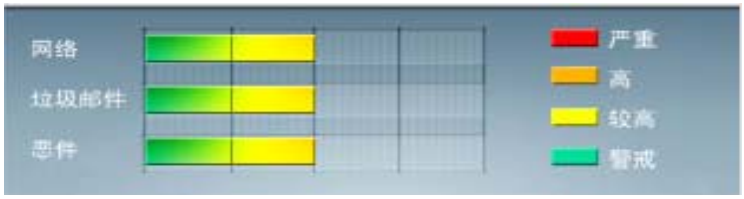
安全威胁每周警讯

2010/11/07～2010/11/13

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	TROJ_DOWNAD.INF	木马	★★★	→	DOWNAD 蠕虫关联木马
2	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
3	TROJ_IFRAME.CP	木马病毒	★★★	→	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
4	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
5	Cryp_Xed-12	木马	★★★	→	疑似病毒
6	JS_EXPLOIT.SMD	网页病毒	★★★	↑	该 JavaScript（JS）的恶意软件可能被托管在一个网站，当用户访问网站时运行并感染。同时，它可能是其他恶意软件的组成部分。通常它检查的 Adobe Flash Player 的系统中安装的版本。然后，它尝试下载一个 SWF 文件根据的 Flash Player 的版本安装。
7	WORM_ECODE.E-CN	蠕虫	★★★★	→	E 语言病毒,产生与当前文件夹同名 exe 文件
8	CRCK_KEYGEN	破解程序	★★	→	非法破解程序
9	HTML_IFRAME.AZ	网页病毒	★★	↑	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
10	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

系统漏洞信息

MS10-085:SChannel 中的漏洞可能允许拒绝服务 (2207566)

受影响的软件：

Windows Vista

Windows Server 2008

Windows 7

描述：请见 http://www.microsoft.com/china/technet/security/bulletin/MS10-085.mspx

系统安全技巧

摘要：保护网银安全我们需要做什么？作为网银用户，网银的安全性不仅仅是银行的责任，作为使用者的我们，身上也担负着保卫网银的责任。让我们从自己做起，保护网银安全。

Active X 安全控件

中国工商银行的网银安全曾经因为“使用工行网银系统资金被盗”一事倍受网友质疑，不过当时银行在解决问题时曾经提到过：“财产被盗的用户大多都是大众版用户。”而很不幸，大众版又多采用的就是 Active X 安全控件。除工行外，招商银行、中国农业银行、交通银行的个人版登陆同样采取的是 Active X 安全控件，也就是说，大部分的银行向非证书认证用户提供的安全手段都是安装安全控件，而不同之处只是安装的方式各有特色。

这种安全技术防止了键盘/消息钩子，而且使通过 IE 的 COM 接口获取密码的方法也无能为力，当控件安装完成后用户才能见到网上银行的登陆界面。不过这被公认为最不安全的一种登陆方式，而且由于一些银行将安全技术通过 Active X 捆绑在了 IE 上，这给其它操作系统和非 IE 用户带来了一些不便。

数字证书和 USB key

较 Active X 安全控件而言，相对安全的就是采用数字证书和 USB key 认证的登陆方式。银行依用户的有效证件，如银行卡号、身份证号码等为依据，生成一个数字证书文件，配合用户自定义的用户名和密码使用以提高安全性。因其成本低，使用方便，因此被众多银行所使用。

USB Key 证书就是一种 USB 接口形式的硬件设备，内置微型智能卡处理器，采用 1024 位非对称密钥算法对网上数据进行加密、解密和数字签名，确保网上交易的保密性、真实性、完整性和不可否认性。因成本问题和设置上的原因被个别银行采用，并且与数字证书共存仅作为可选项。不过交通银行一样不支持单独的数字证书安全方式，他们提供的是数字证书与 USB key 共同发挥作用的一种安全认证。

动态软键盘

采用动态软键盘技术初看确实能使攻击者无法截获密码，但是截取密码不仅仅只有接截获键盘记录一种方法，黑客们还可以通过 IE 的 COM 获取密码。对于中国建设银行和中国银行，通过 IE 的 COM 接口获取的密码框里的内容就是密码，其他大部分采用软键盘技术的网站大都也是这样。中国农业银行曾经也使用过这种安全方式，不过现在已经升级为 Active X 安全控件。

虽然银行为了保护网银绞尽脑汁，但是仍有财产被盗事件出现，也许，作为用户的我们也应该从自身检讨起?

保护网银安全我们需要做什么?

作为网银用户，网银的安全性不仅仅是银行的责任，作为使用者的我们，身上也担负着保卫网银的责任。让我们从自己做起，保护网银安全。

1、谨防钓鱼网站

其实真正由于银行安全漏洞钱财失窃的事情是少数，更多的人是因为上了钓鱼网站的当才不幸中招。当我们打开银行首页时，可以将正确的网址收藏起来，尽量避免在通过“超链接”进入的银行系统上进行操作。

2、保护好帐号密码

银行卡的帐号和密码是绝对私人所有，不要轻易告诉别人。还有，银行不会通过第三方来转告用户一些事情，当接到陌生的电话或者短信、邮件的时候还需要小心核对。

3、定期查询详细交易

做好自己的交易日志，保证对自己的每一项有记录的交易印象深刻。

4、对杀毒软件的使用（瑞星杀毒软件 2011 版 半年免费）

将电脑的防火墙设置最高安全级别，及时升级杀毒软件，避免“网银大盗”的侵入。

5、利用银行提供的各种增值服务

现在很多银行都提供了交易的短信、邮件提醒，用户可以充分利用银行的贴心服务，掌握自己的财务消费状态，反正是免费。

是系统就一定有漏洞，对于银行系统来说也是如此。所以我们也不要埋怨银行的安全系统做的多么不好，只要我们先从自身做起，再加上银行不断升级的安全服务，相信总会有一天“魔高一尺，道高一丈”，毕竟银行背后有千千万万的支持者。

来源： ZDnet