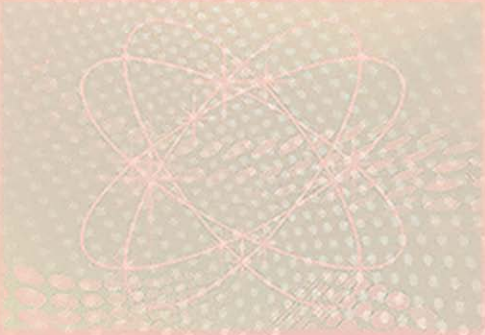
学生课外知识·电脑

计算机网络与病毒



目　录

因特网时代的计算机病毒与防治

计算机病毒自从1986年首次被发现以来，给计算机系统的安全带来了巨大威胁，人们不遗余力地采取措施来制服它。现在随着因特网(Internet，原译为互联网)的普及，计算机病毒的危害也随之加重。出现了可经由电子函件(电子邮件)传播的各种新形态计算机病毒，仅靠原先的抗病毒方法，已经不够。下面介绍一下因特网时代的病毒与防治措施。

一、计算机病毒的定义

关于计算机病毒，存在着种种定义。日本通产省在“计算机病毒对策基准”中作了以下定义：“病毒是为了对第三者的程序和数据库施加某种危害而制作的程序，它含有至少以下的一种功能：感染功能、潜伏功能、发病功能”。

根据以上定义，只要拥有上述功能之一便可视为计算机病毒。实际上现在已经发现的病毒，几乎都三种功能兼而有之。

二、计算机病毒的侵入方式

计算机病毒目前已有几千种，其侵入方式大约可以归纳为以下几种：(1)以软盘为媒介侵入；(2)以软件为媒介侵入；(3)通过安全漏洞侵入。

此为试读，需要完整PDF请访问：www.ertongbook.com

三、以软盘为媒介侵入

感染计算机系统的病毒,多以软盘为媒介侵入。早些时候的例子发生于1990年。当时美国阿托丁格公司在出售一种游戏软件FAR SIDE MOON,该软件存放在3片一组的软盘中。引起问题的病毒侵入其中一片数据盘的引导区。但是,这种类型的计算机病毒仅仅是在用受感染的软盘建立系统时才会侵入。因此它一般不会经由网络侵入。

四、以软件为媒介侵入

这种例子很多。1991年发生的病毒侵入商用个人机通信服务系统NIFTY－Serve事件,便属于这一类型。侵入的病毒叫"维也纳"病毒,侵入的对象是使用NIFTY－Serve网络来交换软件的用户,病毒感染了压缩软件LHarc。从1991年1月14日该程序在此系统开始使用时算起,到4月3日发现该程序受病毒感染约3个月时间,它一直保持在上载时的状态,凡在这期间下载这一软件的用户都受到侵害。

这一侵害事例虽然发生在个人机通信服务系统中,在因特网也同样会发生。通过使用WWW(万维网,曾译为环球网)和FTP(文件传送协议),下载已受病毒感染的软件,并在自己的计算机执行这一软件时,也将感染到这种病毒。

混在电子函件(电子邮件)中侵入

一种名为"淘气程序"的计算机病毒便是用这种方式侵入的,受害者也是个人机通信服务用户。

1988 年 9 月商用个人机通信服务系统 PC－VAN 便受其侵害。它经由二进制码函件发送内容不明的程序，执行它时便会在个人机的系统文件上感染这种“淘气程序”病毒。当用受“淘气程序”侵害的个人机访问 PC－VAN 时，画面会突然停止不动，但很快便恢复正常，似乎什么也没有发生。这时，“淘气程序”乘用户不注意便偷走他们在使用 PC－VAN 时的 ID(身份号)和密码。

这种情况同样会在使用因特网时发生。对于从不相识的人那里发送来的二进制码函件，人们无法知道它输入的是什么程序，而二进制码函件即使使用杀病毒软件也无法进行检查，因此无法判断其是否安全。所以对内容不清楚的程序不仅不能利用，而且要立即删除。

需要指出，能传递病毒的不仅有二进制码函件。1995 年夏天还发现了一种新类型的病毒，它经由因特网混在文本文件形式的函件中侵入。

这种病毒叫做“WordMacro 概念”，也称为宏病毒，它会感染用微软公司出品的文字处理软件 Word 生成的文本文件。通过电子函件得到感染这种病毒的文本文件后，只要用 Word 打开该文本文档，“Word Macro 概念”病毒便会侵入计算机。

