网络安全

安全技巧（十七）

小未 主编

目　录

在 IE 中如何禁用 ADODB.Stream 对象 1
浅析“传奇”木马的防范方法.....6
量子密码：终结黑客的梦想 8
EFS 加密文件夹无法打开怎么办 11
对 WinXP 进行安全分析和配置.....13
特定环境下网关设错也能上网.....20
在 XP 安全模板中修改策略设置.....22
对 WinXP 进行安全分析和配置.....24
特定环境下网关设错也能上网.....32
在 XP 安全模板中修改策略设置.....33
Cookie 的传递流程及安全问题 38
网络安全之审计结果.....44
网络安全之 IDS 系统 69
网络安全讲座之六：侦察与工具.....98
网络安全之文件系统安全 116
网络安全之账号安全.....124

在 IE 中如何禁用 ADODB.Stream 对象

本文包含有关修改注册表的信息。修改注册表之前，一定要备份注册表，并且一定要知道在发生问题时如何还原注册表。有关如何备份、还原和编辑注册表的信息，请单击下面的文章编号，以查看 Microsoft 知识库中相应的文章：256986MicrosoftWindows 注册表说明 ADO 流对象包含用于读写二进制文件和文本文件的方法。当 ADO 流对象与 InternetExplorer 中的已知安全漏洞组合后，Web 站点就可以从本机域执行脚本。为了帮助保护您的计算机免受此类攻击，可以手动修改您的注册表。

简介

ADO 流对象指内存中的一个文件。该流对象包含用于读写二进制文件和文本文件的几个方法。当此项特意设计的功能与 MicrosoftInternetExplorer 中的已知安全漏洞组合后，InternetWeb 站点就可以从本机域执行脚本。出现此问题的原因是，当 InternetExplorer 中存在 ADODB.Stream 对象时，ADODB.Stream 对象允许对硬盘进行访问。

任何需要将文件加载或保存到硬盘上的业务流程 Web 应用程序可能会在 InternetExplorer 中使用 ADODB.Stream 对象。例如，如果 Intranet 服务器上存有一个需要员工下载并填写的表，ADODB.Stream 对象则用来获取该文件并将其保存在本地。用户在本地编辑完该文件并将其提交回服务器后，ADODB.Stream 对象则用来从本地硬盘中读取该文件并将其发送回服务器。

强烈建议您使用其他方法提供此功能。例如，可以使用需要用户审慎访问硬盘的应用程序或控件。

软件更新信息

警告：“注册表编辑器”使用不当可导致严重问题，可能需要重新安装操作系统。Microsoft 不能保证您可以解决因“注册表编辑器”使用不当而导致的问题。使用“注册表编辑器”需要您自担风险。

Microsoft 提供了三种方法用来禁用 InternetExplorer 中的 ADODB.Stream 对象。您可以使用 MicrosoftWindowsUpdate 更新您的计算机、可以从 Microsoft 下载中心下载更新文件，也可以手动禁用 ADODB.Stream 对象。

这些方法将在创建以下注册表项后奏效：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InternetExplorer\ActiveXCompatibility\{00000566-0000-0010-8000-00AA006D2EA4}

该注册表项具有 ADODB.Stream 对象的 GUID。当 InternetExplorer 识别此注册表项时，InternetExplorer 不允许在浏览器中启动此组件。

Windows 更新

要安装此更新，请访问下面的 MicrosoftWeb 站点：

http://v4.windowsupdate.microsoft.com/zhcn/default.asp

Microsoft 下载中心更新

要使用 Microsoft 下载中心提供的注册表项更新来禁用 ADODB.Stream 对象，请访问下列 MicrosoftWeb 站点之一，具体情况视您的操作系统而定：

32-bit

http://www.microsoft.com/downloads/details.aspx?dis

playlang=zh-cn&FamilyID=4D056748-C538-46F6-B7C8-2FBFD0D237E3

64-bit

http://www.microsoft.com/downloads/details.aspx?FamilyId=E7576B19-DE8B-41B0-BBD9-06C39591CECF&displaylang=en

Microsoft 下载中心 Web 站点上提供其他信息以及下载说明。

手动处理

要通过手动创建注册表项来禁用 ADODB.Stream 对象，请按照以下步骤操作：

单击“开始”，然后单击“运行”。

在“打开”框中，键入 Regedit，然后单击“确定”。

在注册表编辑器中，找到以下注册表项：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InternetExplorer\ActiveXCompatibility

