对付恶意软件的策略及方法计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/580/2021_2022__E5_AF_B9_E4_BB_98_E6_81_B6_E6_c98_580361.htm 2009年下半年全国计算机等级考试你准备好了没?考计算机等级考试的朋友,2009年下半年全国计算机等级考试时间是2009年9月19日至23日。更多优质资料尽在百考试题论坛 百考试题在线题库 恶意软件的设计目的是无需得到计算机所有者的明确同意即可渗透进入一台计算机系统，并实施破坏或进一步控制。恶意软件（malware）这个词来自于“ 恶意的（malicious）”和“ 软件（software）”的组合，计算机专家用这个词来意指多种敌意的、可插入的、讨厌的软件或程序代码。 恶意软件的危害 恶意软件的最常见的传播途径是通过互联网、电子邮件、万维网等。它可以劫持浏览器、重定向搜索意图、提供令人厌恶的弹出式广告、跟踪用户所访问的网站等。除了搞大规模的破坏之外，恶意软件还可以导致计算机变慢，或偷窃用户的银行账户等敏感信息。 许多恶意软件在用户清除了之后会重新安装。许多普通的计算机用户对这种软件并不熟悉，以为恶意软件就是病毒。实际上，并非所有的恶意软件都是病毒。 具体来说，恶意软件包括病毒、蠕虫、特洛伊木马、大多数的rootkit、间谍软件、不真实的广告软件，还有其它恶意的、用户不请自来的软件。恶意软件有时被称为有害的计算机垃圾。 有些软件存在缺陷，即包含有害的漏洞，但其目的是合法的，这样的软件不能称之为恶意软件。 恶意软件已经成为了我们网络生活中的现实。不幸的是，恶意软件并非仅仅是十分恼人的东西，对于大量的企业来讲，恶意软件已经

成为企业运营的重大负担，可造成企业巨大的经济损失。 恶意软件怎样潜入 用户可通过多种途径感染恶意软件。恶意软件通常与其它的软件捆绑在一起，一些共享的或免费的软件可成为其最舒服的温床。比如弹出式广告就可以将金钱发送到恶意程序的设计者，还有一些恶意软件是通过其它软件（如浏览器）的漏洞安装到用户计算机上的，它还会诱使用户访问恶意伪造的网站。 然而，多数的恶意软件是通过用户自己安装上的。比如用户在使用共享软件、免费软件时，其安装的软件有可能暗中包含恶意软件。有些用户经常通过超级用户账号上网冲浪，结果是有些恶意网站或被恶意软件控制的网站利用了浏览器中的漏洞，将恶意软件下载并安装到用户的电脑上。还有些用户打开或运行了垃圾邮件附件中的文件。不幸的是，恶意软件是得之容易去之难，它就像夏天的苍蝇一样无法赶尽杀绝。 对于一个恶意程序来说，要实现其目标，它必须在不关闭、用户不删除的情况下，发挥作用。在一个恶意软件将自己伪装为某种善意的程序时，用户可能会受到引诱将其安装到计算机上，完全不知晓其所作所为。这种技术称为特洛伊木马。很多情况下，它会安装更多的有害软件，目的是从长远上为恶意软件的制造者服务。 对付恶意软件威胁 恶意软件可以采取不同的形式,从广义上讲，最臭名昭著的莫过于特洛伊木马、rootkit、后门软件等，病毒和蠕虫也可以看作恶意软件。有些形式的威胁具有某几种恶意软件的特征。 因为恶意软件由多种威胁组成，所以需要采取多处方法和技术来保卫系统。如采用防火墙来过滤潜在的破坏性代码，采用垃圾邮件过滤器、入侵检测系统、入侵防御系统等来加固网络，加强对破坏性代码的防御能力。 作为一

种最强大的反恶意软件防御工具，反病毒程序可以保护计算机免受病毒、蠕虫、特洛伊木马的威胁。近几年来，反病毒软件的开发商已经逐渐将垃圾邮件和间谍软件等威胁的防御功能集成到其产品中。除了这些技术手段之外，企业应当采取措施防止恶意软件在单位网络内传播:1、教育员工正确使用电子邮件和Web 具体来说，特别要注意：◆要教育雇员，如果不知道邮件的来源和附件的属性，不要打开邮件中的附件。◆告诉员工不要从互联网下载和安装未获得授权的程序。◆让雇员清楚社会工程欺诈的骗术，提防其欺骗雇员点击受感染链接的伎俩。◆教育雇员了解最新的攻击手段，学习公司的安全策略和建议，并坚决执行。2、禁止或监督非web源的协议在企业网络内使用 如禁止或限制即时通信及端到端的协议进入企业网络，这些正是僵尸等恶意软件得以通信和传播的工具。3、确保在所有的桌面系统和服务器上安装最新的浏览器、操作系统、应用程序补丁，并确保垃圾邮件和浏览器的安全设置达到适当水平。4、确保安装所有的安全软件，并及时更新并且使用最新的威胁数据库。5、不要授权普通用户使用管理员权限，特别要注意不要让其下载和安装设备驱动程序，因为这正是许多恶意软件乘虚而入的方式。6、制定处理恶意事件的策略，在多个部门组建可实现协调响应职责并能够定期执行安全培训的团队。恶意软件威胁经过几年的发展已经成为一种强大的势力，更确切地说它已经成为一种受经济利益驱使的商业活动；而反恶意软件厂商由于受到各种因素的制约，应对和反击措施相对被动。并且前者在暗处，后者在明处，形式对反恶意软件的开发者不利。但两种力量的斗争将持续下去。2009年上半年全国计算机

等级考试参考答案请进入计算机考试论坛 2009年全国计算机等级考试报名信息汇总 2009年NCRE考试有新变化 2009年全国计算机等级考试大纲 2009年上半年全国计算机二级考试试题及答案 2009年上半年全国计算机等级考试试题答案汇总 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com