Journal of Computer Applications
计算机应用,2015,35(3):756 – 760
ISSN 1001-9081
CODEN JYIIDU
2015-03-10
http://www.joca.cn

文章编号:1001-9081(2015)03-756-05
doi:10.11772/j.issn.1001-9081.2015.03.756

基于运动轨迹分析的启发式木马检测系统

钟明全[1*],范 宇[2],李焕洲[1],唐彰国[1],张 健[1]
(1.四川师范大学 网络与通信技术研究所,成都 610066; 2.四川省标准化研究院 信息发展部,成都 610031)
(*通信作者电子邮箱 mqzhong@sina.com)

摘 要:针对主动防御技术检测准确率不高的问题,提出了一种基于运动轨迹分析的启发式木马检测系统。提出了两种典型的木马运动轨迹,利用运动轨迹上的行为数据,结合判定规则与算法,实现对可疑文件危险等级的检测。实验结果表明,该系统检测未知木马性能优于传统方法,并且能够检测一些特殊木马。

关键词:主动防御;虚拟机;运动轨迹;文件捆绑;隐藏进程
中图分类号:TP309.2 **文献标志码**:A

Heuristic detection system of Trojan based on trajectory analysis

ZHONG Mingquan[1*], FAN Yu[2], LI Huanzhou[1], TANG Zhangguo[1], ZHANG Jian[1]
(*1. Institute of Network and Communication Technology, Sichuan Normal University, Chengdu Sichuan* 610066, *China*;
2. Information Development Department, Sichuan Institute of Standardization, Chengdu Sichuan 610031, *China*)

Abstract: Concerning of the low accurate rate of active defense technology, a heuristic detection system of Trojan based on the analysis of trajectory was proposed. Two kinds of typical Trojan trajectories were presented, and by using the behavioral data on Trojan trajectory the danger level of the suspicious file was detected with the decision rules and algorithm. The experimental results show that the performance of detecting unknown Trojan of this system is better than that of the traditional method, and some special Trojans can also be detected.

Key words: active defense; Virtual Machine (VM); trajectory; file binding; hidden process

0 引言

随着互联网的不断普及,通过互联网实现远程办公、查阅资料、网络购物、下载软件已经是很普遍的事情。人们感受到互联网的巨大魅力,提高了工作效率,改善了生活方式。然而,网络并非十全十美,其中也潜伏着危机。比如,当用户访问了一个未知网站后,轻则计算机速度明显变慢,重则系统崩溃;再者,当用户下载文件后,用杀毒软件扫描无异常,但不久发现自己的重要文件丢失,甚至账号和密码被盗用。这些现象的背后隐藏着一个幕后操作者,这便是恶意文件,其中以木马居多。捆绑木马、盗号木马、网马、潜伏木马等传播速度很快,如果不加预防和控制,将会给更多网民造成更加严重的损害。因此,及早发现木马是减小木马危害的有效措施。

1 木马检测的基本原理

1.1 木马检测技术简介

目前,国内外学术资料上提到的木马检测方法很多,经过分析发现可以将其分为两大类[1]:传统检测技术和主动防御技术。特征码扫描技术是杀毒软件中用得最多的传统检测技术。

特征码扫描技术采用的是一种精确检索一组匹配字符串的工作模式,每个病毒及其变种的特征码都包含在扫描器的特征码库中,而这些特征码是不会出现在未被感染的文件中[2]。特征码扫描技术属于被动防御范畴,检测具有滞后性,即只能在采集到新病毒样本并且将其加入病毒库之后才能扫描检测。

主动防御技术之所以成为信息安全领域的研究热点,原因在于响应时间及时。凡是能够主动检测和拦截未知威胁的防御方法都可以统称为主动防御技术[3-6]。启发式检测技术是典型的主动防御技术,该技术通过在一个虚拟的安全环境中前摄性地执行代码来判断其是否有恶意行为,从而判断该文件是否是木马,其中虚拟的安全环境一般使用虚拟机[7-9]。

