清除间谍软件

清除间谍软件

一位终端用户的网页被篡改到购物页面了。另一种情况是出现大量的弹出广告，甚至是无聊的内容。还有一种是被工具栏所困扰，在每次使用浏览器搜索功能时都会弹出。不知道他们出现这些问题的原因是什么，也不知道他们是如何出现的。作为公司的 IT 管理员或者经理，需要认识到这些问题都是间谍软件造成的。然而，你已经负担过重了，根本没有时间运行电脑修复每个问题。本文将帮助理解间谍软件、它的来源、行为方式和引起的问题，并提供一些清除间谍软件的技术，以及如何防御将来的入侵。

间谍软件简介

间谍软件是信息时代和 Windows 平台上的主要的灾难之一。“间谍软件”是对利用用户的无知或者系统的不安全性来安装的软件的通常名称，它的安装经常是不知不觉或者是不经过同意的。间谍软件程序具有破坏性，而且通产很危险。间谍软件进入电脑通常通过两种方法……

- 认识间谍软件
- 了解间谍软件的来源
- 间谍软件的行为方式

间谍软件灾难

通常的问题可能是对间谍软件的抱怨。弹出的广告窗口、不想要的工具栏、IE 或者系统托盘图标、对系统功能的不希望的改变（例如浏览器开始页面被劫持或者变成其他）都是最常见的受影响的征兆。最严重的间谍软件也会影响基础系统设置。

- 间谍软件引起的灾难

间谍软件的清除

因为间谍软件已经很普遍了，所以有很多反间谍软件工具。而且这些工具可以让个人免费使用，而且他们还在不断更新。Spybot - Search & Destroy 是这一批中的第一个，而且仍然是最好的反间谍软件工具之一。除了扫描和移除大量的不知名的应用，它还在为应对将来的攻击方面可以锁定系统。初用者可以通过点击按钮清洁系统，而专家用户可以把仍然隐藏的细节信息取出来，并用其进行更深入的研究。此外还可以在熟悉的 Windows 系统内部清除间谍软件。

- 选择清除间谍软件的工具
- 采用高级技术清除间谍软件
- 安装服务包防御间谍软件入侵
- 防御间谍软件入侵的另外的主动措施

新间谍软件的应对

现在感染一台计算机要比过去困难很多，间谍软件的制作者都比以前更聪明了，他们它间谍软件作为系统组件注册，而且只能被高手检测到。还好大部分杀毒和防御软件制作者都严肃地把间谍软件作为一种威胁来看待，并寻找更好的方法来执行，而不需要关注程序或者低等级的系统黑客。

- 新间谍软件策略

认识间谍软件

间谍软件是信息时代和 Windows 平台上的主要的灾难之一。“间谍软件”是对利用用户的无知或者系统的不安全性来安装的软件的通常名称，它的安装经常是不知不觉或者是不经过同意的。

间谍软件程序具有破坏性，而且通产很危险。他们可能劫持浏览器攻击市场 Web 网站、发布不希望的广告、或者侦测你的浏览行为和输入习惯，并把这些信息报告给第三方。最后一点也是间谍软件名称的由来，对于很多用户和系统管理员来说，这种程序是和病毒处于同一分类中：都是不希望的有害入侵。

电脑上不能存在这样的内容。它会减缓速度、妨碍工作，有时甚至导致系统完全不能使用。

(作者：SearchWindowsSecurity.com 译者：Tina Guo 来源：TechTarget 中国)

了解间谍软件的来源

间谍软件通常通过以下两种方法中的一种进入电脑：

1.通过 Web 网页隐秘地上传，通常是通过摊开的 Windows 窗口或者隐藏的架构。在这个页面安装程序的时候不会发出警告，除非 Web 浏览器是特别为这样的问题警告用户而设计的。（IE 6 的第一个版本和之前的版本很容易受到这种攻击。）

2.和另外的软件程序捆绑在一起，通常是做为产生广告收入支持程序开发的一种方式。

这两种方法的第一种到目前为止应用最广泛——特别是在桌面没有正确保护以及浏览器插件可以不受阻碍的安装的企业中。第二种的应用不太广泛，但是仍然很受欢迎，因为你可能会安装你认为是免费的应用程序，到后来才发现它是间谍软件。

（作者：SearchWindowsSecurity.com 译者：Tina Guo 来源：TechTarget 中国）

间谍软件的行为方式

和病毒的感染一样，大部分的间谍软件的行为是无声无息的。当一个新程序安装时电脑很少会发出警告——当然新程序不会有明显损害的。当窗口开始弹出或者浏览器杯劫持的时候，你只知道出现问题了。