右键单击“ActiveXCompatibility”，指向“新建”，然后单击“项”。

为新项键入下面的名称：

{00000566-0000-0010-8000-00AA006D2EA4}

右键单击此新项，指向“新建”，然后单击“DWORD 值”。

将该值命名为 CompatibilityFlags。

在右窗格中，右键单击“CompatibilityFlags”，然后单击“修改”。

在“编辑 DWORD 值”对话框中，确保选中“十六进制”选项，在“数值数据”框中键入“400”，然后单击“确定”。

关闭注册表编辑器。

设定兼容性标记后，ADODB.Stream 对象即无法在 InternetExplorer 中访问您的计算机硬盘。但是，ADODB.Stream 对象仍可以在 InternetExplorer 以外访问您的硬盘。

重要说明

添加此注册表项后，只有 InternetExplorer 中的 ADODB.Stream 对象受影响。其他 ADO 对象不会受到此更改的影响。

应用此更新后，当您尝试从 InternetExplorer 的 HTML 页中使用 ADO 流对象时，将收到以下错误信息：

ActiveXcomponentcan＇tcreateobject:＇ADODB.Stream＇

如果您在企业内部网环境中运行应用程序，而当前企业内部网环境在 InternetExplorer 中使用 ADODB.Stream 对象，应用此更新可能导致应用程序停止运行。要恢复应用程序功能，Microsoft 建议首先将您的 InternetExplorer 浏览器的安全级别设为“高”，然后必须清除 ADODB.Stream 对象的兼容性标记

要将您的 InternetExplorer 浏览器设置为高安全级别，请按照这些步骤操作：

在 InternetExplorer 中，单击“工具”菜单中的“Internet 选项”。

单击“安全”选项卡。在“请为不同区域的 Web 内容指定安全设置”下单击“Internet”。

单击“默认级别”，然后将滑动条移动到“高”。

单击“应用”，然后单击“确定”关闭“Internet 选项”对话框。

将值设定为零(0x0)即可清除 InternetExplorerADODB.Stream 对象的兼容性标记。将值设定为零(0x0)可禁用该项并恢复功能。要手动将兼容性标记设置为零，请按照以下步骤操作：

单击“开始”，然后单击“运行”。

在“打开”框中，键入 Regedit，然后单击“确定”。

在注册表编辑器中，找到以下注册表项：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InternetExplorer\ActiveXCompatibility\{00000566-0000-0010-8000-00AA006D2EA4}

在右窗格中，双击“CompatibilityFlags”。

在“编辑 DWORD 值”对话框中，确保选中“十六进制”选项，在“数值数据”框中键入“0”，然后单击“确定”。

关闭注册表编辑器。

参考

有关如何在 InternetExplorer 中加强本机域的其他信息，请单击下面的文章编号，以查看 Microsoft 知识库中相应的文章：

833633HowtostrengthenthesecuritysettingsfortheLocalMachinezoneinInternetExplorer

有关 Internet 安全的更多信息，请访问下面的 MicrosoftWeb 站点：

http://www.microsoft.com/security/incident/settings.mspx

有关如何禁止在您的系统上运行 ActiveX 控件的其他信息，请单击下面的文章编号，以查看 Microsoft 知识库中相应的文章：

240797 如何禁止 ActiveX 控件在 InternetExplorer 中运行

这篇文章中的信息适用于:

MicrosoftInternetExplorer5.01SP3

MicrosoftInternetExplorer5.01SP4

MicrosoftInternetExplorer6.0

MicrosoftInternetExplorer6.0SP1

MicrosoftDataAccessComponents2.5

MicrosoftDataAccessComponents2.6

MicrosoftDataAccessComponents2.7

MicrosoftDataAccessComponents2.8

浅析“传奇”木马的防范方法

防治传奇木马首先要能够认识木马，木马分为捆绑在 EXE 文件上的木马(即通常所说的外挂木马)和网页木马，在你运行外挂和打开网页的时候，木马就种入了你的电脑中，在你进入传奇时，将你的密码和帐号发送到盗号者的邮箱中。

首先，要在自己的电脑上装上杀毒软件，经常升级，一般的杀毒软件都带有防火墙，一旦发现病毒会自动报警，常用的杀毒软件有瑞星 2003，KV3000，金山毒霸 2003，偌顿 8.0，其中瑞星 2003 还有邮件发送监控功能，只要你的电脑里装了其中任何一种软件，并且保持经常升级，那一般的捆绑式木马和网页木马就逃不过它们的眼睛了。因为虽然一般的杀毒软件不会认为木马是病毒，但是用捆绑机捆绑后的木马，都会认为是病毒，网页木

