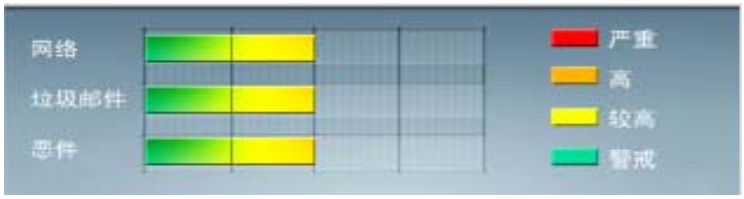
安全威胁每周警讯

2010/11/28～2010/12/04

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	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	木马病毒	★★★	↓	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	★★★	→	疑似病毒
6	CRCK_KEYGEN	破解程序	★★	↑	非法破解程序
7	JS_EXPLOIT.SMD	网页脚本	★★	↑	该网页脚本木马病毒是托管在一个网站上的，当用户访问该网站时会自动运行。当它执行时，且用户访问某些网站，就会感染该类病毒。
8	WORM_ECODE.E-CN	蠕虫	★★★★	→	E 语言病毒,产生与当前文件夹同名 exe 文件
9	TROJ_PIDIEF.PUA	木马病毒	★★	↑	该木马可能是由其他恶意软件下载的，通过远程站点方式下载到本地感染用户机器。
10	PAK_Generic.001	加壳程序	★★	→	对加壳文件的通用检测。病毒通常会使用加壳手法来达到不被杀毒软件检测的目的

系统漏洞信息

MS10-088:Microsoft PowerPoint 中的漏洞可能允许远程执行代码 (2293386)

受影响的软件：

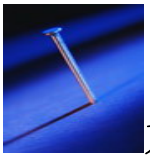
Microsoft Office xp sp2

Microsoft office 2003

Microsoft Office 2004 for mac

Microsoft Power Point Viewer 2007 sp2

描述：请见 http://www.microsoft.com/china/technet/security/bulletin/MS10-088.mspx



系统安全技巧

摘要：目前先进的网络安全设备在阻止网络恶人入侵你的企业方面做了极好的工作。但是，当网络恶人确实进入到你的安全环境中的时候，你要做什么呢?以下是你的网络可能被从内部攻破的 10 个途径，以及你能够采取什么措施来保证企业服务器的安全。

目前先进的网络安全设备在阻止网络恶人入侵你的企业方面做了极好的工作。但是，当网络恶人确实进 入到你的安全环境中的时候，你要做什么呢?遗憾的是世界上的所有手段对于目前最恶毒的网络恶人都没有多少效果。以下是你的网络可能被从内部攻破的 10 个途 径，以及你能够采取什么措施来保证企业服务器的安全。

1. 优盘

不管你是否相信，优盘实际上是你能够从防火墙内部感染一个网络的常用方法，如果不是最常用的方法 的话。这有许多理由：优盘价格便宜，体积小、存储许多数据并且能够在多种设备之间使用。优盘的普遍应用促使黑客开发出一种有针对性的恶意软件，如臭名昭著 的 Conficker 蠕虫。这种蠕虫能够在连接到 USB 端口的时候自动执行。更严重的是默认的操作系统设置一般都允许大多数程序 (包括恶意程序)自动运行。这相当于你的邻居每一个人都有一把你的电子车库门的钥匙，并且利用这个钥匙打开其他人的车库门。

对策：修改计算机默认的自动运行政策。

2. 笔记本电脑和上网本

笔记本电脑是一种考虑周到的便携式设备，包含完整的操作系统，能够使用内置电池工作并且配置了以 太网端口可以直接连接到一个网络。此外，笔记本电脑中也许已经有了在后台运行的恶意代码，其任务是寻找网络和发现其它可供感染的系统。这台笔记本电脑也许 属于一个内部的员工或者属于一个从开放的办公室来访或者工作的客户。

除了被感染的笔记本电脑破坏内部网络之外，重要的是要考虑这些笔记本电脑本身的问题。所有的公司 都拥有绝对不允许带出办公楼的敏感资料(如工资信息、医疗记录、家庭地址、电话号码和社会安全保险号码等)。当这些信息存储在没有安全措施的便携式电脑中 的时候，那是很危险的，因为便携式电脑很容易带出去。我们看到过许多存储了敏感数据的笔记本电脑丢失的例子。除非这个笔记本电脑使用一种严格的加密算法， 否则，任何文件系统的数据都是很容易恢复的。

对策：对于敏感的数据采用一个加密的文件系统。有许多现成的解决方案可供选择，还有开源软件解决方案，如 TrueCrypt。对于进出内部系统的端点实施控制也是重要的。虚拟专用网、DV 和 WiFi 接入等敏感信息不应该永久性地存储在笔记本电脑或者上网本等设备上。

3. 无线接入点

无线接入点为这个网络附近的任何用户提供直接的连接。攻击驾驶员(驾驶汽车搜索没有安全保护措施 的 WiFi 网络的人)实施的无线攻击是很常见的并且曾造成重大损失。例如：Marshalls 和 TJMaxx 公司的东家 TJ Stores 曾经遭受过使用这种方式进行的攻击。入侵者侵入了这家公司处理和存储客户交易数据的计算机系统 。这些交易数据包括客户的信用卡、借记卡、支票和退货交易等信息。据报道，这次入侵使 TJ Stores 商店的损失超过了 5 亿美元。

