安全威胁每周警讯

2012/03/11～2012/03/17

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	疑似病毒	★★★★	→	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	JS_OBFUSCATED.FI	脚本病毒	★★★	↑	当用户访问包含此脚本的网站时，会自动运行此此脚本，并被重定向到其他包含恶意代码的站点。
8	PAK_Generic.001	加壳文件	★★	↑	经过加壳技术加密的文件
9	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
10	Downloader_Agent	灰色软件	★★	↑	这灰色软件下载器会自动下载并安装额外的其他的灰色软件，如广告软件和间谍软件。

系统漏洞信息

MS12-009 ：辅助功能驱动程序中的漏洞可能允许特权提升 (2645640)

Windows XP

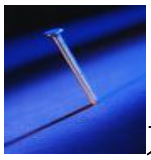
Windows Vista

Windows 7

Windows Server 2003

Windows Server 2008

描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS12-009



系统安全技巧

网络安全是一个永无止境的任务，它需要持续的警惕。保护您的无线网络是件特别棘手的任务，因为未经授权的用户可以看不见，不被发现的悄悄潜入到您的网络里。为了使您的无线局域网更安全，重要的是发现和修复新的无线漏洞。通过定期进行无线网络安全性能评估，可以识别并修复新的安全漏洞。在此之前，黑客可以通过这些安全漏洞渗透进入你的网络里。

进行 WLAN 的脆弱性评估，要搞清楚是什么让你的无线网络联向外界。连到您的网络是否有一个简单的方法？未经授权的设备可以将自己简单的增加到您的网络来？无线安全漏洞评估可以回答这些问题。

1、发现网络上的无线设备。你需要知道有哪些无线设备访问了您的网络，包括无线路由器和无线接入点(AP)以及笔记本电脑和其他一切移动设备。扫描设备将在 2.4GHz 和 5GHz 频段的 802.11a/b/g/n 无线网络中设备。并记录你的网络上的无线设备，包括每个设备的位置和相关的设备信息。

2、追捕流氓设备。比如非法安装的无线接入点 AP，这不应该安装在您的网络上。非法接入点 AP 并不存在于您的网络设备清单上，但它导致内部网络被非法无线转播出去。考虑这会导致您的网络信息外泄，需要马上处理并立即阻止它的网络访问功能。漏洞扫描也要扫瞄办公区域里的任何无线频段，包括你不经常使用的无线信道，这样可以发现新的非法无线接入点。

3、测试授权的接入点。确保网络上的无线接入点是你的设备，可以安全访问。因为任何人都可以通过 AP 无线访问您的网络，所以它必须有最新的安全补丁和固件升级。确保你已经修改了默认的密码，有一个强大的，难以破解的“管理员”密码。此外，检查 WAP 配置为最安全的选项，如最强的身份验证设置和信号加密管理，使用过滤器来阻止未经授权的协议，并发出安全警报。

4、定期更新您的网络设备清单。第一时间找出网络里的新的设备。例如用户从家里带来的任何新的支持无线功能的设备，它们正在访问你的无线局域网。更新您的设备清单库，要保证每一个新智能手机，平板电脑，笔记本电脑，台式机，通过 IP 语音(VoIP)电话，和任何其他无线设备，它们需要被批准才能访问您

的网络。

5、采取行动，消除安全漏洞。最后一步是要堵塞漏洞扫描发现的漏洞。例如，安装到你的网络里的新无线接入点，用户设备新的安全补丁，定制更改网络密码，升级系统补丁，可以让他们更安全。

当然，完成这五个步骤，并不意味着你的安全检查工作已经完成。您应该测试修复工作是否正确完成，确保确实关闭了安全漏洞。并定制下一个 WLAN 安全漏洞评估计划，经常检查您的无线网络新的安全漏洞。执行这五个步骤，将有助于确保您的无线网络安全。

来源：比特网