

远望图书 编

电脑无毒一身轻

DIAN NAO WU DU YI SHEN QING

重庆大学出版社

内 容 提 要

本书针对普通电脑用户在生活、工作、娱乐中使用电脑时会遇到电脑病毒、木马、黑客攻击等情况，将这些大家最关注的电脑安全问题进行通俗地介绍。全书共分7个专题，分别对普通用户在进行影音娱乐、办公、聊天、游戏、浏览网页、电子商务等电脑应用时容易中病毒、木马的地方进行介绍，并对中毒后的实际现象举例说明，让不太懂电脑的用户通过这些说明就能知道自己电脑中了什么样的病毒或木马，而且根据我们提供的步骤性图解流程就能解决问题。并对如何打造一套安全的电脑防护系统作讲解，让用户能更放心地使用自己的电脑。

图书在版编目（CIP）数据

电脑无毒一身轻／远望图书编.—重庆：重庆大学出版社，2007.9

ISBN 978-7-5624-3837-3

Ⅰ.电… Ⅱ.远… Ⅲ.电子计算机－安全技术 Ⅳ.TP309

中国版本图书馆CIP数据核字（2007）第133121号

电脑无毒一身轻

远望图书 编

责任编辑：卢 茂　　版式设计：陆 阳

责任校对：文 鹏　　责任印制：赵 晟

*

重庆大学出版社出版发行

出版人：张鸽盛

社址：重庆市沙坪坝正街174号重庆大学（A区）内

邮编：400030

电话：(023) 65102378 65105781

传真：(023) 65103686 65105565

网址：http://www.cqup.com.cn

邮箱：fxk@cqup.com.cn（市场营销部）

全国新华书店经销

重庆科情印务有限公司印刷

*

开本：787×1092 1/16　　印张：16 字数：250千

2007年9月第1版　　2007年9月第1次印刷

ISBN 978-7-5624-3837-3　　定价：25.00元

FOREWORD

前言

个人电脑早就不再是奢侈物的代名词，其普及开来已经有些年头了。电脑作为一种增加生活乐趣、提高工作效率的工具，在我们身边处处都能见到。我们越来越多的信息和资料被记录在电脑中，而大多数用户却对电脑的安全知识了解不多，没有对电脑进行“防御加固”，因此在这2年来，电脑中资料盗窃案频频发生——网上炒股的账号被盗，所购股票被人恶意高买低卖，损失惨重；网上银行的账号被盗，多年来的存款不翼而飞；QQ消息被人偷看，个人信息被曝光在网络上；游戏账号被盗，苦苦练级打造的极品装备转眼不见；收到带病毒的办公文档，将硬盘中的数据全部删除.....这些事件其实我们是可以避免的，因此就有了本书要为大家介绍的内容。

普通用户对电脑安全方面的知识了解不多，而在一个压力大、时间紧、节奏快的时代，很多人是没有时间彻底地去研究这些比较专业的知识，但是需求又摆在眼前，所以我们就将本书打造得通俗易懂，让不太懂电脑知识的读者都能通过本书的介绍来解决电脑安全的问题。本书分为7个专题，前面4个专题都对使用电脑时各种应用的安全问题分别进行介绍。每篇文章都介绍一类读者关心的电脑安全知识，首先通过电脑中毒或被安装木马软件后的一些表现现象来告诉读者是否遇到类似问题，然后用图解的方式介绍如何查杀病毒或木马，最后再介绍如何防范这类事件的方法。整个介绍过程十分简单，没有过深的技术研究内容，全部以如何解决问题的实际操作为主，就算不太懂电脑的用户照着做同样能将自己的电脑的安全程度提高几个档次。读者可以根据自己的实际情况来翻阅查找相关内容。后3个专题，对如何打造一套安全的电脑防护系统作讲解，同样不涉及过深的技术问题，全程图解应用操作为主，通过对杀毒软件、防火墙的一些设置，利用一些简单的安全工具来教大家打造自己的电脑“防护墙”。希望通过本书的介绍，能为广大电脑初、中级用户解决一些电脑安全方面的难题，让电脑用得放心、省心、舒心。