1.2 木马的生命周期与运动轨迹

1)木马的生命周期。

此处定义的木马生命周期是指木马程序编写完成之后、木马功能得以实现、在被检测软件发现之前的整个时间段。由于早期木马检测技术的缺陷,致使木马的生命周期很长,从而给用户造成很大的危害。一般来说,木马的生命周期包括四个阶段,即:传播阶段、安装阶段、运行阶段和网络通信阶段,由此得到四状态的木马生命周期。其中,网络通信阶段是木马实现其功能的关键阶段,也是必经阶段。基于此思想,一些检测软件重点针对网络通信阶段对木马展开检测。

2)木马的运动轨迹。

此处利用运动轨迹来描述木马的运行过程,如果将木马的某些运行行为定义为一个点,则木马的运动轨迹是指木马在其生命周期内所有行为点连接而成的曲线,它是对木马生

收稿日期:2014-10-09;**修回日期**:2014-11-30。 **基金项目**:四川省教育厅项目(08ZA043)。
作者简介:钟明全(1975 –),男,四川内江人,副教授,硕士,主要研究方向:通信与信息安全; 范宇(1976 –),男,四川隆昌人,高级工程师,硕士研究生,主要研究方向:物品编码与信息追溯; 李焕洲(1974 –),男,四川阆中人,教授,博士,主要研究方向:可信计算; 唐彰国(1978 –),男,广西桂林人,副教授,硕士,主要研究方向:信息安全; 张健(1975 –),女,四川宜宾人,副教授,博士,主要研究方向:网络安全。

命周期描述的延伸与细化[10]。引入该概念后，可以更加清楚地掌握木马的运行过程，在更多行为点上采集木马的行为数据，将这些行为数据按照时间序列进行组合分析，从而有助于提高检测准确率。在对较多木马文献进行分析的基础上，又通过对木马样本的实际测试，总结得到八状态的木马运动轨迹，如图 1 所示。如果木马设置了自启动方式，则可得到五状态的木马运动轨迹，如图 2 所示。

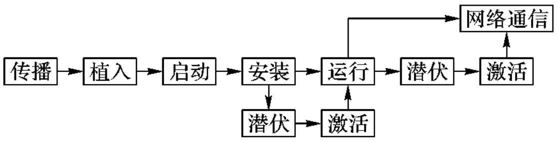

图 1　八状态的木马运动轨迹

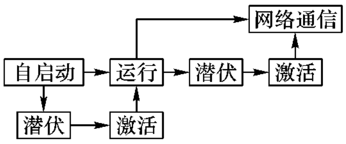

图 2　五状态的木马运动轨迹

在图 1 中，传播和植入概念上比较接近，但传播包含的范畴更广、时序更早一些，比如：通过图片欺骗、通过捆绑欺骗、通过附件欺骗、通过可移动设备感染、网页挂马等都是常见的传播方式，侵入服务器则理解为植入更准确。启动是指木马的加载方式，比如：双击、文件关联、漏洞触发等。安装则是指木马的隐藏及守护操作，比如：文件隐藏、文件备份、文件防删除、设置自启动等。有的隐蔽性高的木马还会有潜伏与激活行为，激活是潜伏的逆过程。运行指的是进线程的创建，是木马功能实现的前提。网络通信阶段木马将与控制端连接，连接成功后实现木马的功能。

2　基于运动轨迹分析启发式木马检测系统设计

2.1　工作流程

由于启发式检测过程要求在虚拟环境中进行，同时考虑到检测系统需要连续进行检测，因此虚拟环境选择 VMware 虚拟机。该虚拟机具有恢复快照功能，利用此功能为下一个被检测文件提供干净检测环境，并且该虚拟机还提供应用程序编程接口（Application Programming Interface，API）函数，用于实现对虚拟机工作的自动控制[11]。检测系统整体上分为两个部分：控制中心和检测引擎，如图 3 所示。其中控制中心工作于主机系统中，检测引擎则工作于虚拟机系统中，虚拟机系统也称为虚拟检测平台。

检测系统检测流程为：1）通过控制中心添加检测任务，一个检测任务对应一个被检测文件；2）控制中心从检测任务中取出一个任务；3）控制中心恢复虚拟检测平台的快照，然后启动虚拟检测平台；4）控制中心将检测任务拷贝到虚拟检测平台；5）控制中心启动检测引擎，同时按照设置的检测时间启动定时器，进入等待状态；6）检测引擎自动读取检测任务，实现被检测文件的检测工作；7）检测引擎检测完一个任务后退出；8）控制中心获取检测完成信号后，将检测结果从虚拟检测平台中拷贝到主机中；9）重复步骤 2）~8），直到最后一个任务，之后由控制中心将虚拟检测平台关闭。

