安全威胁每周警讯

2011/08/20～2011/08/27

本周威胁指数

***TrendMicro* 中国区网络安全监控中心**

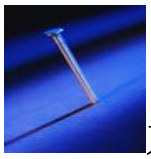
前十大病毒警讯

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	JS_EXPLOIT.SMAD	木马	★★★	↑	这是使用趋势科技智能检测功能所检测出的疑似 Java 脚本病毒程序
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_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
8	ACM_AGENT.AVGL	脚本病毒	★★	↑	AutoCad 脚本病毒
9	TROJ_LAMEWAR.VTG	木马	★★	↑	该木马病毒嵌套在一些广告/灰色/共享软件中，用户在安装这些软件的时候会被执行
10	WORM_VB.DVP	蠕虫	★★	↑	蠕虫病毒，通过访问恶意站点下载感染。感染该病毒后会在每个盘符下生成 autorun.inf 文件已达到用户在访问磁盘时执行该病毒

系统漏洞信息

MS11-065：远程桌面协议中的漏洞可能允许拒绝服务
Windows XP
Windows Server 2003

描述：http://www.microsoft.com/china/technet/security/bulletin/MS11-065.mspx



系统安全技巧

多年来，微软的互联网信息服务（IIS）Web 服务器给许多企业带来了大量的安全问题，包括十二年前臭名昭著的 Code Red 蠕虫病毒。IIS 的一个重要安全隐患是它会默认安装和启用很多功能，比如脚本和虚拟目录等，但这其中的许多功能又被证实是很容易被利用，从而导致重大安全事故。

几年前发布的 IIS 6 采用了一种“默认锁定”的方法，即不安装某些功能，或者安装以后将其默认禁用，而最新版本 IIS 7 则采取了更多措施。Windows Server 2008 甚至没有默认安装 IIS 7，而在安装的时候，IIS 7 网络服务器经过配置后只提供具有匿名身份验证和本地管理的静态内容，虽然生成的只是最简单的网络服务器，但却把受到安全攻击的几率降至最小。

做到这一点是可能的，因为 IIS 7 已被完全模块化。让我们简单的研究一下 IIS 7 更加安全的原因，以及它的安全性是如何实现的。通常而言，管理员可以从 40 多个单独的功能模块中做出选择，实现完全自定义的安装。通过只安装某个网站所需要的功能，管理员可以大大减小潜在的攻击面，并且节省资源。

然而，请注意这只适用于清洁安装（clean install）。如果你在运行老版本的 IIS，你又要升级你的 Windows 操作系统，所有的元数据库和 IIS 状态信息都会被收集并保存。结果，许多不必要的 Web 服务器功能会在升级时被安装到系统中。因此，企业在升级之后最好重新查看应用程序对 IIS 功能的依赖性，并卸载不需要的 IIS 模块。

更少的组件意味着更少的设置管理，以及更少的问题修补，因为人们只需要维护那些正在使用的模块附属内容。这样可以减少停机时间并提高可靠性。此外，标签混乱的 IIS 管理控制台已经被更加直观的 GUI 工具所取代，这让安全设置的可视化更加简单，理解起来也更加容易。比如，如果支持基本身份验证的组件

没有安装在你的系统中，该组件的配置设置就不会出现，以免混淆视听。

那么，安全运行 IIS 可能需要哪些组件呢？下面列出的九个组件中，运行静态网页以及其他功能的网站都需要前六个；而需要加密服务器与客户端之间数据的人则需要第七和第八项；当你拥有一个 Web farm，并且想要 farm 中每个 Web 服务器都使用相同的配置文件和加密密钥时，你将需要第九项共享配置：

1、验证组件，其中包括集成 Windows 验证、客户端证书验证以及基于 ASP.NET 格式的验证，这些验证可以让你在应用层上管理客户端注册和验证，而不是依靠 Windows 账户。

2、URL 验证，它很好地与 ASP.NET 会员和角色管理整合，然后根据用户名和角色来授权或者拒绝应用程序中的 URL，防止没有授权的用户去访问受限制的内容。

3、IPv4 地址和域名规则（Domain Name Rules）提供了基于 IP 地址和域名的内容访问管理。新属性“allowUnlisted”可以更容易的阻止人们访问所有的 IP 地址，除非列表中允许。

4、CGI 和 ISAPI 约束，它们允许你用 CGI 文件方式（.exe）和 ISAPI 扩展方式（.dll）启用或禁用动态内容。

5、请求过滤器，它结合了 UrlScan 工具中限制 HTTP 请求类型的功能，IIS 7 将会拒绝这些包含可疑数据的请求。像 Apache 的 mod_rewrite 属性一样，它可以用正则表达式来阻止攻击或者基于动词、文件扩展名、大小、命名空间和时序的修改请求。

6、日志，它现在可以提供有关应用程序池、进程、网站、应用程序域和运行请求的实时状态信息，并且能够在整个请求与应答过程中跟踪某个请求。

7、服务器证书

8、安全套接层

9、共享配置

其他增强 IIS 7 安全性的功能还包括：Web 服务器专用的新型内置用户帐户和组帐户。该功能启用了一个系统之间通用的安全标识符（SID），从而简化了访问控制列表管理，以及应用程序池保护机制（sandboxing）。同时，应用程序管理员可以配置哪些设置，服务器管理员都能完全控制，同时让他们直接在应用程序上做出配置的改变，无需使用管理权限去访问服务器。

IIS 7 与以前的产品相比非常不同，这对用户来说是一件好事。它的设计与创建遵循了经典的安全原则，它为使用 Windows 系统的企业提供了一个比过去更加安全的、更容易配置和管理的 Web 服务器。从安全的角度看，它可能还做得不够，还不能动摇 Linux 和 Apache 工作站的地位，但是微软的确已经缩小了与它们

的差距。管理员可能还需要一段时间来适应新的模块化方式以及管理工具和任务。尽管管理员都熟悉 Windows 操作系统和框架，但仍需要培训和进行系统测试。

来源：51CTO