特约作者：肖遥

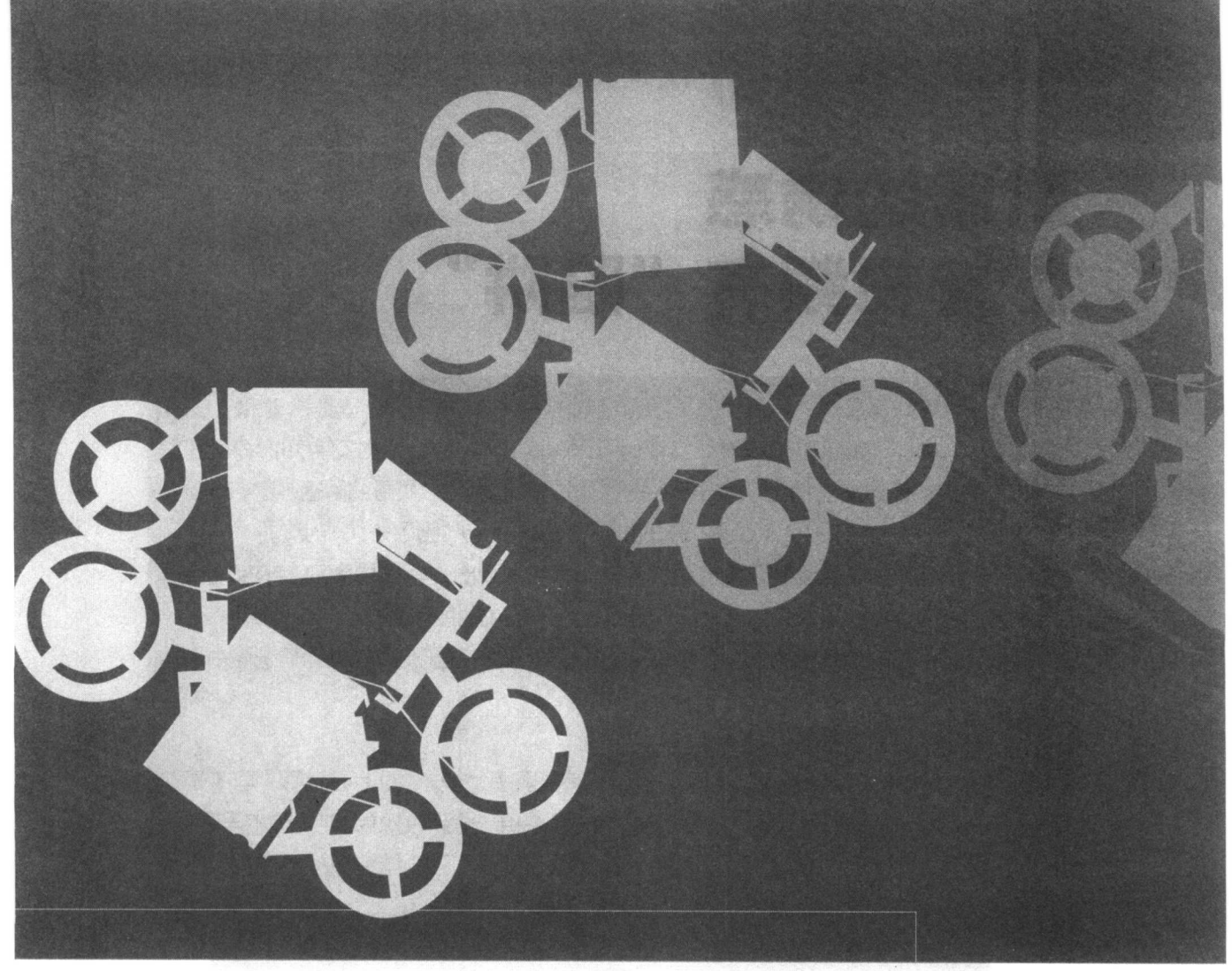
曾献身于国防航空事业，走上了安全技术研究与自由撰稿的SOHO之路，现为多家IT类杂志的特约作者，其稿件大量发表于《电脑迷》、《网友世界》、《大众软件》、《黑客X档案》、《黑客防线》等杂志，尤其引以为荣的是，曾被邀为远望图书打造了一系列电脑安全图书。作者一直希望打造一本普通用户能看得懂的电脑安全图书，让所有的用户都有一个安全的电脑使用环境。

