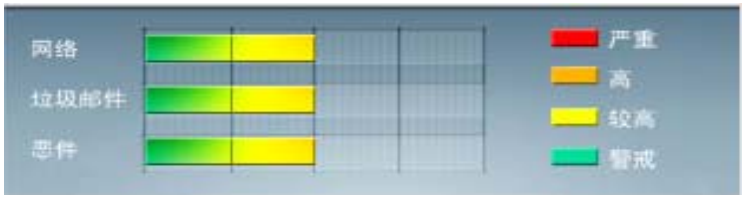
安全威胁每周警讯

2011/01/15～2011/01/22

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	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
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	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
6	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
7	WORM_AUTORUN.CLX	蠕虫	★★	↑	蠕虫病毒，通过网络共享、IRC、P2P、邮件等方式传播。感染该病毒后会在系统自启动项中加入病毒启动信息
8	TROJ_PIDIEF.PUA	木马	★★	↑	木马病毒，通过其他恶意程序释放
9	Adware_Adplus	广告软件	★	↑	广告软件，会植入到 IE 或 Mozilla 浏览器工具中，用户在访问网页的时候会随机弹出广告窗口
10	TROJ_LAMEWAR.VTG	木马	★★	↑	木马病毒，该病毒不具备传播特性，是由其他恶意程序通过网络下载到终端电脑上的

系统漏洞信息

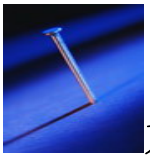
MS10-095:Microsoft Windows 中的漏洞可能允许远程执行代码 (2385678)

受影响的软件:

Windows 7

Windows 2008

描述: 请见http://www.microsoft.com/china/technet/security/bulletin/MS10-095.mspx



系统安全技巧

摘要: 常言道“家贼难防”, 这是由于内部作案的隐蔽性难以防范。那么, 黑客在局域网内的入侵有什么常见方式? 我们又要采取什么样的保护措施呢? 本文也许可以给您一个满意的回答。

常言道“家贼难防”, 这是由于内部作案的隐蔽性难以防范。那么, 黑客在局域网内的入侵有什么常见方式? 我们又要采取什么样的保护措施呢? 本文也许可以给您一个满意的回答。

防范共享入侵

比如, 在某局域网中, 服务器装有 Win2000 Server 系统且采用 NTFS 分区, 客户机计算机分别为 Workl、Work2……WorkN, 并装有 Win98 或 Win2000 Pro 系统。假如其中一台客户机的用户名为 YD_xlpos, 密码为 Ei(9, 已经登录到域 domain, 则它可使用默认共享方式入侵服务器: 在该客户机 的网络邻居地址栏中输入/serveradmin$, 便可进入 Win2000 的系统目录 Win NT, 此时该用户可以删除文件。若再输入/serverd$, 即可进入服务器上的 D 盘, 此时该客户机用户已经具备服务器的管理员权限, 这是相当危险的。居 心叵测的人可以通过新建 Winstart.bat 或者 Wininit.ini 文件, 并在其中加入格式化 C 盘的语句, 使系统丢失所有 C 盘文件; 或是在服务 器的启动项中加入现在任何流行木马的启动程序, 后果也不堪设想。

Win2000 采用默认共享方式以便远程维护, 但同样给了黑客可乘之机。打开注册表编辑器, 定位 到 HKEY_L0 CAl_MACHINE SYSTEMCurrent Control SetServiceslanmanserver, 若系统为 Win2000 Pro, 则新建 Autosharewks 的 DWORD 值, 并设键值为 0;若系统为 Win2000 Server, 则新建 Autoshareserver 的 DWORD 值, 并设键值为 0。重新启动计算机后默认共享便不会再出现。

不过危险并没有消除, 装有 Win2000 平台的客户机还可以通过 IPS$的空连接入侵服务器。客户机用户可以先用端口扫描软件 X-Scan 填入服务器的 IP, 在扫描模块里选择 sqlserver 弱口令和 nt- server 弱口令, 当得到 nt-server 弱口令后, 可在客户机的 cmd 窗口中输入“net use /192.168.0.88ips$”/user: ’用户’”来建立空连接, 然后激活 Guest, 并添加管理员权限, 安装后门(如 netcat)后就可 以进行远程控制。管理员怎么禁止 IPS$空连接呢?可定位到注册表 HKEY_LOCAL_MACHINE SYSTEMCurrent Control SetControlLSA,修改 Restrict Anony-mous 的 DWORD 值为 0000001。

