广西科学院学报
Journal of Guangxi Academy of Sciences

2007,23(4):353~355
Vol. 23,No. 4 November 2007

广西柳工机械股份有限公司计算机网络恶意程序防护体系建设

An Anti-Malicious-Program System for the Industrial Machinery Co. ltd of Liuzhou, Guangxi

邢海韬[1],罗 海[2],李 玥[2],曾锻成[2]
XING Hai-tao[1],LUO Hai[2],LI Yue[2],ZENG Duan-cheng[2]

(1.广西柳工机械股份有限公司,广西柳州 545007;2.广西计算中心,广西南宁 530022)
(1. Guangxi Liugong Machinery Co., Ltd, Liuzhou, Guangxi, 545007, China; 2. Computing Center of Guangxi, Nanning, Guangxi, 530022, China)

摘要:在介绍广西柳工机械股份有限公司(以下简称柳工)面临的威胁及恶意程序传播途径的基础上,阐述柳工计算机网络恶意程序防护体系的建设情况。柳工计算机网络恶意程序防护体系建设了网关、网络防护、在线杀毒及损害清除、桌面端防护、系统补丁升级、专业厂家服务和用户教育,共七道防线来对抗恶意程序的攻击。柳工计算机网络恶意程序防护体系解决了柳工网络内的恶意程序与病毒程序的多重威胁,使企业能够以较快的速度来把精力集中在业务系统及应用上,从而促进企业的发展。

关键词:网络安全 恶意程序 病毒
中图法分类号:TP393.09 **文献标识码**:A **文章编号**:1002-7378(2007)04-0353-03

Abstract: This paper analyses the risk of malicious program the Industrial Machinery Co. ltd of Liuzhou faces and presents its defence system against malicious program. Defences such as Network Patch Upgrade, Enterprise Service and User Education are designed to resist the malicious programs.

Key words: network security, malware, virus

随着计算机应用的发展,企业计算机网络受到的威胁也越来越多,不仅影响企业的单机使用,更严重的是对整个企业的设计、生产和经营等应用也产生了严重的影响。本文以广西柳工机械股份有限公司(以下简称柳工)的恶意程序防护体系建设为例,探讨在企业复杂网络环境中,如何建设一个有效的计算机恶意程序防护体系。

1 柳工网络面临的威胁及恶意程序的传播途径

柳工和大多数企业一样,现有的计算机网络是由原来各部门的网络不断连接起来的。虽然企业已经投入了较多的资金进行网络改造,但是硬件上的投入与改造不能和软件环境相适应及配套。软件环境相对滞后使企业的应用受到限制,常常会受到恶意程序的威胁。

1.1 WEB浏览引发的问题

上网浏览的计算机在浏览带有恶意网页的网站或者恶意网站时会导致计算机被动下载恶意程序,以致造成数据丢失和信息泄密。

HTTP/FTP被动下载型恶意程序多数利用了ActiveX或网页浏览器的漏洞,多数会对注册表进行修改,导致计算机启动后就会直接调用病毒。此时,使用浏览器的用户权限较小时,对计算机的影响会相对小一些。但是,如果是笔记本电脑的用户,就会造成比较大的问题,病毒会在注册表的键值RUN、WINDOWS、WINNT等几个地方进行修改[1]。

1.2 被感染的计算机主动访问互联网

被动下载了恶意程序的计算机受感染后,会主动连接互联网进行恶意程序的更新与下载,同时带来了信息泄密的威胁。

收稿日期:2007-09-30
作者简介:邢海韬(1975-),男,工程师,主要从事网络管理、网络安全研究。

目前最新型的网络恶意程序传播方式都使用了这种主动访问互联网的传播方式，此方式一是可以使用户计算机上的恶意程序保持最新的版本，以便恶意程序的发布者对用户进行了解和控制，二是直接会导致信息的泄露。通过HTTP/FTP主动下载型恶意程序，由于是计算机主动发起连接，所以防护难度更大。

1.3 网络内病毒传播

恶意程序感染到计算机后，会在计算机网络内通过各种方式进行传播。一般有文件共享型的传播和网络层传播(即网络蠕虫病毒)。这时候如果防病毒软件的病毒码没有更新、计算机上的系统漏洞和补丁没有及时处理，那么会很快造成恶意程序在网络内的泛滥。

