

2010预测：Windows7暴露缺陷让病毒悄悄上身Microsoft认证  
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\\_ti2020/644/2021\\_2022\\_2010\\_E9\\_A2\\_84\\_E6\\_B5\\_8B\\_c100\\_644379.htm](https://www.100test.com/kao_ti2020/644/2021_2022_2010_E9_A2_84_E6_B5_8B_c100_644379.htm) 1月14日消息，2010开年喜气人人爱，但是网络病毒也如影随形来报到，网络安全业者预测，病毒乱真的面貌百变，将渗透进生活中的大小事，变得成为让你误认为很熟悉的事物，最后就是要骗到你说出个资，而智能型手机、Windows 7、网络搜寻引擎和网络广告都难逃黑客的利用成为媒介，无法幸免于难。Websense安全实验室11日公布2010年八大网安威胁预警，首席技术总监Dan Hubbard说，网络威胁的成长及发展和使用者的网络行为息息相关，甚至相互滋长，如近几年Web 2.0的兴起聚焦众人的目光、吸引群众聚集，威胁也会并存于Web 2.0的环境，另外，多元整合的操作系统和平台，也变相成为被黑客利用的媒介。这八大威胁首恶是，随Web 2.0而衍生的攻击将更趋成熟而普及，Websense指出，社交型网站和搜寻引擎如Google和Topsy.com等，将聚集大量病毒和垃圾讯息，2009年就已有此态势出现，2010年将会继续呈倍数衍生。黑客在去年利用在社交网站中彼此互信度高的社群网友作为攻击媒介或发送垃圾讯息，类似的手法2010年将被继续使用。其次，2010年会出现尸病毒横行且相互抢占地盘、火药味浓厚的情形，Websense安全实验室预测，今年的尸病毒将更具强大攻击性，且不同群体将相互竞争、攻城略地，抢先霸占尚未被感染的计算机或网络，使用者必须提高警觉。而诈骗集团一再得手的假亲友装熟技俩也在网络大行其道，假借熟识者的伪Email因攻击成功率高，再度成为黑客使用媒介首选。

Websense预测，在2010年，利用Email、以假乱真的攻击手法将更趋成熟，除了既有的威胁需注意，更要留意黑客可能会藉由邮件中隐藏的恶意程序窃取重要数据。 Websense并警告，Windows 7中的User Access Control警示弹跳窗口是Vista版本原本内建用以阻挡恶意攻击的工具，但由于它的过度敏感和窗口跳出次数过于频繁，例如只是改变IP地址或重新设定时区，都会跳出警示窗口，让使用者不堪其扰，最后索性关闭该功能，而导致失去其原存在目的，进而使计算机系统暴露于遭受恶意程序侵袭的潜在风险之中。 Windows 7操作系统也尝试调整该功能，提供四种安全层级设定，以便利使用者，然而，却已无法改变其操作系统暴露在潜在威胁中的事实。另外，智能型手机也会是黑客发动攻击的新媒介，专家说，智能型手机在2010年的普及率会继续增高，相对的，风险也将逐渐浮现，由于目前针对智能型手机的资安解决方案，普遍尚未发展健全，因此，在手机里关于个人或企业的资料将面临极大风险；而习惯用手机处理金融交易的使用者，更要加倍留意黑客窃取重要数据。 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](http://www.100test.com)