安全威胁每周警讯

2011/07/24～2011/07/31

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	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	TROJ_SPNR.0BGL11	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	WORM_ECODE.E-CN	蠕虫	★★★★	→	E 语言病毒,产生与当前文件夹同名 exe 文件
8	CRCK_KEYGEN	破解程序	★★	↑	非法破解程
9	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
10	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

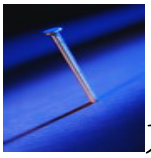
系统漏洞信息

MS11-053：**Bluetooth 堆栈中的漏洞可能允许远程执行代码**

Windows Vista

Windows 7

描述： http://www.microsoft.com/china/technet/security/bulletin/MS11-053.mspx



系统安全技巧

对于企业来说，桌面计算机是核心。毕竟，这里是业务一线阵地。但是在花费大量对我们的服务器(这确实拥有充足的理由)进行全面保护的时间，桌面领域往往就属于被忽略的部分。这种情况是不应该发生的。除了标准的防病毒、恶意软件、防火墙工具之外，还有不少使用者和技术人员没有想到的方法可以用来提高台式机的安全性。下面，就让我们来了解一下这些小技巧。

1：为操作系统安装更新补丁

尽管很多更新属于功能方面的增加，但还是有部分更新属于修补安全方面出现的问题。在部署桌面系统时，首先要做的事情之一，就是确保已经安装了所有的补丁。不要部署存在已知未修复漏洞的桌面系统。如果正在部署的桌面系统没有及时更新的话，就意味着系统中的漏洞是从一开始就存在的。这一要求适用于所有类型的平台，而不是仅仅限于 Windows。

2：关闭文件共享功能

如果在日常工作中需要使用文件共享功能的话，可以选择忽略该措施。但对于没有文件共享需求的桌面系统

来说，就应该选择关闭该功能。对于 Windows XP 来说，单击打开控制面板，选择|网络连接|本地连接属性。在该窗口中选择取消文件和打印机共享功能，就完成了设置。在 Windows 7 中，单击打开控制面板，进入到网络和共享中心中。现在，单击更改在左窗格中的高级共享设置。在这个新窗口中，选择需要禁用共享的网络范围，并选择关闭文件和打印机共享功能。任务完成，以后就不用担心了。

3：禁用来宾帐户并删除未使用的帐户

来宾帐户可能导致很多问题出现。尤其是在大量用户在使用来宾账户的时间都不设置密码保护的情况下，就更容易出现问题。尽管看起来来宾账户使用的范围有限，所以，似乎不会是什么问题。但是，让来宾可以进行连接本身就带来了安全方面的风险。所以，最好的做法是禁用所有的来宾账户。这种情况同样适用于未使用的账户。这属于一种常见的错误。在很多公司中，机器被一名使用者移交给另一名使用者，而原有的用户账户却并没有被删除。不要让这样的情况发生在自己身上。确保系统中的用户都是有效的，并且存在连接机器的需求。否则的话，这也属于安全方面的漏洞。

4：选择功能强大的密码策略

这个问题该不用多说了。确实是这样。但使用“password”这样的单词作为密码的情况出现了多少次?用户使用简单密码的情况是不应该被容许的。如果密码可以和容易地被猜测到，就不应该被容许使用。我们应该在服务器端设定这样的策略。但是，如果不利用安全策略的话，就不得不选择在用户层面上进行强制执行了。不要对该问题掉以轻心。脆弱的密码是导致机器被破坏的最普遍原因之一。

5：将个人文件及文件夹标注出来

在开启了文件夹/文件共享功能的机器上，可能还会存在个人文件夹。对于个人信息来说，这是非常重要的。某些公司可能会禁止员工将私人文件保存在台式机上，不过这样的情况极为罕见。如果贵公司容许员工将个

人信息保存在工作系统中的话，他们可能不希望其它员工可以访问。

这一问题的处理措施依据于平台类型的不同而有所差别(在 Windows 平台上，依据版本的不同在处理措施方面的差别也非常大)。但总的来说，都是需要更改文件夹的安全权限，这样只有使用者可以访问该部分。为此，需要在文件夹上面右键单击选择属性。从属性窗口中，选择安全和编辑的权限，以限制其它使用者的访问。

其它措施?

我希望自己可以找到一个保证桌面系统绝对安全的方法。但是，能够做到这一点的唯一方法就是拔掉网线并关闭电源。这样的措施并不能提高工作环境中的效率。不过，只要遵循我在上面给出的提示，桌面系统将比现在更加安全。

来源：ZDNet