防范 Ping 入侵

Ping 入侵方式也叫 ICMP 入侵，它也利用了 Windows 系统的漏洞。在 Work1 的 DOS 窗口中输入“ping -1 65500 -t192.168.0.88”(服务器的 IP 地址)，则可看到服务器上系统托盘的小电脑一直在闪动，那是客户机 Work1 在向服务器发出请求。我们试 想，如果局域网内的计算机很多，并在每台计算机的 Aotoexec.bat 文件中加入“ping -l 65500 -t192.168.0.88”，那会怎么样?服务器将会因 CPU 使用率居高不下而崩溃，这也就是有名的 DoS 服务(拒绝服务)攻击：在一个时段内连续向 服务器发出大量请求，服务器来不及回应而死机。

对付这类攻击可安装网络防火墙，如天网等，在设置里面选择“不允许别人用 Ping 命令探测本机”； 或者在“管理工具”中点击“本地安全策略”，进入“IP 安全策略”，在本地机器中进行设置。

维护和管理服务器

黑客入侵服务器，必须知道服务器的 IP 地址和所开放的端口，因此可以在网上邻居中隐藏服务器的 IP 地址，为服务器的计算机名保密。建立服务器通讯端口列表，屏蔽一些敏感的端口如 139、3389、5000，了解部分病毒或者木马的常用连接端口，如“冰河”的 7626 端口、“广外女生”的 6267 端口。

安装病毒防火墙和网络防火墙，定期对病毒库进行更新，按计划查毒杀毒。定期用 DOS 命令 netstat -a 或者 SuperScan 软件对服务器开放的端口进行检测，将检测结果和以往备份的端口列表进行比较。若发现未知端口有异常连接建立或者正在监听，特别 是高端端口，则立即断开网络，用检测木马的软件如 Trojan Remover 等进行检测。用进程检测软件如 Windows 优化大师监测服务器所开的进程，并和以往的进程列表作比较，留意不明进程。注意观察 Win2000 的服务，因为它是在系统启动前加载的。可将 Task Scheduler、Run As Service、FTP 等改为手动，最好能够了解各种服务的作用，了解服务器所开的共享，可用 net share 命令来查看。尽可能不要设置文件共享，不要打开写文件的权限。即使开启共享，也应设置相应密码。

打开“计算机管理”，检查用户和组里是否有非法用户，尤其小心管理员权限的非法用户。禁止系统提 供的 Guest 用户，因为黑客常用 Guest 进行系统控制，对于 Administrator 则应进行改名操作。在 C:Documents and Settings 下查看用户，对于有非法用户的目录，应仔细察看并定期对事件查看器进行筛选和分析。审核安全日志，选择“管理工具”里面的“本地安全策 略”，在本地策略里的审核策略中进行审核操作。

若英文功底良好，则推荐使用 Win2000 英文版，因为中文版的 Bug 较多，补丁推出也相对较 晚。多去微软的站点检测，及时更新微软的 SP 补丁包，注意微软发布的安全公告。了解病毒和系统漏洞的最新动态，堵上系统存在的漏洞。对于系统管理员，则要 合理选择安装相关组件，不需要的不必安装，当然需要的组件除外，如网络监视器。另外，尽量修改一些特殊的 DOS 命令的扩展名，尽量少用超级用户登录，其密 码也要做到科学配置，大小写加特殊字符，从而减低被暴力破解的几率。

此外，系统管理员不要私自在服务器上试用新软件，尤其是大型软件和 Beta 版软件，不要用服务器作为上网的主机，不要让不具备权限的人接近服务器。Win2000 Server 系统的稳定性和安全性还是非常高的，系统的崩溃多由于人为的误删除或者误操作所致。

总之，服务器的安全问题应引起极大的重视，应挂接多个硬盘做好备份，使服务器在出错后能够快速恢复。

来源： ZDNET

免责声明