目录 CONTENTS

专题1 娱乐与下载，网络藏陷阱

专题2 给我一个安全的办公环境吧

专题3 聊天与网游，我要安全



娱乐与下载，网络藏陷阱

互联网上资讯多姿多彩，看的、听的、玩的，应有尽有，各种丰富的资源让你眼花缭乱。但是，网络上也同样存在着许多整人的陷阱，在这些视频与音乐让你赏心悦目的同时，背后可能有一只黑手正悄悄地伸向你的电脑——这就是可恶的电脑木马。

网上木马横行，网页中、图片中、Flash 动画里、电子书中，甚至视频里面都可能有木马，让人防不胜防。中了这些木马后电脑会有怎样的反应？如何才能清除、防范这些木马，还我们一个清净的网络天空？就让安全公司的冰河老师来告诉我们答案。

专题 1

眼睛的诱惑
影音视频有“陷阱”

安全培训课堂开讲好几课了，冰河老师的“渊博”学识与“幽默”谈吐，深深地吸引了参加培训的安全小菜们。几堂课下来，小菜们已经开始对安全知识有所了解了，而且喜欢在课堂上提出一些千奇百怪的问题，让冰河老师帮助解答。这不，趁着冰河老师讲课休息的间隙，爱提问题的小胖又给冰河老师出了一个“难题”——

“冰河老师，最近我上网看电影，总是动不动就弹出一些网页窗口。本来是全屏播放的，被弹出网页影响，中断播放，烦死了！”小胖抱怨着。

“哦，只是弹出广告，没有系统变慢、鼠标乱动、QQ号被盗之类的情况呢？”冰河老师问到。

“没有，不像中病毒了。”小胖肯定地说。

“嗯，看来你运气不错。”冰河老师语气有些凝重地说，“网上看电影，可不是这么简单的事情，一不小心，不仅是弹出广告这么简单，搞不好就要中视频木马啊！”

“网上看电影会中木马！”这么严重的问题立刻吸引了小胖和其他菜菜们，于是冰河老师干脆以此为题，给大家上了一堂安全课。

一、无声无息的视频木马

所谓“视频木马”，并不是指木马伪装成视频文件的格式，诱骗电脑用户点击运行，那只是一种很低级的木马伪装形式。这里说的“视频木马”，是指各种远程控制木马或盗号木马，直接暗藏在视频中。其特点是，视频可正常播放，但在播放过程中，系统后台已经悄悄下载并运行了各种木马程序。

这是由于木马利用了各种视频文件的漏洞，或者是利用系统漏洞，通过漏洞调用攻击者事先制作的网页木马。从而使得用户在观看视频时，在后台自动打开浏览器访问木马网页，导致系统中植入木马被黑客控制或账号丢失。

常见的视频媒体有很多种，其中WMV、RM、MOV三种视频格式，是最易被木马所利用的。因此，视频木马可分为WMV视频木马、RM视频木马，以及MOV视频木马三种。

1.WMV视频木马，数量群最大的视频木马

WMV是网上最常见的一种视频格式，网上提供的各种下载或在线观看的电影视频，有百分之五十以上是采用此格式。因此，WMV视频木马有着非常广泛的“生存”环境，任何一个电影站点，都存在着遭受WMV视频木马攻击的威胁。

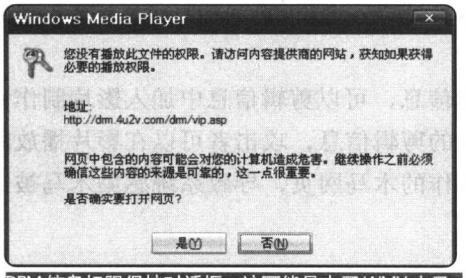
冰河老师提示：

WMV视频一般是采用Microsoft Media Player播放器进行播放的。但是在Microsoft Media Player 9.0和Microsoft Media Player 10.0版播放器中存在着一个严重的漏洞，此漏洞名为“Microsoft Windows媒体播放器数字权限管理加载任意网页漏洞”。

该漏洞是指Media Player数字权限管理(DRM)中存在加载任意网页漏洞，攻击者可能利用此漏洞诱使用户执行恶意代码。攻击者可能会创建一个恶意的WMV视频文件，如果用户播放该视频文件的话，将会自动加载木马网页，木马网页可能诱骗用户下载执行恶意软件。

