安全威胁每周警讯

2012/08/13～2012/08/18

本周威胁指数

***TrendMicro* 中国区网络安全监控中心**

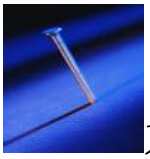
前十大病毒警讯

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	疑似病毒	★★★	→	疑似木马病毒，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	CRCK_KEYGEN	黑客程序	★★	↑	非法破解程序
7	X97M_LAROUX.BK	宏病毒	★★	↑	宏病毒，主要通过用户浏览恶意网站感染，该病毒主要感染 Office Excel 文件，并且会在 Excel 中创建一个名为 StartUp 的宏脚本
8	X97M_LAROUX.CO	宏病毒	★★	↑	宏病毒，主要通过用户浏览恶意网站感染，该病毒主要感染 Office Excel 文件，并且会在 Excel 中创建一个名为 StartUp 的宏脚本
9	PAK_Generic.001	加壳文件	★★	↑	经过加壳技术加密的文件
10	WORM_ECODE.E-CN	蠕虫	★★	↑	它通过将受感染的移动驱动器与系统连接起来而入侵。 它可能是由远程站点的其他恶意软件/灰色软件/间谍软件下载而来。 它可能是用户在访问恶意网站时在无意中下载而来。

系统漏洞信息

MS12-048 ： Windows Shell 中的漏洞可能允许远程执行代码 (2691442)

Windows XP
Windows Vista
Windows 7
Windows Server 2003
Windows Server 2008
描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS12-048



系统安全技巧

短短一个月时间，Android 上的恶意软件数量就已经翻了一倍，从一万变到两万。快速增长的 Android 威胁已经是个值得大家关注的焦点。

官方 Android 软件商店 - Google Play 变成有毒应用程序的温床。假冒的 Skype、Imstagram、愤怒小鸟太空版，以及其他假冒知名应用程序的恶意软件可以向增值服务商发送短信，让用户产生额外费用。用户好奇的天性也被间谍程序（例如 Spy Tool 和 Spy Phone Pro+）用来赚钱。设计复杂的 BotPanda 甚至会隐藏自己的行为，在 Root 过的设备上开启远程访问功能。

本季列出的 Android 设备上的七种恶意软件类型，几乎有一半都是会滥用增值服务的恶意软件，它们会替用户订阅并不需要的服务。广告软件最近也增多了，这类软件会不停地发布伪装成紧急通知的广告，位居第二。数据窃取软件、恶意下载软件、恶意破解软件、点击诈骗软件，以及间谍工具都紧随其后。这些移动软件会带来个人和金融数据被窃的危险。

Android 恶意软件随着 Android 市场占有率的上升而水涨船高。2012 年一季度共出现 5000 个新增的 Android 恶意软件，而到了 2012 年而进度，一个月内就发现了 10000 个新增的恶意软件！

Android 平台检测率前十位的恶意软件家族

1. FAKE 滥用增值服务的软件

2. ADWAIRPUSH 广告软件

3. BOXER 滥用增值服务的软件

4. DROIDKUNGFU 数据窃取、点击诈骗、恶意下载、恶意破解软件

5.PLANKTON 数据窃取软件

6.JIFAKE 滥用增值服务的软件

7.GEINIMI 数据窃取、恶意下载、间谍程序

8.GAPPUSIN 恶意下载、数据窃取、广告软件

9.GINMASTER 恶意破解、恶意下载软件

10.OPFAKE 滥用增值服务的软件

常见攻击手法

1.滥用知名移动软件品牌：假借知名手机软件，利用这些软件的知名度诱骗用户下载。

2.Google Play 成为恶意软件来源：虽然 Google 也在努力进行过滤和扫描，但还是有恶意软件出现在 Google Play 供人下载。迷思：“Google 会检查所有上架的手机应用程式，因此我应该很安全才对。”

3.利用窃听软件来赚钱：间谍移动软件 Spy Tool 和 Spy Phone PRO+宣称自己是合法的监控软件，已经出现在 Google Play 上。

来源：51CTO