马也一般逃不过病毒防火墙的防范。

第二，要在电脑中装上常用的专杀木马的软件.一般的杀木马软件有木马克星，PC 绿鹰万能精灵，噬菌体密码防盗专家，超级兔子 ms98，其中由于噬菌体密码防盗专家经常会误报，在 IE 地址栏输入字母也会报告键盘监听，并不太实用.有些比较厉害的木马，杀毒软件没有升级到最新是查不出来的，还有些木马，运行后会自动关闭杀毒软件防火墙，这时候，专杀木马的工具就有用了，用它们可以查出系统进程中的木马，还有些木马，运行后会强制关闭木马克星和绿鹰 PC 万能精灵。这时候就要用系统进程检查工具，我认为比较好用的是 MS98，因为它并不是专杀木马的工具，所以木马都不会强制关闭它，如果你的电脑上已经运行不了木马克星和绿鹰精灵了，那就运行它来检查系统进程，看看有没有可疑的进程，运行这个软件后，里面有一项是自动运行，点开它，出现一个窗口，左边是进程管理，也就是目前正在运行的进程，右边是自动运行，也就是每次开机时自动运行的进程。由于木马运行后都会在系统中留下进程，也会随电脑自动运行，而这时在 MS98 里的系统进程和随机自动运行的进程都一目了然了，所以也就很好查杀了。找出可疑的进程，终止进程就可以了。下面我根据我防治传奇木马总结出的经验把常见的木马的进程列在下面:

传奇黑眼睛:

c:\windows\Taskmon32.exe，自动运行进程:Taskmon32

传奇叛逆:

c:\windows\system\internet.exe，自动运行进程:Intel

传奇终结者:

c:\windows\scanrew.exe，**自动运行进程**:scanrew

传奇密码使者:

c:\windows\system\cleanmgl.exe **和** c:\windows\system\sticpl.exe

自动运行进程:Microsoft

传奇猎手:

c:\windows\system\winsys.exe，**自动运行进程**:winsys

传奇幽灵:

c:\windows\internet.exe，**自动运行进程**:internet

传奇天使:

c:\windows\kiss.exe，**自动运行进程**:kiss

量子密码：终结黑客的梦想

科学家们认为它是最安全的密码，最高明的黑客也将对它一筹莫展。

美国《商业周刊》把它列在了“改变人们未来生活的十大发明”的第三位。

上个世纪 90 **年代以来，越来越多的科学家醉心于量子密码的研究。**2004 **年** 6 **月** 3 **日，世界上第一个量子密码通信网络正式投入运行，使得科学家们“绝对安全密码”的梦想向现实迈近了一步。**

无法破译的数据

马萨诸塞州的剑桥城在美国名声显赫，并不仅仅是由于它风光宜人，更是由于这里有着美国人最引以为豪

的哈佛大学和麻省理工学院，是美国新技术的摇篮。世界上第一个正式投入量子密码通信网络正是诞生在这里。

乍看起来，这个由美国 BBN 技术公司研发的量子密码通信网络和现有的宽带网并没有太大的不同——采用普通光纤传输数据，并且与普通网络完全兼容。与普通网络不同的是，该网络中传输的数据采用了量子密码技术进行加密。目前，网络有 6 个节点，已经从 BBN 公司铺设到了哈佛大学，预计今年年底将延伸至波士顿大学。

BNN 公司的负责人声称，采用量子密码术加密的数据是不可破译的，一旦有人非法获取这些信息，使用者会立即知道，并采取措施。

他们假设了黑客入侵网络的场景：黑客必须用一个特殊的接收设施从一连串的量子中“吸”出一个来获取信息，但这样一来，发出量子密码的一方立即就会发现量子流中出现了空格。为了避免被发现，一般黑客会再发射一个量子来填补这个空格。但是，由于“量子密码”是采用量子的极化方式（波的运动方向）来编排密码的，而根据量子学原理，要同时检测出量子的 4 种极化方式，几乎毫无可能，黑客填补进去的量子只能是根据自己的猜测随便发射的——这样，这个“不合群”的量子很快就会被发现，从而防止信息被窃取。

“神秘的远距离活动”独一无二

自人类文明诞生伊始，就有了保密的需要。古希腊的斯巴达人把重要的信息写在一条大约 1 厘米宽、20 厘米长的羊皮带上，写的时候，把羊皮带一圈一圈呈螺旋状绕在特定粗细的木棍上，然后从左到右开始写，写完