2.2　控制中心

检测系统的控制中心是检测任务的管理平台，通过控制中心可以向虚拟检测平台发出命令，从而控制虚拟检测平台的各个动作，也可以控制检测引擎的执行，因而本系统能够实现对被检测文件的连续自动检测，控制中心的组成如图 4 所示。

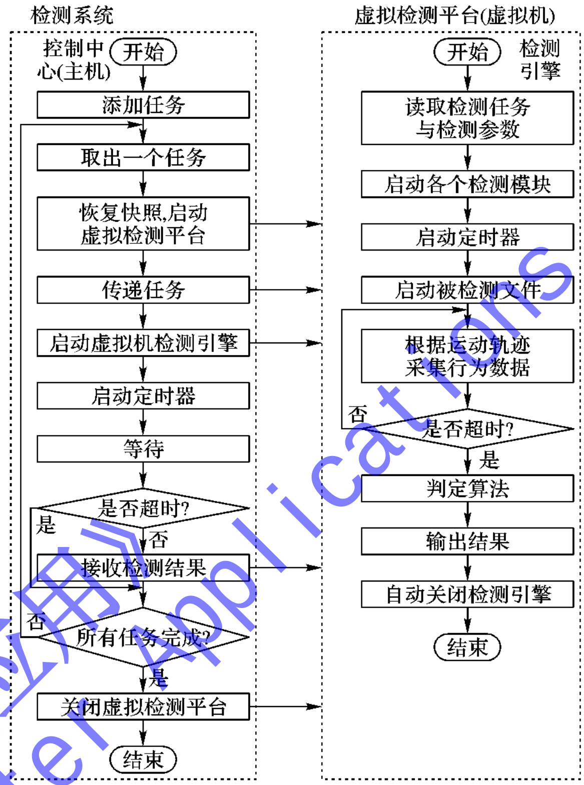

图 3　系统工作流程

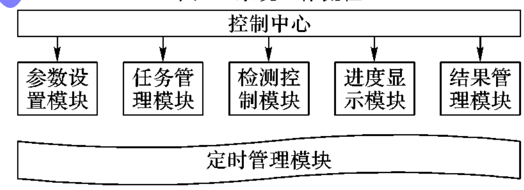

图 4　控制中心组成

控制中心包括 6 个主要模块。其中，参数设置模块用于设置虚拟检测平台文件路径、任务的检测时间等参数；任务管理模块实现检测任务的添加与删除；检测控制模块控制任务按序进行检测，并能处理检测异常情况；进度显示模块用于显示检测任务的进展情况；结果管理模块收集检测任务的检测报告；定时管理模块监控任务的检测状况，若遇异常或超时，进行异常处理。

控制中心包含的 6 个模块中，由检测控制模块与虚拟检测平台进行通信，从而对虚拟检测平台实现控制。该模块通过 VMware 虚拟机提供的专用 API 函数发出控制命令[11]。比如：通过 VixHost_Connect、VixVM_Open 两个 API 函数实现主机与虚拟机的连接，调用 VixVM_RevertToSnapshot 函数将虚拟检测平台恢复到干净状态，调用 VixVM_LoginInGuest 和 VixVM_CopyFileFromHostToGuest 函数将被检测文件拷贝到虚拟机中，调用 VixVM_RunProgramInGuest 函数启动检测引擎实施检测。

2.3　检测引擎

检测系统的检测引擎是整个系统的核心，实现对被检测文件的动态检测，检测引擎是在虚拟机系统中执行的。检测引擎的主要任务是：启动被检测文件，采集被检测文件运动轨

迹中的行为数据，结合自定义木马特征库判定被检测文件的危险等级。本检测引擎从八状态木马运动轨迹中筛选出传播、启动、安装、运行、网络通信五个状态，形成五个检测模块：捆绑检测模块、自启动检测模块、文件检测模块、进程检测模块、网络检测模块，如图 5 所示。