2.WMV视频木马症状表现

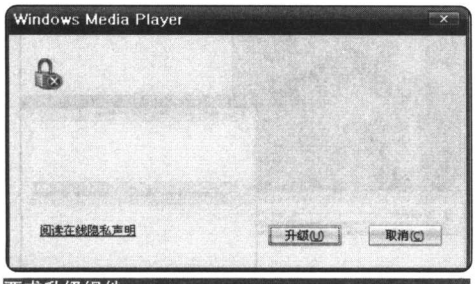
用户用Windows Media Player播放器，打开夹带有木马文件的WMV视频时，可能会弹出一个DRM权限保护确认对话框。点击“否”按钮的话，视频将无法正常播放。只有点击“是”按钮，才能够正常播放视频文件，但是同时会打开木马网页，木马也随之进入系统中，并且在后台自动运行了。



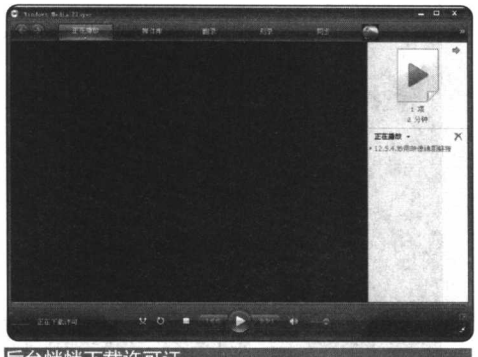
DRM信息权限保护对话框，这可能是中了WMV木马的表现

DRM打开的网页很可疑

也有一些WMV视频木马，在打开运行时，首先是要求升级组件，并不会弹出DRM权限保护对话框，而是直接在WMP播放器的状态栏处显示提示信息，提示“正在下载许可证”。碰到这种情况也需要注意。



要求升级组件



后台悄悄下载许可证

3.占据“半壁江山”的RM视频木马

在各种网络影音视频中，RM视频格式与WMV视频格式的应用一样广泛，尤其是在视频电影下载或在线播放中，RM视频格式都是极为常见的。同样，网络上的RM视频木马也随处可见，一不留神就会中招。

与其他视频格式相比，RM视频在压缩体积上有着明显的优势，一部大小为700 MB左右的DVD影片，如果将其转录成同样视听品质的RMVB格式，最多也就400 MB左右。由于压缩比非常大，因此RM视频很适合网络电影在线播放。再加上RM视频具有内置字幕和无需外挂插件支持等独特优点，因此使得RM视频甚至比WMV视频的应用更为广泛一些，也使得RMVB视频木马极其泛滥。

冰河老师提示：

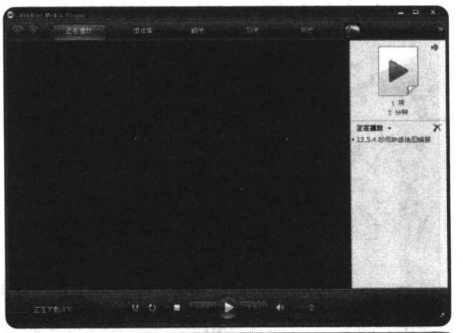
这里所指的RM视频木马，包括RM格式的视频木马，以及RMVB格式的视频木马。

RM视频格式，可使用RealOne Player2.0或RealPlayer8.0加RealVideo9.0以上版本的解码器形式进行播放。但是由于这些播放器存在着漏洞，因此攻击者可利用漏洞制作出带有木马攻击能力的RM视频。

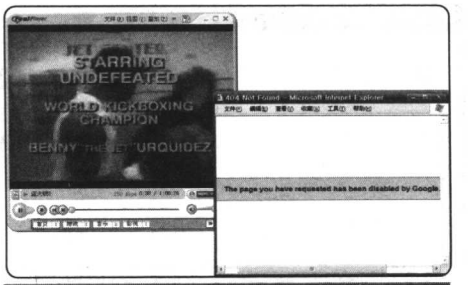
另外，RM格式的影片允许用户修改剪辑信息，可以剪辑信息中加入影片制作者的姓名身份，以及制作者网页等。通过修改影片的剪辑信息，攻击者可以在影片播放的指定时间打开指定的网页窗口，从而浏览事先制作的木马网页，导致系统感染木马被远程控制或窃取机密信息。

4.RM视频木马症状表现

对于第一类，利用漏洞攻击的RM视频木马，其文件后缀名一般是“.smil”。用户在打开夹带木马的smil文件时，会自动调用RealPlayer程序开始进行播放。RealPlayer打开之后过一段时间就会因为程序溢出而失去响应，此时被攻击主机上将会自动打开“13579”端口。



