一种启发式反病毒技术的研究

谭云松
武汉工程大学计算机科学与工程学院 湖北 430073

摘要：本文主要讨论了反病毒技术的一般原理和技术，并针对常用反病毒方法存在的问题，提出了启发式反病毒的基本原理与实现方法。

关键词：病毒；扫描技术；启发式分析

0 引言

随着个人计算机的日益普及和因特网快速发展，计算机病毒越来越受到人们的普遍关注，计算机病毒是具有自我复制能力的计算机程序，它能影响计算机软件、硬件的正常运行，破坏数据的正确性与完整性，造成计算机或计算机网络瘫痪，给人们的经济和社会生活造成巨大的损失。面临这一问题，人们采取了许多行之有效的反病毒措施，本文分析的就是一种启发式反病毒技术。

1 反病毒技术原理

目前的反病毒技术主要有虚拟机分析器和病毒代码文件定位两种方式，其主要操作方法是：取得病毒代码后，对其进行分析，找到病毒在文件中的偏移位置，再将其删除。这种技术对于查杀早期的病毒十分有效，因早期的病毒相对稳定且变种较少，一般感染可执行文件，因此反病毒技术主要针对二进制可执行代码，但随着网络的日益普及，网络病毒日益猖獗，且病毒种类多，变化快。

1.1 反病毒技术的一般方法

反病毒杀毒软件是对付计算机病毒的最有效方法，但没有杀毒软件能100%地保证系统不被病毒感染。试验者Fred Cohen已证实在有限理论的基础上不可能存在绝对的防毒，从杀毒技术上来讲当前最流行的杀毒软件常用到扫描器技术，扫描的算法有多种，通常为了使杀毒软件功能更强大，会结合使用好几种扫描方法和技术，其一般可分为特征代码法、校验和法、行为监测法、软件模拟法、VICE先知扫描法等，这些方法原理各不相同，检测范围也不同，各有所长。特征代码法是分析出病毒的特征病毒码并集中存放于病毒代码库文件中，在扫描的时候将扫描对象与特征代码库比较，如有吻合则判断为染上病毒；校验和法就是根据被感染的程序大小的增加或者日期的改变这种行为来进行判断；行为监视法就是引入一些人工智能技术，通过分析检查对象的逻辑结构，将其分为多个模块，分别引入虚拟机中执行并监测，从而查出使用特定触发条件的病毒；VICE先知扫描法是直接模拟CPU的动作来侦测出某些变种病毒的活动情况，并且分析出该病毒的病毒码。

1.2 扫描技术的分析

反病毒中的扫描技术能对系统的完整性、安全性进行检查，目前有如下常用的扫描方式：

(1) 病毒扫描，病毒扫描是当前最主要的查杀病毒方式，它主要通过检查文件，扇区和系统内存，用标记查找已知病毒，病毒标记就是病毒常用代码的特征。

(2) 启发式扫描，启发式扫描是通过分析指令出现的顺序，或组合几种情况来决定文件是否被感染，每个对象都要检查。这种方式查毒效果是最好的，但也最有可能出现误报。

(3) CRC扫描的原理是计算磁盘中的实际文件或系统扇区的CRC值，这些CRC值被杀毒软件保存到它自己的数据库中。在执行杀毒软件时，用备份的CRC值与当前计算的值比较，可知道文件是否已被修改或被病毒感染。

各种扫描都有自己的优缺点，拥有一个病毒库是它们的基本特征。但如果病毒库过大的话，查毒速度会变得很慢。有些方法还能够根据病毒修改注册表的特点，提供了注册表扫描功能。它们会将已知病毒常用的数百注册表项列出，让用户判断是否删除相应的项目，病毒试着修改这些键值时，实时检测工具还能阻止并询问用户是不是要执行。这类软件对新病毒的预防提供了很大帮助。另外，类似Microsoft Base Secttrity Analyzer、SREng等工具可以扫描系统的漏洞、配置错误和其他风险，并自动修补系统漏洞．系统扫描技术面对更新颖的攻击思路时显得无能为力，一旦病毒超出了已知的攻击行为，原有的行为特征便不再有效。这需要一种新的模式来对付未知病毒和病毒变种。

