几种检测计算机病毒的方法研究

姚学武,李 广

(大同供电分公司科技信息中心,山西 大同 037008)

摘 要:随着网络技术的迅猛发展,人们日常生活和工作已经越来越离不开计算机网络,这使得计算机的安全问题显得特别重要。基于这些原因,目前在反病毒技术中,最重要的就是"防杀结合,防范为主"。文章介绍了几种检测计算机病毒的方法。

关键词:计算机病毒;检测;防范
doi:10.3969/j.issn.1006-8554.2011.06.191

根据计算机病毒的特点,人们找到了许多检测计算机病毒的方法。由于计算机病毒与反病毒是互相对抗发展的,任何一种检测方法都不可能是万能的。综合运用各种检测方法,并在此基础上根据病毒的最新特点,不断改进或发现新的方法才能更准确地发现病毒。

1 外观检测法

外观检测法是在病毒防治过程中起着重要辅助作用的一个环节。当病毒侵入计算机系统后,会使计算机系统的某些部分发生变化,出现一些异常,如屏幕显示的异常现象、系统运行速度的异常、打印机并行端口的异常、通信串行口的异常等现象。可以根据这些异常现象来判断病毒的存在,及时地发现病毒,并作相应处理。

2 特征代码法

将各种已知病毒的特征代码串组成病毒特征代码数据库。这样,可以在通过各种工具软件检查、搜索可疑计算机系统时,用特征代码数据库中的病毒特征代码逐一比较,就可以确定被检计算机系统感染了何种病毒。

在很多著名的病毒检测工具中广泛使用特征代码法。专家认为,特征代码法是检测已知病毒的最简单、最适用的方法。

一种病毒可能感染很多文件或计算机系统的多个地方,而且,在每个被感染的文件中,病毒程序所在的仿造也不尽相同。但是,计算机病毒程序一般都具有明显的特征代码,这些特征代码,可能是病毒的感染标记特征代码,不一定是连续的。只要是同一种病毒,在任何一个被该病毒感染的文件或计算机系统中,总能找到这些特征代码。

3 虚拟机技术

多态性病毒或多型性病毒,即俗称变形病毒。多态性病毒每次感染后都改变其病毒密码,这类病毒的代表是幽灵病毒。多态和变形病毒的出现,让传统的特征值查毒技术无能为力。之所以造成这种局面,是因为特征值查毒技术是对于静态文件进行查杀的,而多态和变形病毒只有在开始运行后才能够显露原形。

虚拟机技术是一种软件分析器,在机器的虚拟内存中,用软件方法来模拟和分析不明程序的运行。在执行过程中,从虚拟机环境内截获文件数据。如果含有可疑病毒代码,则杀毒后将其还原到原文件中,从而实现对各类可执行文件内病毒的查杀。

4 启发式扫描技术

病毒和正常程序的区别可以体现在许多方面。一个运用启发式扫描技术的病毒检测软件,实际上就是以特定方式实现的动态高度器或反编译器,通过对有关指令序列的反编译逐步理解和确定其蕴藏的真正动机。

在具体实践上,启发式扫描技术是相当复杂的。通常这类病毒检测软件要能够识别并探测许多可疑的程序代码指令序列,这些功能操作将被按照安全和可疑的等级进行排序,并且根据操作特点赋予不同的加权值。如果对于一个程序的加权值的总和超过一个事先定义的数值,那么,病毒检测程序就可以声称"发现病毒"。为减少谎报,最好把多种可疑功能操作同时并发。另外,目标代码的前后逻辑关系也是启发式扫描需要注意的问题。

对于蠕虫病毒来说,蠕虫的传播技术是其本质。一个蠕虫病毒可以以文件的形式独立存在,清除这样的蠕虫病毒比较简单,只需要删除其可执行文件就可以了。当然,蠕虫病毒也可以感染文件,但那是与传统病毒技术相结合的产物。清除技术并不只是删除蠕虫可执行文件那么简单,要把蠕虫病毒对系统所作的修改尽量恢复回来。对于已知病毒,人们可以通过对路径详细剖析来得知蠕虫所做的修改行为,再把系统恢复过来,但这仅限于已知蠕虫。对于未知蠕虫病毒,各种关键技术还不成熟。要对系统进行恢复,就要知道蠕虫究竟对系统做了些什么。以前,都是通过人工的方法,由反病毒工程师完成这项工作。现在,如果改由程序自动实现,其难度很大。

5 防范计算机病毒的基本方法

目前,反病毒的主流技术还是以传统的"特征码技术"为主,以新的反病毒技术为辅。因为新的反病毒技术还不成熟,在查杀病毒的准确率上,与传统的反病毒技术还有一定的差距。特征码技术是传统的反病毒技术,但是,"特征码技术"只能查杀已知病毒,对未知病毒则毫无办法。所以,很多时候都是计算机已经感染了病毒,并且对机器或数据造成很大破坏后才去杀毒。防范计算机病毒的基本方法有以下几种。

(1)不轻易上一些不正规的网站。在浏览网页的时候,很多人有猎奇心理,而一些病毒、木马制造者正是利用人们的猎奇心理,引诱大家浏览他的网页,甚至下载文件,殊不知这样很容易使计算机染上病毒。

(2)提防电子邮件病毒的传播。能发送包含ActiveX控件的HTML格式邮件可以在浏览邮件内容时被激活,所以,在收到陌生可疑邮件时,尽量不要打开,特别是对于带有附件的电子邮件更要小心。很多病毒都是通过这种方式传播的,甚至有的是从你的好友发送的邮件中传到你机器上感染你的计算机的。

(3)对于渠道不明的光盘、软盘、U盘等便携存储器,使用之前应该查毒。对于从网络上下载的文件同样如此。因此,计算机上应该装有杀毒软件,并且及时更新。

(4)经常关注一些网站、BBS发布的病毒报告,这样可以在未感染病毒的时候做到预先防范。

(5)对于重要文件、数据做到定期备份。

(6)不能因为担心病毒而不敢使用网络,那样网络就失去了意义。只要思想上高度重视,时刻具有防范意识,就不容易受到病毒侵扰。

参考文献:

[1] 孟宏涛.计算机病毒的危害及防范[J].科技情报开发与经济,2006,(16).

[2] 于泠,陈波.计算机网络反病毒解决方案[J].南京师大学报(自然科学版),2001,(2).