一行，将木棍旋转 90 度，再从左到右写。这样，写完之后，从木棍上解下的羊皮带上的字，就是一段密码。收到羊皮带的人，再把它缠绕到同样粗细的木棍上，才能读出完整的信息。

后来，人们渐渐开始利用数学计算方法，用复杂的数字串对信息进行加密。然而，再复杂的数学密钥也可以找到规律。第一台现代计算机的诞生，就是为了破解复杂的数学密码。随着计算机的飞速发展，破译数学密码的难度也逐渐降低。

上个世纪 90 年代开始，科学家们的眼光锁定在了“量子密码”上。

“量子密码”就是用量子状态来作为信息加密和解密技术的密钥。其原理就是被爱因斯坦称为“神秘的远距离活动”的量子纠缠。光子被分割开之后，即使相距十分遥远，也是相互联结的。只要测量出一个“被纠缠”光子的属性，就很容易推断出其他光子的属性。而这些相互纠缠的光子产生的密码，只有通过特定的发送器和接收器才能阅读。

更重要的是，这些光子之间“神秘的远距离活动”是独一无二的，只要有人非法破译这些密码，就不可避免地要扰乱光子的性质，而且，异动的光子会像警铃一样会显示出入侵者的踪迹。再高明的黑客对这种加密术也将一筹莫展。

各国发力“量子密码”

这种绝对安全的“量子密码”将最先运用于军事、国家安全等领域，并成为各国科学家角逐的新战场。

2002 年 10 月，德国慕尼黑大学和英国军方的研究机构合作，在德国、奥地利边境的楚格峰和卡尔文的峰

之间用激光成功传输了量子密码。这项研究的负责人慕尼黑大学教授哈拉尔德·魏因富尔特在报告中表示，这次试验传输的距离达到了 23.4 公里。

今年 5 月，日本的科学家称他们开发出传输速度最快的量子密码，实验中，研究小组利用 10.5 公里长的光纤进行信号传递，接收一方用光子探测器降低干扰，大幅缩短了传送时间，使得通信时间缩短到原来的 1/100。

中国也在近几年展开了量子保密通信系统的研究。2003 年 7 月，中国科学技术大学中科院量子信息重点实验室的科学家在该校成功铺设一条总长为 3.2 公里的“特殊光缆”——一套基于量子密码的保密通信系统。

由于在光纤传输过程中，光子很容易消耗，目前量子密码还只能在短距离内传输。一旦这个瓶颈被突破，量子密码将迎来大发展。科学家们表示，保密与窃密就像矛与盾一样形影相随，它们之间的斗争已经持续了几千年，量子密码的出现，将成为这场斗争的终结者。

EFS 加密文件夹无法打开怎么办

EFS（EncryptingFileSystem，加密文件系统）是从 Windows2000 开始就提出的一种基于 NTFS 文件系统的核心文件加密技术，主要是用于保护本地数据。在使用 EFS 加密文件的同时，也产生了诸多麻烦，比如重装系统后无法打开 EFS 加密过的文件夹等等，那么我们该如何解密?现在让我们先来看看大家的讨论。

备份及导入密钥来解密

为了防止在重装系统后无法打开加密文件夹，我们

可以通过下面的方法来备份及导入密钥：点击“开始→运行”，输入“certmgr.msc”，回车后打开证书管理器。展开“证书/个人/证书”，右键单击在右侧窗口中以用户名为名称的证书，在“所有任务”中选择“导出”打开证书导出向导。单击“下一步”之后选择“是，导出私钥”，单击“下一步”，选择默认导出文件格式，再单击“下一步”，输入保护密码和确认密码，单击“下一步”后指定文件名，最后单击“完成”即可。

这样在重装系统之后，右键单击导出的私钥文件，选择“安装 PFX”之后就可以一步一步导入私钥。导入完成后，就可以顺利地打开 EFS 加密的文件夹。

软件的方法不可靠

在没有备份密钥的情况下，要对 EFS 解密几乎是不可能的，虽然网上流行很多种方法，但是可行性微乎其微，劝大家放弃。因为某些 EFS 使用的是公钥证书对文件加密，而且在 Windows2000/XP 中，每一个用户都使用了惟一的 SID（安全标志）。第一次加密文件夹时，系统会根据加密者的 SID 生成该用户的密钥，并且会将公钥和密钥分开保存。如果在重装系统之前没有对当前的密钥进行备份，那就意味着无论如何都不可能生成此前的用户密钥，而解密文件不仅需要公钥，还需要密码，所以也就根本不能打开此前 EFS 加密过的文件夹。