被攻击主机上打开了“13579”端口



播放RM视频木马时会自动弹出网页木马窗口

当用户打开并播放夹带有网页木马的RM视频时，会在播放过程自动弹出一个IE网页窗口，连接并打开指定的木马网页。如果用户不留心的话，很可能中了木马也不知道。

小胖：

为什么看电影时，弹出了网页，却没有中木马呀？

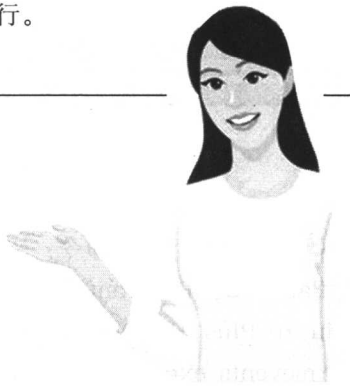
冰河老师：

我们在线或下载播放一些网络RM视频文件时，经常在播放过程中会自动打开一个带有各种宣传信息，但是没有危害的网页。其实这是别人做广告的一个方法，他们把网页资料保存在Real文件的剪辑信息中就会这样了。

5.新片热片藏猫腻——MOV视频木马

随着网络娱乐信息的丰富与流行，网上随处可见新热电影预告或广告宣传片，这些影片往往都使用一种新的视频格式——MOV格式。WMV和RMVB视频中，可能会藏有木马，有一定上网经验的电脑用户，都对此有所了解，对这些视频提防小心。但是对于一些MOV这类比较少见的视频格式，可能还是有人不知道其中也有可能藏有木马。其实MOV视频与前两种视频一样极具威胁性，而且由于其并不太常见，反而更易让视频播放者中招。

现在各种万能的播放器非常多，通常都集成了MOV解码功能，可以直接播放MOV视频。不过，也有一些电脑用户安装了专用于播放MOV格式视频的播放器QuickTime Plyaer。但在QuickTime 7.0以前的版本中，存在着一个“HREFTrack轨道程序执行”漏洞，有可能造成被攻击者在MOV视频中嵌入木马执行。



冰河老师提示：

MOV视频是多轨道视频，包括音频、视频、字幕等多个轨道。HREF轨道是MOV视频中一个比较特殊的文本轨道，它可以使QuickTime具有交互式、超链接的功能。HREF轨道支持URLs，这样可以用简单的语句实现别的影片替代当前影片的功能，或者在别的框架窗口中打开，或者打开QuickTime Player(QuickTime播放器)来播放。也可以调用JavaScript语言或者在特殊的框架窗口或其他窗口中打开某网页等。

6.MOV 视频木马症状表现

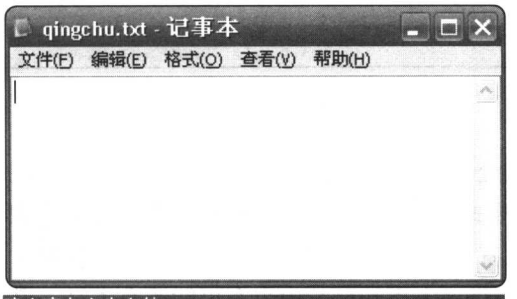
MOV 视频木马被嵌入某个网页中时，当电脑用户打开此网页时，如果系统中安装了 QuickTime Player 播放器，就会自动调用 QuickTime Player 进行播放。播放到了指定的时段，就会在播放器中悄悄地打开一个“隐形”的网页框架，在框架中会访问打开指定的木马网页。

由于木马网页是在播放器中隐藏着的，并不是像 WMV 或 RM 视频木马一样弹出网页窗口，因此隐蔽性极强，用户在不知不觉中就会被木马所控制。

二、安安全全看电影，清除各类视频木马

从上面介绍的内容可以看出，危险的网络视频很可能让我们一不小心就中了招。那么如何才能安全地在网上欣赏电影呢？当然首先是不要访问一些不知名的带有诱惑性的视频站点，其次还可有针对性地对在线或下载视频，进行如下防范。

