安全威胁每周警讯

2011/03/20～2011/03/26

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	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_SPNR.03CG11	木马	★★	↑	该木马程序是一个恶意软件，但危险低，不具备自动传播到其他系统的能力。它通常是从网上下载，并在用户不知情的情况下自动安装。 通常携带有效载荷木马或其他恶意行为，可从轻度恼人的范围到无可挽回的破坏。他们也可以修改系统设置为自动启动。
4	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
5	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
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	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
8	TROJ_GEN.USEGB28	木马	★★	↑	该木马程序是一个恶意软件，但危险低，不具备自动传播到其他系统的能力。它通常是从网上下载，并在用户不知情的情况下自动安装。
9	Dialer_Win32Dial	拨号软件	★★★	↑	这是个拨号器文件/组件。 它尝试修改的 Internet Explorer（IE）的主页，直接影响用户浏览网站。
10	ACM_AGENT.AVGL	脚本病毒	★★	↓	AutoCad 脚本病毒

系统漏洞信息

MS11-004:Internet Information Services (IIS) FTP 服务中的漏洞可能允许远程执行代码 (2489256)

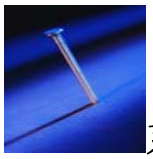
受影响的软件:

Windows Vista

Windows 2008

Windows 7

描述: 请见http://www.microsoft.com/china/technet/security/bulletin/MS11-004.mspx



系统安全技巧

摘要: SQL 注入攻击的原理本身非常简单，相关攻击工具容易下载，攻击者获得权限后有利可图。针对这一攻击手段，安全专家认为，最根本的措施是对 Web 应用的用户输入进行过滤。并针对 Web 应用的基本特性，对 Web 应用的整体安全工作采取以下具体措施。

随着 B/S 模式应用开发的发展，使用这种模式编写应用程序的程序员也越来越多。但是由于程序员的 水平及经验参差不齐，相当大一部分程序员在编写代码的时候，没有对用户输入数据的合法性进行判断，使应用程序存在安全隐患。所谓 SQL 注入，就是通过把 SQL 命令插入到 Web 表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令，比如先前的很多影视网站 VIP 会员密码泄露 大多就是通过 Web 表单递交查询字符实现的，这类表单特别容易受到 SQL 注入式攻击。

SQL 注入攻击的原理本身非常简单，相关攻击工具容易下载，攻击者获得权限后有利可图。这使得它成为最有效的、攻击者最常采用的 Web 入侵手段，是众多网站成为恶意代码传播平台的起因之一。

针对这一攻击手段，安全专家认为，最根本的措施是对 Web 应用的用户输入进行过滤。并针对 Web 应用的基本特性，对 Web 应用的整体安全工作采取以下具体措施:

1、Web 应用安全评估: 结合应用的开发周期，通过安全扫描、人工检查、渗透测试、代码审计、架构分析等方法，全面发现 Web 应用本身的脆弱性及系统架构导致的安全问题。应用程序的安全问题可能是软件生命周期的各个阶段产生的，其各个阶段可能会影响系统安全的要点主要有:

2、Web 应用安全加固: 对应用代码及其中间件、数据库、操作系统进行加固，并改善其应用部署的合理性。从补丁、管理接口、账号权限、文件权限、通信加密、日志审核等方面对应用支持环境和应用模块间部署方式划分的安全性进行增强。

3、对外部威胁的过滤: 通过部署 Web 防火墙、IPS 等设备，监控并过滤恶意的外部访问，并对恶意访问进行统计记录，作为安全工作决策及处置的依据。

4、 Web 安全状态检测: 持续地检测被保护应用页面的当前状态，判断页面是否被攻击者加入恶意代码。同时通过

检测 Web 访问日志及 Web 程序的存放目录，检测是否存在文件篡改及是否被加入 Web Shell 一类的网页后门。

5、事件应急响应：提前做好发生几率较大的安全事件的预案及演练工作，力争以最高效、最合理的方式申报并处置安全事件，并整理总结。

6、安全知识培训：让开发和运维人员了解并掌握相关知识，在系统的建设阶段和运维阶段同步考虑安全问题，在应用发布前最大程度地减少脆弱点。

在现在和将来，由于受互联网地下黑色产业链中盗取用户账号及虚拟财产等行为的利益驱动，攻击者仍 将 Web 应用作为传播木马等恶意程序的主要手段。尽管这会对广大的运维人员和安全工作者造成很大的工作压力，但是通过持续不断地执行并改进相关安全措施， 可以最大限度地保障 Web 应用的安全，将关键系统可能发生的风险控制在可接受的范围之内。

来源： 51CTO