文章编号:1000 - 582X(2003)09 - 0141 - 04

网络型病毒与计算机网络安全*

姚渝春,李 杰,王成红
(重庆大学 应用技术学院,重庆 400030)

摘 要:传统的计算机病毒分类法常以寄生对象为标准将病毒分为文件型、引导型和混合型,但根据当前病毒发展的趋势,应增加一类网络型病毒。网络型病毒的寄生对象广泛、传播速度快、危害广,它利用 Internet 的开放性和软件系统的缺陷,破坏网络中的各种资源以及网络通讯,某些种类的网络病毒还是黑客工具。因此结合多个具体实例,分析了网络型病毒对网络安全的危害,提出网络型病毒的防治应首先从管理措施上着手,并综合防火墙技术、病毒防治软件、软件更新、数据备份等多种技术措施。

关键词:计算机病毒分类;计算机病毒;计算机网络安全;网络型病毒;病毒防治
中图分类号:TP309.5 **文献标识码**:A

2003 年 1 月 25 日对于 Internet 来说是灾难的一天,从北京时间当天上午开始,国际互联网在全球范围内遭受不明病毒攻击,网络服务大面积中断,许多商务网站和 ISP 损失惨重;预计全球至少有 22 000 个系统遭到了攻击,具体的损失暂时无法估计……。该病毒的机理已经基本查清,这是一种专门针对微软 SQL Server 2000 的 1434 端口缓冲区溢出漏洞对其服务进行攻击的蠕虫病毒。该病毒暂定名为“Win32. SQLExp. Worm”或“蠕虫王”。

此次灾难再次向我们敲响警钟,正如赛门铁克的高级经理奥利佛 - 弗里德里希所说:“互联网仍然不是很稳定”。若疏与管理和防范,网络灾难将给我们造成巨大的损失。并且,随着世界对互联网的依赖程度增加,损失会进一步增大。

1 影响网络安全的几个因素

网络安全的一个通用定义是:网络安全是指网络系统的硬件、软件及其系统中的数据受到保护,不因偶然的或者恶意的原因而遭到破坏、更改、泄漏;系统连续可靠正常地运行,网络服务不被中断。网络安全的内容包括了系统安全和信息安全 2 个部分。系统安全主要指网络设备的硬件、操作系统和应用软件的安全;信息安全主要指各种信息的存储、传输的安全,具体体现在信息的完整性、可用性和保密性上[1]。

对计算机网络安全的威胁主要来自 5 个方面:1)人为的失误,如错误的指令、错误删除修改数据、不适当的系统配置等;2)自然灾害,如地震、火灾、雷击等;3)计算机病毒;4)人为的主动攻击和入侵,也就是常说的“黑客”(Hacker);5)计算机由操作系统、应用软件以及各类通讯协议的“BUG”所引起的安全漏洞。在网络时代的早期,安全问题失主要是由第一、二两个方面造成的,特别是人为失误,NCSA(美国国家计算机安全联合会)1994 年的调查报告表明,在当时的网络安全问题中有 75% 左右是由人为失误造成的[2]。随着科技水平的发展,设备性能和人员素质不断提高,由人为失误和自然灾害引起的网络安全问题逐年减少。取而代之的是由黑客、病毒、和各种“BUG”造成的网络安全问题已经占到 80% 以上,这与国际互联网的开放性、广泛性和不稳定性是相关的[3]。因此,目前在考虑网络安全问题时,应把重点放在对病毒、黑客和“BUG”的防治上。

2 网络型病毒的特点

病毒是人为编制的对计算机系统有危害的计算机程序或代码。从 20 世纪 80 年代初病毒开始大范围流行至今,在短短 20 年的时间里,病毒的种类、数量、传播速度、传播范围以及危害程度大大增加。病毒的分类方法多种多样,如按病毒的寄生对象、危害程度、链接方式、特有算法等,较多采用的是按寄生对象将病毒分为引导型、文件型和混合型 3 种。但根据目前病毒发展的趋势,普遍认为应增加一类网络型病毒[4]。在按病毒寄生对象分类法中提出网络型病毒,似乎有分

* 收稿日期:2003 - 04 - 01
作者简介:姚渝春(1967 -),男,重庆人,重庆大学工程师,主要从事计算机实验技术研究。

类重叠的嫌疑,但网络型病毒的很多特点是以上3类病毒所没有的。因此,将它单独列为一类是必要的。网络型病毒主要有以下一些特点:

1)它主要通过网络传播,在网络环境才能发挥最大破坏作用。比如"木马"类病毒,离开网络,它最大的危害仅仅是消耗一点点系统资源而已。

2)它的寄生宿主广泛,可能会寄生在HTM、ASP等多种文件中,也可能隐藏在邮件中,甚至可能不感染任何对象,仅存在于源宿主中,但可通过网络传播对计算机的端口、服务、数据、缓冲区进行攻击的指令,所以网络型病毒的检测、防范难度很大。

3)网络型病毒一般是利用Internet的开放性、操作系统及各类应用程序的漏洞来对计算机系统进行攻击,为了防范它往往要对某些网络功能进行限制。

4)一些网络型病毒还常常与黑客有联系,最典型的就是"木马"类病毒。

5)网络型病毒发展趋势迅猛,近3年来流行的病毒,除宏病毒外,基本都属于网络型病毒。网络型病毒的传播速度快、危害范围广。

目前,病毒的传播途径大多数都是通过网络,但不是所有通过网络传播的病毒都是网络型病毒,必须符合以上特征才属于网络型病毒。

3 网络型病毒的种类及传播方式

3.1 网络型病毒的分类

对于网络型病毒的分类,目前还没有统一的标准,特别是病毒的命名尤其混乱。这对病毒研究以及病毒防治知识的普及很不利。笔者认为:对于网络型病毒,以操作系统平台或传播方式分类有严重的重叠分类问题,以病毒名分类随意性太大,比较合理的分类方法是依据病毒的攻击手段。从目前的情况来看,以攻击手段可将网络型病毒分为蠕虫和木马两大类型。

蠕虫(Worm)是通过分布式网络来扩散传播特定信息或错误,破坏网络中的信息或造成网络服务中断的病毒。蠕虫泛滥发生在近几年,但早在1982年,Shock和Hupp就提出了一种"蠕虫"(Worm)程序的思想,这种"蠕虫"程序常驻于一台或多台机器中,并有自动重新定位的能力。如果它检测到网络中的某台机器未被占用,它就把自身的一个拷贝(一个程序段)发送给那台机器。早期的"蠕虫"程序不一定是有害的,它可用作Ethernet网络设备的诊断工具。"蠕虫"一般由两部分组成:一个主程序和一个引导程序。主程序一旦在机器上执行,就会通过读取公共配置文件并收集当前网络状态信息,获得与当前机器联网的其它机器的信息和软件缺陷,主动尝试利用所获得的信息以及其他机器的缺陷在这些远程机器上建立其引导程序。

从以上描述可以看出,蠕虫病毒最主要的特点是利用网络中软件系统的缺陷,进行自我复制和主动传播。2003年1月25日首次发作Win32.SQLExp.Worm病毒就是一个非常典型的蠕虫病毒,它具备了蠕虫病毒所有的典型特征。

木马又称特洛伊木马(Trojan horse),它原本属于一类基于远程控制的工具。木马的运行模式属于客户/服务模式,它包括两大部分,即客户端和服务端。其原理是一台主机提供服务(服务器),另一台主机接受服务(客户机),作为服务器的主机一般会打开一个默认的端口进行监听。如果有客户机向服务器的这一端口提出连接请求,服务器上的相应程序就会自动运行,来应答客户机的请求。这个程序被称为守护进程。木马通常的攻击步骤是:1)设定好服务器程序;2)骗取对方执行服务器程序;3)寻找对方的地址IP;4)用客户端程序来控制对方的计算机。木马之所以能够运行的原因是由于用户的程序通常继承了与用户相同的、唯一的优先权和存取权。它能够在不触犯系统任何安全规则的情况下进行非法活动,系统本身不能区分木马和合法程序[5]。通常所说的木马病毒其实就是这个服务端程序,它通过电子邮件或网页传播到用户的计算机中,一旦计算机执行这段程序,它就变成一个受客户端控制的服务器。木马常常被黑客用来作为窃取信息以及非法使用资源的工具。

