安全威胁每周警讯

2012/07/15～2012/07/21

本周威胁指数

***TrendMicro* 中国区网络安全监控中心**

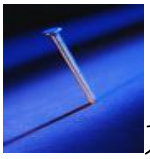
前十大病毒警讯

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	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.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
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	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
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	X97M_LAROUX.CO	脚本病毒	★★	↑	Office 宏病毒，由其他恶意软件或访问恶意网站感染
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	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	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

系统漏洞信息

MS12-041 ： Windows 内核模式驱动程序中的漏洞可能允许特权提升 (2709162)

Windows XP
Windows Vista
Windows 7
Windows Server 2003
Windows Server 2008
Windows Server 2008 R2
描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS12-041



系统安全技巧

几乎所有企业对于网络安全的重视程度一下子提高了，纷纷采购防火墙等设备希望堵住来自 Internet 的不安全因素。然而，Intranet 内部的攻击和入侵却依然猖狂。事实证明，公司内部的不安全因素远比外部的危害更恐怖。

大多企业重视提高企业网的边界安全，暂且不提它们在这方面的投资多少，但是大多数企业网络的核心内网还是非常脆弱的。企业也对内部网络实施了相应保护措施，如：安装动辄数万甚至数十万的网络防火墙、入侵检测软件等，并希望以此实现内网与 Internet 的安全隔离，然而，情况并非如此!企业中经常会有人私自以 Modem 拨号方式、手机或无线网卡等方式上网，而这些机器通常又置于企业内网中，这种情况的存在给企业网络带来了巨大的潜在威胁，从某种意义来讲，企业耗费巨资配备的防火墙已失去意义。

这种接入方式的存在，极有可能使得黑客绕过防火墙而在企业毫不知情的情况下侵入内部网络，从而造成敏感数据泄密、传播病毒等严重后果。实践证明，很多成功防范企业网边界安全的技术对保护企业内网却没有效用。于是网络维护者开始大规模致力于增强内网的防卫能力。

下面给出了应对企业内网安全挑战的 10 种策略。这 10 种策略即是内网的防御策略，同时也是一个提高大型企业网络安全的策略。

1、注意内网安全与网络边界安全的不同

内网安全的威胁不同于网络边界的威胁。网络边界安全技术防范来自 Internet 上的攻击，主要是防范来自公共的网络服务器如 HTTP 或 SMTP 的攻击。网络边界防范(如边界防火墙系统等)减小了资深黑客仅仅只需接入互联网、写程序就可访问企业网的几率。内网安全威胁主要源于企业内部。恶性的黑客攻击事件一般都会先控制局域网络内部的一台 Server，然后以此为基地，对 Internet 上其他主机发起恶性攻击。因此，应在边界展开黑客防护措施，同时建立并加强内网防范策略。

2、限制 VPN 的访问

虚拟专用网(VPN)用户的访问对内网的安全造成了巨大的威胁。因为它们将弱化的桌面操作系统置于企业防火墙的防护之外。很明显 VPN 用户是可以访问企业内网的。因此要避免给每一位 VPN 用户访问内网的全部权限。这样可以利用登录控制权限列表来限制 VPN 用户的登录权限的级别，即只需赋予他们所需要的访问权限级别即可，如访问邮件服务器或其他可选择的网络资源的权限。

3、为合作企业网建立内网型的边界防护

合作企业网也是造成内网安全问题的一大原因。例如安全管理员虽然知道怎样利用实际技术来完固防火墙，保护 MS-SQL，但是 Slammer 蠕虫仍能侵入内网，这就是因为企业给了他们的合作伙伴进入内部资源的访问权限。由此，既然不能控制合作者的网络安全策略和活动，那么就应该为每一个合作企业创建一个 DMZ，并将他们所需要访问的资源放置在相应的 DMZ 中，不允许他们对内网其他资源的访问。

4、自动跟踪的安全策略

智能的自动执行实时跟踪的安全策略是有效地实现网络安全实践的关键。它带来了商业活动中一大改革，极大的超过了手动安全策略的功效。商业活动的现状需要企业利用一种自动检测方法来探测商业活动中的各种变更，因此，安全策略也必须与相适应。例如实时跟踪企业员工的雇佣和解雇、实时跟踪网络利用情况并记录与该计算机对话的文件服务器。总之，要做到确保每天的所有的活动都遵循安全策略。

5、关掉无用的网络服务器

大型企业网可能同时支持四到五个服务器传送 e-mail，有的企业网还会出现几十个其他服务器监视 SMTP 端口的情况。这些主机中很可能有潜在的邮件服务器的攻击点。因此要逐个中断网络服务器来进行审查。若一个程序(或程序中的逻辑单元)作为一个 windows 文件服务器在运行但是又不具有文件服务器作用的，关掉该文件的共享协议。

6、首先保护重要资源

若一个内网上连了千万台(例如 30000 台)机子，那么要期望保持每一台主机都处于锁定状态和补丁状态是非常不现实的。大型企业网的安全考虑一般都有择优问题。这样，首先要对服务器做效益分析评估，然后对内网的每一台网络服务器进行检查、分类、修补和强化工作。必定找出重要的网络服务器(例如实时跟踪客户的服务器)并对他们进行限制管理。这样就能迅速准确地确定企业最重要的资产，并做好在内网的定位和权限限制工作。

7、建立可靠的无线访问

审查网络，为实现无线访问建立基础。排除无意义的无线访问点，确保无线网络访问的强制性和可利用性，并提供安全的无线访问接口。将访问点置于边界防火墙之外，并允许用户通过 VPN 技术进行访问。

8、建立安全过客访问

对于过客不必给予其公开访问内网的权限。许多安全技术人员执行的“内部无 Internet 访问”的策略，使得员工给客户一些非法的访问权限，导致了内网实时跟踪的困难。因此，须在边界防火墙之外建立过客访问网络块。

9、创建虚拟边界防护

主机是被攻击的主要对象。与其努力使所有主机不遭攻击(这是不可能的)，还不如在如何使攻击者无法通过受攻击的主机来攻击内网方面努力。于是必须解决企业网络的使用和在企业经营范围建立虚拟边界防护这个问题。这样，如果一个市场用户的客户机被侵入了，攻击者也不会由此而进入到公司的 R&D。因此要实现公司 R&D 与市场之间的访问权限控制。大家都知道怎样建立互联网与内网之间的边界防火墙防护，现在也应该意识到建立网上不同商业用户群之间的边界防护。

10、可靠的安全决策

网络用户也存在着安全隐患。有的用户或许对网络安全知识非常欠缺，例如不知道 RADIUS 和 TACACS 之间的不同，或不知道代理网关和分组过滤防火墙之间的不同等等，但是他们作为公司的合作者，也是网络的使用者。因此企业网就要让这些用户也容易使用，这样才能引导他们自动的响应网络安全策略。

另外，在技术上，采用安全交换机、重要数据的备份、使用代理网关、确保操作系统的安全、使用主机防护系统和入侵检测系统等等措施也不可缺少。

来源：51CTO