无线接入点本身是不安全的，无论是否使用加密措施都是如此。无线加密协议等协议都包含已知的安全漏洞，使用 Aircrack 等攻击框架就很容易攻破。如果不使用强口令，WPA(无线保护接入)和 WPA2 等更安全的协议也容易受到字典攻击。

对策：建议使用带 RADIUS(远程认证拨入用户服务协议)的 WPA2 企业版以及能够进行身份识别和强制执行安全措施的接入点。应该使用强混合口令并且不断地更换口令。一般来说，无线接入点只是为了连接方便，因此，通常没有必要把无线接入点连接到工作环境。

4. 各种各样的 USB 接口设备

优盘并不是 IT 部门需要担心的唯一的 USB 接口设备。许多设备都能够把数据存储到普通的文件系统 中并且通过一个 USB 接口或者类似的连接进行读写。由于这不是这些设备的主要功能，这些设备通常被忘记是一种潜在的威胁。事实是，如果一个端点能够从这个 设备上读取和执行数据，这种设备就能够同优盘一样造成威胁。这些设备包括数码相机、MP3 播放机、打印机、扫描仪、传真机、甚至还有数码相框。在 2008 年，百思买报告称，他们在圣诞节销售的 Insignia 数码相框中发现了一种病毒。这种病毒直接来自于厂商。

对策：实施和强制执行资产控制和政策，规定什么设备可以进入这个环境以及什么时候可以进入这个环境。然后，定期使用政策提醒程序检测这些政策的执行情况。2008 年，美国国防部制定了一些政策，禁止优盘和其它可移动介质进/出他们的环境。

5. 内部连接

公司内部员工也可能意外地或者故意地进入他们不会或者不应该接入的网络，使用本文介绍的一些手段破坏端点。也许一位员工在同事吃午饭的时候“借用”那个同事的电脑。也许一位员工让一位同事帮助他访问他无权访问的网络中的一个区域。

对策：应该经常改变口令。为员工规定身份识别和接入等级是必须的。他应该只有访问系统、文件共享等权限。任何特殊的要求应该呈报给有权批准这个请求的团队(而不是有权的一个用户)。

6. 特洛伊人

同特洛伊木马一样，特洛伊人以某种伪装的方式进入企业。他可能身穿工作服或者穿着合法的维修工的 服装。这类骗子曾经进入过许多非常保密的环境，包括服务器机房等。根据我们自己的社交经验，我们一般不会阻止或者询问在我们的办公环境中的不认识的身穿工 作服的人。一个员工也许不会认真思考一下就刷自己的入门卡让一个身穿工作服的人进入他们的环境提供服务。一个无人监视的人不用 1 分钟就能进入服务器机房去 感染整个网络。

对策：应该提醒员工有关授权第三方进入的事情。要通过询问一些问题来确定来人的身份，不要通过推测。

7. 光盘

在 2010 年 6 月，一个陆军情报分析师被指控窃取并且在公网上泄露保密数据而被逮捕。知情人士说，这位分析师是使用一张伪装成流行歌手 CD 的光盘把数据带出 去的。一旦他进入一台网络工作站，他就能访问到他有权访问的机密信息并且把数据以加密的方式存储在他的“音乐”CD 盘中。为了掩人耳目，这个分析师在使用 工作站的时候还会假唱假装存储在 CD 盘中的歌曲。表面上合法的可记录介质能够用来拷贝数据进出网络。同上面提到的优盘一样，光盘也是网络感染的一个原因。

对策：同优盘的技巧一样，重要的是实施和强制执行资产控制和政策，规定什么设备什么时候可以进入这个环境。然后，定期使用政策提醒程序跟踪执行情况。

8. 事后诸葛亮

虽然这个列表重点介绍缓解利用数字技术的威胁，但是，我们不应该忘记人类的大脑在存储信息方面也是非常有效的。当你登录你的笔记本电脑的时候谁在注意你?你的复印件存储在什么地方?你在咖啡厅、机场等地方在笔记本电脑上阅读了什么保密的文件?

对策：最好的防御措施是只要操作敏感的数据就要谨慎并且对这种威胁保持警惕，你甚至要立即停下来观察你的周围环境。

9. 智能手机和其它数字设备

现在，手机除了让你给世界各地的人打电话之外还能做更多的事情。智能手机是功能齐全的计算机，配 置了 WiFi 连接、多线程操作系统、大存储容量、高分辨率摄像头和大量的应用程序支持。与其它便携式平板电脑一样，智能手机开始获准在企业中使用。智能手 机能够引起上面所说的优盘和笔记本电脑引起的同样的威胁。而且，智能手机有可能避开传统的数据泄漏保护解决方案。如何阻止一个用户拍摄计算机显示屏的高清 照片并且通过手机的 3G 网络用电子邮件把这个照片发出去?

对策：这里适用针对 USB 设备和光盘的同样的规则。实施和强制执行资产控制和政策，规定什么设备什么时候可以进入这个环境。

10. 电子邮件

电子邮件是企业收发数据中经常使用的方法。然而，电子邮件经常被滥用。包含保密信息的邮件很容易发送到外部目标。此外，电子邮件本身也可能携带病毒。一个有针对性的电子邮件可能是为了窃取一个员工的访问证书。这些窃取的证书可以在第二阶段的攻击中使用。

对策：对于电子邮件的安全，来源的身份识别是关键。使用 PGP 等技术识别发件人的身份或者在发送敏感的信息之前提出一些简单的问题。应该强制执行对于广泛的化名电子邮件地址的访问控制。政策和提醒程序应该发给员工。

来源 51CTO