Source: *Lianhe Zaobao,* p8
Date: 22 June 2017

调查：含恶意软件

盗版软件网站都不安全

国大受微软公司委任展开的调查发现，提供盗版软件下载服务的网站或链接，全都有各种网络安全威胁。此外，近四分之一附在盗版软件中的恶意软件会自动解除电脑的防毒设置，使电脑更易遭入侵。

苏德铭　报道
tohtm@sph.com.sg

新加坡国立大学展开的一项调查结果发现，所有供下载盗版软件的网站都有网络安全威胁，包括以不同方式诱导用户让恶意软件入侵电脑系统，让黑客有机会盗取资料或控制受害者的电脑发动其他网络攻击。

国大受微软（Microsoft）公司委任展开上述调查，负责调查的国大工程学院电机与电脑工程系副教授比拉伯（Biplab Sikdar）昨天在微软举办的一场网络安全分享会上报告了调查结果。

比拉伯透露，调查团队约四个月内上网下载了203个盗版软件，发现他们使用的下载网站或链接全数都有各种网络安全威胁。

有些网站会标示可疑广告或“点击下载”的链接，但其实是下载恶意软件（malware）的陷阱，有的恶意软件则直接附在盗版软件中，当下载完毕或安装时便入侵电脑系统。

调查发现，近四分之一附在盗版软件中的恶意软件会自动解除电脑的防毒设置，使电脑更易遭入侵。

比拉伯说：“若用户下载或使用的是盗版防毒软件（anti-virus software），电脑不但可能被附在盗版软件上的恶意软件侵袭，用户还会有‘电脑已受保护’的错觉，但事实正好相反。”

他指出，附在盗版软件上约一半属“木马程序”（Trojan）恶意软件，侵入电脑后会在系统内安装“后门”（backdoor），让黑客控制电脑盗取资料或进行其他攻击。

他也举例说，一类名为“ChePro”的木马程序会潜伏在电脑中，只要用户上银行网站或进行网上付款交易，程序会自动启动进行屏幕截图（screenshot）或记录键盘上的活动，盗取信用卡密码等资料。

另外，调查团队也从印度尼西亚、韩国和泰国等八个亚洲国家向不法商家引进90台已安装盗版软件的新电脑，以及165片盗版软件的安装光碟进行测试。由于本地较少有在售卖新电脑时安装盗版软件的不法行为，因此新加坡没被纳入这方面的调查范围。

不要贪小便宜

测试显示，约九成安装在新电脑的盗版软件附有恶意软件，而约六成的盗版安装光碟有同样情况。

比拉伯提醒用户和企业要特别当心，勿因贪小便宜使用盗版软件。“本次调查证实盗版软件已成为传播恶意软件的有效手段，尤其是网上下载的盗版软件。希望这项调查能让人们意识到，使用盗版软件所省下的金钱，远远不及个人或商业上将面对的风险与损失。”

他也指出，就算能避开恶意软件成功下载与安装盗版软件，但由于官方的软件“补丁”（patch）不适用于盗版软件，因此电脑系统的病毒防御能力久而久之会降低，用户便会面对较高的网络安全威胁。

个人用户和小型企业能如何“防毒”？

- 向信誉良好的商家购买电脑，并坚持要正版软件。
- 购买电脑时，确保发票上清楚标出电脑安装的软件名称及版本。
- 确保不时更新最新的软件及安全补丁（patch），并使用可靠的防毒软件，以加强电脑系统的病毒防御能力。
- 避免使用如Windows XP般较旧款的电脑操作系统（operating system）。