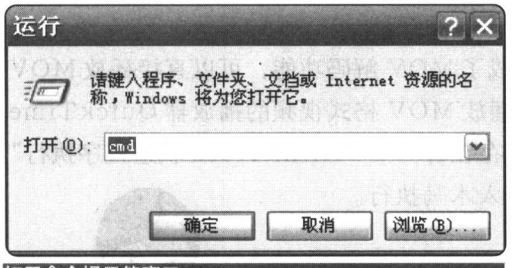
1.利用 Helix Producer Plus 清除 RM 视频木马



建立空白文本文件

碰到 RM 格式的视频文件，只需要清除视频中的所有剪辑信息，就可彻底清除 RM 视频木马了。如果电脑中安装有软件“Helix Producer Plus”，可利用该软件来清除视频中夹带木马的剪辑信息。

Step1:用记事本建立一个名为“qingchu.txt”的空白文本文件，将其与要清除木马的 RM 视频，一起放在 C 盘根目录下。



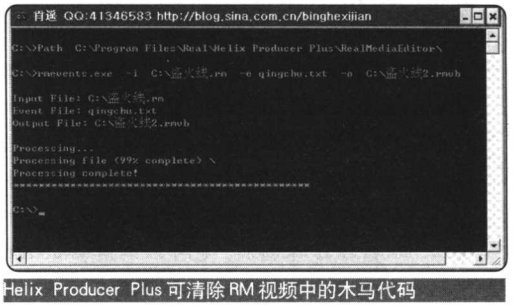
打开命令提示符窗口

Step2:在“运行”中输入“CMD”命令，打开命令提示符窗口。

Step3:执行如下命令：

Path C:\Program Files\Real\Helix Producer Plus\RealMediaEditor\

rmevents.exe -i C:\盗火线.rm -e qingchu.txt -o C:\盗火线2.rmvb



Helix Producer Plus 可清除 RM 视频中的木马代码

Step4:命令执行后，就可以将原有RM视频中的剪辑信息覆盖，也就间接地清除了木马。生成的新RM视频，已经是干净无木马的视频了。

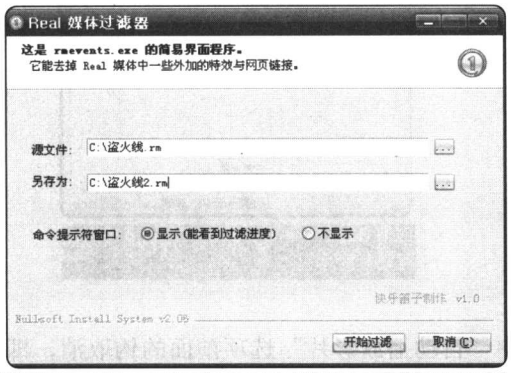
冰河老师提示：

清除的方法很简单，其原理是建立一个空白的剪辑信息文件，然后将空白信息导入视频，覆盖原有的剪辑信息，因此完全清除了RM视频木马代码。

2.自动过滤木马——Real媒体过滤器

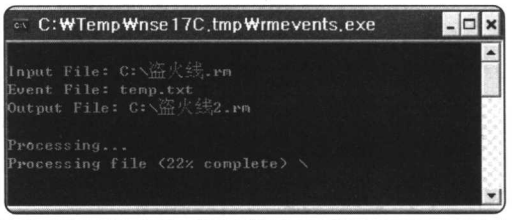
此外，可以使用一些专门的工具来清除RM视频中的木马。“Real恶意事件清除工具 V1.0”就是一个专用于解决RM视频网页木马问题的小工具，无需安装Helix Producer Plus，使用非常方便。

