安全威胁每周警讯

2012/04/01～2012/04/07

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	Cryp_Xed-12	疑似病毒	★★★	↑	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	JS_MALAGENT.CEOX	脚本病毒	★★	→	该病毒为 Java 脚本病毒，通常是用户访问恶意网站是所感染的。
7	CRCK_KEYGEN	黑客程序	★★	↑	非法破解程序
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	PAK_Generic.001	加壳文件	★★	↑	经过加壳技术加密的文件

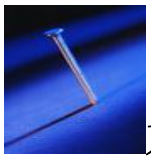
系统漏洞信息

MS12-012 ：颜色控制面板中的漏洞可能允许远程执行代码 (2643719)

Microsoft Windows Server 2008

Microsoft Windows Server 2008 R2

描述： http://technet.microsoft.com/zh-cn/security/bulletin/MS12-012



系统安全技巧

1、优化物理安全

安全行业有句老话：如果坏人可以获取计算机的物理控制，那就完蛋了。一旦他们拿到物理控制权，他们就可以使用各种工具来访问磁盘甚至是内存的数据，当然，他们还可以访问“p0wnd”计算机移出和移入的任何信息。所以说，在考虑部署其他安全方法之前，物理安全是首先要考虑的。

物理安全包括：

进入电脑机房的密钥、智能卡或者生物识别门控技术

对电脑机房进出情况的视频记录

对电脑机房进出情况的日志记录和报告

在电脑机房的入口和出口部署保安或者其他观察员

在防止攻击者攻入你的系统方面，物理安全能发挥很大作用。但是物理安全只是第一步，我们都非常清楚，如果计算机连接到网络，坏人不需要物理访问就能进行破坏活动。

2、使用基于主机的防火墙

网络防火墙似乎受到极大关注，网络防火墙确实有优点，但是很多人似乎夸大了它的保护能力。事实上，现在市面上大多数防火墙只能提供很小的安全保障，原因之一在于大多数最严重的攻击往往来自于网络内部，所以网络防火墙阻止外部用户访问内部网资源的功能似乎没有多大作用。

相比之下，基于主机的防火墙就能够保护企业资产阻止所有攻击者，无论时内部还是外部攻击者。此外，高级主机防火墙还可以配置为只允许计算机向用户提供的特定服务的入站连接。这些基于主机的防火墙(例如具有 AdvancedSecurity 的 Windows 防火墙)甚至可以要求用户或者机器再网络层进行身份验证，这样的话，没有通过验证或者没有授权的用户就不能进入应用程序层，应用程序层时大多数漏洞存在的地方，也是

所有数据存储的地方。

3、将你的网络划分为安全区

在涉及安全分区方面来看，前端 web 防火墙与数据库防火墙有所不同。托管公共可用文件的文件服务器与托管机密营销计划的 SharePoint 服务器也不相同。出战 SMTP 中继与反向 web 代理服务器不同，因为它们位于不同的安全区。

你应该将你的资源划分到不同的安全区，然后在这些区之间创建物理或者逻辑分区。如果你想要使用物理分区，你应该要确保分配到不同区域的资源有防火墙或者其他网络访问控制设备来分隔。如果你想要使用逻辑安全分区，你可以利用 IPsec 和服务器以及域名隔离来创建安全区之间的虚拟分区。

创建安全区可以让你集中安全力量，来保护最重要的资产。分配给较低安全区的不太重要的资产同样也受到了保护，但是你花在较低安全区的时间和精力相对要少得多，因为泄漏的成本比较高安全区的资产的成本要低得多。

4、对所有资产执行最小特权

最小权限原则是指用户和管理员只能访问他们的工作需要的资源和控制。用户只能访问他们工作需要访问的网站，他们只能使用工作需要使用的应用程序，而管理员只能进行符合他们权限的配置更改。

最近这段时间，最小权限的整个原则似乎已经改变了，但是最小权限的价值和有效性并没有改变。对于每个特权级别，如果用户或管理员拥有比其需要的更高权限，就增加了泄漏的风险。用户要使用 ipad 连接到企业资产，并不是好主意，我们经常迁就用户的需求，而不是考虑他们必须的东西。

对于管理员而言，这个问题更加重要，因为他们经常具有完整权限来进行任何操作。Exchange 管理员、数据库管理员、SharePoint 管理员、CRM 管理员和其他服务管理员都应该具有符合他们管理角色的访问控制权限。现代应用程序允许你将适当的权限分配给不同层次的管理员，可以利用这个功能来分配权限。

对于最终用户而言，为他们提供工作需要的服务和数据访问权限，防止他们访问其他资产。这同样适用于应用程序。如果应用程序没有位于批准名单上，那么使用自动化的方法来防止应用程序安装。

