安全威胁每周警讯

2012/06/17～2012/06/23

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	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
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	Cryp_Xed-12	疑似病毒	★★★	↑	疑似木马病毒，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	CRCK_KEYGEN	黑客程序	★★	↓	非法破解程序
7	X97M_LAROUX.BK	宏病毒	★★	↑	宏病毒，主要通过用户浏览恶意网站感染，该病毒主要感染 Office Excel 文件，并且会在 Excel 中创建一个名为 StartUp 的宏脚本
8	X97M_LAROUX.CO	宏病毒	★★	→	宏病毒，主要通过用户浏览恶意网站感染，该病毒主要感染 Office Excel 文件，并且会在 Excel 中创建一个名为 StartUp 的宏脚本
9	PAK_Generic.001	加壳文件	★★	↓	经过加壳技术加密的文件
10	WORM_ECODE.E-CN	蠕虫	★★	↑	它通过将受感染的移动驱动器与系统连接起来而入侵。 它可能是由远程站点的其他恶意软件/灰色软件/间谍软件下载而来。 它可能是用户在访问恶意网站时在无意中下载而来。

系统漏洞信息

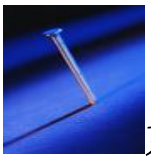
MS12-033 ： Windows 分区管理器中的漏洞可能允许特权提升 (2690533)

Windows Vista

Windows 7

Windows Server 2008

描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS12-033



系统安全技巧

现在几乎所有企业都会在互联网上建立网站，他们不仅通过网站提供信息，而且还通过 Web 应用程序、博客和论坛与他们的客户进行互动。从网上零售商的互动婴儿注册表，到电子交易网站的投资计算器，或者软件供应商的互动支持论坛，企业每天都会产生新的 Web 应用程序来使获取信息。

以业务为中心的 Web 互动迅速发展也带来了新的信息安全威胁，而企业以前的静态网页并没有这些威胁。这些威胁主要是针对 Web 应用程序，包括补充的 Web 服务器、数据库和其他支持基础设施。

在本文中，我们将讨论 Web 应用程序面临的最严重的威胁以及安全团队应该如何保护应用程序。

Web 应用程序面临的紧迫威胁

多家供应商评估了当今企业面临的 Web 应用程序威胁，其中最常见的两种 Web 应用程序威胁是跨站脚本（XSS）和 SQL 注入攻击。这两种攻击已经存在多年了，但 Web 应用程序仍然容易受到它们的困扰。

鉴于这两种攻击的广泛影响范围以及丰富的攻击工具，企业必须加强 Web 应用程序安全性来降低攻击风险。虽然新的 Web 应用程序威胁也已经出现，但是大多数攻击仍然是利用这些最基本的薄弱点。

如何让 Web 应用程序更加安全

安全团队可以采用一些基本的方法来加强 Web 应用程序的安全性，包括改善 web 应用程序开发和部署新工具来帮助管理 Web 应用程序面临的新信息安全风险。这些方法应该配合使用，而不是单独使用，同时部署其他安全控制。

改善 Web 应用程序开发来提高 Web 应用程序的安全性应该作为任何软件或安全开发生命周期的一部分。在软件开发生命周期（SDLC）方面有很多资源，例如微软以及美国国土安全部网络安全处提供的资源。开放 Web 应用程序安全项目（OWASP）也提供了开发指南，包括 Development Guide 2010，其中讨论了安全 Web 应用程序开发的方法。作为软件开发生命周期的一部分，用户可能需要定期检查 Web 应用程序面对的最普遍

的威胁，并且定期更新威胁列表。所有这些技巧都可以用于培训开发人员以改善应用程序，确保最小化安全漏洞，更快发现漏洞和更快修复漏洞。

另外，缓解 Web 应用程序威胁的其他重要方法包括部署新工具来帮助管理 web 应用程序安全。这些工具可能并不是真正意义上的新工具，但是对于很多企业而言，Web 应用程序防火墙和 Web 应用程序安全扫描仪等产品从来没有列入考虑范围，因为他们能够规避规定使用这些产品的合规要求，或者说因为 web 威胁从来不是他们的重点关注问题。

然而，这些和其他相关的新兴 Web 防御技术可以成功地阻止 web 应用程序层攻击以及扫描 web 应用程序漏洞。Web 应用程序安全扫描仪可以涵盖在你的软件开发生命周期测试阶段，或者作为一个独立的项目，以积极地评估你的 web 应用程序的安全状态。Web 应用程序防火墙能够对攻击 Web 应用程序的网络流量进行检查，阻止最常见的攻击。但是 Web 应用程序防火墙和 Web 应用程序安全扫描仪并不能阻止或者检测所有攻击或者漏洞，这些工具需要不断更新以发现新威胁。

这些工具扩展你现有安全控制，但同时你应该了解紧迫的威胁如何绕过很多传统的安全控制。例如，如果你允许 HTTP 通过端口 80 到你的防火墙再到 web 服务器，你的防火墙通常无法判断该网络流量是否是合法 HTTP 流量，或者是否有用于 SQL 注入攻击的潜在恶意 SQL 代码。但 Web 应用程序防火墙可以检测 HTTP 流量，发现和（多数情况下）阻止大多数 SQL 注入攻击。请记住，没有哪个单一的安全工具或者控制方法可以保护所有企业的 web 应用程序，而结合使用 Web 应用程序防火墙和 web 安全扫描能够提供坚实的保护，来抵御最常见的 XSS 和 SQL 攻击。

结论

尽管新 web 应用程序能让企业与客户进行互动，改善与客户的关系，但这些 web 应用程序也带来了新的信息安全风险。传统安全控制本身通常无法抵御这些 web 应用程序威胁，不过，我们对传统控制进行扩展，将 web 应用程序安全融入软件开发生命周期，并部署新的 web 应用程序安全工具，可以帮助减小这些威胁的风险。那些没有使用这些技术或者没有计划这样做的企业应该仔细想想：这些应用可能会扩大他们潜在的 Web 安全威胁。对于当今企业信息安全计划而言，保护 web 系统免受新型威胁已经成为重要且优先的事项。

来源：51CTO