黑客入侵无线网络常用手段

现在无线宽频上网越来越流行，但许多无线网络并没有采取安全防护措施，不但易遭黑客入侵，而且事后追查凶手都很困难。

专家提醒，黑客入侵无线网络通常采用以下四种手段:

方法一:现成的开放网络

过程:黑客扫瞄所有开放型无线存取点(Access Point)，其中，部分网络的确是专供大众使用，但多数则是因为使用者没有做好设定。

企图:免费上网、透过你的网络攻击第三方、探索其它人的网络。

方法二:侦测入侵无线存取设备

过程:黑客先在某一企图网络或公共地点设置一个伪装的无线存取设备，好让受害者误以为该处有无线网络可使用。若黑客的伪装设备讯号强过真正无线存取设备的讯号，受害者计算机便会选择讯号较强的伪装设备连上网络。此时，黑客便可等着收取受害者键入的密码，或将病毒码输入受害者计算机中。

企图:不肖侦测入侵、盗取密码或身份，取得网络权限。

方法三:WEP 加密攻击

过程:黑客侦测 WEP 安全协议漏洞，破解无线存取设备与客户之间的通讯。若黑客只是采监视方式的被动式攻击，可能得花上好几天的时间才能破解，但有些主动式的攻击手法只需数小时便可破解。

企图:非法侦测入侵、盗取密码或身份，取得网络权限。

方法四:偷天换日攻击

过程:跟第二种方式类似，黑客架设一个伪装的无线存取设备，以及与企图网络相同的及虚拟私人网络(VPN)服务器(如 SSH)。若受害者要连接服务器时，冒牌服务器会送出响应讯息，使得受害者连上冒牌的服务器。

企图:非法侦测入侵、盗取密码或身份，取得网络权限。