3.2 网络型病毒的传播方式

网络型病毒的传播方式主要有3种:电子邮件、网页、文件传输。其中主要是通过前2种方式,特别是电子邮件。

通过电子邮件传播的病毒,其病毒体一般隐藏在邮件附件中,只要执行附件,病毒就可能发作。有些种类的邮件病毒,甚至没有附件,病毒体就隐藏在邮件中,只要打开或预览邮件,都会遇到麻烦。邮件病毒的编写者很热衷于使用脚本,特别是使用VBScript脚本编写病毒代码,VBScript又通过Windows Script Host来解释执行,一个脚本程序能调用功能更大的组件来完成自己的功能,病毒还可能将代码自动加入到附件发送到网络中,实现病毒的主动传播。近年来流行的很多病毒,如"梅丽莎"、"爱虫"等都是通过邮件传播的。

为了增加网页的交互性、可视性,通常需要在网页中加入某些Java程序或者ActiveX组件,这些程序或组件正是病毒的宿主。如果你浏览了包含病毒代码的这类网页,且浏览器未限制Java或ActiveX的执行,其结果就相当于执行病毒程序。

4 网络型病毒的防治措施

同传统的病毒防治措施一样,网络型病毒的防止措施应包括管理措施和技术措施两个方面,只有两者

完美的结合，才能达到最佳的防治效果。

4.1 管理措施

在管理措施方面，至少应做到以下 3 点：1）树立病毒防范意识，让每个操作人员都了解病毒的危害，并自觉地采用防护手段；2）根据各自的特点，制定严格的、可行的操作规程，并保证制度落实；3）及时掌握病毒动态，根据流行病毒的特点，修改和完善防治措施。CA 的工程师们曾说过：在病毒攻击面前损失最小的往往不是使用最先进防护软件的专家，而是循规蹈矩执行制度的人。这说明了严格执行管理制度的重要性。

4.2 技术措施

由于网络型病毒固有的特性，采用传统的病毒防治技术是远远不够的。在考虑技术措施时，首先应遵循“木桶原则”，即从最薄弱环节着手。既然网络型病毒的主要传播方式是电子邮件、浏览器，那么安装防火墙和带有病毒实时检测、邮件监控、浏览器监控、文件传输监控功能的病毒防治软件是所有技术措施中最重要的部分。当然，其他的辅助措施也是不可少的。

1）使用防火墙与病毒防治软件

防火墙能选择性地限制网络中的各类访问，如共享资源访问、IP 探测、NETBIOS 名称探测、UDP 和 TCP 端口访问等等，它能有效地将内部网络和外部网络隔离，切断病毒的传播途径。“探测”往往是攻击的前奏，端口访问权限是许多蠕虫和木马发作的必要条件，切断这些途径，一般网络型病毒是不能产生破坏作用的。

防火墙的功能只是限制网络的访问，检测和清除病毒还要靠病毒防治软件。目前的病毒检测原理大致有特征码法、校验和法、行为码法 3 种类型。特征码法能有效地检测和清除已知病毒；校验和法对要改变文件内容或属性的病毒非常敏感，但误报率较高，且不能清除；行为码法对于未知病毒效果好，但同样存在误报率高的缺陷。目前的病毒防治软件基本上同时采用了这 3 种方法，以提高病毒的检测和清除率。

根据《2002 年国产病毒防治软件测评报告》所公布的结果来看，目前的病毒软件一般都加入防火墙功能，是集反毒、反黑、救护于一身的产品，对于网络型病毒的防治是很有效的。在选择这些软件时，应结合具体情况，普通的小型办公网络使用国产的瑞星、金山毒霸、KV3000 等软件即可，这些软件的通用性好、防毒防黑的效果理想、升级方便、价格也很便宜；但对于重要的电子商务网站，则应该考虑安装专业性更强、可靠性更高、安全机制更严密的系统，如 CA 的 E－Trust 等。使用防火墙和病毒检测软件会降低整个系统的性能，比如限制端口访问可有效预防木马，同时也会使某些服务无法启动，因此，病毒的防治还应掌握“适度原则”[6]。

2）及时升级软件

利用软件系统的缺陷是网络型病毒的一个重要特点，因此，及时升级软件、弥补缺陷是防治网络型病毒的有效手段。微软公司于 2002 年 7 月公布了 Microsoft SQL Server 2000 的一个“关键性”漏洞，并提供了名为“sql2sp3”的补丁程序，2003 年 1 月 25 日的在世界范围内爆发的“蠕虫王”正是利用了这一缺陷，在此次事件中直接受损的均是未安装补丁的用户。病毒防治软件中的病毒数据库也需要经常更新，防毒软件生产商不断在收集新的病毒特征码，以保证对新型病毒的准确检测。

