安全威胁每周警讯

2011/09/11～2011/09/17

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

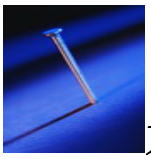
排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	WORM_DOWNAD.AD	蠕虫	★★★★	↑	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
2	TROJ_DOWNAD.INF	木马	★★★	↓	DOWNAD 蠕虫关联木马
3	WORM_DOWNAD	蠕虫	★★★★	→	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
4	TROJ_IFRAME.CP	木马	★★★	→	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	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	CRCK_KEYGEN	木马	★★	→	非法破解程序
7	PAK_Generic.001	木马	★★★	↑	疑似病毒
8	TROJ_SPNR.03CG11	木马	★★★	↑	木马病毒
9	WORM_ECODE.E-CN	蠕虫	★★★★	↓	易语言编写的蠕虫病毒，会在文件夹下生成同名 exe 文件
10	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

系统漏洞信息

MS11-066：Microsoft 图表控件中的漏洞可能导致信息泄露

Windows XP
Windows Server 2003
Windows Server 2008
Windows Vista
Windows 7

描述：http://www.microsoft.com/china/technet/security/bulletin/MS11-066.mspx



系统安全技巧

采用防火墙、杀毒软件和其它安全机制保护企业网络，攻击者是如何突破企业的计算机系统的呢?简单地利用这个安全链条中的最薄弱的环节就可以。最新的方法之一是利用“浏览器中间者”(Man-in-the-Browser，MitB)攻击在员工的浏览器中建立一个隧道。

MitB 攻击首先是利用恶意软件(通常是像 Zeus 或者 SpyEye 那样的木马程序)在表面上无害的网站上引诱用户。当访问者来到这个网站的时候，这个恶意软件就控制用户的网络浏览器并且修改网页、内容或者显示这个用户的交易数据。

所有这些都是在用户完全不知情的隐蔽情况下完成的。根据浏览器的使用目的，MitB 攻击能够让攻击者悄悄地窃取从登录证书到账户号码或者金融数据等任何信息。由于浏览器进程中通常包含电子邮件系统、虚拟专用网(VPN)和云服务(如云 CRM)的登录细节，在不影响性能的情况下锁定这些进程是非常重要的。移动设备的爆炸式增长和许多人能够远程访问企业资源使这个情况更加严重。

员工被这种网站感染或者成为偷渡式(drive-by)感染的受害者并不困难，因为每一天都会创建出许多欺骗性的网站。犯罪分子甚至使用搜索引擎优化技术提升这些网站在搜索列表中的排名。但是，许多合法的网站也受到感染。像最近的 LinkedIn 网站的电子邮件钓鱼促销活动那样，许多设计好的攻击用来伏击个人用户并且安装 Bugat 和 Clampi 等高级的恶意软件。

这种恶意软件旨在躲过传统的杀毒软件解决方案的雷达，绕过令牌或者网络接入控制系统等强大的身份识别技术。接下来，这种攻击捕捉浏览器处理的所有数据并且把这些数据传送给犯罪分子。所有这些都是在不引起报警的情况下完成的。

最近破解了 Zeus 木马程序对流行的思杰接入网关的攻击，说明了犯罪分子正在设法在安全控制方面领先一步。

为了保护自己的 SSL VPN 产品阻止键盘记录恶意软件的攻击，思杰允许企业客户化这个登录页，包括一个替代物理键盘的一个虚拟键盘。不用使用物理键盘输入口令，使用鼠标点击屏幕上显示的按键从理论上说可以绕过键盘记录器。

但是，最近破解的一个 Zeus 2.0 木马程序包括如下代码：

用英语解释，“@”意味着当点击鼠标左键时，捕捉鼠标附近的文本的截屏图像。“*/citrix/*”具体指明当这个文本“*/citrix/*”出现在浏览器地址栏的时候，捕捉这个截屏图像。

这个 Zeus 木马程序片段是专门为打败虚拟键盘设计的。通过捕捉在点击鼠标时鼠标指针附近的截屏图像，Zeus 木马程序能够读取在点击鼠标时随着鼠标指针点击的按键的顺序显示出来的用户的口令。

如果安全行业要在阻止网络攻击的浪潮中取得任何进展的话，我们需要解决在这个攻击点解决这种危险。这个新的攻击点已经变成了浏览器。