安全威胁每周警讯

2012/07/29～2012/08/04

本周威胁指数

***TrendMicro* 中国区网络安全监控中心**

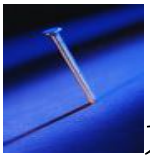
前十大病毒警讯

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	★★★	→	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	X97M_OLEMAL.A	宏病毒	★★	→	宏病毒，它会将本身的下列副本放置到受影响的系统：%User Profile%\Application Data\Microsoft\Excel\XLSTART\k4.xls
7	Adware_Adplus	广告程序	★★	↑	广告软件，常见行为如在 Internet Explorer 和 Mozilla 的 Web 浏览器上显示广告横幅。虽然没有将此归类为恶意软件，但是此类广告软件通常会对系统造成不良影响，如弹出式广告、影响网络连接速度或降低系统性能等。
8	CRCK_KEYGEN	黑客程序	★★	↑	非法破解程序
9	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。
10	X97M_LAROUX.BK	脚本病毒	★★	↓	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

系统漏洞信息

MS12-045 ： Microsoft Data Access Components 中的漏洞可能允许远程执行代码 (2698365)

Windows XP
Windows Vista
Windows 7
Windows Server 2003
Windows Server 2008
描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS12-045



系统安全技巧

社交工程已经成为目前最盛行的攻击方式之一，而且在一些较大的数据泄漏案例中也总是出现。例如，2011 年 RSA breach 就遭遇了定向钓鱼和加载了漏洞的 Excel 文件。因此，对于有能力模拟真实攻击的企业而言，社工渗透测试应该成为每个渗透测试工具包的强制性策略。

社工行为非常依赖心理学，有很多非常可疑的诱饵，可以让社工人员劝服人们从事某项操作。例如，Robert Cialdini 在其著作《影响力：说服心理学》(Influence: The Psychology of Persuasion)中描述了六种刺激人们行为的动机：

1、互惠：因为某人帮助了你而感到歉疚；

2、社交认同：向其他人学习如何进行行为操作；

3、承诺/一致性：发展行为模式并使之成为习惯；

4、喜好：人更容易被有好感的人说服；

5、权威：对权威人物所提要求的默许；

6、短缺：当某个东西的供应受限或仅供专用时，对这个东西的需求就会增加。

渗透测试员在执行社工评估的时候可以利用这些刺激因素。有四种社工技巧可供渗透测试员测试企业的信息安全，分别是钓鱼、假托、介质投放和追尾。

社工渗透安全测试：钓鱼攻击

钓鱼是指向用户发送邮件以便说服用户进行某项操作。在渗透测试中，大多数钓鱼邮件的目的只是诱导

用户点击某个东西，然后记录下这一行为或是为稍后更大规模的渗透测试安装一个程序。这之后，就可以利用客户端软件的某个特定漏洞，如浏览器和动态内容/媒体插件和软件。

成功实施钓鱼攻击的关键是个性化！向目标用户发送特制邮件，如从受信任的邮箱地址发出此邮件，可以增加用户阅读该邮件或是遵照邮件提示操作的几率。一名好的渗透测试员一般都会仔细检查邮件中的拼写和语法错误;一封内容比较少的邮件，如果措辞得体，可能会让人觉得更具可信度。

创建钓鱼攻击最常用的工具可能是开源社工工具包(SET)。通过菜单驱动的邮件和攻击创建系统，它成为了最简单的钓鱼方式之一。而 PhishMe Inc.公司的 PhishMe 和 Wombat Security 的 PhishGuru 也很有用。

社工渗透安全测试：假托(Pretexting)

假托(Pretexting)是指打电话给攻击目标，试图从目标对象那里套取信息。在渗透测试中，这种技巧适用于能提供有用信息的非技术型用户。

最佳策略是提出一些小要求，并给出企业中一些真实员工的名字。在假托对话中，渗透测试员会解释称需要目标对象的帮助(大多数人都愿意配合完成一些看上去没什么可疑的小任务)。一旦双方创建友好关系，渗透测试员便会伺机套取更多信息。

在实施假托之前的侦查需要使用谷歌和 Paterva Maltego 等工具，这些侦查可以提供必要的背景信息。类似 SpoofCard 和 SpoofApp 这种电话代理工具以及 Asterisk PBX 插件可以隐藏渗透测试员的电话号码，甚至是使显示的号码看似来自某个企业。

社工渗透安全测试：介质投放 (Media dropping)

介质投放(Media dropping)通常是指放在某个显眼位置的 USB 闪存设备，如停车场或者建筑入口处。社工在闪存设备上存放了一些非常有趣的文件，而一旦这个闪存被打开便会在客户端发起某种攻击。

Metasploit 是可用于创建此类文件的一款免费工具，它带有内置恶意负载生成器。SET 中的“传染型介质生成器”选项虽然也可以利用 Metasploit，但是却有助于进程自动化。SET 可以创建“合法的”可执行文件。目标电脑启用自动运行时就会自动执行这个文件。自动执行技巧和有趣文件相结合可以增加攻击成功的几率。

而执行介质投放更为复杂的方法则是开发出能通过 USB 闪盘进行自定义攻击或是购买能预置此类程序的 USB 闪盘。为了增加 USB 攻击的成功几率，还可以为设备添加自动利用漏洞和攻击加载文件(以 PDF，Word 和 Excel 为宜)。然后在该 USB 上贴上能吸引人的标签，如“HR 数据”或者“就业”之类的。

社交渗透安全测试：追尾(Tailgating)

追尾(Tailgating)是指通过强迫或愚弄的方式进入物理设备。通常，这类测试所关注的问题是证明渗透测试员可以绕过物理安全防御。

渗透测试员应该计划好获取敏感数据或是快速安装设备以证明自己成功渗透，因为在他们离开设备前所

能利用的时间很短。渗透测试员可以将打印机或者桌上暴露的信息拍照，抑或是安装一个渗透测试盒来提供 wifi 或 3G 网络以便渗透员回访。

通过使用上述四个社工技巧，渗透测试员可以发现企业的漏洞，并给予相关的安全控件推荐和培训，这样可以减少企业遭受恶意社工攻击的几率。

来源：51CTO