1.4 恶意程序通过邮件传播

恶意程序通过各种伪装的邮件对用户实行欺骗或自动运行邮件带可执行附件，使用户防不胜防。网络欺骗和网络钓鱼多数都是通过邮件进行传播的。

垃圾邮件及病毒邮件已经成为网络内的公害，它们对整个网络的影响不仅是造成企业内部的计算机应用受到影响，也直接影响企业计算机使用人员的工作效率。现在的恶意程序最主要的传播途径正在从邮件应用转向Web应用[2]。

1.5 笔记本电脑或移动办公带来影响

已经被恶意程序感染的外来笔记本电脑或出外回来的笔记本电脑连入企业内部网络时，其带来的恶意程序会借着已经连入的网络，对网络内其它计算机进行攻击。

企业内的计算机并不每一台计算机都得到了最新的补丁更新及保护，所以感染了恶意程序的笔记本电脑接入到企业内部网络的时候，即使是已经做好对外部防护，仍然会有很大的威胁性。

2 柳工网络防护体系的建设

Internet访问不受保护、局域网共享管理没跟上以及帐号/密码管理缺失、系统漏洞补丁没有及时更新等是导致恶意程序进入柳工网络并快速蔓延及感染的重要原因。为了减少及消除柳工计算机网络内的恶意程序泛滥，使网络内的恶意程序减少到最低限度，使企业网络内的计算机因为恶意程序影响造成的损失减少到最小，所以柳工企业搭建了柳工计算机网络恶意程序防护体系。

2.1 网关

网关防毒墙是柳工网络恶意程序防护体系的第一道防线。网关病毒防护包括两个病毒墙，一个是WEB防护，一个是邮局防护。

因为柳工自己建立了企业内部邮局、外部公务邮局，所以，邮件防护网关也是需要的。柳工也在较早就认识到邮局防护的重要性，最早的网关防护也是从邮件系统的防护做起来的。从目前来看，邮件网关的防护使企业每个月减少了至少40000～50000封垃圾及病毒邮件，对企业内的邮件处理效率的提高以及病毒的防护都起到了较好的作用。

WEB网关防护是最难做的。其中最主要的原因在于，如何能够减少对恶意网站的访问以及WEB网关可以自动防护恶意程序的下载。经过多方对比和实际测试，柳工采用了趋势公司的IWSA－2500－EE－M型。该硬件产品可以支持超过500个用户的在线访问，平均一天至少有2000多条访问阻止记录以及病毒下载被清除的记录信息。IWSA还采用了网络信誉等级服务和URL自动阻止的技术，可以对在TREND的恶意网站库中的网站自动拒绝访问，这样可以减少很多需要我们自己去手工监控的麻烦。

2.2 网络层防护

网络层防护是防护体系的第二道防线。我们按照微软标准的深层防毒指南中对网络层防护的建议，在网络层设备上部署网络病毒防护设备来帮助减少网络内蠕虫病毒(冲击波、震荡波等)的传播。

网络层部署的防护设备是NVW设备，主要用它实现网络蠕虫扫描和病毒爆发监控和防御，协助企业防止Internet蠕虫之类的网络病毒和爆发病毒疫情时隔绝高危险的网络脆弱环节。网络层防护能够在网络层清除带毒数据包、定位可疑计算机以及强制实施安全策略，隔离特定的网络、IP段以及聊天软件和文件传播。

2.3 网络内在线杀毒及损害清除

外来笔记本、在外面使用后带回来的笔记本电脑，以及公司内已经部署或未部署杀毒软件但是希望能够交叉杀毒的计算机是整个网络防护体系的短板和薄弱环节，为减少这些薄弱环节带来的影响，我们在网络内部署了“在线杀毒”及“损害清除”服务器，这是防护体系的第三道防线。

“在线杀毒”(HouseCall)服务主要是用于清除计算机内的木马程序，还可以自动清除隐藏在计算机系统中的病毒程序，并恢复到原始设定。这个服务对于柳工有一个很实际的作用在于，由于柳工的国际化不断发展，也不断有国际上的经销商和我们的

