安全威胁每周警讯

2012/07/22～2012/07/28

本周威胁指数

***TrendMicro* 中国区网络安全监控中心**

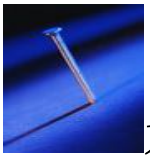
前十大病毒警讯

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	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.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
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	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
7	X97M_LAROUX.CO	脚本病毒	★★	→	Office 宏病毒，由其他恶意软件或访问恶意网站感染
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	Downloader_Agent	灰色软件	★★	→	这灰色软件下载器会自动下载并安装额外的其他的灰色软件，如广告软件和间谍软件。
10	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

系统漏洞信息

MS12-043 ： Microsoft XML Core Services 中的漏洞可能允许远程执行代码 (2722479)

Windows XP
Windows Vista
Windows 7
Windows Server 2003
Windows Server 2008
Windows Server 2008 R2
Microsoft Office 2003
Microsoft Office 2007
描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS12-043



系统安全技巧

一、内部人员错误

数据库安全的一个潜在风险就是“非故意的授权用户攻击”和内部人员错误。这种安全事件类型的最常见表现包括：由于不慎而造成意外删除或泄漏，非故意的规避安全策略。在授权用户无意访问敏感数据并错误地修改或删除信息时，就会发生第一种风险。在用户为了备份或“将工作带回家”而作了非授权的备份时，就会发生第二种风险。虽然这并不是一种恶意行为，但很明显，它违反了公司的安全策略，并会造成数据存放到存储设备上，在该设备遭到恶意攻击时，就会导致非故意的安全事件。例如，笔记本电脑就能造成这种风险。

经常进行用户权利的检查可以使审计人员、IT 顾问等知道企业的数据所有权、访问控制、对敏感信息的权利等详细信息。这个过程可以使企业确立有效的责任分离制度，更好地满足合规要求。

监视责任的分离变得日益重要。适当的访问权限是一个关键的安全问题，责任分离的控制是合规要求的一个基本原则。

为确保这些无意的违反不会发生，企业应当将关键的保护从网络和 Web 应用程序层扩展到数据库。常规的数据库安全评估包括审计和渗透测试，而且应当执行错误配置的检查，以尽量减少这些风险。此外，还可以实施活动监视，以保证不会无意下载或传输敏感数据。

二、社交工程

由于攻击者使用的高级钓鱼技术，在合法用户不知不觉地将安全机密提供给攻击者时，就会发生大量的

严重攻击。这些新型攻击的成功，意味着此趋势在 2012 年继续。在这种情况下，用户会通过一个受到损害的网站或通过一个电子邮件响应将信息提供给看似合法的请求。应当通知雇员这种非法的请求，并教育他们不要做出响应。此外，企业还可以通过适时地检测可疑活动，来减轻成功的钓鱼攻击的影响。数据库活动监视和审计可以使这种攻击的影响最小化。

三、内部人员攻击

很多数据库攻击源自企业内部。当前的经济环境和有关的裁员方法都有可能引起雇员的不满，从而导致内部人员攻击的增加。这些内部人员受到贪欲或报复欲的驱使，且不受防火墙及入侵防御系统等的影响，容易给企业带来风险。

常见的内部人员攻击包括口令猜测或窃取、特权提升、数据窃取、恶意软件部署、拒绝服务攻击等。例如，如果某雇员准备离职，在对目前的公司不满时，就有可能访问并窃取大量的私密文档。这表明，仅有防火墙和网络安全是远远不够的。企业应定期执行用户权力的检查、评估漏洞并监视特权活动（包括受信任的雇员和合伙人）等，这至关重要。

在不少企业，很多人可以访问需要特定权限才能访问的数据。或者，雇员拥有过高的权限，可被用于访问敏感数据。从本质上讲，公司网络上的通道越多，利用网络访问点的机会就越多，企业就更容易遭到攻击。

在任何企业中，知道最敏感的数据在哪里至关重要。首要的一步是全面分析哪些用户可以访问每个系统，他们可以访问哪些数据和功能，根据用户的业务功能验证用户是否被授予了适当的访问水平。具有前瞻性思维的企业必须主动地实施用户权利的最佳实践，确保将数据的适当访问和所有权分配给机密数据。如果不执行全面的用户权利检查，就会增加企业的数据访问被滥用的风险，并增加不遵守合规要求的风险。