5、加密所有信息

使用 BitLocker 进行全磁盘加密可以很好的保护你的关键信息，甚至还可以帮助你防止物理泄漏。例如，如果有人从你的服务器机房窃取了一台服务器，攻击者会将驱动装再服务器上，读取文件系统，也就是所谓的离线攻击。好消息是使用 BitLocker 加密磁盘可以防止离线攻击。

但是整个磁盘加密不再仅限于内置硬盘驱动。在 Windows7 和 Windows Server2008R2 中，你可以在 USB 密钥、USB 驱动和其他类型的可移动媒介上使用磁盘加密。制定政策要求存储了公司数据的可移动媒介必须使用 BitLocker 加密。

连接到用户智能手机的可移动媒介也应该被加密。政策应该要求对智能手机操作系统的使用必须支持

microSD 卡加密，如果公司数据将存储在上面。存储在手机内置内存的数据也应该被加密，用户应该使用可以进行远程清除的手机，以防丢失和被盗的情况。

6、更新、更新、更新!

可能你已经知道这一点，但是提高企业整体安全状态的最有效的方法之一就是保持应用程序和安全更新的更新。虽然很多管理员会抱怨微软产品经常需要更新，事实上，微软比其他供应商更具安全意识，因为他们非常注重软件更新，如果你使用的软件的供应商很少更新，不要认为这样很安全。安全更新其实是供应商对其软件安全问题关注程度的反映。

更新应该尽可能快地完成，因为一旦安全补丁被发现，攻击者和黑客就已经知道漏洞，并会试图在补丁发布和用户安装补丁的时间内利用它们。这也就是“零日”期间，这也是漏洞最容易被利用的时间。如果你使用自动更新，那么漏洞利用期就会小得多。

然而，很多公司需要先对安全更新进行测试，因为他们有很多业务应用程序可能会受到每次安全更新的影响，所以他们需要提前测试兼容性问题。在这种情况下，你可以通过部署外围设备，这样就可以缩短关键漏洞利用时期。

7、使用安全身份验证机制

密码破解技术的不断发展使短密码很容易被发现，先进的破解技术甚至能够破解强度高的密码。如果你必须使用帐户和密码来作用你唯一的身份验证机制，那么必须要求所有密码必须使 15 个或更多字符组成，包括大写、小写、数字和非字母数字字符。使用对于用户有意义的复杂密码(通常简称为“密码短语”)可以让用户更好地记住密码。但是在越来越移动化的世界，还有另一个问题。虽然记住长密码短语很容易，但是将这么长的密码输入智能手机或者其他设备非常麻烦。

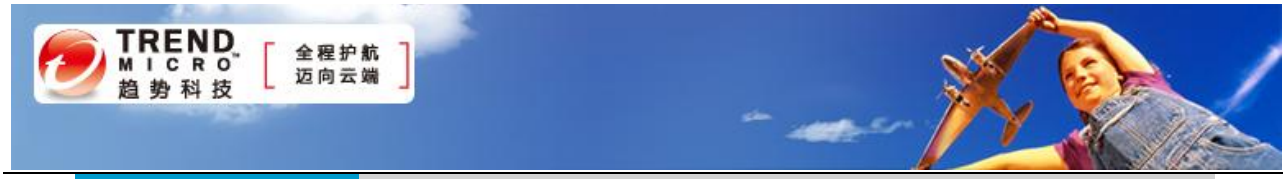
更好的方法就是双因素身份验证，这要求用户使用某种设备(例如智能卡或者令牌)以及密码(在 2FA 空间有时也被称为 PIN)。当使用双因素身份验证时，即使密码被破解了，仍然意义不大，除非攻击者拿到了设备本身。对于更安全的部署，应该添加额外的因素，例如语音识别、面部识别、指纹或者视网膜识别。

8、SecureAgainstDataLeakage

随着云计算对我们的生活带来越来越大的影响，基于网络的安全将开始对你的安全设计和购买具有更小的影响，因为安全将需要与数据更加靠近。这也是数据泄漏保护的用武之地。你可以对信息进行严格访问控制，所以只有授权用户能够访问信息。但是然后呢?授权用户可以怎样使用这个信息?可以将信息传给未授权用户吗?用户可以打印出来或者邮寄给别人吗?用户对其进行修改并放回存储库，而该信息应该设置为只读?

考虑一下如何保护授权用户对数据的操作。如果你在使用微软 Office 和 SharePoint 和 Exchange，你可以利用微软权限管理服务来制定政策，控制用户对信息的操作。

来源：51CTO



免责声明

该邮件列表仅用于提供信息，此邮件列表内容不负任何担保责任，没有明示或默示的保证，包括但不限于对适销性、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。