安全威胁每周警讯

2011/05/14～2011/05/21

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	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
6	TROJ_SPNR.03CG11	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
7	TROJ_DLOADER.UVD	木马	★★★	↓	该木马程序是一个恶意软件，但危险低，不具备自动传播到其他系统的能力。它通常是从网上下载，并在用户不知情的情况下自动安装。 通常携带有效载荷木马或其他恶意行为，可从轻度恼人的范围到无可挽回的破坏。他们也可以修改系统设置为自动启动。
8	HTML_IFRAME.AZ	网页病毒	★★	→	网页病毒,通常在网页在插入一个恶意 iframe,用户在访问该网页时会下载恶意文件或重定向到恶意网站
9	TROJ_SPNR.03CL11	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	ACM_AGENT.AVGL	脚本病毒	★★	↑	AutoCad 脚本病毒

系统漏洞信息

MS11-035: WINS 中的漏洞可能允许远程执行代码 (2524426)

受影响的软件:

Windows XP

Windows Vista

Windows 7

Windows Server 2008

描述: 请见http://www.microsoft.com/china/technet/security/bulletin/MS11-035.mspx

系统安全技巧

2010 年 9 月，微软委托了一项研究，试图发现 Web 浏览器能如何有效地保护其用户免受社会工程恶意软件和恶意网站。这些网站看起来无害，但会诱骗用户下载并执行恶意软件。 NSS 实验室使用真实出现过的威胁对六个浏览器进行了测试，得出的结果表明微软 Internet Explorer 9(IE 9)的测试版在防护真实的恶意软件上比其他浏览器做得更好。

事实上，在发现潜在危险后警告用户这一项上，IE 9 的得分比其最接近的对手，Mozilla 的 Firefox 浏览器高 5 倍。根据 NSS 实验室对 636 个网站的测试数据,IE 9 能够屏蔽 99%的恶意软件分派网站,而 IE 8 的这一数据为 90%，其他浏览器如 Firefox 3.6 版本仅为 19%，Safari 5、Chrome 6 和 Opera 10 分别为 11%、3%和 0%。

那么，为什么 Internet Explorer 9 的表现会如此好呢?仅仅是因为这项测试是专门为 IE 9 和微软设定的，或者这些结果是真实的吗?现在，IE 9 已于 3 月 14 日正式发布，是不是每个人都应该转向 IE 9?这些都是本文将要讨论的问题。

NSS 实验室把 IE 9 取得的高分数归功于一个叫做 SmartScreen 应用程序信誉度(SmartScreen application reputation)的新功能。在某个可疑应用程序准备要下载危险内容时，该功能就会对用户发出警告。它会检查该文件的哈希值(hash)和数字证书(如果存在的话)，从而确定该文件是否为一个已知的有信誉的文件。如果该算法按照下载流量、下载历史、过去的防病毒结果以及 URL 信誉这些标准将该文件被评级为未知的，那么它会对用户运行或者保存该软件的行为发出警告。这种评级方法背后的思想是，当一个程序被认为是高风险的时候，尽量减少用户看到的普通警告的数目，并提供相关度更高的警告。

IE 9 的这个功能严格来讲不是应用程序白名单，因此用户仍然可以忽略警告，但是如果加入一个禁止忽略警告的安全策略，则可以大大减少恶意下载所带来的感染程度。该功能还提供了对新出现的恶意软件变种的防护，而不是在它们被发现并被添加到反病毒更新库后才采取行动。

不幸的是，SmartScreen 应用程序信誉度还存在一些不足。例如，有大量完全合规的应用软件没有数字证书，就会在这个评级标准中取得很低的分数。此外，该功能只对应用程序进行检查，并不包括被篡改过的、包含攻击代

码的 PDF 文件和图片，因为这种情况实在是太多了。最后，它能否发挥作用取决于用户选择听从其发出的警告还是忽略。

IE 9 其他一些主要的保护技术还有 SmartScreen URL 过滤，这在 IE 8 就引入了，而 FireFox、Safari 和 Chrome 使用谷歌提供的类似的 SafeBrowsing 来替代。这些基于信誉的系统会在互联网上搜索恶意网站，并对其内容进行标注。IE 浏览器会对用户请求的每一个网站提出检查其信誉的请求，一旦发现其内容被标注为潜在危险时就会发出警告。

NSS 的研究结果对微软和 IE 浏览器的用户而言是个好消息，但它并没有评估浏览器插件的漏洞或者浏览器本身的安全。

Secunia 的安全情况报道是评估一个浏览器容易受到攻击程序的优质信息资源。回顾 2010 年第四季度安全情况报道中的 Firefox 3.6(.PDF)和 IE 8(.PDF)部分(没有 IE 9 的说明书，因为当时它还只是测试版)，你会看到 IE 8 存在 51 个漏洞，而 Firefox 存在 88 个。该文中还提供了 11 条建议，这一数目约等同于已发生安全事件数或管理操作所需操作数的总和。IE 8 有 8 个标记为“高”或者“极高”的漏洞，而 Firefox 有 10 个。这两家公司都拥有在漏洞被公布的 30 天内提供补丁的良好记录。

当然，这些统计资料显示微软已经在浏览器安全问题上和 Firefox 缩小了差距，这对一直为谁是最安全的浏览器争论不休的人来说是个好消息。所有的浏览器都有漏洞，因此问题集中于选择一个能够在提供补丁的问题上不断给用户以信心的厂商。正如你从事实和数字看到那样，微软不仅在提高浏览器整体安全和维护上做出了很大改进，同时还强化了在上网冲浪时能对用户提供的保护。

随着针对用户的攻击越来越复杂化，由浏览器提供的保护层正在成为一个越来越重要的功能，目前看来微软似乎已经在这方面取得了领先。对于没有安装 Internet Explorer 的公司而言，投入 IE 9 的怀抱是一件很值得考虑的事情，尤其是现在运行着 Windows 7 的那些公司。这样，意味着公司可以少同一家厂商的补丁以及插件打交道，而且根据现有的情况看，这将提供一个更安全的上网体验。

来源：techtarget