五、通过安全漏洞侵入

1988 年 11 月，美国纽约州康奈尔大学计算机科学专业的研究生罗巴特·莫里斯，有意把一种计算机病毒放入因特

网作实验。这种病毒被称为“网络虫”。它徘徊在网络之中，不断地复制自己并进行扩散，是一种危害很严重的病毒。

网络虫并不感染计算机系统区和软件，所以有人认为它不是计算机病毒。但从它侵入计算机后会造成危害这一点看，它同前面谈到的“淘气程序”是一样的，所以也应把它看作计算机病毒的一种。

网络虫通过网络的安全漏洞而侵入。所谓安全漏洞是指使用链接于特定网络的计算机工作时，用于确认计算机用户合法性的软件的“缺陷”。如果知道了认证系统有什么样的缺陷，尽管未拥有正式的用户 ID，也能使用计算机。

由链接于网络的计算机所启动的网络虫，将收集链接于该网络的相邻计算机的信息，还会为了把自身的复制品送入网络而进行线路链接处理。一旦线路链接上，网络虫的一部分即引导网络虫用的程序，便通过安全漏洞送入邻近的计算机。这种程序通常用 C 语言源码段编制。进入相邻计算机的引导程序，经过远程编译后，便会被启动。程序经由线路，同所引导的网络虫联络，把二进制码段的网络虫读入到相邻的计算机。

在这一阶段，网络虫会被复制到所有相邻的计算机上。同时这些网络虫还会在各自的计算机中反复进行一连串的自身复制行为，因此在因特网中的网络虫便扩散到鼠标算式中。

六、采取新的抗病毒措施已非常必要

对于混在二进制代码的电子函件中侵入的病毒，一般还

无法判别其内容是否安全。因此所采取的措施，只有对发送者确认的内容后才使用，不能确认时只能删除掉。

至于以其它几种方式侵入的病毒，则应采用以下三种防范措施：

七、利用杀病毒软件

对于以软件为媒介侵入的病毒和混在文本文件形式的电子函件中侵入的病毒，使用杀病毒软件是对付它们的有效措施。

但每种杀病毒软件所能检测到的病毒都有限，因此最好多用几种软件检查。

八、利用完整性法

为了弥补杀病毒软件的缺陷，还可以利用完整性法。它是 IPA(日本信息处理振兴事业协会)于 1993 年开始进行研究的。

这种措施对上述两种病毒很有效。当软件感染上这两类病毒时，在感染处不再保持信息的完整性。利用这一点便可发现病毒。

采用这种措施需要有软件销售者或分发者的配合。首先，由他们制作两种密钥，并规定署名方法。

一种密钥是给销售者或分发者在对软件进行数字署名时使用的。这种密钥不对外公开，防止附于软件上的数字签名被更改。先由软件销售者按署名方法制作署名数据，再用密

钥对署名数据加密成为数字署名,然后把加密后的数字署名附于软件上,最后出售软件。

另一种密钥由销售者和分发者事前在钥管理机构登录。它被称为公开钥。用户在验证所购入软件内容时使用从钥管理机构得到的公开钥,对附在所购入软件上的数字签名进行译码,另外还可对所购入的软件另作署名数据。署名方法由销售者及分发者公开,用户也可以从钥管理机构取得。

如果软件感染了病毒,它的内容便和原来不一样。这样,用户用所得到的署名方法生成的署名数据,同用公开钥对附于软件的数字署名进行解密而获得的署名数据不一致。由此便可发现计算机病毒的侵入。

为了实现这一措施,需要软件销售者和分发者进行数据署名,并设立钥管理机构。抗病毒软件无法发现还不知道的计算机病毒,而完整性法则能发现尚不知道的计算机病毒的侵入。所以作为今后抗病毒的措施将是非常有效的。

九、防止安全漏洞

在上面提到的被网络虫破坏的例子中,被通过的安全漏洞是 Sendmail(UNIX 的电子函件功能)的 DEBUG 选项。现在链接于因特网的计算机,还有使用这一老式 Sendmail 的,因此还会发生同样问题。除 Sendmail 外,还未发现和它一样的网络虫通过安全漏洞的情况。但 Sendmail 之外也发现了不少安全漏洞。有可能出现新的网络虫通过这些安全漏洞的情况。对付的办法只有一一堵住这些安全漏洞。

查询 CERT－CC(设于卡内基梅隆大学内的保护因特网安全的机构)的忠告清单和新闻组网点的 Comp. security. announce 等便可获得网络漏洞信息,所以应及时获得网络漏洞信息,并采取相应措施。

