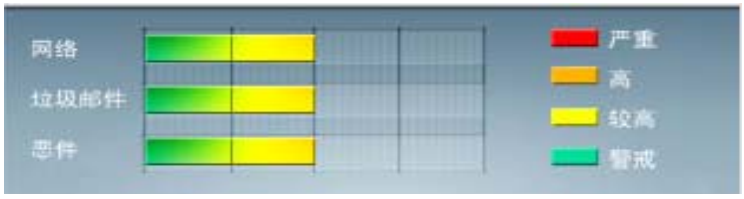
安全威胁每周警讯

2011/05/01～2011/05/07

本周威胁指数



TrendMicro 中国区网络安全监控中心

前十大病毒警讯

排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	WORM_DOWNAD.AD	蠕虫	★★★★	↑	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
2	TROJ_DOWNAD.INF	木马	★★★	↓	DOWNAD 蠕虫关联木马
3	WORM_DOWNAD	蠕虫	★★★★	→	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
4	TROJ_IFRAME.CP	木马	★★★	→	GIF、jpg 和 SWF 文件中被插入一个恶意的 iframe 标记时，趋势科技会将其判断为 TROJ_IFRAME.CP 病毒。当这些文件被执行时，会重定向到这些 URL，并下载恶意程序
5	Cryp_Xed-12	木马	★★★	↑	经过加壳处理的可疑文件
6	TROJ_DLOADER.UVD	木马	★★★	↑	该木马程序是一个恶意软件，但危险低，不具备自动传播到其他系统的能力。它通常是从网上下载，并在用户不知情的情况下自动安装。 通常携带有效载荷木马或其他恶意行为，可从轻度恼人的范围到无可挽回的破坏。他们也可以修改系统设置为自动启动。
7	CRCK_KEYGEN	破解程序	★★	↑	用于破解正版软件的程序,可能夹带恶意软件
8	PAK_Generic.001	加壳程序	★★	↑	对加壳文件的通用检测。病毒通常会使用加壳手法来达到不被杀毒软件检测的目的
9	WORM_ECODE.E-CN	蠕虫	★★★★	↓	E 语言病毒,产生与当前文件夹同名 exe 文件
10	TROJ_SPNR.03CG11	木马	★★	↓	该木马程序是一个恶意软件，但危险低，不具备自动传播到其他系统的能力。它通常是从网上下载，并在用户不知情的情况下自动安装。 通常携带有效载荷木马或其他恶意行为，可从轻度恼人的范围到无可挽回的破坏。他们也可以修改系统设置为自动启动。

系统漏洞信息

MS11-034: Windows 内核模式驱动程序中的漏洞可能允许特权提升 (2506223)

受影响的软件:

Windows xp

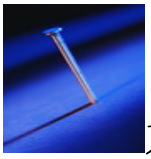
Windows Server 2003

Windows Vista

Windows Server 2008

Windows 7

描述: 请见http://www.microsoft.com/china/technet/security/bulletin/MS11-034.mspx



系统安全技巧

摘要: 随着与网上银行有关的经济案件频频发生，作为使用者的您，肯定会心存疑虑: 网上银行到底安不安全? 怎样才能预防这方面的风险呢? 希望本文对大家安全使用网银有所帮助。

随着与网上银行有关的经济案件频频发生，作为使用者的您，肯定会心存疑虑: 网上银行到底安不安全?怎样才能预防这方面的风险呢?

大体而言，您可以从使用者、电脑、互联网和网上银行四个角度来关注网上银行的使用要点:

从使用者的角度出发，您应该养成良好的使用习惯，不要随便开启来历不明并载有附件的电子邮件，切勿按动可疑邮件内的超级链接。 也不要进入可疑网站，只从可靠的来源下载软件。不要在网上随便透露个人资料(如身份证号码、地址、银行账号、信用卡号码、用户名称及密码)，除非确认您使用的是可靠及信誉良好的网站。在提供个人资料给网站前，先查阅网站的保密条款及安全防护措施声明。定期更改上网密码，并查看您的交易，核对银行对账单。

从使用电脑的角度出发，应该避免让太多人使用您的个人电脑，并应设定使用电脑的个人密码。在电脑上安装个人防火墙软件及防电脑病毒软件，并定期为您的防毒软件、操作系统及互联网浏览器下载更新文档。此外，使用网上银行的电脑不要作为资料、文件共享等类型的服务器。文件型数字证书不要备份在电脑硬盘或邮箱中。您如果使用 Windows XP，请打开 Windows XP 自带的防火墙，还需要关闭远程功能。

另外，从互联网的角度来看，您在每次使用网银后，应中断与互联网的连接，并只在可靠及信誉良好的网站进行网上交易。

而从网上银行的角度而言，还有许多方面值得您注意：比如网上银行用户名和密码必须易记但难被猜中，切勿使用简单数字排列(如 888888、123456)、出生日期、电话号码、家人的名字或常用的名字(例如常用的人名及卡通人物名字)。为您的网上银行设置专门的密码，区别于其他用户名和密码，避免因某项密码的丢失而造成其他密码的泄漏。将网上银行登录密码和用以对外转账的支付密码设置为不同的密码，多重验证以保证您的资金安全。不要向任何人(包括银行职员及警方)透露密码，或把密码记录下来。不要将登录网上银行的用户号和密码，用作使用电子邮箱或登录其他网站的密码。切勿经电子邮件内的链接或网上搜索引擎登录网上银行。每次应在浏览器上输入网址或将真正的网站记录在电脑的收藏夹内，由此进入您的银行账户。登入网上银行前，应先关闭所有浏览器窗口，以免其他网站非法取得你的个人资料。取消浏览器提供的“自动记忆”功能，坚持每次重新输入用户名和密码。每次使用网上银行后，请您切记“登出”或“退出”账户，不要简单的关闭窗口。不要使用公用电脑(如网吧、图书馆提供的电脑等)登录网上银行。随时查阅银行账户余额及交易记录，如发现任何错漏或未经授权的交易，请立即通知您的银行。定期留意银行提供的安全提示。

来源：上海证券网
