以不变应万变常见木马入侵防范宝典 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/469/2021_2022__E4_BB_A5_E4_B8_8D_E5_8F_98_E5_c67_469469.htm 奇虎360安全中心最近发布的《互联网不安全报告》中披露，2007年上半年奇虎共截获病毒、恶意软件及木马程序共计168135个，其中木马程序占据了80%的比例。比如著名的“ 灰鸽子 ”木马，仅不完全统计就有大概6万个变种。 可见在现今阶段的互联网，木马的危害已经占据了主导。 谈“ 马 ”色变并不是空穴来风，你可能觉得自己已经安装了最新版本的杀毒软件和防火墙，自认铜墙铁壁、百毒不侵。可要命的变种木马程序让病毒库防不胜防。毕竟是先有病毒，再有病毒库更新。目前各大杀毒公司纷纷进入主动杀毒/防御领域，正是因为大家已经意识到面对最新木马病毒的查杀，时间是最关键的因素！ 那现阶段呢？我们这些饱受侵害的用户该做些什么呢？其实木马发展到现在，最重要的因素就是其很好的利用了社会工程学原理，在伪装和侵入方式上下足了功夫。这对于木马的整个入侵程序来说最为重要换句话说：你需要运行木马，才能让自己的计算机中招！今天就针对这一环节，分析当前木马惯用伎俩，不用杀毒软件也能分辨出木马程序。 木马攻击原理 木马变种再多，功能再强大，整个木马病毒的体系也只分为两大部分：客户端和服务端。一般情况下黑客会使用客户端编译出一个负责其自己要求的服务器端，倘若有人运行了这个服务器端程序，则他的电脑就真的成为了黑客的服务器，任其宰割了。当然，杀毒软件和电脑使用者不会这么“ 笨 ”，它们可以通过病毒的关键码和形态上分出该程序的性质，

所以黑客就需要对木马进行包装和加强也就是伪装和变种。特别提示：现在大部分的木马都已经采用了反弹式连接，普通防火墙很难再防御住这些木马，这主要是由于防火墙针对外部连接比较敏感，而对于内部向外连接的审查力度却小很多造成的。 原程序伪装 这种属于木马伪装中最基本的方式。以灰鸽子为例，在服务端配置的安装选项里可以更改程序的图标和释放路径，在启动设置中能够自定义注册表和服务的名称，甚至可以关联到iexplore.exe，让木马程序随时整装待命。丰富的伪装功能 试想你运行的程序图标如果和常见的setup类似，而且将木马以system.exe放到windows目录下，并且与iexplore.exe一同启动，即便是在注册表和服务中也找不到蛛丝马迹。此时你还会认为刚才运行的程序是木马吗？防范这些其实很简单。程序图标变，我们可以显示所有文件的类型，倘若发现一个看起来像文本的文件在显示后缀名后变成了exe类型，赶紧删了吧，它肯定不是什么好东西。注册表和系统服务有变化，可以利用杀毒软件的监视功能，或者是Regsnap等进行比照，然后将看起来很像系统服务名的内容送给google检查，没有这方面的信息？那它可以消失了！ 可能最难防范的就属在系统目录中放置程序的问题了。除了平常监视诸如system、windowns目录外，还需要对文件名称做直观的判断，由于目前木马伪装越来越成熟，这里建议大家：越是看起来像系统文件的越要注意。 捆绑伪装 文件捆绑技术并不是什么新玩艺。这种技术应用在木马上的最主要原因是对上面提到的原程序伪装的延续。换句话说，上面原程序伪装了半天，用户一旦运行发现没有任何效果肯定会产生疑问，而此时如果将一个其它程序注入到木马中同时进行，就会

更好的遮人耳目了。 如果我们遇到一些程序，可以使用一些查捆绑的工具（点击下载），如果查询到存在捆绑文件，还是小心为妙。捆绑分析 网页伪装保护 网页木马现在非常常见，因为黑客只要将木马嵌入到网页中，诱骗用户浏览该网页就可让其中招，同样类似的还有电子邮件木马，方式上二者类似。 这种木马最难防范，在主动防御技术还没有得到广泛应用之前，我们通过提升IE的安全级别，禁止脚本运行等方式来杜绝这类木马。但现在的嵌入技术包含了代码保护，所以防范起来还是不具有普遍性。 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