安全威胁每周警讯

2012/09/30～2012/10/06

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	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_DOWNAD.INF	木马	★★★	→	DOWNAD 蠕虫关联木马
4	X97M_OLEMAL.A	宏病毒	★★	→	宏病毒，它会将本身的下列副本放置到受影响的系统：%User Profile%\Application Data\Microsoft\Excel\XLSTART\k4.xls
5	CRCK_KEYGEN	加壳文件	★★	↑	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	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
7	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
8	PAK_Generic.001	加壳文件	★★	↑	经过加壳技术加密的文件
9	WORM_ECODE.E-CN	蠕虫	★★★★	→	E 语言病毒,产生与当前文件夹同名 exe 文件
10	TROJ_SPNR.15IH12	木马	★★★	↓	木马程序

系统漏洞信息

SQL 注入和跨站脚本仍然是最有针对性的 Web 应用漏洞，然而专家称，一些新技术（例如 HTML 5）本身就具有危险的漏洞。在 2012 年前两个季度之间，SQL 注入（SQLi）攻击上升了 69%。在 SQL 攻击中，攻击者将恶意代码输入 web 表单输入框以获取资源或更改数据。

排在漏洞榜首的是跨站脚本（XSS），在一个网站中至少存在一个 XSS 安全漏洞的可能性是 55%。在 XSS 攻击中，攻击者将恶意代码插入链接，看起来似乎是来自值得信赖的来源，通过点击链接，用户将释放嵌入式编程，这作为该客户端 web 请求的一部分被提交，并可以在用户的计算机上执行，从而让攻击者窃取信息。

安全专家称，其他漏洞虽然比主要漏洞的普及率更低，也没那么危险，但它们仍然构成威胁。授权问题引起越来越多的关注，即用户可以访问其授权级别以上的信息。还有一种业务逻辑漏洞，当两个安全步骤发生冲突时，最终会制造漏洞，这也是一个问题。

HTML 5——增长的攻击目标

最新版本的网页标准编程语言 HTML 5 旨在使 web 应用和文件在每种类型的浏览器中都是一致的，但这个新兴技术却带来新的威胁。HTML 5 对客户端方面的侧重使攻击者从用户角度实施攻击变得更容易。HTML 5 等新技术是危险的，因为威胁更难找到，开发者也更难以修复。当你引进新技术时，例如云计算和 HTML 5 等，你也带来了新的复杂性。对于攻击，HTML 5 更加滞后，因为攻击者坚持使用较旧的更广泛应用的编程语言，例如 Java。

新颖可能是保护不足的 HTML 5 面临的问题，但这并不是 SQL 注入和 XSS 攻击漏洞的理由，这两个漏洞已经有十多年的历史。安全专家称，在开发 web 应用时，安全并不是首要考虑问题。重点在于速度、功能和整体体验。“我们听说了很多关于安全的问题，也有各种相关新闻报道，”但当涉及安全因素时，应用开发人员意识到他们必须花费更多时间和金钱才能让产品得以发布，这使他们总是忽视安全因素。

当企业 IT 安全团队为 web 应用解决安全问题时，资金和重点往往在网络层面。企业将花更多钱在应用上，而不是专门针对这些应用的安全因素上。

缺乏具有安全意识的程序员

一些专家发现行业内普遍缺乏安全人员。“没有人来做这个工作。很多 SQL 注入和 XSS 攻击针对传统的旧代码，因为旧代码在较新版本中存在漏洞。有 15 年的不安全 web 代码需要我们清理。不过，新代码中的漏洞可以避免，只是在开发应用时，这些安全步骤有时候被忽略了。”

安全分析师认为参数化 SQL 语句是缓解 SQL 注入攻击的最佳途径之一。通过参数化语句，只有特定条目能被 web 表单的输入框接受，这是基于开发人员设置的限制。例如，他举了一个好的语句，“我的名字是 Jeremiah”，而“我的名字是 Jeremiah；”就会被拒绝。因为标点符号不被接受，这可以防止攻击者向输入框输入代码。对于 XSS，上下文感知

的输出编码是一个很好的防御。输入验证是可用于保护 web 应用免受 XSS 和 SQL 注入攻击的另一个方法。

在开发 web 应用时，重要的是在开发过程的每一步都考虑安全因素。确定在 web 应用的整个生命周期解决安全问题的三个角色：开发人员（builder）首先创建安全代码来开始这个过程，然后破坏者（breaker）进行测试并找出安全威胁，防御者（defender）专注于监测启动 web 应用后的攻击。

专家们认为，安全规范需要由公司高管来确定。只有通过高管施加压力，开发人员才会认真地编写代码、检查代码以及为安全措施（例如输入验证）编写额外代码。软件开发人员被聘请来工作，如果雇佣他们的人强调使用 web 应用的方便性和体验，那么最终的产品将会反映这一点。高管应该对其想要部署的安全措施给出明确的指示。

当在创建 web 应用的整个过程中都考虑了安全因素时，这最终可以节省时间和金钱，虽然这个优势在初期没有显现出来。例如，在开发过程快结束时，当审计员表示 web 应用不符合某个要求时。审计员会停止生产，让开发团队回去解决问题。在这种情况下，生产可能会被推迟一个星期，但如果最初采取了适当的安全措施的话，这可能只需要一两天。

最后，管理人员需要决定对于最终产品而言，什么是重要的。如果安全很重要，那么，企业将需要采取一切措施来保护其 web 应用。

来源：51CTO