3）合理安装和设置软件

网络型病毒很少像传统病毒一样调用汇编程序来实现破坏功能，而常常利用操作系统提供某些功能模块。用 VBScript 脚本语言编写蠕虫病毒就是通过 Windows Script Host 来解释执行的。因此，在安装软件时一定不要贪图大而全，不要安装和启动那些不需要服务程序或组件，如 FTP、IIS、TELNET、Windows Script Host 等等。正是这些服务支持了 Internet 的开放性，同时也为病毒和黑客提供了可乘之机。

合理设置软件对于防止病毒的传播很有效，大多数利用 VBscript 编写的病毒是利用程序将自身的脚本内容复制到一个临时文件中，然后再将其作为附件发送出去。该功能的实现离不开" FileSystemObject" 对象，因此利用 regsvr32 scrrun. dll /u 命令禁止了" FileSystemObject" 就能有效地控制 VBS 病毒的传播；合理地设置浏览器的参数（如禁用 Java、ActiveX 控件及插件等），可防止多数通过网页传播的病毒；此外，杜绝随意共享资源、不设置用户密码、随意接收转发来历不明的邮件等不良操作习惯，也可一定程度地防止网络病毒的入侵和传播。

4）定期备份重要数据

除了以上防治措施，数据备份是一个很好的补救办法，它可将由病毒造成的损失减小到最低程度。数据备份的频率、手段以及范围由数据的重要程度决定。

5 结束语

网络型病毒利用 Internet 的开放性，针对软件系统和通信协议的特定缺陷，对网络中的各种资源和网络通讯进行攻击，具有传播速度快、危害广、防治难的特点，它已经成为危害网络安全最重要的因素之一。网络型病毒的防治应首先从管理措施上着手，并结合防火墙技术、病毒防治软件、软件更新、数据备份等多种技术措施。

参考文献:

[1] 中华人民共和国国家经济与贸易贸委员会. 中国企业互联网应用和电子商务发展水平综合调查报告[EB/OL]. http: //www. xixia. org/xixianews/news/137. html,2002 - 10 - 20.

[2] OTHMAR KAYS. 网络安全技术[M]. 北京:中国水利水电出版社,1998.

[3] 李冰. 网络攻击的六大趋势[J]. 科技广场, 2002,(8): 1 - 4.

[4] 宁章. 计算机及网络安全与防护基础[M]. 北京:北京航空航天大学出版社,1999.

[5] 霍宝锋. 常见网络攻击方法及其对策研究[J]. 计算机工程,2002,(8):9 - 11.

[6] 卢文斌. 网络环境下计算机病毒的防治策略[J]. 湖北电力,武汉:2002,(4):30 - 32.

Network Virus & Network Security

YAO Yu-chun, LI Jie, WANG Cheng-hong

(College of Polytechnic , Chongqing University , Chongqing 400030, China)

Abstract: Computer virus is usually divided into file mould virus , boot virus and compound virus . But now , we should add network virus in it . Network virus has wide host objects , high spread speed and high dangers . It destroys information and data communication in network by making full use of Internet and software BUG . Some network virus can be used by hacker . This paper analyses the harm of network virus, and suggests some solutions.

Key words: computer virus classification; computer virus; network security; network virus; anti - virus

(编辑 张 苹)

(上接第 133 页)

Immune Algorithm and Its Application to Multi - modal Function Optimization Based on Immune Response Principle

ZHANG Zhu-hong[1,2], *HUANG Xi-yue*[1]

(1. College of Automation, Chongqing University, Chongqing 400044, China;
2. Deparetment of Mathmaticsa, Guizhou University, Guizhou 550025, China)

Abstract: An immune algorithm, applied to multi - modal function optimization, is proposed based on real decoding and niche and immune response principle of the immune system to be compared with GA. Its key is to design evaluating rule for antibodies and affinition mutation operator, and introduce niching technology to strength population diversity. It has such properties as determining population size automatically, parallel search optimum, strong robustness, and so forth. Besides, its convergence is proved. Simulation shows that the algorithm is better than the algorithm REGA, which hints that immune algorithms are a potential research area.

Key words: immune algorithm; immune response; niche; global convergence

(编辑 吕赛英)