2 启发式模块分析

2.1 启发式分析的工作流程

启发式指的是具有自我发现的能力、运用某种方式和方法来判定事物的知识和技能。启发式分析就是利用计算机病毒的行为特征，结合以往的知识和经验，对未知的可疑病毒进行分析与识别。

启发式分析流程如图1所示。

启发式分析模块可以通过对某些行为进行分析，或者对代码进行反编译并对指令序列进行分析，从而获得感兴趣的数据。启发式分析技术中使用了启发式系统参数扫描和启发式代码扫描两种技术。启发式分析软件在对代码反编译以后，

作者简介：谭云松(1972-)，男，武汉工程大学计算学院。研究方向：网络信息安全。

使用启发式扫描技术对反编译代码进行扫描，一旦发现这样的异常的行为，就有理由怀疑该驻留软件有病毒。

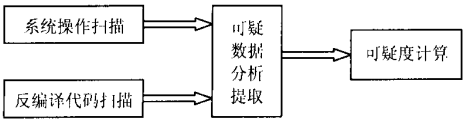

图1 启发式分析模块流程

2.2 启发式分析的实现原理

在具体实现上，启发式扫描技术是相当复杂的，通常这类检测软件不仅要对系统进行扫描，还要能够识别并探测许多可疑的程序代码指令序列，如格式化磁盘类操作，搜索和定位各种可执行程序的操作，实现驻留内存的操作，发现非常的或未公开的系统功能调用的操作，同时还要根据各个可疑指标的可疑程度，制定权值，并使用特定的规则进行计算，将得到的值与事先确定的临界值比较，如果比临界值大，则确定为病毒。

可以定义 F=a1*Oper1+a2*Oper2+……+an*Oper n，其中，an 表示相应参数的权值，Oper n 表示操作或行为，满足 a1+a2+……+an = 1，an的取值体现了相应标志在病毒特征中的重要程度。F的值反映了程序为病毒程序的可疑度，显然F的取值范围为0与1之间。

我们还必须指定一个临界值，使得当F大于临界值时，系统通过信使向后台的专家系统发信息，取得专家系统的帮助。当然，临界值的取法，不能够凭空臆断，也不可能通过严格的计算或证明得到，因为病毒具有不可预见性。我们只有通过大量的实验，结合要进行分析的数据，综合考察之后，抽取各异常度，才能够获得这样一个至关重要的值。这个值的取值的好坏，会直接关系到这个启发式分析模块的工作效率。

3 提高启发式分析的效率

为了使漏报率和误报率达到最小，必须努力做好以下几点：

(1) 对常规程序代码和特定程序的识别能力。某些编译器提供运行时的实时解压或解码的功能，为了避免检测时的误报，应当在检测程序中加入识别这些情况的功能模块。

(2) 对临界值行为的准确把握，精确定义可疑功能调用标志集合。结合大量的实验，准确定义公有特征，以及其对应的加权值。

(3) 对于特定的类似于病毒的程序，只要用户不同意启发式分析就不报警，并且将其特征写入数据库中记忆下来。也就是说，启发式分析模块要设计出自学习的功能模块，记住那些非病毒的文件，避免再次报警。

当然，不管采用什么样的措施，虚警谎报现象总是要存在的。用户的参与对查杀软件来说也是必不可少的，他们要在某些报警信息出现时作出自己的判断，这通常取决于应用启发式代码分析检测技术查病毒程序的具体解释。

4 结论

不管启发式分析有怎样的缺点和不足，启发式分析技术代表着未来反病毒技术发展的必然趋势，是一种正在发展和不断完善中的新技术，和其它的扫描分析技术相比，启发式分析扫描技术几乎总能提供足够的辅助判断信息，让我们最终判定被检测的目标对象是否为病毒，启发式扫描技术，难免存在对病毒的误报和漏报，所以我们在实际的应用中，最好将其与传统的扫描技术相结合，这样才能够更有效地对病毒实施检测，从而提高查杀病毒的效率，为未来的一般性防毒杀毒技术奠定基础。

参考文献

[1]张友生,米安然.计算机病毒与木马程序剖析.北京科海电子出版社.2003.

