

以恶意木马程序为首的计算机病毒已无孔不入,信息网络安全问题成为一个热点话题——

# 如何防范木马入侵

本报记者 余建斌

古希腊传说中,一匹巨大的木马帮助希腊人战胜了特洛伊人,“特洛伊木马”从此成为比喻在敌人营垒里埋下伏兵的典故。人们没有想到的是,几千年后,“特洛伊木马”居然会从《荷马史诗》所描述的传说中“跳”出来,侵入现代社会的计算机中。这就是“木马病毒”。

几天前,瑞星公司发布红色一级安全警报,正有数万个木马病毒每天以“木马群”的形式,利用最新的Flash漏洞攻击用户电脑,已有超过300万台电脑被该类病毒袭击,被感染电脑数量还在急剧增长。

国家计算机病毒应急处理中心和各大反病毒软件公司定期发布的病毒警报已揭示一个事实:以恶意木马程序为首的计算机病毒已经无孔不入地渗入到普通用户的电脑,一些有专人维护的企业、政府的计算机也未能幸免,成为危害国家和公众信息安全的主要顽疾。

## 计算机病毒恶意变身 木马程序成最大危害

在一家杂志做编辑的刘小姐告诉记者,她的电脑最近一段时间突然变慢,打开一个网页浏览器要花几十秒钟,有时候甚至死机。记者在刘小姐电脑上发现,有许多她没有使用的程序正在连接网络,占用大量计算机内存,明显是中了木马病毒的症状。“一下子感觉毫无隐私可言。”刘小姐得知后惊出一身冷汗。

“如果无效防范,要想不感染病毒,除非不再用软件”。仅据瑞星公司一家的统计分析,2007年我国大陆地区就有7300多万台电脑曾被病毒感染,

成为计算机病毒的“重灾区”。包括木马病毒在内的计算机病毒已经成为窃取信息并造成信息泄漏的主要方式。

计算机病毒泛滥尤以木马病毒为甚。木马病毒是一种远程控制程序,“黑客”利用计算机系统和软件的漏洞将一段程序植入远端电脑后,可以借助其配套的控制程序来远程控制中毒电脑,肆无忌惮地查看、下载他人电脑中的内容。除了以前的点击电子邮件附件外,目前感染U盘、ARP局域网攻击、网页挂马已成为木马病毒传播的主要方式。像点击QQ、MSN、电子邮件中病毒网址、浏览被黑的网站,都会导致感染木马病毒。

“从监测来看,木马病毒是互联网最大的危害之一,安全部门破获很多通过木马窃取信息的案件。我们2007年监测到,大陆地区被植入木马的主机数量,比2006年增加了26倍。”国家计算机网络应急技术处理协调中心运行管理部高级工程师孙蔚敏说。

计算机病毒“诞生”20多年,作为一种蓄意设计的软件程序,它的功能从传统的“干扰计算机操作,毁坏或删除数据,并能自我复制和自行传播到其他计算机和整个互联网”,转变到“利用系统和软件漏洞,侵入目标系统,记录并窃取信息”的木马等恶意程序,计算机病毒的发作模式也和“早期大举进攻、损毁数据的暴露型不同,变得更‘安静’,如木马程序一样远程控制他人电脑,窃取数据等信息”。

## 计算机病毒制造工业化 形成不法利益“产业链”

以窃取信息为目的的计算机病

毒泛滥,毫无疑问其背后的最大动力就是谋取经济收益。因为“木马、后门这两类病毒都以侵入用户电脑,窃取网游账号、银行和股票账号等信息为目的,带有直接的经济利益特征”。在去年瑞星截获的病毒样本数中,窃取用户的账号木马和后门病毒占84.5%。

“我们去年杀掉的病毒里面91%是木马,可能还有2%是广告程序,像以前所谓的非营利型软件基本没有了。”反病毒软件企业卡巴斯基的一位专家说。

“病毒的驱力性进一步增强,网上制作和贩卖病毒、木马的活动日益猖獗,利用病毒木马技术进行网络盗窃、诈骗的网络犯罪活动呈快速上升趋势,这些进一步显示计算机病毒新的发展趋势。”印证国家计算机病毒应急处理中心这段结论的其中一个例子,就是网上泛滥的出售盗取网络游戏账号的木马程序的现象。

