安全威胁每周警讯

2011/05/22～2011/05/28

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	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	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
4	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
5	TROJ_DLOADER.UVD	木马	★★★	↑	该木马程序是一个恶意软件，但危险低，不具备自动传播到其他系统的能力。它通常是从网上下载，并在用户不知情的情况下自动安装。 通常携带有效载荷木马或其他恶意行为，可从轻度恼人的范围到无可挽回的破坏。他们也可以修改系统设置为自动启动。
6	Cryp_Xed-12	木马	★★★	↑	疑似病毒
7	WORM_ECODE.E-CN	蠕虫	★★★★	↓	E 语言病毒,产生与当前文件夹同名 exe 文件
8	CRCK_KEYGEN	网页病毒	★★	→	非法破解程序
9	TROJ_SPNR.03CG11	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
10	PAK_Generic.001	木马	★★★	↑	疑似病毒

系统漏洞信息

MS11-036: Microsoft PowerPoint 中的漏洞可能允许远程执行代码 (2545814)

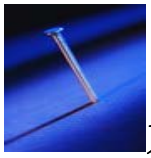
受影响的软件:

Microsoft Office XP Service Pack 3

Microsoft Office 2003 Service Pack 3

Microsoft Office 2007 Service Pack 2

描述: 请见http://www.microsoft.com/china/technet/security/bulletin/MS11-036.mspx



系统安全技巧

【你的存储安全吗?】

有很多文档，作者希望更多的人看到。你写了一篇博客，放到网上，当然希望点击率很高，粉丝越多越好。

但是也有很多文档，只限于自己和少数的人能够看到，你希望这些文档是保密的。比如：你的内部会议纪要，你的企业营销计划……

在这个开放的互联网时代，数据共享很容易。你几乎可以在任何时间，任何地方，以很多种方式，把文件发送给需要的人。

问题是，你希望保密的数据，能够真正地保密吗?你能够确保你的数据不会外泄吗?

如果你的计算机中了病毒木马，数据和文件你能够保证不被盗取吗?

如果你的计算机需要维护，你能够保证硬盘里的文档数据不会被拷走吗?

如果组织机构出现“内鬼”，你确定“内鬼”拿不走任何数据吗?

……

维基解密事件告诉我们，在这个世界上，即使是政府的机密文档，也有可能遭遇泄漏的危险。

政府机构高度机密的文档，尚且有这么多安全漏洞，企业网、个人计算机那就更不用提了。形形色色的“艳照门”、“日记门”事件，时时刻刻在提醒我们，如果数据存储不安全，任何组织和个人，随时有可能是下一个受害者。

在网络时代，有没有可靠的安全的存储?

【加密和认证是安全存储的基础】

从原理上来说，安全存储要解决的问题是两个，如何保证文件数据完整可靠不泄密?如何保证只有合法的用户，才能够访问相关的文件?

解决上述两个问题，需要使用数据加密和认证授权管理技术，这也是安全存储的核心技术。

在安全存储中，利用技术手段把文件变为乱码(加密)存储，在使用文件的时候，用相同或不同的手段还原(解密)。这样，存储和使用，文件就在密文和明文状态两种方式切换。既保证了安全，又能够方便的使用。

加密包括两个元素：算法和密钥。

对数据加密的技术分为两类，即对称加密(私人密钥加密)和非对称加密(公开密钥加密)。对称加密以数据加密标准(DES，Data Encryption Standard)算法为典型代表，非对称加密通常以 RSA(Rivest Shamir Ad1eman)算法为代表。对称加密的加密密钥和解密密钥相同，而非对称加密的加密密钥和解密密钥不同，加密密钥可以公开而解密密钥需要保密。

一般来说，非对称密钥主要用于身份认证，或者保护对称密钥。而日常的数据加密，一般都使用对称密钥。

现代的成熟加密解密算法，都具有可靠的加密强度，除非能够持有正确的密钥，否则很难强行破解。在安全存储产品实际部署的时候，如果需要更高强度的身份认证，还可以使用 U-key，这种认证设备，在网上银行应用很普遍。

采用加密和身份认证技术，存储就有了可靠的保障。

【安全存储应用漫谈】

安全存储本质上还是存储，可以作为文件和数据的存放中心。与一般的存储相比，它更安全更可靠，能够胜任需要保密的领域。

安全存储以其可靠、加密、授权认证这些功能特点，在很多具体的存储应用中，可以发挥其特长：

作为主存储设备，安全存储可以实现“数据集中，客户端不留密”。例如：在一个工作组中，把安全存储作为唯一存储节点，所有的工作数据都集中到安全存储服务器上。工作机可以采用无盘工作站等方式，也可以封堵 USB 口、打印口等输出设备。这样， 可以作为文件归档管理服务器。将需要归档的数据，以加密的方式，存放在安全存储系统中。在需要查询和调阅的时候，由授权用户存取访问。

作为文档备份服务器。将个人的工作文档，备份存放在安全存储服务器上。认证体系确保只有本人才能够存取这些文件，密码体系保证只有本人能够加密解密这些文件。

用于服务器后台存储设备，需要发布的信息，以明文的方式发布，而其他的数据，就以加密的方式，存放在后台的服务器上。例如：Web 页的后端存储。

前面描述的，是几个典型的应用场景。 实际上，在任何需要保护存储数据文件的地方，安全存储都可以发挥用

武之地。

来源：中国软件网

免责声明