安全威胁每周警讯

2011/12/18～2011/12/24

本周威胁指数

***TrendMicro* 中国区网络安全监控中心**

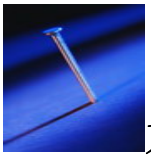
前十大病毒警讯

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	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	★★★★	→	木马病毒，通过访问恶意站点下载感染或由其他恶意程序下载感染
6	WORM_ECODE.E-CN	蠕虫	★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
7	TROJ_SPNR.08JR11	木马	★★★	↓	木马病毒，由趋势科技主动式云端拦截技术检测，这类病毒通常是由于用户从恶意的 WEB 页面下载感染
8	Adware_Adplus	灰色软件	★★	↑	广告软件
9	Downloader_Agent	木马	★★★	↑	木马病毒，通过访问恶意站点下载感染或由其他恶意程序下载感染
10	TROJ_SPNR.03CG11	木马	★★★	→	木马病毒，由趋势科技主动式云端拦截技术检测，这类病毒通常是由于用户从恶意的 WEB 页面下载感染

系统漏洞信息

MS11-085：Windows Mail 和 Windows 会议室中的漏洞可能允许远程执行代码 (2620704)
Windows Vista
Windows Server 2008
Windows 7
Windows Server 2008 R2

描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS11-085



系统安全技巧

病毒侵害、数据被盗和系统被破坏，人们通常认为这些 IT 领域的危害只会发生在电脑上，而事实上手机也是病毒和黑客入侵的重点对象。IT 安全专家担心，手机病毒危害可能很快会成为家常便饭的事，尤其是商务手机和联网的掌上电脑。

目前已有超过 162 种手机病毒被发现，其中一种叫“Doomboot.S”的病毒可以使智能手机的运行系统瘫痪；“RedBrowser.A”病毒可以偷发使用户支付价格不菲的手机短信；“Pbstealer.D”病毒可以通过“蓝牙”连接，盗取用户手机中存储的联系人地址、日记内容。还有一种叫“Cardblock.A”的病毒可以盗取手机的开机密码。“Brador.A”的病毒具有后门程序，可以盗取手机用户的内存数据。

据德国 IT 和防病毒专家安德烈亚斯.拉姆介绍，目前主要遭到攻击的是使用“Symbian””运行系统的手机，“Symbian”作为智能手机的主要操作平台，其功能犹如计算机中的微软“视窗”软件。专家称，过去认为手机相对于计算机遭受病毒的危害较小，但现在看来由于手机使用费高，遭受的损失可能更大。例如，黑客仅仅靠发多媒体短信（MMS）就可获利不浅，一条 40 欧分的 MMS，通过病毒群发到 100 个地址，就可获得 40 欧

元。

专家称，大部分的手机用户对手机病毒还知之甚少，甚至无意中在帮助手机病毒的传染。如收到来路不明的短信，要求你将短信分发给亲友和同事，携带病毒的短信就有可能扩散。或称是否接受免费赠送的 100 条短信，或免费安装防毒软件，如果你确认为是，则手机就可能感染上病毒。

智能手机与计算机连接下载数据也容易带入病毒，一种叫“Crossover”的病毒就是专门入侵“视窗”运行系统的智能手机。专家警告说，手机的软件越复杂，越容易受到病毒的侵害，尤其是有“蓝牙”功能的手机，最容易受到黑客的入侵，甚至被远程遥控。

专家对预防手机病毒提出五点建议：

第一，使用密码。手机不用时尽量关机，并习惯使用密码开机，这样一旦手机丢失，私人数据可以得到保护。

第二，隐藏“蓝牙”。许多手机病毒是通过“蓝牙”短程发射的功能，盗取手机数据或将病毒传染给其他手机的，因此，最好在不使用“蓝牙”功能时将其关闭，这样还有利于让电池少耗电。

第三，不予信任。对来路不明的手机短信千万不要打开，即使是同事或亲友发来的推荐下载软件或彩铃等短信，也最好事先打电话询问，确定是否安全。

第四，经常检查。经常检查手机显示屏上的菜单符号，如果突然出现不熟悉的符号，或熟悉的符号消失，表明黑客已经入侵，要及时与手机制造商或电信网络运营商联系处理。

第五，加载保险。如同现在计算机销售时已经普遍加载了防毒软件和防火墙一样，将来手机销售时也会有这些固定配置。目前，个人可以到正规的防毒软件公司付费下载防毒软件。

转自:51CTO

免责声明

该邮件列表仅用于提供信息，此邮件列表内容不负任何担保责任，没有明示或默示的保证，包括但不限于对适销性、特定用途适用性以及不受侵害的暗示保证。用户对此邮件列表的准确性和使用承担全部风险，因依赖该资料所致的任何损失，趋势科技均不负责。