“木马出售或定做木马……做假杀,挂马业务请联系QQ……”记者在雅虎论坛上看到,这则发于去年5月的帖子,到今年4月份还有“请教教我,怎么盗号”的回复。在新浪博客、百度贴吧等这些国内访问量较大的商业网站频道中,出售、出租、定做木马,承接“挂马”业务等帖子随处可见。

“这些病毒、木马等恶意软件制造者不再是个人或者小团体,而是演变为散步在网络上的分工严密的组织,以追逐利益为目标,形成了发现漏洞、制造木马、传播木马并窃取信息的利益链条。受害者不仅限于个人用户,还包括了企业等用户。”信息安全专家李元正说。

“工业化生产”病毒的出现使这种趋势提速。像利用加壳工具可以改变已有病毒的“面貌”,使得杀毒软件无法识别。任何具备基础电脑知识的人,只要从网上下载加壳工具,就可以自动生产出病毒。这导致病毒数量暴增,变种速度加快。“一个熟练的病毒工程师,每天可以分析40—50个样本,而现在每天出现在网上的病毒样本平均为3000—4000个”。

“如果使用木马生成器,可能一个小学生就会做木马。木马不厉害,但它窃取信息和密码的结果是致命的。”卡巴斯基的专家评论说。

## 北京奥运大赛在即 网络安全不容忽视

以木马病毒为主的计算机病毒当前已成为对互联网安全的最大威胁之一,对于日益临近的奥运会的网络安全保障来说不容忽视。对于计算机病毒的防治,需要从信息安全的高度来看待。

北京奥组委专家刘云介绍说,北京奥组委管理网、运动会网、奥运官方网站、奥运会票务网以及其他互联网接人等均面临着不同的风险,例如对网页的恶意篡改、对网站的恶意攻击、病毒的大面积传播、网络访问量过大导致网络瘫痪等等。而除了这些与奥运直接相关的信息网络系统,外围相关部分如国家电信系统、网上



李明绘

银行和ATM网络等也面临安全威胁。

前几届奥运会曾发生奥运会官方网站被攻击事件。北京奥组委技术部部长贾胜文说,目前奥运信息安全方面所面对的形势还是比较严峻的,对于奥运信息网络各种形式的攻击一直存在,而且随着奥运会的临近,还有加剧的趋势。不过奥组委已经制定了相关应对措施。

专家指出,奥运网络与信息安全涉及面广、影响范围大、关注度高,需要全社会的参与。同时也可利用这一机会,最大范围地提高公众信息安全意识,包括“驱除”身边的计算机病毒。

从长远来看,面对现状,国内的反计算机病毒软件商都在煞费苦心地开发防御手段,国家有关部门也提出加强监督检查和打击防范的力度,积极研发新技术新装备,提高对网络犯罪能力的发现能力和网上侦查、取证能力,遏制网络犯罪活动的上升势头。

但有关专家也指出,互联网不可能是百分百的安全,病毒也可能向手机等新平台上更快地传播,反主动防御技术可能也会出现,在人们的安全意识整体水平提高之前,清除计算机病毒还有很长的路要走。



## 感受高科技

上图:6月29日,“感受泉城·科普行”活动在山东省科技馆举行,400余名在济南学习的四川北川擂鼓镇的小学生们免费参观了科技馆。图为小学生被山东省科技馆里高科技产品所吸引。

汤序民摄

右图:湖北省宜昌市首届“盲人电脑培训班”日前开班,30多位学员将参加1个月的培训。图为一位学员(右)在老师帮助下学习电脑。

黄翔摄(新华社发)

本版责任编辑:施 芳

电话:010—65368548

传真:010—65368561



今年,国家自然基金委员会将安排资助计划64亿元左右,同比增长28.0%,是基金委成立以来最多的一年。

64亿元资助经费将怎样安排?记者日前走访了国家自然科学基金委主任陈宜瑜院士。

基础研究

保证各学科均衡发展

记者:今年的资助格局将会发生怎样的变化?

陈宜瑜:作为国家资助自然科学基金研究的主要渠道,自然科学基金主要是支持基础研究,鼓励自由探索,培养科学人才。今年的资助计划将在把握“前沿探索为主、人才培养优先、战略导向加强、总体基本稳定”的基础上,进一步调整资助格局,加强宏观协调,重点用好增量经费,促进项目支持、人才培养和环境条件等三大资助系列的协调发展。

根据这一原则,今年三大资助系列的计划经费分别为:项目支持43.96亿元,人才培养17.9亿元,环境条件1.8亿元,分别比去年增加31.8%、23.8%和16%。

记者:基础研究是自然科学基金资助的重中之重,这方面将如何安排?

