网页木马深度剖析以及手工清除1 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/474/2021_2022__E7_BD_91_E9_A1_B5_E6_9C_A8_E9_c67_474165.htm 阅读提示：杀毒软件风靡全球的今天，各式各样的病毒仍然在网络上横行，其形式的多样化，自身之隐蔽性都大大的提高。其中，网页病毒、网页木马就是这个新型病毒大军中危害面最广泛，传播效果最佳的。之所以会出此篇，也是在考虑到太多的人都在网页病毒中“ 应声倒下 ”，却不知自己是如何中毒，以及中毒后如何去处理。就此问题，我们开始以下，对网页病毒、网页木马这一“ 新概念 ”做个详细的剖析。 前言 杀毒软件风靡全球的今天，各式各样的病毒仍然在网络上横行，其形式的多样化，自身之隐蔽性都大大的提高。其中，网页病毒、网页木马就是这个新型病毒大军中危害面最广泛，传播效果最佳的。之所以会出此篇，也是在考虑到太多的人都在网页病毒中“ 应声倒下 ”，却不知自己是如何中毒，以及中毒后如何去处理。就此问题，我们开始以下，对网页病毒、网页木马这一“ 新概念 ”做个详细的剖析。 注：为什么会用这么大的篇幅去介绍网页病毒、网页木马的常识和运行机理，而非机械地去介绍如何如何做，大家在通读全文后便有个新的了解。 第一章 恶意网页的基本常识 第一节 什么是网页病毒 网页病毒是利用网页来进行破坏的病毒，它存在于网页之中，其实是使用一些script语言编写的一些恶意代码利用IE的漏洞来实现病毒植入。当用户登录某些含有网页病毒的网站时，网页病毒便被悄悄激活，这些病毒一旦激活，可以利用系统的一些资源进行破坏。轻则修改用户的注册表，使用户的

首页、浏览器标题改变，重则可以关闭系统的很多功能，装上木马，染上病毒，使用户无法正常使用计算机系统，严重者则可以将用户的系统进行格式化。而这种网页病毒容易编写和修改，使用户防不胜防。 目前的网页病毒都是利用JS.ActiveX、WSH共同合作来实现对客户端计算机，进行本地的写*作，如改写你的注册表，在你的本地计算机硬盘上添加、删除、更改文件夹或文件等*作。而这一功能却恰恰使网页病毒、网页木马有了可乘之机。 而在我们分析网页病毒前，先叫我们知道促使病毒形成的罪魁祸首：Windows脚本宿主和MicrosoftInternetExplorer漏洞利用 第二节 Windows脚本宿主，InternetExplorer漏洞以及相关 WSH，是“ Windows scripting Host ”的缩略形式，其通用的中文译名为“ Windows脚本宿主 ”。对于这个较为抽象的名词，我们可以先作这样一个笼统的理解：它是内嵌于Windows*作系统中的脚本语言工作环境。 Windows scripting Host这个概念最早出现于Windows98*作系统。大家一定还记得MS-Dos下的批处理命令，它曾有效地简化了我们的工作、带给我们方便，这一点就有点类似于如今大行其道的脚本语言。但就算我们把批处理命令看成是一种脚本语言，那它也是98版之前的Windows*作系统所唯一支持的“ 脚本语言 ”。而此后随着各种真正的脚本语言不断出现，批处理命令显然就很是力不从心了。面临这一危机，微软在研发Windows 98时，为了实现多类脚本文件在Windows界面或Dos命令提示符下的直接运行，就在系统内植入了一个基于32位Windows平台、并独立于语言的脚本运行环境，并将其命名为“ Windows scripting Host ”。WSH架构于ActiveX之上，通过充当ActiveX的脚本引擎控制

器，WSH为Windows用户充分利用威力强大的脚本指令语言扫清了障碍。 WSH也有它的不足之处，任何事物都有两面性，WSH也不例外。应该说，WSH的优点在于它使我们可以充分利用脚本来实现计算机工作的自动化；但不可否认，也正是它的这一特点，使我们的系统又有了新的安全隐患。许多计算机病毒制造者正在热衷于用脚本语言来编制病毒，并利用WSH的支持功能，让这些隐藏着病毒的脚本在网络中广为传播。借助WSH的这一缺陷，通过JAVAscript，VBscript，ACTIVEX等网页脚本语言，就形成了现在的“ 网页危机 ”。 促使这一问题发生的还有问题多多InternetExplorer的自身漏洞。比如：“ 错误的MIMEMultipurposeInternetMailExtentions，多用途的网际邮件扩充协议头 ”，“ MicrosoftInternetExplorer浏览器弹出窗口Object类型验证漏洞 ”。而以下介绍的几个组件存在的问题或漏洞或是在安全问题上的过滤不严密问题，却又造成了“ 网页危机 ”的另外一个重要因素。 