 2009年，计算机病毒和木马处于一个“ 低调增长期 ”，虽然一些类似熊猫烧香的重大恶性病毒越来越少见，但一些小范围、针对性强的新病毒、木马的数量依然在飞速增长。在岁初年末，金山反病毒专家对2010年中国互联网病毒发展趋势进行了预测。 1、0Day漏洞层出不穷 0Day漏洞仍然是黑客入侵的主要方式，新年伊始谷歌被入侵事件就证明了这一点。由于0Day漏洞和安全补丁的推出，这两者之间在时间上有一段空白期。所以黑客可以利用这段时间，大规模的入侵计算机用户的电脑系统，从中获取大量有价值的信息内容。正是由于0Day漏洞的巨大威力，以及可以从中获取大量的经济利益，因此黑客必然会更加挖掘系统和软件中的0Day漏洞，尤其是像Windows 7操作系统等可能存在的漏洞。 2、网页挂马、钓鱼网站将继续增加 网页挂马已经成为木马、病毒传播的主要途径之一。由于各种系统漏洞和软件漏洞的存在，因此通过挂马进行入侵的数量会继续增加。黑客在入侵网站系统以后，通过篡改网站网页或数据库的内容，就可以植入各种各样的下载脚本代码。用户只要浏览被植入木马的网站，如果系统存在漏洞就会遭遇木马入侵，从而造成个人信息和网络财富的损失。不过现在金山毒霸已经开发出，一款免费专业的浏览器保护工具金山网盾。计算机用户可以通过下载安装“ 金山网盾 ”，避免自己的系统受到网页木马的攻击和入侵。 3、木马捆绑东山再起 随着网络用户对网页挂马认识的提高，造成通过网页挂马入

侵的可能有所降低。但是与此相反的是通过传统的文件捆绑，进行入侵的事件则成明显上升的趋势。黑客通过将木马病毒，和图片、FLASH动画、文本文件等进行捆绑。然后再配以迷惑性的文件图标，这样用户稍不注意就可能上当受骗。而且现在最新版本的捆绑软件，不仅可以完成木马病毒的捆绑，有的还可以增加文件属性等虚假信息，而且更加增加了用户进行识别的难度。 4、无线攻击快速增加 随着3G时代的来到，智能手机、上网本、无线路由器等无线接入设备，开始成为黑客攻击的全新目标。现在网络中已经出现大量无线破解的技术，轻则可以让攻击者免费的蹭网，重则可以通过ARP攻击植入木马窃取信息。除此以外，利用手机短信或者移动飞信，进行诈骗的事件也会越来越多。 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