编者按：通过各位大虾的谈论，至少应该得出这样一个结论，在进行 EFS 加密后一定要进行证书备份。否则遇到特殊情况，那被加密过的文件夹就无法打开了。

对 WinXP 进行安全分析和配置

一旦合适的安全模板被更改，就可以通过安全配置和分析组件或者命令行工具进行安全分析和配置。这个过程可以在应用安全模板到本地系统的时候进行。

警告：给 WindowsXP 系统应用安全模板可能造成性能和功能的丧失。

向 MMC 中载入安全配置和分析组件

要向 MMC 中载入安全配置和分析组件：

运行微软管理控制台（mmc.exe）

选择控制台-添加/删除组件

点击添加

选择安全配置和分析

点击添加

点击关闭

点击确定

为了避免下次使用 MMC 时重新载入需要的组件，我们可以把控制台设置保存起来：在控制台菜单，选择保存。默认情况下，文件将会被保存在当前登录用户的管理工具菜单中。

输入你要保存的控制台的名称

从这时开始，可以直接从开始-所有程序-管理工具直接访问保存后的控制台。

注意：MMC 中同时可以载入多个不同的组件，例如，安全模板还有安全配置和分析模板可以一起载入 MMC 并保存供以后使用。

安全配置数据库

安全配置和分析组件使用数据库保存分析或者配置的设置，要使用 GUI 打开一个已有的或者新数据库：

在 MMC 中，在安全配置和分析节点上点击鼠标右键

选择打开数据库

输入已有或者新建的数据库的名称

点击打开

注意：建议每次进行新的配置和分析都创建一个新数据库。

配置文件可以通过以下几种方法导入数据库：

如果在打开数据库时已经输入了新数据库的名称，用户将被自动要求输入要导入的配置文件，否则：

在 MMC 左侧面板的安全配置和分析节点上点击鼠标右键

选择导入模板

在导入模板对话框，选择需要导入的 inf 文件

选中导入前清空数据库选项，以删除任何之前保存在数据库中的无用数据，见图 10

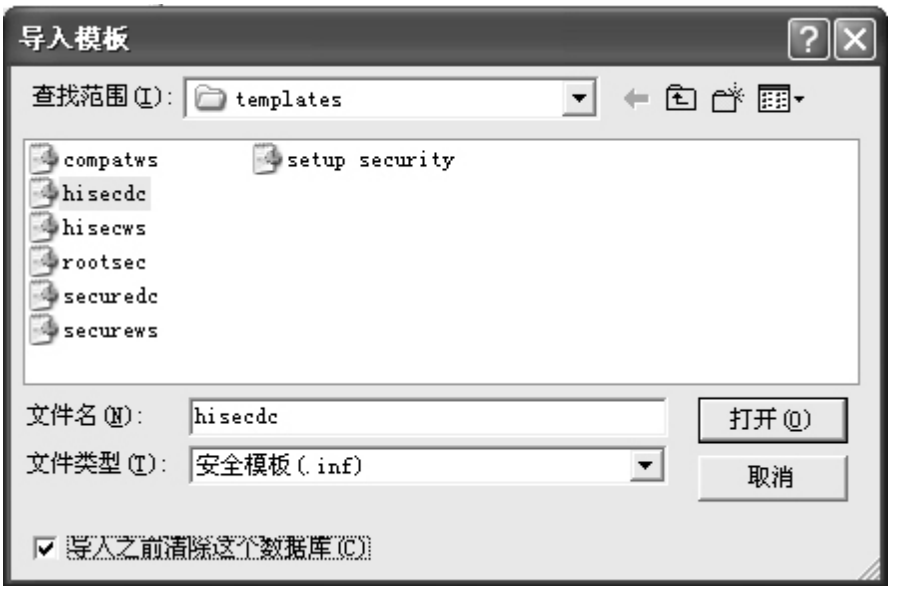

图 10

注意：导入操作可能会附加或者复写之前导入的数据库信息，默认是附加。如果用户不想把几次分析的配置信息都综合起来，就在导入模板前选中"导入前清空数据库"选项。

警告：为了避免配置文件的混乱和混合，建议每次进行新的分析和配置前都选中这个选项。

点击打开

Secedit **命令行选项**

Secedit.exe，**曾经在第二章介绍过，是通过命令行或者批处理和/或计划任务的方式进行安全分析和配置时的有用工具。用** secedit **进行系统分析和配置时可用的参数有：**

secedit{/analyze|/configure}[/cfgfilename][/dbfilename]