网络安全中灰色软件的症状与防范 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/252/2021_2022__E7_BD_91_E7_BB_9C_E5_AE_89_E5_c101_252860.htm 随着病毒、蠕虫、木马、后门和混合威胁的泛滥，当前针对新漏洞的攻击产生速度比以前要快得多，而社会工程(social engineering)陷阱也成为新型攻击的一大重点。带有社会工程陷阱元素的攻击包括间谍软件、网络欺诈、基于邮件的攻击和恶意Web站点等。这些攻击往往伪装为合法应用程序和邮件信息，设计为欺骗用户暴露敏感信息、下载和安装恶意程序，传统的安全设备很难加以阻挡，往往需要先进的检测和安全技术。本文着重介绍灰色软件的特征和防护方法。 一、什么是灰色软件 灰色软件是一个概括性词汇，它是指安装在计算机上跟踪或向某目标汇报特定信息的一类软件。这些软件通常是在没有得到允许的情况下安装和执行的。很多灰色软件是在需要下载和运行应用时，就能悄然地完成工作，比如跟踪计算机使用，窃取隐私等。在大量的邮件病毒成为每月新闻头条的时候，用户可能会意识到如果打开不确定的邮件会带来什么风险。但是对于灰色软件，用户根本就不需要打开附件或执行被感染的程序，仅仅访问使用该技术的网站，就会变成灰色软件的牺牲品。很多灰色软件只产生垃圾信息，比如说弹出式窗口。诚然，在“无害”的灰色软件和盗取信用卡账号、密码和身份证号这些有价值信息的攻击之间，还是有着明确的区分标准的。 灰色软件常常来源于以下行为:(1)下载共享软件，免费软件或其他形式共享文件.(2)打开被感染过的邮件.(3)点击弹出广告.(4)访问不负责任或欺骗网站.(5)安装木马

程序。 灰色软件不一定是恶意软件。很多灰色软件的最终目标是跟踪网站访问者来获得搜索结果，以达到某个商业目的。灰色软件的典型症状是系统缓慢、弹出广告、主页定向到别的网站等，从而造成骚扰。不过，黑客常会把灰色软件技术用作其他目的，例如利用浏览器来加载和运行某些程序。这些程序可以公开访问系统，收集信息，跟踪键盘输入，修改设置，或者制造某些破坏。 灰色软件大体可以分为以下几类: (1)广告软件 广告软件通常是嵌入到用户免费下载和安装的软件中。安装以后会不时地弹出浏览器窗口来传播广告，干扰用户正常使用。 (2)间谍软件 间谍软件通常嵌入在免费软件中。它可以跟踪和分析用户的行为，比如说用户的浏览网页的习惯。跟踪信息会返回到编写人员的网站，在那里进行记录和分析。它会引起计算机性能的改变。 (3)拨号软件 拨号软件是控制计算机的Modem的灰色软件。这些程序通常是拨打长途电话或者呼叫昂贵的电话号码来为窃取者创收。 (4)玩笑软件 玩笑软件修改系统的设置，但是并不摧毁系统。例如将系统鼠标或者Windows背景图片加以修改，还有些游戏软件通常是开些小玩笑或者恶作剧。 (5)点对点软件 点对点软件(P2P)可以完成文件交换。用它完成商业目标也许是合法的，而用它来交换非法音乐、电影和其他文件的时候，往往是非法的。(6)键盘记录软件 键盘记录也许是最危险的灰色软件之一。这些程序可以捕捉键盘的输入，由此获得用户名和密码、信用卡号，用于Email、聊天、即时通讯等。 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