对关键系统建立强健的基于策略的访问和活动监视可以阻止内部人员攻击。活动监视和审计提供对可疑活动的警告功能，从而可以对可疑活动及时采取行动。数据库安全解决方案允许 IT 和安全人根据不同的活动类型设置不同的警告级别，可以用不同的格式智能地过滤这些警告，并根据预先定义的策略来定义用户组或个人。

管理员应当为插入、更新、删除等命令创建存储过程。在存储过程中，管理员可以将一条记录插入到日志表中，要记录所需要的细节。管理员可以用存储过程来撤销对数据库表的插入、更新、删除等语句。注意，属于特定角色（如 db_owner）的任何人仍能够直接对表进行操作。

管理员还应当对表的更新、插入、删除等建立触发器。在触发器中，可以将任何东西记录到日志表中。通过此法，可以将所有的数据修改操作记录下来，而不管其实现方式（直接的 SQL 语句或通过存储过程）。

四、错误配置

黑客可以使用数据库的错误配置控制“肉机”访问点，借以绕过认证方法并访问敏感信息。这种配置缺陷成为攻击者借助特权提升发动某些攻击的主要手段。如果没有正确的重新设置数据库的默认配置，非特权用户就有可能访问未加密的文件，未打补丁的漏洞就有可能导致非授权用户访问敏感数据。

1、修复默认的、空白的、弱口令。确保所有的数据库都拥有复杂的口令，并清除空白的、默认的及弱

口令。要保证每一个实例都使用独立的口令，要强化企业当前正在使用的口令策略，并将其扩展到所有的网络登录中。如果数据库支持，可以考虑使用网络认证，如活动目录，而不使用用户名和口令认证。

2、加密静态和动态的敏感数据。不要把敏感数据以明文形式存放到数据库中的表中。通过修复数据库漏洞，并密切监视对敏感数据存储的访问，数据库专业人员可以发现并阻止攻击。防御 SQL 注入攻击要求一种多层的方法，保护措施必须与端到端的检查结合起来，这意味着无论是 Web 应用程序还是数据库的基础架构都要纳入到解决方案中。

五、未打补丁的漏洞

如今攻击已经从公开的漏洞利用发展到更精细的方法，并敢于挑战传统的入侵检测机制。漏洞利用的脚本在数据库补丁发布的几小时内就可以被发到网上。当即就可以使用的漏洞利用代码，再加上几十天的补丁周期（在多数企业中如此），实质上几乎把数据库的大门完全打开了。

使用专业工具发现并修复这些漏洞，然后再结合监视没有打补丁的漏洞可以保护企业免受这种风险。

六、高级持续性威胁

之所以称其为高级持续性威胁，是因为实施这种威胁的是有组织的专业公司或政府机构，它们掌握了威胁数据库安全的大量技术和技巧，而且是“咬定青山不放松”“立根原在‘金钱（有资金支持）’中”,“千磨万击还坚劲，任尔东西南北风”。这是一种正甚嚣尘上的风险：热衷于窃取数据的公司甚至外国政府专门窃取存储在数据库中的大量关键数据，不再满足于获得一些简单的数据。特别是一些个人的私密及金融信息，一旦失窃，这些数据记录就可以在信息黑市上销售或使用，并被其它政府机构操纵。鉴于数据库攻击涉及到成千上万甚至上百万的记录，所以其日益增长和普遍。通过锁定数据库漏洞并密切监视对关键数据存储的访问，数据库的专家们可以及时发现并阻止这些攻击。

小结：将安全作为一个过程

不少企业的安全解决方案是作为应对已知风险的一系列技术而部署的，而不是作为一种保障企业安全的综合方法和过程。安全并不是购买并部署了安全产品那么简单，它是一个需要持续关注的过程。例如，在企业部署了 Web 应用程序防火墙后，还应当经常检查其有效性和可用性，随着业务的开展而对其进行调整。再比如，在购买了某软件后，你还得关注它有没有漏洞，开发商什么时候提供补丁下载和安装。

此外，企业如果不把对雇员的教育放在首位，任何安全措施都会成为空谈。所以，构建一种能够随着企业的增长和变化而演变的系统化的动态过程，才能更有效地保障当今的动态环境。

来源：51CTO

赖该资料所致的任何损失，趋势科技均不负责。