安全威胁每周警讯

2012/06/10～2012/06/16

本周威胁指数

***TrendMicro* 中国区网络安全监控中心**

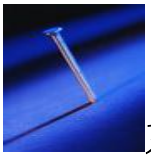
前十大病毒警讯

排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	TROJ_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
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	TROJ_DOWNAD.INF	木马	★★★	↓	DOWNAD 蠕虫关联木马
4	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
5	CRCK_KEYGEN	黑客程序	★★★	↑	非法破解程序
6	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
7	PAK_Generic.001	加壳文件	★★	↑	经过加壳技术加密的文件
8	X97M_LAROUX.CO	宏病毒	★★	→	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
9	X97M_LAROUX.BK	宏病毒	★★	↓	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
10	Adware_Adplus	灰色软件	★★	↑	广告程序，它可能是用户在访问恶意网站时在无意中下载而来。

系统漏洞信息

MS12-032 ： TCP/IP 中的漏洞可能允许特权提升 (2688338)

Windows Vista
Windows 7
Windows Server 2008
Windows Server 2008 R2
描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS12-032



系统安全技巧

1: 使用脆弱的密码

曾经有段时间，有些人自作聪明的用“password”作为密码，用来愚弄那些千方百计猜测密码的黑客和其它恶意分子。毕竟很多人都不会用这么明显的词语作为密码。如今，很多人意识到了用这种密码所能实现的安全性实在是脆弱，但仍然有很多人乐意使用这种简单易猜的密码，尤其是在如今高度社交化的网络中。比如，有人会用自己的名字缩写加上生日作为密码，而这方面的信息数据很容易通过 Facebook 或其它渠道获取，有心的黑客只要将少量的信息组合一下就能破解这种密码了。而就算是在一些拥有强力密码策略的企业中，只要有人存在，就会有这种脆弱的密码存在。

解决方案: 不要用明显的模式来设置密码。将各种因素混杂起来，比如用感叹号代替数字 1，&标记代替数字 8。密码设置的越复杂，被破解的几率就越小。如果你在为企业设置密码策略，应该要求密码中使用多个字符集。

2: 从来不改密码

很多人多年来一直不曾更改密码，而且这个密码还被用于多个网站。这是一个很大的安全漏洞。在企业里，就算有密码修改的策略，但是很多员工还是能找到办法绕过这种强制策略。比如，我的公司里曾经有一个拥有域管理员权限的员工，他将自己的账户排除在了密码策略之外。发现后我严厉的批评了他，并让他将自己的账户至于密码策略规范之内(后来我觉得真的应该开除这个人，因为他滥用了自己的权利)。当然，我说的情况可能比较特殊，但是我们可以想想，有多少人在使用相同或近似的密码来访问不同的网站呢?而到了必须修改密码的时候，是不是有很多人只改掉一个字符来应付密码策略的强制要求呢?

解决方案: 对员工或用户进行培训，让他们知道一个强壮的密码有多么重要，以及为什么要定期更换密码。作为密码策略的一部分，你也可以考虑采用第三方软件来禁止用户使用类似的密码应付密码策略的强制

要求。

3: 不安装杀毒软件

这个疏忽是完全可以避免的。如果你的工作环境中没有安装反病毒软件，那么你真的是大错特错了。就算有最好的防火墙，仍然要记住安全屏障的层次概念。一旦防火墙没有成功拦截恶意代码，反病毒软件将成为终端系统上最后的屏障。

解决方案: 马上安装杀毒软件。

4: 不使用防火墙或设置不严谨

不论是在家还是在企业 IT 环境中，都应该使用防火墙设备。虽然 Windows 和其它操作系统现在都自带有内置的防火墙，我仍然建议大家购置一部硬件防火墙设备，或类似的设备，硬件防火墙与软件防火墙相配合，是最好的安全方案。另外，如果使用防火墙，就要对其进行严谨的设置。

解决方案: 有条件就在家或在企业环境都配备上防火墙硬件设备。确保防火墙不会允许不必要的数据从外部流入内网环境。

5: 从不给系统打补丁

操作系统开发商和应用程序开发商定期推出补丁程序是有其原因的。虽然很多升级或更新都是为了增加新功能，但仍然有不少更新是纯粹为了弥补系统和软件的安全漏洞的。我见过很多家用电脑系统中，用户都将系统自动更新选项关闭了。而在企业环境，很多时候人们觉得网络边缘有了防火墙，就不需要再为系统安装升级补丁了。这并不正确，因为很多攻击代码会通过防火墙的防护进入企业内网。