(1)计算机病毒:是一种人为编制的、特殊的计算机程序,它通过自我复制传染给其他健康的程序和数据,对计算机系统的正常运行造成破坏和干扰,后果可能十分严重。

计算机病毒具有隐蔽性、潜伏性、传染性及破坏性等基本特点。

计算机病毒主要是通过软件的拷贝、共用或借用软盘及运行外来程序等途径传播。计算机病毒主要有文件型病毒、系统引导型病毒和复合型病毒等三大类。

(2)病毒预防的主要措施:防毒软件,主要由 SCAN 功能来检查病毒,再用 KILL 功能消除病毒。如 KV100、KV200 开放式自升级反(杀)病毒软件、CPAV 软件;

防病毒卡,是一种软、硬件结合的防毒技术。此卡插于计算机扩展槽中,监视、阻止病毒入侵或在病毒开始侵入时提醒操作者留意。

计算机病毒与防治

一、计算机病毒

计算机病毒是一种人为编制的、特殊的计算机程序,它通过自我复制传染给其他健康的程序和数据,对计算机系统的

此为试读,需要完整PDF请访问: www.ertongbook.com

正常运行造成破坏和干扰,后果可能十分严重。

计算机病毒具有隐蔽性、潜伏性、传染性及破坏性等基本特点。

计算机病毒主要是通过软件的拷贝、共用或借用软盘及运行外来程序等途径传播。

计算机病毒主要有文件型病毒、系统引导型病毒和复合型病毒等三大类。

病毒预防的主要措施:

(1)防毒软件:主要由 SCAN 功能来检查病毒,再用 KILL 功能消除病毒。如 KV100、KV200 开放式自升级反(杀)病毒软件;CPAV 软件,该软件既能消除病毒,还可实施免疫。

(2)防病毒卡:是一种软、硬件结合的防毒技术。此卡插于计算机扩展槽中,监视、阻止病毒入侵或在病毒开始侵入时提醒操作者留意。

特别注意:既不存在一个能检查出所有病毒的软件,也不存在能消除所有病毒的软件。

二、防治

(一)病毒预防

积极预防病毒感染是最重要的。预防的办法主要是:不使用来路不明的磁盘;对所有磁盘文件都要先检测后使用;安装防病毒卡或软件;对重要的文件或数据事先备份;发现可疑

情况及时采取措施。

(二)病毒检测

计算机感染了病毒以后往往不会马上发作,所以我们应当随时注意检测,及早发现及早清除。

(三)病毒清除

常用的杀毒软件有 KILL、KV300 和 AV95 等。

三、计算机一般操作、维护注意事项

注意为计算机供电的电源及其所处环境,切记要遵循合理的开机、关机顺序,整机搬运时做好软、硬驱的保护措施,注意将待用的软盘清洁并妥善保管,自觉保护知识产权、制止盗版非法软件的使用和流通。

垃圾邮件生态圈

时值 2004 年初,有关垃圾邮件的问题早已不再是一个单一的道德、法律或技术难题。当各种单一的手段都无法解决时,面对它、接受它,似乎就是不可避免的选择。这样的结局令人沮丧。但问题当然要比这复杂的多,如果仔细观察,我们就不难发现:围绕垃圾邮件,正在形成一个新的生态系统,活跃其中的包括了发送商、购买商、立法者、普通用户、反垃圾邮

件的IT厂商等多个主角。

垃圾邮件是继病毒之后又一个互联网怪胎。与病毒泛滥不同的是,病毒的制造者只追求个人改变世界的快感,而垃圾邮件却牵扯了太多的商业利益。反垃圾邮件是2003年互联网行业的热门话题之一,这个人人喊打的互联网公害是否真的完全是"垃圾"?

一、爱恨莫辨的垃圾邮件

第一个用电子邮件进行宣传和营销活动的人,或许把这种方式看作一个创举,但他一定不会预想到今天的广告电子邮件会泛滥以至成为危害。十几年前,当电子邮件作为一种新鲜应用刚刚进入网民生活的时候,能收到一两封信息丰富的陌生邮件还是令人兴奋的事情。然而网络发展到了今天,情况已经完全不同。据不完全统计,目前全球的电子邮件中,50%以上都是垃圾邮件。网民平均每天花费6.5分钟来处理这些无用的邮件。仅仅是计算下载并删除这些垃圾邮件所需要的上网费和电话费,全年就要花掉94亿美元。著名网络安全研究机构Radicati Group推测,垃圾邮件横行的情形若不进行有效的管束与遏止,则2007年时企业因垃圾邮件损失的金额将暴增到1980亿美元。

根据SBL database著名垃圾邮件对比资料库统计,全球10大垃圾邮件最严重的国家和地区,亚洲占了绝大部分,而中国更是仅次于美国高居第二。中国的6800万网民每年收到的垃圾邮件为460亿封,占全球的10.4%。中国互联网协

