 现如今，说到互联网肯定是无人不知，无人不晓。但是，对于互联网黑暗的一面，大家又了解多少呢？我这里说互联网的黑暗并不是指其本身的不洁净，而是在这样一个大的平台上，引来了一群好事之者，例如，黑客、网络诈骗者和网络盗窃者，他们也就是互联网黑暗一面的肇事者，他们时时刻刻变着法子攻击您的电脑和盗取您的个人隐私，给您的网络生活带来种种的不便。 所以，我不得不无休止地为电脑操作系统打补丁，以及通过更新好的反病毒软件和反间谍软件扫描器定期对电脑进行扫描。而就在我写这篇文章时，我的电脑还遭到了特洛伊木马病毒(Trojan.Winloginhook.Delf.A)的攻击，由于该病毒只是在近段时间才开始传播，所以我的反病毒软件并不能及时地捕捉它。我们暂且不管该病毒是不是先前某特洛伊木马病毒的最新变种，或是一种完全新型的攻击病毒。但我们有一点要肯定的是，不管我们的安全防范意识怎么加强，病毒攻击的脚步并不会却止。 那我们是不是就只能等待病毒的降临，或是默认病毒攻击这一事实呢？尽管对于病毒的攻击，我们并不能做到百分之百的防范，但我们能把这种风险降低到最低点。而要做到这一点，我们首先要做的就是为电脑做好防御工作，这样我们就能了解到有那些病毒在入侵电脑。为了能够让大家对目前的网络安全有深入的了解，我整理了一张您必须知道的十大严重网络安全问题清单。如果您想进一步保护您的系统安全，您还必须知道如何为您的电脑系统打补丁，

或是定期更新您的反间谍软件工具。另外，我还为大家提供了一些解决方案和防范措施，以帮助大家避免这些新威胁。如果您的电脑受到这些病毒的入侵，这些解决方案能够帮助您在最大程度消除这些危害。 僵尸电脑大军兵临城下 危害度: 高 可能性: 高 目标: Windows用户 僵尸电脑是指接入互联网的计算机被病毒或蠕虫感染后，受控于黑客，可以随时按照黑客的指令展开DoS攻击，或者发送垃圾邮件、实施网络钓鱼，而真正的用户却毫不知情，就仿佛僵尸一般。僵尸电脑可以被利用来散发垃圾邮件、盗取信息、行业间谍，以及DOS攻击或威胁。但现在，病毒创建者的意图发生了改变，他们不再以散发垃圾邮件，或是盗取信息为最终目的。据最新调查表明，这些僵尸电脑通过攻击您的电脑，然后再向您出售一些简单的工具，并以此为赢利目标。 而据我们所知，很多僵尸电脑都是在“ 放牧人 ”(操控僵尸电脑的人，称为放牧人)的受控下出售软件工具包。而这些工具包的出售价格从20美元到3000美元不等。为了让这样工具包能够吸引购买者的注意力，“ 放牧人 ”把它们伪装成功能完整的软件产品，其实这些工具中包括很多的恶意代码，一旦用户运行这些软件，恶意代码就会通过键盘侧录植入到电脑中。“ 其实，这些软件工具包有很多种50种，60种，甚至上百种不同的工具包。 ”Sunbelt软件公司的研究调查组副总裁Eric Sites表示。Sunbelt是一家制造反间谍软件程序的公司。 聪明的网络控制 目前，这种情况变的更加糟糕，当黑客创建了一种新的僵尸病毒时，然后就把它植入到无防备的电脑上。一旦这种病毒植入到电脑中，这些非法的黑客就能够使用诡异的指挥控制工具，轻而易举就能控制您的电脑。 100Test 下载频道开通