直到最近，IE 才向用户提供简单的方法，可以决定哪些低水平的插件被安装了，否则样不希望的插件造成破坏的时间就很难监测了。IE6 和更高的版本可以带有这样的功能；更多的细节可以查阅“高级清除”。

在有些情况下，恶意程序在添加和删除程序中显示了新的入口，也可以通过这种方法移除。很多更加“光明正大的”间谍软件都是设计为工作方式相同的其他软件（例如，TopMoxie）的可以产生利益的附加软件，但是如果移除了间谍软件，安装间谍软件的父级程序就可能不能正常工作了。如果其中一个出现了问题，他们都会出现问题。

（作者：SearchWindowsSecurity.com 译者：Tina Guo 来源：TechTarget 中国）

间谍软件引起的灾难

通常的问题可能是对间谍软件的抱怨。弹出的广告窗口、不想要的工具栏、IE 或者系统托盘图标、对系统功能的不希望的改变（例如浏览器开始页面被劫持或者变成其他）都是最常见的受影响的征兆。

这是问题自身已经造成威胁了，但是很多间谍软件程序加起来要比简单混合更危险——他们具有入侵性和破坏性。他们可以登录并跟踪用户的浏览习惯，这是典型的隐私入侵。他们可能造成其他程序的关闭，可能是因为他们没有友好交互作用（例如，劫持某些文件扩展）或者因为间谍软件程序导致了系统资源紊乱。

最严重的间谍软件也会影响低基础的系统设置。有些会重写 HOSTS 文件，改变一般网络地址名并劫持网络流量。其他的可能自由改变注册设置或者安装伪装为系统服务的程序，这些程序几乎不可能轻易删除。有些甚至把自己作为低等级的网络组件，进行更多的网络窃听。还好，因为大部分的间谍软件的行为方式是相当讨厌的，他们最低在出现后不是太长的时间内向用户发出警告。

（作者：SearchWindowsSecurity.com　译者：Tina Guo　来源：TechTarget 中国）

选择清除间谍软件的工具

好消息是因为间谍软件已经很流行了，所以有很多反间谍软件工具。

更好的是这些最好的工具可以让个人免费使用，而且他们在不断更新，这要感谢很多贡献者不懈努力。

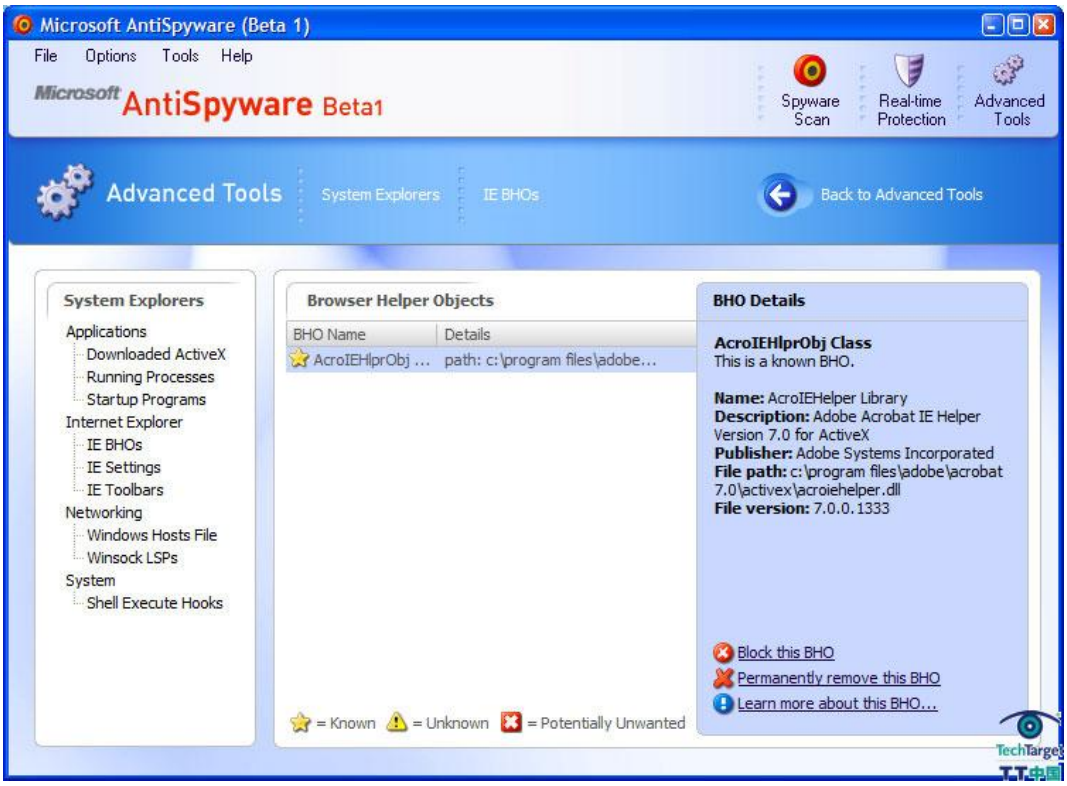
Spybot - Search & Destroy 是这一批中的第一个，而且仍然是最好的反间谍软件工具之一。除了扫描和移除大量的不知名的应用，它还在为应对将来的攻击方面可以锁定系统。初用者可以通过点击按钮清洁系统，而专家用户可以把仍然隐藏的细节信息取出来，并用其进行更深入的研究。