营销人员回到柳工总部进行工作交流。这些交流是需要连接入柳工内部网络的,如果不做好这些计算机的防护,那么柳工的内部网络会很快受到恶意程序的攻击。我们同时采用了趋势的"损害清除"服务,该服务可以与 IWSA 及 IGSA 等网关防护设备联动,自动消除病毒和间谍软件感染。

2.4 桌面端防护

桌面端防护是防护体系的第四道防线,是计算机系统的基础防护线。柳工原来一直在使用的是 Mcafee 和瑞星等网络版的杀毒软件,近来由于国内病毒的泛滥,也使用了一部分的国产杀毒软件,如金山毒霸等。但是,从计算机的统一管理的角度,我们对桌面端的病毒防护重新进行选择。选择的标准是:(1)杀毒软件要能够进行统一的管理与维护(即使用网络版);(2)客户端的程序应该带有网络/网页型病毒防护的能力;(3)技术支持稳定、安全,同时能够有良好的服务响应速度;(4)要有良好的国际化支持能力;(5)能够针对区域化的病毒发展趋势做出快速响应和服务。

2.5 计算机系统补丁升级

计算机系统的漏洞以及在系统上应用软件的补丁升级是防护体系的第五道防线,是防护的基准线之一。可以说做好了补丁升级工作,防护体系的防护能力至少提高 30%。

在建设第五道防线的时候,我们首先采用微软公司的 SUS2 方案来解决,下一步的工作在测试中准备结合网络管理的要求来选择第三方的方案。

2.6 专业厂家服务

由于柳工内从事计算机病毒安全工作人员的素质与数量均不足,在进行计算机病毒防护的时候,越来越倾向于应用来自防毒软件厂商的服务,一方面可以提高防毒力,一方面可以让员工通过厂家进行专业服务的学习,从中提高专业素质。这是防护体系的第六道防线。

2.7 用户教育

对于一个设计良好的防护体系,如果使用者没有配合或者说实际上在不断违背安全防护的规则做事情,那么设计再良好的防护体系也是等于一张白纸。因此,我们建设了防护体系的终极防线,即对用户进行使用教育。

用户教育是教会用户使用电脑的时候,尽量不使用管理员账户,而是使用受限制的用户;个人账户的密码不得随意告诉他人;定期(至少两天一次)更新自己的计算机杀毒软件病毒库,开启 WEB 访问时保护功能,尽量不访问未知的非安全网站;网络内部的共享尽量不开放,或者开放的时候设置较高强度的密码。

3 结束语

建立柳工计算机网络恶意程序防护体系,最主要的是解决在柳工计算机网络内的恶意程序与病毒程序的多重威胁,使企业能够以较快的速度来把精力集中在业务系统及应用上,从而促进企业的发展。柳工计算机网络恶意程序防护体系的建设,使得柳工内部网络的计算机使用变得变快捷灵活,提高了整个企业的工作效率。

参考文献:

[1] 祁海英. ASP 技术在信息权限安全中的应用[J]. 青海师范大学学报:自然科学版,2005(2):61-63.

[2] 李晓,张晓辉,李祥胜,等. SQL Server 2000 管理及应用系统开发[M]. 北京:人民邮电出版社,2002.

(责任编辑:邓大玉)

韩国利用人类胚胎干细胞治愈下肢坏死实验鼠

韩国抱川中文医科大学附属车氏医院教授郑炯敏和汉阳大学教授金炳沫带领的一个联合研究小组表示,该小组的研究人员在实验中掌握了将人类胚胎干细胞诱导分裂为治疗用的 ES 细胞(血管内皮细胞)的技术,以及分离和培养这些细胞的有效方法,日前更利用这项技术获得了一种血管细胞,并且使用这种血管细胞成功治愈了患有下肢血管闭塞症的实验鼠。在实验中,研究人员通过肌肉注射将 ES 细胞注入到 11 只染有下肢血管闭塞症的实验鼠腿部之后,4 只鼠的下肢基本得到保全,3 只鼠的下肢轻微坏死,另外 3 只鼠下肢完全坏死。而对照组 10 只实验鼠中的 9 只下肢完全坏死,1 只严重坏死。研究人员表示,在这项技术基础上开发具有临床价值的产品只需要大约 2 至 3 年时间。

韩国学者评论指出,该研究成果将大幅度改写心血管等血管系统疾病的治疗方案和治疗效果,促进人类胚胎干细胞治疗时代的到来。(据科学网)