安全威胁每周警讯

2011/10/09～2011/10/015

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	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	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
5	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
6	PAK_Generic.001	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	木马	★★	→	非法破解程序
9	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
10	TROJ_SPNR.03CG11	木马	★★	↑	木马病毒

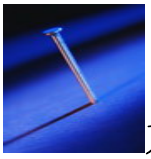
系统漏洞信息

MS11-080：辅助功能驱动程序中的漏洞可能允许特权提升

Microsoft Windows XP

Microsoft Windows 2003

描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS11-080



系统安全技巧

随着企业信息化管理的普及，网络安全在企业中的作用可以说日益重要。不过可惜的是，很多 IT 负责人对于内网安全这一块，还只是停留在口号上。对于安全方面的设计存在着种种弊病。笔者在这里做了一些总结，希望对各位提高内网的安全有一定的警示作用。

弊病一：客户端补丁升级依赖于员工的自觉

现在企业中大部分用户采用的都是 Windows 客户端。而这个客户端的特点就是补丁特别的多，包括 IE 补丁、Office 办公软件补丁等等。如果不及时打上补丁的话，则很容易病毒利用，成为其传播的便捷渠道。不过可惜的是，有不少的 IT 负责人不重视补丁方面的管理与控制。如有些管理员，纯粹依靠用户的自觉，来进行补丁的管理。如在客户端上通过自动更新服务来对给系统打补丁。采取这个操作是，需要客户端用户的手工操作。如需要进行手工确认是否需要进行补丁升级、升级完成后可能还需要重新启动等等。现实的情况是有些用户认为这么操作比较麻烦，为此都不会自觉的去升级补丁。如此的话，就给内网的安全造成了比必要的安全隐患。

为此笔者建议，对于补丁的管理，最好采取统一的解决方案。如微软有一个补丁管理的工具，可以在服务器上控制强制对客户端系统打补丁。如在下次启动之前给系统自动打补丁等等。这么设计即可以保障内部网络的安全，也可以对用户的不利影响降至到最低。总之笔者认为，最好不要将补丁更新的权利交给用户。大部分用户并不会正确行使这个权力。

弊病二：自签名证书不兼容会惹祸

IE 浏览器一直是微软操作系统与服务器的安全重灾区。其中用户的不正确设置是其总要的一个原因。微软为了改善这种情况，在微软的一些产品中，如 Exchange 中加入了自签名证书。简单的说，就是当企业用户没有采取任何安全措施的话，那么系统就会自动启用自签名证书，以启用一定的安全加密机制，如 SSL 加密等等。

这种默认的安全措施在一定程度上提高了系统应用的安全性。特别是对于那些没有安全观念的用户来说，能够启动不少的帮助。但是到现在为止，这个自签名证书的作用只限于微软的产品。如企业现在使用的是 Exchange 的服务器，然后采用 IE 浏览器去访问这个邮箱的话，没有问题。但是如果采用其他的浏览器去访问的话，就可能会出现不兼容的问题。如浏览器会提示用户系统并不信任这一类的证书。有些管理员为了减少这种麻烦，就索性将自签名证书的功能也禁用掉。这无疑减弱了企业内部网络服务器的安全性。

弊病三：不注重后续的追踪

有不少的企业，在网络设计与组建时，非常关注企业内部网络的安全。如禁用不必要的服务、禁止使用移动设备等等。但是在这方面他们也存在着一定的误区。就是非常重视前期的设计与配置，但是却缺少后续的追踪机制。

如对于文件服务器来说，企业可能有比较安全的权限访问机制等安全措施。但是却缺少访问审核机制。也就是说无法判断这个安全措施是否到位，也无法分析用户是否存在着越权的访问。在这种情况下，可能只有在最后出现问题的时候，才能够发现这方面的不足。笔者建议，在前期做好安全设计与相关的配置固然重要，但是在后续日常工作中也需要最好追踪分析的工作。当发现原有的配置跟不上企业安全的需求时，需要进行及时的调整。如对于文件服务器来说，可以启用审计功能。将用户的未经授权的访问都记录在案。然后对这个数据进行分析，以判断用户可能的攻击行为。

弊病四：没有使用逆向代理来减少端口的开销

随着企业信息化管理的普及，现在企业越来越不满足于内部用户使用企业的信息化系统。如有些企业可能会在外地开设办事处。企业就希望这些办事处的人员也能够访问企业内部的服务器。再如为了出差在外的员工工作的方便，也允许他们从公共网络连接企业内部的服务器。

如果要允许企业内部的服务器被外部用户通过互联网进行访问，那么就必须要在防火墙上开启多个端口。而这种情形就会增加企业内部的安全隐患。道理很简单，这就好像是开一幢房子开了多个门。管理员无法兼顾到多个门的安全。如企业部署了微软的即时通信套件。如果需要允许外部用户使用这个即时通信服务器的话，那么就需要在防火墙上开启十几个端口。这无疑大大降低了企业内部网络的安全性。当遇到这种情况是，笔者建议使用逆向代理机制。逆向代理的服务器一般位于互联网和本地需要开发多个端口的服务器之间，基本上跟防火墙服务器是并列的。采用逆向代理的话，可以让服务器在进入外网前先隐藏起来，同时还可以保障外部的恶意请求不会到达服务器。在安全方面，跟 NAT 技术有异曲同工之妙。不过从管理成本与性能开销上来说，要比 NAT 服务器低很多。

弊病五：在同一个服务器上部署过多的应用程序

在同一个服务器上部署多个应用程序，这种情况在企业中也是司空见惯的事情。这虽然可以在一定程度上降低企业信息化部署的成本，但是也增加了服务器的安全隐患。假设现在一家企业的一个服务器上部署了三种应用，此时包括操作系统在内的话，其实就有四种信息化系统。如果一种信息化系统存在 2 个安全漏洞的话，那么这台服务器现在就有了 8 个漏洞。如果没有采取严格安全措施的话，那么攻击者只要利用其中的任何一个漏洞，就有可能窃取服务器上的内容，甚至控制服务器。

这就好像一条链条。如果链条上的一个个环越多，其安全性能相对来说就越差。因为任何一个环断掉的话，整条链条就会报废掉。而环越多的话，则出现断掉的可能性就会越大。总的来说，企业如果需要在一台服务器上部署多个应用程序并不是不行，但是在数量上需要有所限制。一般情况下不要超过三个。同时对于一些重要的应用，如数据库等的功能，最好采

取单独的应用服务器，以保障其安全。而且还需要采取一些必要的措施，如虚拟 CPU 等技术，来给多个应用程序提供相对独立的工作环境。

弊病六：对邮件等需要授权的访问没有采取 SSL 加密机制

企业中不少的信息化系统需要授权才能够进行访问。如对于邮件系统，用户只能够访问自己的邮箱。对于文件服务器，也只能够访问授权允许访问的文件。而这些控制，基本上都是通过用户名与密码来进行限制的。

在内部网络中，先主要采用的是 HTTP 与 HTTPS 两种访问机制。前者 HTTP 其特点是对于传输中的数据没有进行任何的加密措施。即用户名与密码在网络中都是明文传输的。如此的话，通过网络嗅探器等工具，就可以轻而易举的窃取到用户的用户名与密码。从而进行破坏活动。而如果用户名与密码信息泄露的话，最好的安全措施也无济于事。笔者的建议是，对于一些重要的应用，如邮件、文件服务器等等，最好采用 HTTPS 协议。这个协议的特点是在数据传输过程中采用 SSL 加密机制对数据进行加密，以确保用户名与密码的安全。

来源:51CTO