陈宜瑜:基础研究不能过分强调“有所为有所不为”。因为基础研究具有很强的探索性、不可预测性,谁也无法预测未来10年、20年科技前沿在什么地方,哪项基础研究更重要、更有应用前景。为防止出现“木桶效应”,自然科学基金的首要任务就是保证自然科学各个学科均衡协调可持续发展。

为培育创新思想,面上项目首先要得到主要经费的保证,以继续为科学家自由探索提供广阔空间。今年面上项目安排计划额度29亿元,占各类项目总经费的45.3%。我们将继续实行“控制资助规模,提高强度”的资助政策,力争项目平均资助强度提高到34万元/项左右,资助率控制在17%左右。

在重点项目方面,将适度加大投入,安排计划额度7.92亿元,约资助430项,平均资助强度为每项185万元左右。

在重大项目和重大研究计划方面,则稳步推进。根据“十一五”发展规划的整体安排,2008年将完成去年立项的8个重大项目的评审和资助工作,启动“十一五”第二批重大项目的立项和评审遴选工作,总体安排计划额度2亿元,占各类项目总经费的3.1%;重大研究计划共安排资助计划额度3.36亿元。

人才资助

大幅度提高支持力度

记者:人才资源是第一资源,基金委今年在人才资助方面有什么新举措?

陈宜瑜:今年将较大幅度加大对青年科学基金的支持力度,安排计划额度9.3亿元,同比去年增加3.3亿元,资助率可望提高到22%;地区科学基金重点用于提高资助强度,安排资助计划1.7亿元,力争资助项目的平均资助强度能达到25万元/项,资助率在20%左右。

其中,杰出青年科学基金今年资助人数仍控制在180人以内,资助金额每人200万元;创新研究群体拟资助28个,资助额度为500万元/个。

绩效评估

将首次引进国际评估

记者:科学基金资助绩效是大家非常关心的问题,这方面基金委有什么新举措?

陈宜瑜:这一问题不光社会关注,我们也高度重视。为此,我们将第一次参照国际经验,组织国际性的基金绩效整体评估。

根据计划,评估工作主要分3个阶段。第一阶段,对日本和德国等国家相关基金会进行国际性绩效评估的方法和效果进行考察。目前考察已结束,正在整理总结报告。第二阶段,继续调研美国的相关经验,在调研基础上借鉴国际经验结合中国国情,制定初步方案,争取与财政部就评估指标体系达成一致意见。第三阶段,如果前两阶段工作进展顺利的话,预计在2010年正式实施国际评估。

我们希望,通过这次国际性的绩效评估,不断完善科学基金管理体系和运行机制,提高运作效率与效益,加强管理队伍建设,全面提升驾驭和管理科学基金的能力。

## 秦大河获国际气象组织奖

本报北京电 (记者刘毅)记者日前从中国气象局获悉:6月25日,世界气象组织执行理事会第六十次届会经过投票,将第五十三届国际气象组织奖授予中国的秦大河院士。这是时隔5年,我国科学家第二次获得这一世界气象组织最高荣誉。

国际气象组织奖每年颁发给1位在气象、水文和地球物理科学领域做出杰出贡献的人士。秦大河院士是世界著名的冰川学家和气候学家、中国科学院院士、第三世界科学院院士。

## 我国疫苗研发不断取得突破

本报北京电 (蒋蒲)记者从日前召开的第二届健康科技高峰论坛上获悉:我国正由疫苗的生产和使用大国迈向疫苗的研发和生产强国。

我国高度重视疫苗的生产和研发工作。近年来,科技部会同有关部门在863计划、支撑计划、“重大新药创制”国家重大科技专项等计划中,对疫苗的研究开发与产业化都做出了重点安排。我国在传统疫苗的技术提升、新型基因工程疫苗等方面均取得了众多突破,包括艾滋病疫苗在内的一批新型疫苗正在开展临床研究,幽门螺杆菌疫苗等完成了临床研究正申请上市。

## 我国软件产业规模居世界第四

本报北京电 (记者余建斌)记者从日前召开的第十二届中国国际软件博览会上获悉:我国软件产业规模已达5834亿元,居世界第四位。

我国软件产业目前已发展成为国家基础性、先导性、战略性新兴产业,成为信息产业、先进制造业和现代服务业的核心。软件产业的收入由2000年的593亿元上升到2007年的5834亿元,占全球软件产业的份额从1.2%提升到8.7%。