安全威胁每周警讯

2011/10/30～2011/11/05

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	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_SPNR.03JR11	木马	★★★	↑	疑似病毒
4	TROJ_SPNR.08JR11	木马	★★★	↑	疑似病毒
5	Cryp_Xed-12	木马	★★★	→	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
6	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
7	PAK_Generic.001	木马	★★★	↑	疑似病毒
8	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
9	TROJ_SPNR.08JS11	木马	★★★	↑	疑似病毒
10	TROJ_SPNR.0BJR11	木马	★★★	↑	疑似病毒

系统漏洞信息

MS11-081：Internet Explorer 的累积性安全更新 (2586448)

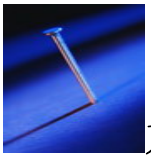
Internet Explorer 6

Internet Explorer 7

Internet Explorer 8

Internet Explorer 9

描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS11-081



系统安全技巧

虽然所有企业管理者都知道网络安全的重要性，但是真正实现的安全高度却并不理想。对于任何一家企业来说，网络安全都应该是最首要解决的问题。下面，我将列出十点建议，帮助企业实现尽可能高的安全水平。

1: 尽可能减少被攻击范围

强化系统安全的第一步，就是减少系统被攻击的范围。一台系统运行的代码越多，就越有可能出现漏洞。因此，加强安全性的第一步就是卸载那些不必要的操作系统组件和应用程序。

2: 只是用信誉良好的软件

鉴于目前的经济环境还不够好，很多企业都试图尝试免费软件，廉价软件或者开源软件。首先，我必须承认，我在自己的公司里曾经使用过小部分此类软件。在这种情况下，最重要的是在使用前对软件进行调研和评估。一些免费软件或廉价软件本身设计时就考虑通过广告来盈利，另外一些则是通过收集用户信息或者跟踪用户上网浏览行为来获利。

3:尽可能以普通用户权限进行操作

在日常工作中，管理员最好以普通用户权限登录进行一般性工作。如果此时发生了恶意软件入侵，恶意软件通常都会获取与当前用户权限相同的权限。因此，如果管理员经常以管理员权限登录，一旦发生此类问题，就会造成较大的破坏。

4: 建立多个管理员账户

上一条我们说的是在正常工作时使用普通用户权限，而仅在必要时以管理员权限登录。但是这并不意味着你就要以域的 Administrator 这个账户登录。

如果你的企业有多个网络管理员，那么应该给每个网管创建一个个人的管理员账号。这样做可以让管理员知道每一项网络管理工作都是谁操作的。比如，公司有个网管叫 John Doe，你就应该给这个管理员建立两个账号。其中一个是具有普通用户权限的账号，用于日常工作，另一个是具有管理权限的账号，只在需要进行管理操作时才使用。这两个账户可以叫做 JohnDoe 以及 Admin-JohnDoe。

5: 监控记录不要太多

很多网管都喜欢建立审查策略，记录每一个系统事件，但是系统发生的事件太多了，大部分都是良性的。如果将所有系统事件都记录下来，那么审计日志将迅速膨胀，管理员将很难从中找到自己所需的内容。因此，与其将所有事件都记录下来，不如只选择记录那些可能造成问题的事件。

6: 利用本地安全策略

使用基于活动目录的组策略并不意味着就可以不用设置本地安全策略了。记住，组策略只针对那些使用域账号登陆的用户才有效。如果有人以本地用户账户登陆，则不会受到组策略限制。本地安全策略此时就可以帮助网管来保护系统安全。

7: 检查防火墙配置

企业应该通过防火墙来保护网络以及网络中的每一台电脑，但是这并不表示有了防火墙就足够了。网管应该定期检查防火墙的端口异常日志，确保只开放了必须的端口。

重点关注的端口是 Windows 系统常用的各个端口，另外还要在防火墙规则中注意 1433 和 1434 端口。这两个端口是用来监控和远程连接 SQL 服务器的，也是黑客最喜欢利用的端口。

8: 隔离服务

如果可能，你应该为每个服务器设置它专属的工作内容。一旦某个服务器被黑客入侵，那么黑客也只能获取相应服务内容的访问权限。我注意到由于财务压力，很多企业的服务器都在身兼数职。在这种情况下，企业可以通过虚拟化技术，再不怎么增加成本的前提下尽可能提高安全性。在一些环境下，微软可以让企业实现多个运行 Windows Server 2008 R2 系统的虚拟服务器，而只需要一个服务器操作系统许可证。

9: 及时为系统打安全补丁

在给服务器打补丁之前，管理员最好先测试一下补丁的效果。但是大部分企业都跳过了这一步。虽然我不反对确保服务器稳定是很重要的，但是管理员最好能对某些补丁的效果进行测试，做到万无一失。

微软每次推出的系统补丁都是在有充分理由(确有漏洞存在)的前提下进行的。这意味着黑客已经知道该漏洞的存在，甚至正在开发工具用来探查互联网上的系统是否由于没有正确安装补丁包。

10: 使用 Security Configuration Wizard

Security Configuration Wizard 可以让管理员建立基于 XML 语言的安全策略并应用到服务器上。该策略可用于启动服务器功能，进行系统配置，设置防火墙规则等。但是要记住，通过 Security Configuration Wizard 创建的策略与安全模板(后缀.INF)不同。而且，你也不能用组策略来部署 Security Configuration Wizard 创建的策略。

来源：ZDNet 系统安全

免责声明