Lavasoft's Ad-Aware 存在免费和付费版本，但是免费个人版被广泛地认为是“另外的”最好的反间谍人间工具。它没有 Spybot - Search & Destroy 工具的广阔性（至少在免费版本中没有），但是它通常可以清楚更广范围的问题，而且它的扫描引擎可以更频繁的更新。

如果你是初用者，而且只想做一些清楚的工作，可以先使用 Ad-Aware。如果你经验丰富，或者拥有电脑高手的支持，可以使用 Spybot。首先在初用者的模式下进行基本的清除工作，然后转换到高级模式察看可以揭示的其他内容。

微软还发布了 AntiSpyware 的测试版本，它有一些系统分析和清除工具，而且可以允许用户向微软提交可疑的间谍软件供分析。

最后，很多杀毒软件包可以识别并处理间谍软件作为病毒的子类——很明显需要长时间的。（查看诺顿互联网安全 2005 反间谍软件版本和趋势科技的 PC-cillin.）。

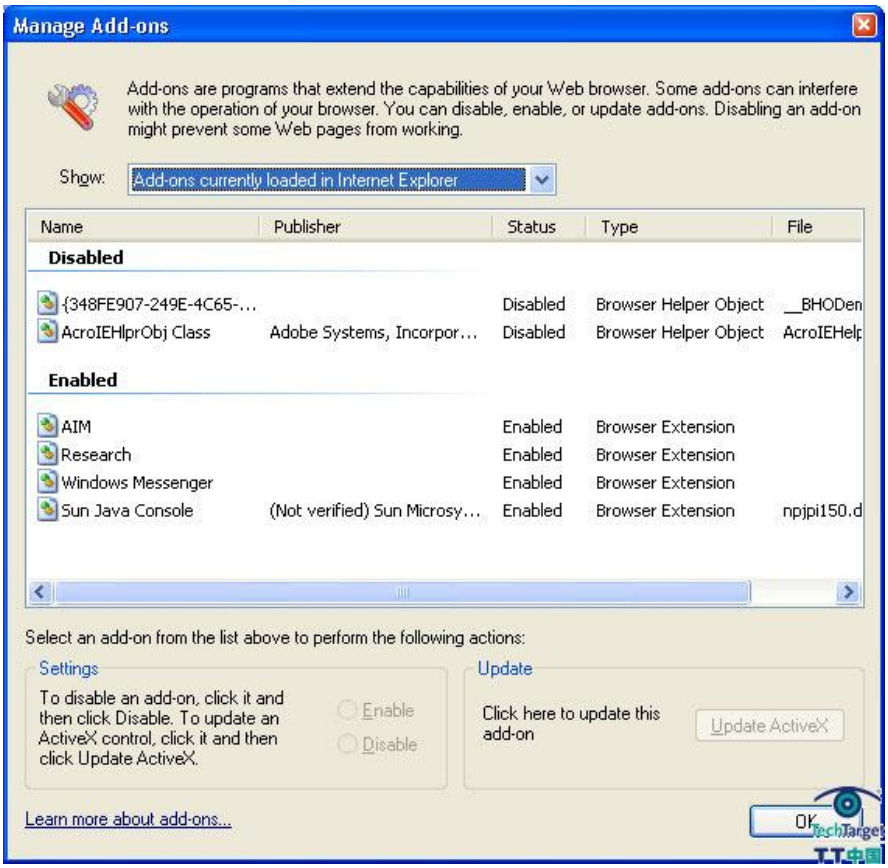


(作者：SearchWindowsSecurity.com 译者：Tina Guo 来源：TechTarget 中国)

