互联网疫情通报

– 大中华地区

2011/08/01-2011/08/14

赛门铁克安全响应中心

内容

热门病毒排行榜

排名	走势	病毒名	病毒类型	风险级别	表现/描述
1	→	W32.Downadup.B	蠕虫	低	W32.Downadup.B 通过微软 Windows Server Service RPC 的远程代码执行漏洞 (BID 31874) 进行传播。使用弱密码保护的网络共享容易感染此蠕虫，此外，它还会阻止对安全相关网站的访问。
2	→	Trojan Horse	木马	非常低	Trojan Horse 表明检测到各种木马程序。
3	→	Trojan.Gen	木马	非常低	Trojan.Gen 表明检测到多种木马程序。
4	→	W32.Almanahe.B!inf	病毒	非常低	W32.Almanahe.B!inf 表明检测到感染了 W32.Almanahe 蠕虫的文件。
5	↑	Trojan.Gen.2	木马	非常低	Trojan.Gen.2 表明检测到多个木马程序。
6	↑	Trojan.ADH	木马	非常低	Trojan.ADH 表明检测到不具备传统特征的全新恶意软件威胁。
7	↑	W32.SillyFDC.BDP!lnk	病毒	非常低	W32.SillyFDC.BDP!lnk 表明检测到 W32.SillyFDC.BDP 蠕虫所创建的 .lnk 文件。
8	↑	ALS.Bursted.B	病毒	非常低	ALS.Bursted.B 是一种病毒，它是用 AutoCAD 采用的 AutoLisp 脚本语言编写的。
9	↑	W32.Downadup!autorun	蠕虫	非常低	W32.Downadup!autorun 表明检测到 W32.Downadup 变体所置入的 autorun.inf 文件。
10	→	Downloader	木马	非常低	Downloader 会连接到 Internet 并下载其他木马或组件。

疫情趋势

微软新近发布了 2011 年 8 月的安全公告。本月公告数量呈现持平状态 — 该公司发布公告 13 则，总共修复漏洞 22 个。

其中三个漏洞的风险等级为“严重”，所影响对象为 Internet Explorer 和 Windows DNS。DNS 漏洞可能会导致攻击者完全掌控受感染的电脑。其他漏洞的风险等级从“重要”到“中度”不等，所影响对象包括 Internet Explorer、Windows、Windows DNS、Visio、Visual Studio 和 Windows 内核。

与往常一样，建议客户在第一时间安装微软提供的补丁；在保证正常功能的前提下以所需最低权限运行所有软件；在网络外围阻止对所有关键系统的外部访问，仅在必要的情况下才允许特定访问。

热点病毒

病毒名	Trojan.Badfaker
病毒类型	木马
受感染系统	Windows 95/98/Me/NT/2000/ XP/Vista, Windows Server 2003

运行后，Trojan.Badfaker 会修改注册表，以实现以下功能：1）绕过 Windows 系统防火墙；2）当操作系统进入安全模式时，木马自身也会随系统自启动；3）降低系统的安全设置。

Trojan.Badfaker 还会关闭系统的安全软件并删除相应的安全软件注册表信息，并且提示虚假的安全警告。同时，Trojan.Badfaker 会从指定的网站（如 http://fre[removed]ac.net/distrib_serv/ip_list.php）下载更多恶意程序至受感染电脑中运行。

Trojan.Badfaker 主要通过互联网下载进行传播。

垃圾邮件趋势

垃圾邮件传播者从未放弃寻找绕开邮件过滤程序的新方法，毕竟，这是他们成功入侵的关键。近来，我们发现了一类虽然不多但数量稳定的垃圾邮件，其中 URL（指向垃圾网站）的特定字符被替换成了看似相近或相同的 Unicode 字符。这是另外一种 URL 混淆方法，其目的在于加大 URL 的分析难度。

当网页浏览器或电子邮件客户端的 HTML 转译引擎处理此类 URL 时，通常会对其进行 Unicode 标准化处理，即使用标准字符替换 Unicode 字符。这些经过处理后的 URL 就会将用户定向至垃圾邮件站点。

Symantec.cloud 和 Symantec Brightmail 的 URL 过滤技术具有处理这类字符的固有功能，可保护客户免遭此类攻击。

热门钓鱼网站

目标域	URL	解析后的 IP
taobao.com	http://item.taobao.com.cxes.cu.cc/view_shop.asp	112.121.187.5
	http://iten.taobao-com-dfed.gv.vg/item.htm.asp	113.10.148.124
	http://item.taobao-com-ikc.cu.cc/item.htm.asp	113.10.148.53
runescape.com	http://secure.runescape.com.kalogin.com/m=weblogin/pass.htm	118.140.16.241
	http://secure.runescgpe.com/m-weblogin/loginform/ws	175.41.20.34
yahoo.com	http://gear2010.gicp.net/NewTest/yahoo_hk/newurl.asp	59.172.208.123