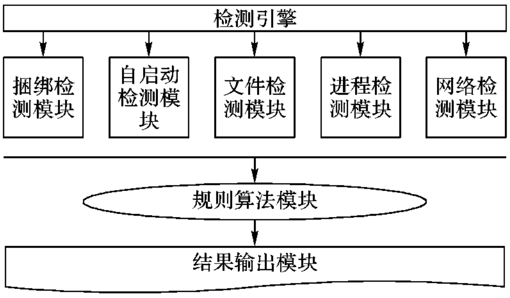

图 5　检测引擎组成

图 5 中，检测引擎的五个检测模块检测原理在接下来的内容中将分别进行论述。此外，规则算法模块采用自定义的木马行为特征库，加上判定规则和判定算法，对被检测文件行为数据进行匹配或组合判定，从而得出被检测文件的危险等级。结果输出模块输出被检测文件的运动轨迹信息和检测结果。

2.3.1　捆绑检测模块

文件捆绑是木马传播的一种重要方式，也是木马隐藏的一种常用方式。由于网络下载非常普遍，并且许多杀毒软件对捆绑木马检测效果不理想，如今网络上捆绑木马越来越多。捆绑有多种形式，比如：木马与图片的捆绑、木马与 doc 文档的捆绑、木马与 exe 文件的捆绑、自解压文件捆绑木马等。互联网上常见的捆绑工具有 BindHider、文件捆绑器、EXE 捆绑机等。

通过文本编辑软件 UltraEdit 对一些捆绑后的文件进行分析发现：由于各种捆绑软件实现原理不同，捆绑后文件的内部结构必然不同，因此目前没有较通用的捆绑检测算法。图 6 是利用文件捆绑器 V3.5 将 exe 文件与 jpg 图片捆绑后的文件结构，被捆绑的 exe 文件隐藏在新文件中的起始地址为 00048710h。图 7 是利用 WinRAR 自解压功能将两个 exe 文件捆绑后的文件结构，与图 6 比较可以看出，字符串对“MZ”与“PE”之间的距离明显增大。

对于捆绑检测的一些可行思路有：1）后缀名检测。文件包含两个以上的常见后缀，且最后一个后缀为“. exe”。2）导入函数检测。在文件的导入表中，BeginUpdateResource、UpdateResource、EndUpdateResource 三个 API 函数同时出现。3）可移植可执行（Portable Executable，PE）文件头检测。在 PE 文件中包含字符串对“MZ”和“PE\0\0”，且该两字符串之间包含字符串“This program”，此三个字符串出现两次及以上。

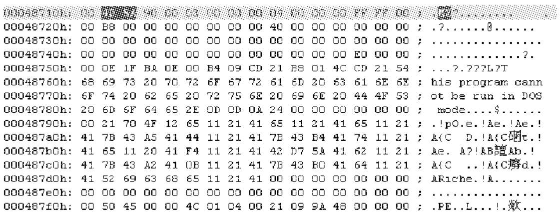

图 6　文件捆绑器 V3.5 捆绑后的文件结构

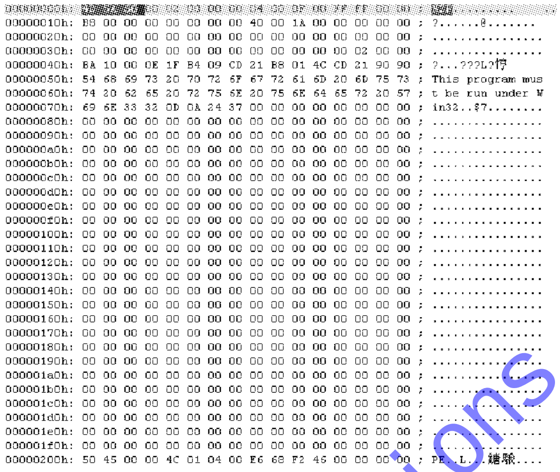

图 7　WinRAR 自解压捆绑后的文件结构

2.3.2　自启动检测模块

自启动原本是操作系统提供给文件使用的一种便捷加载方式，一旦设置之后就不需要用户的干预，具有一定的隐蔽性。但是，这种加载方式也被木马利用了，因此自启动可以作为一个木马检测的行为点。自启动的实现方式归纳起来只有两大类：一类方法是通过将可执行文件信息写入 ini、inf 或 bat 等脚本文件中，常见的脚本文件包括 System. ini、Win. ini、AutoRun. inf、AUTOEXEC. BAT、WinStart. BAT 等；另一类方法是将可执行文件信息写入系统注册表的一些特殊路径，这些路径下键值对应的文件在系统启动时会被操作系统加载，从而实现文件的自启动。通过注册表实现自启动的路径很多，一些学术论文也总结得比较全，典型的注册表自启动路径包含字符串“Run”、“RunOnce”、“RunServices”、“RunServicesOnce”等[12-13]。