Step1:运行Real恶意事件清除工具，点击工具栏上的“源文件”按钮，指定要清除网页木马的RM视频文件路径。在“另存为”中指定清除木马后的视频保存路径。



图形界面清除RM视频木马

Step2:勾选“显示过滤进度”项，点击“开始过滤”按钮，即可开始清除Real视频中的各种网页木马和广告信息了。

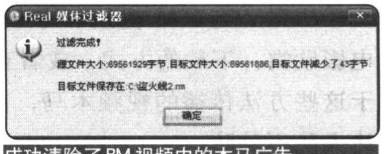


在弹出窗口中可看到清除过滤进度

冰河老师提示：

Real恶意事件清除工具实际上是调用了Helix Producer Plus的“rmevents.exe”插件程序，进行过滤清除的。

Step3:清除完毕后，弹出完成提示对话框，并显示清除了视频中的多少信息及文件减小的体积，生成的就是一个去掉木马网页或广告的干净视频了。



成功清除了RM视频中的木马广告

3.打补丁，堵住视频木马之门

对于WMA视频木马，以及Rmil溢出的RM视频木马，其实都是利用了媒体播放器的程序漏洞进行攻击的，因此防范此类木马，应该及时地打上播放补丁程序。

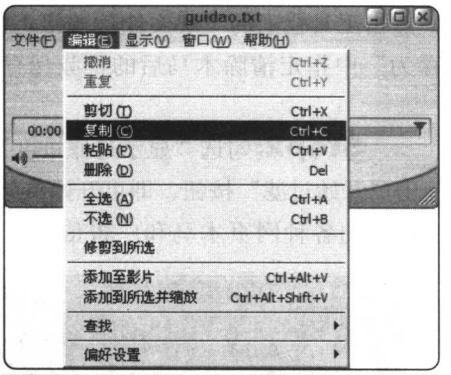
要防范WMA视频木马，需要下载“Microsoft Windows媒体播放器数字权限管理加载任意网页漏洞”的补丁程序。

要防范Smil溢出类视频木马，则需要升级播放器版本，或安装“RealNetworks RealPlayer.smil文件处理缓冲区溢出漏洞”补丁(可在本书网站上下载)。

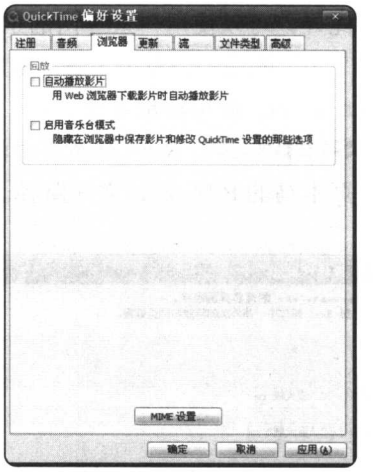
4.MOV视频木马病毒的防范

防范MOV视频木马，其实很简单：

Step1:运行QuickTime Plyaer，点击菜单“编辑”→“偏好设置”→“QuickTime偏好设置”，打开偏好设置对话框。



打开QuickTime偏好设置



取消QuickTime Plyaer网页自动播放功能可防视频木马

Step2:切换到“浏览器”标签，将其中“自动播放影片”选项前面的钩取消，即可防止QuickTime Player自动运行播放。

三、视频木马常见的传播方式和预防

各种视频木马在网上虽然很泛滥，但是为什么偏偏自己就会碰上这些视频木马呢？是视频木马盯上了自己，还是自己运气太糟糕，让视频木马主动碰上了？了解一下视频木马常见的传播途径，遇到视频木马就可绕道而行了。

1.WMV与RM视频木马的传播

WMV与RM视频木马传播的方式实在是太广了，攻击者可能会采用在线提供免费电影欣赏、下载的方式，或者直接将视频通过聊天工具、邮件之类的传输发布。不过对于这些方法传播的视频木马，都是可以避免的，有一种更为广泛的视频木马传播方式，让人防不胜防。

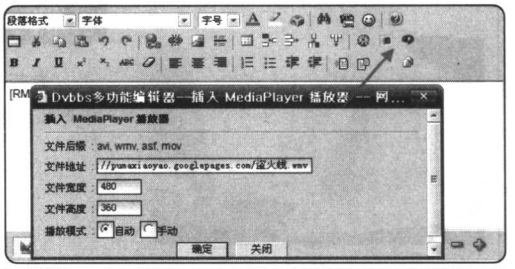
很多用户都喜欢上论坛、博客、群组、社区之类的站点，攻击者会利用这些热门的地方，通过发帖的方式传播恶意的视频木马。由于论坛、社区、群组及博客等站点，人气非常旺，发帖留言的人又多，用户很容易就被视频木马攻击，并且很难知道是谁发布的恶意帖子。下面以在论坛中常见的传播视频木马的例子来介绍。

Step1:攻击者会将视频上传到某个网站空间中，例如这里为“http://***.***.com/导火线.wmv”。

Step2:攻击者登录某个论坛，这里以一个Dvbbs7动网论坛的电脑技术论坛为例。登录论坛后，选择发表新主题。

Step3:将帖子的主题起得吸引人一些，比如在电脑技术论坛中，可以将标题起为“** 正版软件序列号放送”；在一些影视论坛中，则可将标题起为最新热门的影片下载，或者“** 火热性感演出”之类的。