解决方案: 为系统打补丁!打开系统和软件的自动更新功能，并立即为企业建立补丁管理策略并实施。

6: 不安全的数据存储

你将多少敏感数据(比如个人信息，公司业务数据等)存放在了 U 盘里?你是不是曾经带着这种存有敏感信息的 U 盘外出过?我见过很多人将 U 盘作为钥匙链，带在身上到处走动。有的时候，U 盘就和钥匙一起放在了食堂的饭桌上忘记拿走。

现在，还有多少人会将企业数据备份在磁带上?这些磁带是否会被搬离备份场所，这个过程是否处于你的控制之中?

不受保护的数据是安全的一大问题。一次简单的丢失 U 盘、笔记本、iPad 或备份磁带的事件，就会让企业面临财务、司法以及公共关系上的巨大挑战。

解决方案: 对任何可移动的存储数据进行加密保存。大多数备份软件都支持对备份数据进行加密，比如 BitLocker 以及 BitLocker To Go 可以用来保护笔记本设备和 U 盘。对于其他设备，比如 iPad，可以考虑使用移动安全管理软件对其中的数据进行加密保存。

7: 过于慷慨的权限

在企业环境中，权限决定了一个用户能做什么不能做什么。要让员工顺利工作，最简单的方式是给他们赋予管理员权限，以便让他们能够访问企业网络的所有内容。但是这种方式很快就会带来混乱。因此大多数公司都会根据员工的工作关系，通过权限策略为其赋予适当的权限。不幸的是，就算有这种策略，还是会发生权限蔓延的情况。比如员工从一个岗位调换到另一个岗位，而之前的权限并没有被移除。

解决方案: Make 确保企业应用了明确的权限管理策略。企业的权限管理策略和实施方法应该定期的进行审视和调整，以便适应企业当前的需求。不需要的权限要及时清除。

8: 薄弱的或没有 Wi-Fi 安全设置

就算现在很多人都知道开放的 Wi-Fi 网络具有很大安全风险，仍然有很多家庭或企业让自己的无线网络保持开放和不安全的状态。另外，由于 WEP 加密方式的普及，仍然有很多网络在使用这种加密验证方式，但是这种方式已经很不安全了，甚至四秒钟就可以破解 WEP 密码。不过就算如此，这样比完全开放的无线网络要安全一些。

解决方案: 使用 WPA 或者更高级的 WPA2 加密验证措施。WPA2 是目前流行的无线网络安全标准，多数操作系统都支持这个标准。另外，在采用 WPA2 标准后，还要设置一个足够强壮的密码，这个密码应该是不容易被猜测出的，或者不容易被暴力破解的，否则再好的加密标准也是虚设。WPA2 加密也有可能被破解，但是破解 WPA2 的难度要远高于破解 WEP 或 WPA。

9: 忽视简单的移动设备安全措施

未来几年，移动设备将成为黑客们的天堂。很多人随身携带的移动数码设备都存储有未加密的个人信息，这些设备中存储的信息可以在短时间内被黑客获取。而且这种设备很容易被盗或丢失。前面我提到过，你应该留意该在移动设备中存储什么样的信息，并将敏感的信息删除或加密。但是利用移动设备的联网功能进入企业网络并窃取信息的情况还是会出现的。

解决方案: 虽然很简单，但是非常必要，即当移动设备试图访问企业网络时，要求使用密码登录。虽然这种方式不能跟不上杜绝移动设备窃取企业网络数据的情况发生，但是会让那些偶尔获得移动设备的人知难而退。

10: 从来不检查备份

让我们假设一种情景，企业的所有安全机制都失效了，企业数据和网络已经遭到了严重的入侵和破坏，系统和数据都已经不再可靠了。这时候，可能唯一能做的就是通过备份数据来回复整个环境。但是，如果遇到如下几种情况，对于企业来说，就真的是无可挽回了：

- 备份数据损坏。
- 备份磁带有损伤。

- 虽然每晚备份系统都在向磁带上记录备份数据，但实际上没有任何数据被备份。

以上任何一条出现，对企业来说都是致命的打击。

解决方案: 立即制定和实施相应的策略和工作程序，定期检查备份数据。另外，考虑添加额外的备份系统，将备份数据进行再次备份，并存储在与网络隔离的环境中，防止备份数据在企业网络遭遇黑客攻击时被一起破坏。

来源：51CTO