会12月公布的数据显示，截至11月底，2003年向中国服务器发送的垃圾邮件约有1500亿封，占我国互联网用户收到的电子邮件总数的30%，2003年垃圾邮件浪费的GDP高达48亿元人民币。

另外，由于接近90%的恶性病毒都是通过邮件传播，由此带来的影响和破坏程度更为严重。中国互联网协会秘书处处长李欲晓表示："垃圾邮件已经成为了一种社会公害，而且到了非除不可的地步。"

是谁发出了这些邮件？商业广告、宣传资料、传播病毒的谣言、网上杂志的订阅以及连环信式的Email，是垃圾邮件的主要构成。与电脑病毒不同的是，病毒大多是程序爱好者和黑客们的个人行为，带有明显的攻击性。而发送垃圾邮件大多是有组织的商业行为。收集邮件地址并出售的人，向企业提供电子邮件服务的人，购买这些地址、接受地址服务的人，电子邮件营销者都是这个垃圾邮件"产业链"不可缺少的环节。

邮件地址的提供者们声称自己拥有大量的邮件地址，比如1.6亿综合地址、8000万行业地址，最少的也是以10万为最低起付单位。获取邮件地址的方法多种多样，有人通过一些网页自动搜索软件，收集每个页面上的信箱。然而更多的是一些"技术落后"的个人垃圾信制造者，他们靠人工收集，登录到他人服务器，获取用户列表等方法来收集邮件地址。虽然此类垃圾信制造者取得的信箱数量不像自动软件那么多，但是因为是靠人工分析，所获地址大多都是真实的，危害反而

更大。更有甚者则是从一些提供邮件服务器的公司手里直接获得大量的用户信息。

在这个半地下的行业中,利用网络营销作幌子是一个好办法。使用这些服务的以中小企业为主,因为大规模的营销计划、广告投放可能会带来高额的费用,对他们而言,采用免费的电子邮件来散发广告似乎性价比更高,而他们也并不重视向他们提供地址服务的企业本身是否是垃圾邮件的制造者。一家企业管理培训公司的客户经理不无得意地说,每月付给地址提供商 1800 元,就能获得每月发送两次"企业、行业 1000 万邮件套餐"的服务,而收益竟然能够达到投资的三至七倍,"基本没有赔过"。据调查,邮件地址价格之间的差价高达 7040 倍,国内最低的价格为 20 元/1.6 亿个,最高的为 88 元/10 万个,价格的水分究竟有多大,外行实在难以揣测。而价格的高低则是根据服务的好坏,除了卖邮件地址,一些价格比较昂贵的地址提供商还会提供全程服务——帮客户制作简单的 Html 格式的广告并发送。

在中国,由于新闻组的不发达,深受垃圾邮件骚扰的大多是个人电子信箱,其中当然也不乏企业为员工所定制的工作邮箱。对于个人而言,删除这些垃圾固然是个麻烦事,但更加困扰的还是企业。当企业的邮件服务器被大量的垃圾邮件占据空间时,因为垃圾邮件而导致网络传输速率下降时,他们会迫不及待地寻求解决方案,于是企业级的反垃圾邮件方案成为了这个市场中最有吸引力的部分。

二、网民商家恩怨交织

也许垃圾邮件将引发出IT产业的下一个增长点。当年因为有了病毒,人们开始重视对数据和计算机本身的保护,数据存储业开始兴起,并且直到今天还是IT产业中最有前途和最为重要的领域。时至今日,已经没有人再怀疑反病毒软件的市场究竟有多大。三年前,互联网业遭受前所未有的泡沫大破灭时,网络安全和存储业却成为一剂强心针,在随时就可能倒下的IT大厦前重新树立起了人们对互联网的信心。垃圾邮件的发展与病毒何其相似!同属网络安全问题,同样具有强大的影响力和破坏性,同样经历了漫长时间的积累才最终爆发。

补漏是互联网以及任何行业进步的重要渠道。也许垃圾邮件的出现根本上在于网络本身的缺陷。定义电子邮件20多年的协议SMTP存在一个致命的缺陷就是“信任”。SMTP原型协议的共同作者、新墨西哥大学访问讲师Sluizer认为,该协议建立在真实身份的基础上,这种信任没有考虑到之后出现的病毒、非法电子邮件和大量的宣传广告。而人们需要对这个原有的协议进行不断的改进和修订,以改变信任所带来的危机,但是试图在现有系统上修复问题总是比制定新的协议更难。问题的解决还有待于下一代IPv6网络的广泛应用。

无法从源头遏制垃圾邮件,面对来势汹涌的垃圾邮件,人们开始为反垃圾邮件“买单”。有机构预测,销售反垃圾邮件

此为试读,需要完整PDF请访问: www.ertongbook.com