安全威胁每周警讯

2010/03/13～2010/03/20

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。
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_HIFRM.A-CN	网页感染	★★★	↑	该病毒通常是用户访问网页时感染，一旦使用者访问了插入恶意脚本的网站，可能会在不知情的状况下下载病毒文件，或连接到其他恶意网站。
7	Cryp_Xed-12	木马病毒	★★★	↓	疑似病毒
8	GRAY_Gen	灰色软件	★★★	↓	智能检测技术检测出的后门类病毒,需要收集样本后进一步分析
9	CRCK_KEYGEN	破解程序	★★	↑	非法破解程序
10	HTML_IFRAME.AZ	网页感染	★★★	↓	该病毒通常是用户访问网页时感染，一旦使用者访问了插入恶意脚本的网站，可能会在不知情的状况下下载病毒文件，或连接到其他恶意网站。

系统漏洞信息

MS10-013: Microsoft DirectShow 中的漏洞可能允许远程执行代码

受影响的系统:

Windows 2000

Windows XP

Windows Server 2003

Windows Vista

Windows Server 2008

Windows 7

描述: 请见http://www.microsoft.com/china/technet/security/bulletin/MS10-013.mspx

系统安全技巧

摘要: 我们可以通过设置各个文件夹的权限，来让 apache 用户只能执行我们想让它能干的事情。本文将介绍网站服务器如何有效防御 PHP 木马攻击?

1、防止跳出 web 目录

首先修改 httpd.conf，如果你只允许你的 php 脚本程序在 web 目录里操作，还可以修改 httpd.conf 文件限制 php 的操作路径。比如你的 web 目录是/usr/local/apache/htdocs，那么在 httpd.conf 里加上这么几行:

php_admin_value open_basedir /usr/local/apache/htdocs

这样，如果脚本要读取/usr/local/apache/htdocs 以外的文件将不会被允许，如果错误显示打开的话会提示这样的错误:

Warning: open_basedir restriction in effect. File is in wrong directory in

/usr/local/apache/htdocs/open.php on line 4

等等。

2、防止 php 木马执行 webshell

打开 safe_mode，

在，php.ini 中设置

disable_functions= passthru，exec，shell_exec，system

二者选一即可，也可都选

3、防止 php 木马读写文件目录

在 php.ini 中的

disable_functions= passthru，exec，shell_exec，system

后面加上 php 处理文件的函数

主要有

fopen，mkdir，rmdir，chmod，unlink，dir

fopen，fread，fclose，fwrite，file_exists

closedir，is_dir，readdir.opendir

fileperms.copy，unlink，delfile

即成为

disable_functions= passthru，exec，shell_exec，system，fopen，mkdir，rmdir，chmod，unlink，dir，

fopen，fread，fclose，fwrite，file_exists，

closedir，is_dir，readdir.opendir，

fileperms.copy，unlink，delfile

ok，大功告成，php 木马拿我们没辙了，遗憾的是这样的话，利用文本数据库的那些东西就都不能用了。

如果是在 windos 平台下搭建的 apache 我们还需要注意一点，apache 默认运行是 system 权限，这很恐怖，这让人感觉很不爽.那我们就给 apache 降降权限吧。

net user apache fuckmicrosoft /add

net localgroup users apache /del

ok.我们建立了一个不属于任何组的用户 apche。

我们打开计算机管理器，选服务，点 apache 服务的属性，我们选择 log on，选择 this account，我们填入上面所建立的账户和密码，重启 apache 服务，ok，apache 运行在低权限下了。

实际上我们还可以通过设置各个文件夹的权限，来让 apache 用户只能执行我们想让它能干的事情，给每一个目录建立一个单独能读写的用户。这也是当前很多虚拟主机提供商的流行配置方法哦，不过这种方法用于防止这里就显的有点大材小用了。

来源：ZDNET