[2]单长虹,张焕国,孟庆树,彭国军.一种启发式木马查杀软件的设计与分析.计算机工程与应用.2004.

[3]曾宪伟,张智军,张志.基于虚拟机的启发式扫描反病毒技术.计算机应用与软件.2002.

The Research on a Heuristic Technique of Computer Antivirus

Tan Yunsong

School of Computer in Wuhan Institute of Technology,Hubei,430073

Abstract:A principle and technology of antivirus theory is discussed in this paper.A heuristic technique of Computer Antivirus is presented against the disadvantage of the conventional antivirus methods.

Keywords:virus,scanning technology,heuristic analysis

[上接81页]

The Strategy Research for Campus Network's Stable Working

Chen Yijun

Modern Educational Technology Center of Nantong University,Jiangsu,226007

Abstract:At the time of raising the teaching quantity and lifting work efficiency,network also provide the place for the virus dissemination and the attack.If we don't respond to rightly and immediately,they will be obstruct the campus network's stable working.Campus network faces more and more safe threat when its application extends contiously, we need to adopt measure to guarantee campus network.

Keywords:campus network;network security;virus

一种启发式反病毒技术的研究

作者： 谭云松， Tan Yunsong
作者单位： 武汉工程大学计算机科学与工程学院,湖北,430073
刊名： 网络安全技术与应用
英文刊名： NETWORK SECURITY TECHNOLOGY & APPLICATION
年，卷(期)： 2006(11)
被引用次数： 1次

参考文献(3条)

1. 张友生;米安然 计算机病毒与术马程序剖析 2003

2. 单长虹;张焕国;孟庆树;彭国军 一种启发式木马查杀软件的设计与分析[期刊论文]-计算机工程与应用 2004(20)

3. 曾宪伟;张智军;张志 基于虚拟机的启发式扫描反病毒技术[期刊论文]-计算机应用与软件 2002(9)

本文读者也读过(9条)

1. 孙伟.冯萍.SUN Wei.FENG Ping 一种启发式宏病毒扫描技术[期刊论文]-长春大学学报（自然科学版） 2007,17(1)

2. 崔鹏.CUI Peng 基于形式化语义的启发式病毒检测引擎研究[期刊论文]-辽东学院学报（自然科学版） 2008,15(3)

3. 曾宪伟.张智军.张志.Zeng Xianwei.Zhang Zhijun.Zhang Zhi 基于虚拟机的启发式扫描反病毒技术[期刊论文]-计算机应用与软件2005,22(9)

4. 黄锦煜 浅谈基于主动防御的网络病毒防御技术[期刊论文]-科教导刊2009(4)

5. 崔鹏.CUI Peng 基于语义的启发式病毒检测引擎研究[期刊论文]-常熟理工学院学报2008,22(10)

6. 张青霞.杨吉峰 二进制病毒的启发式扫描技术[期刊论文]-农业网络信息2006(8)

7. 王振海.王海峰.WANG Zhen-hai.WANG Hai-feng 基于多态病毒行为的启发式扫描检测引擎的研究[期刊论文]-实验室研究与探索2006,25(9)

8. 任师尊.REN Shi-zun 病毒检测技术在查杀"熊猫烧香"中的实证分析[期刊论文]-长春大学学报（自然科学版） 2007,17(6)

9. 王振海.王海峰.Wang,Zhenhai.Wang,Haifeng 针对多态病毒的反病毒检测引擎的研究[期刊论文]-微计算机信息 2006,22(27)

引证文献(1条)

1. 曾志军.唐文胜.尹丹 基于入侵检测模型的蠕虫病毒诱捕系统的研究[期刊论文]-电脑知识与技术 2009(21)