安全威胁每周警讯

2011/08/07～2011/08/13

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

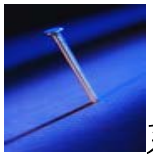
排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	TROJ_DOWNAD.INF	木马	★★★	→	DOWNAD 蠕虫关联木马
2	WORM_DOWNAD.AD	蠕虫	★★★★	→	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
3	WORM_DOWNAD	蠕虫	★★★★	↑	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
4	TROJ_IFRAME.CP	木马	★★★	↓	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	木马	★★	↑	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	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	Expl_ShellCodeSM	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
8	PAK_Generic.001	木马	★★	↑	加壳程序，疑似病毒文件
9	CRCK_KEYGEN	破解程序	★★	↑	非法破解程
10	TROJ_DLOADER.UVD	木马	★★	↑	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

系统漏洞信息

1.1. MS11-068：Windows 内核中的漏洞可能允许拒绝服务

Windows Vista
Windows Server 2008
Windows 7

描述：http://www.microsoft.com/china/technet/security/bulletin/MS11-068.mspx



系统安全技巧

面对安全，你可能会有很多问题，那么焦头烂额之际，你会问什么才是最好的企业数据库安全策略。随着网络攻击和互联网数据泄漏的增加，数据库安全也随即受到传统验证，授权许可和访问控制等企业信息安全团队的重视。

针对私有数据，如信用卡数据和金融数据的单一型入侵可以对企业造成集中性损害，更不用说会引发法律纠纷了。Forrester 研究公司建议企业重新制定自己的数据库安全策略，并寻求新的安全功能，用来应对新的威胁。

任何成功的数据库安全策略都需要了解保护每个数据库的意图，需要了解所保护的对象以及怎样保护数据免受各类威胁的袭击，维持各种规则的遵循——如 SOX，HIPAA，PCI DSS， GLBA 和欧盟指令行为。在最近的调查中，Forrester 推荐企业在下列三个基础之上创建一个综合的数据安全策略：

企业数据库安全策略 1. 用验证，授权，访问控制，恢复和分类以及分批管理来创建强大的基础。

了解哪个数据库包含敏感信息是对任何数据库安全策略提出的基本要求。企业应该保持对数据库的更新，创新及完整，包括产品与非产品，然后将其归类到应该遵循相同安全策略的不同目录。所有数据库，特别是那些保留有隐私数据的数据库应该具备强大的验证，授权和访问控制功能，即便是应用层也要进行验证和授权。如果缺乏强大的基础，那么其他安全措施，如审计，监控和加密就会逊色不少。

此外，如果不是每个季度都进行数据库修补的话，那至少应该半年为关键数据库进行修补，以此类消除已知的漏洞。调查数据库管理系统供应商发布的补丁和产品以便缩短应用数据库时产生的停工期。要经常在测试环境中测试安全补丁，运行常规测试脚本来确保这些补丁不会对应用程序的功能和性能有任何影

响。

企业数据库安全策略 2. 通过数据掩码，加密和更改管理采取防御性措施。

在创建好一个稳定的，基础型数据库安全策略后，就可以采取防御性措施保护关键数据库。这意味着要为产品和非产品数据库添加新的保护层。数据隐私不会止步于产品系统;我们应该同时扩展非产品环境，包括测试，开发，质量保证，分段传输和训练实例，特别是存储隐私数据的地方。数据库安全专家应该评估数据掩码的使用情况以及测试数据的生成以便在测试环境中或者外包应用开发的时候保护隐私数据。

可考虑用网络加密来防止数据泄漏或者对静态数据加密。在处理不同威胁的过程中，两种加密方法可以相互独立使用。通常，二者都不会对应用程序的功能产生影响。

我们还可以对管理进程进行规范化的修改以便保护重要的数据库结构。过去，生产环境中架构或数据库的更改需要先停止数据库的运行，但是新的 DBMS 允许在联机的数据库上进行修改操作，而这也带来了新的安全威胁。对管理进程进行规范化的更改确保管理员只在管理被核准后才能更改产品数据库，而管理员也可以跟踪所有更改。企业应该更新自己的恢复和可用计划以解决这类更改所带来的数据或元数据事故。

企业数据库安全策略 3. 用审计，监控和漏洞评估创建数据库侵入侦查。

不论重要的数据发生意料之外的更改还是我们发现有可疑数据发出访问请求。企业都需要尽快展开调查寻找事故缘由。数据库中的数据和元数据可以在数秒之内被访问，更改甚至是删除。数据库审计可以回答一些棘手的问题，如“谁改变了数据?”“何时更改了数据?”。要支持常规的标准，如前所述，安全和风险管理专家应该追踪对隐私数据(如信用卡号码，社交安全号码，重要数据库的姓名和地址)发出的所有访问和更改。如果隐私数据在未授权的情况下被访问或被更改，企业应该找到责任人追究责任。最后，漏洞评估报告可用来识别数据库环境中的安全缺陷，如较弱的密码，过量的访问优先权，补充型 DBA 和安全组监测。

企业数据库安全策略 4. 不要忘记安全策略，标准，角色分离和可用性。

数据库安全策略不仅仅是关乎审计和监控，还关乎端对端的进程设置，这些设置侧重于最小化风险，符合常规要求以及防御内部和外部攻击。数据库安全需要更广泛的关注，要弥补安全方面的不足，符合通用策略以及规范安全方案。当起草安全策略的时候，要协调数据库安全策略与信息安全策略间的关系，将重心放在行业安全标准上，促使角色分离，将数据恢复和数据可用性进程顺利连接起来。

来源：比特网

适销性、特定用途适用性以及不受侵害的暗示保证。用户对此邮件列表的准确性和使用承担全部风险，因依赖该资料所致的任何损失，趋势科技均不负责。