采用高级技术清除间谍软件

如果你已经熟悉了 Windows 系统的内部工作，你可以进行下一步，并进行谨慎的清除。这里就是你要寻找的最好的工具。（注意 Spybot - Search & Destroy 有些内置工具来管理这些问题。）

BHO：也就是 Browser Helper Objects，就像上面描述的，是 IE 的插件，可以通过 Web 页面安装。有些是良性的，甚至是有用的(例如微软自己的研究 BHO)，但是很多不出名的 BHO 应该不要激活。在 IE 中，选择工具/Internet 选项/程序/管理加载项来查看浏览器插件列表或者在 IE 中表现的浏览器帮助者对象(BHO)。



启动：不想要的程序通常在启动时加载。Sybot-Search&Destroy 可以帮助浏览启动列表并删除不属于这里的内容。尽管如此，要谨慎对待要关闭的程序：有些程序可能是合法的。

HOST 文件的变更：Host 文件是一个没有扩展的简单的文本文件。它存在于 windowssystem32driversetc.中，包括一个预解决的网络地址列表。通常它包含一个本地文件的入口，除非它已经被设置为只读，很多间谍程序系统喜欢使用错误的入口上传。例如，间谍软件可以把 Microsoft.com 导向岛自己的服务器上。再可能的把 HOST 设置为只读（这是 Spybot - Search & Destroy 所允许的。）

（作者：SearchWindowsSecurity.com 译者：Tina Guo 来源：TechTarget 中国）

安装服务包防御间谍软件入侵

微软发布了服务包，对间谍软件敞开了 IE 的大门——或者不如说窗口，并在 Windows XP SP2 中对 IE6 作了重大变更。IE 目前不允许在 BHO 在没有经过用户允许的情况下安装，这样就防御了大量浏览器间谍软件在电脑中找到立足之地。

在任何新的 Windows 电脑上安装 XP SP2 在这一点上多少都应该有些强制性。 所有的厂家建立的系统都可以起到带动作用，而且现存的任何系统都没有打上应该打的补丁。通常，通过 Windows 更新安装 SP2，但是如果你选择手动来做，或者为了更容易更新堕胎电脑而刻录到 CD 中，微软提供了它的单独下载。

(作者：SearchWindowsSecurity.com 译者：Tina Guo 来源：TechTarget 中国)

防御间谍软件入侵的另外的主动措施

不管是过去还是现在，很多人都选择换到完全不同的浏览器，而不是仍然坚持微软和 IE 的不安全性。而选择的浏览器不能向第三方提供直接的路径在一台电脑上安装不想要的软件。 Mozilla 的 Firefox 浏览器很受欢迎，不止是个人，而且在企业也是如此。 （到目前为止）在 Windows 的域名管理功能的整合上缺乏的组成了新的功能和更好的安全基础——特别是因为它不能默认运行 ActiveX 控件（例如，BHO）。

至于和其他应用程序捆绑的间谍软件，唯一有意义的是自我监管。 如果问题被列为“免费软件”，需要全面阅读安装说明，并注意安装过程的每一步。 如果你察觉了另一个完全不了解的程序的安装，停止安装的过程并作一些工具，或者至少在发现后运行间谍软件扫描应用。 可能的情况是间谍软件运行需要的免费应用程序不值得付出沉痛的代价。

(作者：SearchWindowsSecurity.com 译者：Tina Guo 来源：TechTarget 中国)

新间谍软件策略

现在感染一台计算机要比过去困难很多，间谍软件的制作者都比以前更聪明了。例如，Firefox 的流量程度的增加让人担心 Firefox 的工具可以很快在电脑中写入间谍软件。 很多更复杂的间谍软件的新类型把自己作为操作系统组件来注册，而且只能被经验丰富的用户测试到。

好消息是对间谍软件的防线还在迅速增长。 大部分不需安装的 Windows 电脑（在写这篇文章的时候）几乎都容易受到间谍软件的工具，因为他们是在六个月前的。 较好的是，大部分杀毒和防御软件制作者都严肃地把间谍软件作为一种威胁来看待，并寻找更好的方法来执行，而不需要关注程序或者低等级的系统黑客。

(作者：SearchWindowsSecurity.com 译者：Tina Guo 来源：TechTarget 中国)