安全威胁每周警讯

2012/01/22～2012/01/29

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	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	JS_AGENT.BBCK	脚本病毒	★★	↑	该程序为 Java 脚本病毒，通常是用户访问恶意网站是所感染的。
6	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
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	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
9	TROJ_DOWNAD.E	木马	★★★	↑	木马病毒，该病毒会在系统目录中产生随机数字的.TMP 文件
10	PE_PATCHED.ASA	文件感染型病毒	★★★	↑	文件感染性病毒，会感染电脑中的 EXE 可执行文件

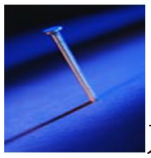
系统漏洞信息

MS12-002 ： Windows 对象包装程序中的漏洞可能允许远程执行代码 (2603381)

Windows XP

Windows Server 2003

描述： http://technet.microsoft.com/zh-cn/security/bulletin/MS12-002



系统安全技巧

随着新的一年日益临近，各企业也开始为未来的业务进程秣马厉兵，而这也正是我们着眼于流程与技术，并重新评估它们如何切实降低安全风险的最佳时机。在数据库级别的日常应用中，某些根本性措施在不少企业中仍然没能得到有效开展。

下面这份操作清单根据数据库安全专家们在 2011 年内所公布的意见汇总得出。认真学习并仔细考量能够为我们制定一套完善的安全计划带来巨大帮助，进而指导 2012 年及之后阶段的发展方针。

1. 确保我们的数据库无法轻易在网上被检索到

数家企业都在今年遭遇窘境，因为他们的 IT 部门在配置数据库时保留了面向网络的接口；在情况下，数据库本身将很容易被从网上检索到。

"当下存在的众多数据库都在处理来自不同位置、不同设备的访问请求方面下足了功夫。在大多数人的观念中，他们认为要对某台服务器进行访问，必须要通过其上运行的某款应用程序方可实现，而在应用程序之下的实际数据理应由于应用本身的安全性保障而同样比较安全，"RedSeal System 公司 CTO Mike Lloyd 博士如是说。"但大家的数据库就摆在那里，而且在很多情况下，从投入使用的那一刻开始，它就被配置成与网络相连的状态。"

2. 更好地对数据加以分类

当企业在尝试将数据库中的高价值数据与低敏感信息加以分类时，他们也就同时获得了按优先级别管理安全风险以及部署更有针对性的保护机制的能力。

"大中型企业在分类工作上做得仍然不够到位，"Verizon Business 首席主管 Chris Novak 指出。"在这些企业中，大家面对的是分布的世界各地的办公室、高校以及其它复合型设施。而问题在于，如果来自这么多分支机构的大量信息不能加以有效分类，那么原本只存在于其中一地的风险很可能扩散到整个整个体系中去。"

3. 确保密码以非纯文本形式存储

安全措施的一大核心内容是拨乱反正，而在大多数机构中，将数据库密码以纯文本形式存储就是这"乱"中最为致命

的疏漏之一。

"这种情况真的相当普遍，尤其是在那些大型乃至巨型规模的企业中更为明显--相比之下新兴企业由于自身业务刚刚起步，尽管处于高增长状态下，但却较少成为攻击者的目标，"Vormetric 公司市场营销与产品管理部门副总裁 Gretchen Hellman 如是说。

在匿名恶意组织的觊觎之下，这些密码基本上等于是处在开门揖盗的状态下。

4. 加强自身配置

如果让数据库安全专家给出一条能够对未来一年起到广泛辅助作用的提示，那就是提醒我们对数据库的现有疏漏进行修补。

在这方面，更新默认登录、系统削减过多的执行特权以及自动检测流程以找出存在隐患的流氓数据库都是降低安全风险的有效手段。

5. 检查明显的加密失误

尽管数据库加密工作在部署方面可谓蒸蒸日上，但其中仍然存在着大量失误，例如将数据库加密密钥存储在同一台服务器中以及使用过时的加密算法等等。

"如果大家对自己数据库中的敏感数据进行加密的话，有一种严重的违规行为需要当心，即将用于加密数据的密钥或者用于获取密钥的身份验证资格同加密数据存储在同一套数据库系统内，"Voltage Security 公司安全架构主管 Luther Martin 提醒道。"这么会导致我们在安全工作上所做的努力化为泡影。尽管表面上看来似乎整套体系似乎相当坚固，但事实上它基本没能提供什么有效的保护机制。"

6. 对投保三思而后行

许多机构都将希望寄托在言辞美妙、承诺诱人的数据故障保险政策上，意图以此作为对小概率突发事件的防范机制。但专家们认为这些保险规划中其实存在着许多值得注意的问题。

"与企业购买的其它各类保险项目不同，目前数据安全保险还没有一套标准化形式--也就是说计算机行业由于自身特性而存在一种不确定性，因此无法像常见的员工投保、财产投保一样采用普遍的责任划分，"Innovation 保险集团资深顾问兼创始人 Ty Sagalow 解释道。"另外，这类保险属于所谓盈余投保范畴，这意味着它们并非得到政府批准并备案过的项目，也就是说保险公司可以自主设定其条款及理赔条件。"

7. 部署一套有序的事故警示机制

许多安全专家都认为，对于大多数机构而言，遭遇安全事故其实可以算是种必然情况，惟一的区别在于具体的发生时间。有鉴于此，他们建议打造一套有序的事故警示机制，以期尽可能减少问题所带来的影响及损失。

"如果大家为此准备一套应对方案，那就表示你已经走在了大多数机构的前面，"灾后响应咨询公司 ID Expert 总裁兼创始人 Rick Kam 表示。"大部分管理者都准备了备份恢复计划、业务连续性计划，甚至针对火灾情况也准备了必要的方案；但由于事故警示机制不会显露出不可或缺的特性，因此人们往往忽略了这种能够大幅度降低损失的宝贵

方案。”

来源：51CTO

免责声明