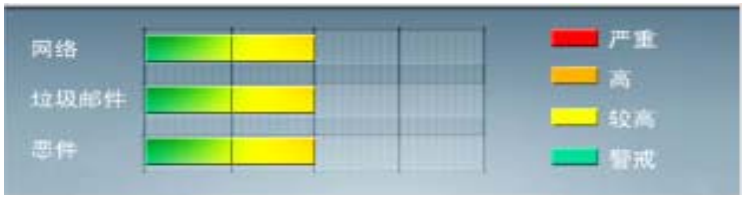
安全威胁每周警讯

2011/02/20～2011/02/26

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	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	Cryp_Xed-12	木马	★★★	↑	疑似病毒
6	CRCK_KEYGEN	破解程序	★★	↑	非法破解程序
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	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
9	Gray_Gen	灰色软件	★★★	↑	灰色软件的通用检测名。在用户不知情的情况下，在其电脑上安装后门、收集用户信息的软件
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

MS10-100:Consent 用户界面中的漏洞可能允许特权提升 (2442962)

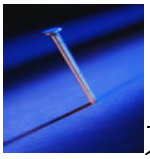
受影响的软件:

Windows Vista

Windows 2008

Windows 7

描述: 请见http://www.microsoft.com/china/technet/security/bulletin/MS10-100.mspx



系统安全技巧

摘要: 黑客信息收集型攻击是目前非常主流的一种攻击形式，信息收集型攻击并不对目标本身造成危害，如名所示这类黑客攻击被用来为进一步入侵提供有用的信息。而假消息攻击是用于攻击目标配置不正确的消息，主要包括: 扫描技术、体系结构刺探、利用信息服务。

黑客信息收集型攻击是目前非常主流的一种攻击形式，信息收集型攻击并不对目标本身造成危害，如名所示这类黑客攻击被用来为进一步入侵提供有用的信息。而假消息攻击是用于攻击目标配置不正确的消息，主要包括: 扫描技术、体系结构刺探、利用信息服务。

黑客攻防之信息收集型攻击

1.扫描技术

(1)地址扫描

概览: 运用 ping 这样的程序探测目标地址，对此作出响应的表示其存在。

防御: 在防火墙上过滤掉 ICMP 应答消息。

(2)端口扫描

概览: 通常使用一些软件，向大范围的主机连接一系列的 TCP 端口，扫描软件报告它成功的建立了连接的主机所开的端口。

防御: 许多防火墙能检测到是否被扫描，并自动阻断扫描企图。

(3)反响映射

概览: 黑客向主机发送虚假消息，然后根据返回“hostunreachable”这一消息特征判 断出哪些主机是存在的。目前由于正常的扫描活动容易被防火墙侦测到，黑客转而使用不会触发防火墙规则的常见消息类型，这些类型包括:

RESET 消息、 SYN-ACK 消息、DNS 响应包。

防御：NAT 和非路由代理服务器能够自动抵御此类攻击，也可以在防火墙上过滤“hostunreachable”ICMP 应答。

(4)慢速扫描

概览：由于一般扫描侦测器的实现是通过监视某个时间桢里一台特定主机发起的连接的数目(例如每秒 10 次)来决定是否在被扫描，这样黑客可以通过使用扫描速度慢一些的扫描软件进行扫描。

防御：通过引诱服务来对慢速扫描进行侦测。

2.体系结构探测

概览：黑客使用具有已知响应类型的数据库的自动工具，对来自目标主机的、对坏数据包传送所作出的 响应进行检查。由于每种操作系统都有其独特的响应方法(例 NT 和 Solaris 的 TCP/IP 堆栈具体实现有所不同)，通过将此独特的响应与数据库中的已知响应进行对比，黑客经常能够确定出目标主机所运行的操作 系统。

防御：去掉或修改各种 Banner，包括操作系统和各种应用服务的，阻断用于识别的端口扰乱对方的攻击计划。

3.DNS 域转换

概览：DNS 协议不对转换或信息性的更新进行身份认证，这使得该协议被人以一些不同的方式加以利用。如果你维护着一台公共的 DNS 服务器，黑客只需实施一次域转换操作就能得到你所有主机的名称以及内部 IP 地址。

防御：在防火墙处过滤掉域转换请求。

4.Finger 服务

概览：黑客使用 finger 命令来刺探一台 finger 服务器以获取关于该系统的用户的信息。

防御：关闭 finger 服务并记录尝试连接该服务的对方 IP 地址，或者在防火墙上进行过滤。

5.LDAP 服务

概览：黑客使用 LDAP 协议窥探网络内部的系统和它们的用户的信息。

防御：对于刺探内部网络的 LDAP 进行阻断并记录，如果在公共机器上提供 LDAP 服务，那么应把 LDAP 服务器放入 DMZ。

黑客攻防之假消息攻击

1.DNS 高速缓存污染

概览：由于 DNS 服务器与其他名称服务器交换信息的时候并不进行身份验证，这就使得黑客可以将不正确的信息掺进来并把用户引向黑客自己的主机。

防御：在防火墙上过滤入站的 DNS 更新，外部 DNS 服务器不应能更改你的内部服务器对内部机器的认识。

2.伪造电子邮件

概览：由于 SMTP 并不对邮件的发送者的身份进行鉴定，因此黑客可以对你的内部客户伪造电子邮件，声称是来自某个客户认识并相信的人，并附带上可安装的特洛伊木马程序，或者是一个引向恶意网站的连接。

防御：使用 PGP 等安全工具并安装电子邮件证书。

来源： 赛迪网