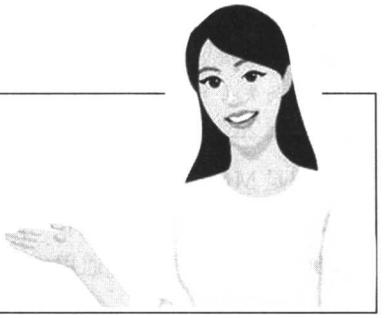
Step4:在帖子正文输入框上方点击“插入Windows Media”或“插入Real Media”按钮，在弹出的对话框中输入上传的视频链接地址。



在动网论坛中发布视频木马

冰河老师提示：

攻击者往往不会直接发布新帖，而是在已有的帖子中进行回复。由于在同一页中回复的人很多，因此浏览者中了木马后，也不知道究竟是什么原因。

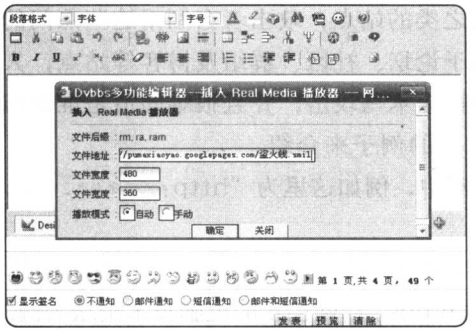


Step5:输入完毕后，点击发表帖子。当其他用户点击帖子链接时，就会自动播放包含了木马的视频文件，木马就会悄悄地被执行了。

对于这类以欺骗方式传播的视频木马，唯一的办法就是洁身自好，尽量不要上一些不安全、陌生的站点或论坛。特别是现在一些打着情色擦边球的网站，上面的木马病毒非常多。此外，上网看电影时，开着杀毒软件的即时网页监控功能，可以有效地防范各种木马病毒。

2.Smil溢出RM视频木马的传播

攻击者传播Smil溢出视频木马的方法与上面两种视频木马相同。



smil 文件可直接以 RM 视频类型方式插入

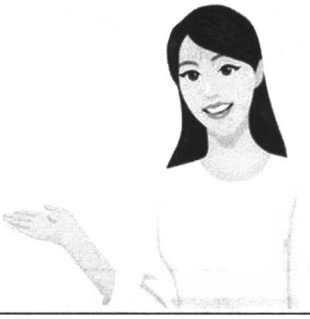
将生成的 smil 文件上传到网站空间中，在论坛中发布帖子时，选择“插入 Real Media”，然后输入 smil 文件的网址即可。

3.MOV 视频木马的传播

直接用播放器播放这个 MOV 视频木马是不会弹出木马网页来的，原因是 HREF 需要整合在网页中才能够生效。也就是说，需要将 MOV 视频放置在某个网页中，在网页中播放 MOV 视频木马时，才能达到攻击的效果。因此攻击者只有采用网页在线播放的方式，才能进行 MOV 视频木马攻击，下载或直接传送播放是没有效果的。

小胖：

老师，如果攻击者能欺骗我们访问到他的网页，直接制作网页木马不是更好？何必还要通过 MOV 视频播放这么麻烦呢？



冰河老师：

其实，在网页木马的利用过程中，并不是那么容易的，因为一个陌生的网页，谁敢打开呢？这就使攻击者制作的网页木马失去了效果。

但是 MOV 视频木马不同，可以将它添加到任意的访问量大的网页中，因为许多网站或论坛之类的站点，都允许用户在发帖或发布文章时添加多媒体视频。攻击者就可将视频更换为 MOV 视频木马，普通用户浏览网站或论坛者，就会在后台不知不觉中被木马攻击了。

总结

通过这节课，同学们应该了解到视频中是如何被加入木马的了吧，以后在网上看电影时可要小心了。

一般来说，我们最好不要到一些不知名的站点去看电影。尤其是一些打着免费电影，或者是“激情”、“火爆”之类诱惑性词眼的网站，更要特别小心，不要随便进入。

网上下载的视频文件，最好用前面提到的广告清除工具，将其中的不管是广告网页也好，还是木马网页，全部清除掉。

另外，千万记得及时更新各种播放程序的补丁。有不少同学很注意 Windows 系统更新，可是对于常用的软件却不太关心。及时升级软件的新版本，这也是必不可少的。对于视频软件来说，其实我们完全可以使用一些万能播放器，一个播放器就可播放所有的视频格式，既简单，还具备过滤木马网页的功能。