2.3.3　文件检测模块

文件检测分为静态检测和动态检测，本模块采用动态检测方式，即检测文件的操作行为。文件操作行为包括新增、删除、压缩、修改等，单独分析每个行为都是正常的。但是，如果把这些行为组合起来分析或者与其他阶段的行为关联起来分析，就可以发现一些异常情况。比如：删除自身、删除系统重要文件、新增的可执行文件是某个文件释放的。文件是木马的载体，因此，也可以将文件操作作为一个重要的木马行为检测点。

2.3.4　进程检测模块

无论木马按照怎样的轨迹工作，运行是其必经的一个行为点，因此设计了进程检测模块。但是，木马为了生存，通常会对其进程作一些隐藏处理，比如：将木马进程隐藏、创建远程线程等。这些特征既然能够被木马利用来掩饰自己，反过来在对抗木马时也能加以利用，这就为进程检测模块提供了一些检测思路。对于隐藏进程的检测可以采用内核态枚举进程与用户态枚举进程求差获得。因为内核态枚举进程的方法没有使用 API 函数调用，而是直接来自系统内部的数据结构。如果从这些系统内核数据结构中删除掉某进程信息，将会直接导致该进程完全失效。除了隐藏进程检测，在进程检测模块常用的其他检测思路包括：进程创建检测、远程线程检测、进程终止检测、调用 CMD 检测[14]。

2.3.5　网络检测模块

网络通信行为是网络软件的共有行为，如果单独通过网络通信行为来检测木马，必然造成很高的误报率。因而对于网络通信行为，只能通过其他行为进行组合判断。经过研究与实验，网络检测模块可以采用的一些检测思路包括：1）非浏览器软件通过 80 端口通信；2）系统进程正在通信，但微软资料表明该进程不具有通信行为；3）正在通信的进程名与重要系统进程名相似，如：svch0st. exe。网络检测模块在技术上可以采用服务提供者接口（Service Provider Interface，SPI）技术与网络驱动接口规范挂钩（Network Driver Interface Specification Hook，NDIS Hook）技术相结合的方式。

3　测试及结果分析

提高检测系统准确率要求：1）选择合适的行为点；2）建立一个丰富的木马行为特征库；3）设计一套实用的木马判定规则和算法。在进行系统测试之前，通过网络搜集、安全实验室等多种途径采集了大量实验样本，借助于人工分析，建立了一个自定义木马行为特征库[15]。

主机和虚拟机的操作系统均采用 Windows XP SP3，虚拟机选用 VMware Worksation 6.0。经过测试，检测系统能够按照设计的工作流程稳定工作，能够快速地输出检测结果。检测系统能够检测常见的各种可执行文件，也可以检测捆绑文件。检测系统对两个样本的检测信息如表 1 所示。

表 1　两个检测样本的检测信息

项目	大白鲨远控 1.5. exe	eMule-0.47c-VeryCD070418-Setup. exe
捆绑分析	捆绑了 1 个 PE 文件，并且被释放出来，文件名为：dbs. exe	捆绑了 3 个 PE 文件，并且 3 个被释放，文件名分别为：vcinst. dll、System. dll、InstallOptions. dll
自启动分析	设置了安装自启动（路径为：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components）	未设置自启动
文件操作分析	1. 在 C:\program files 下新增了 1 个文件，新增文件为：dbs. exe； 2. 在 C:\windows 下修改了 1 个文件，被修改的文件为：regmon. log	在 C:\WINDOWS\Temp\nst3. tmp 下新增了 4 个文件，新增文件为：CustomPageGoogle. ini、System. dll、ioSpecial. ini、InstallOptions. dll
进程分析	1. 进程“大白鲨远控 1.5. exe”（PID：1720）启动了进程“dbs. exe”（PID：1772）； 2. 进程“dbs. exe”（PID：1772）启动了进程“userinit. exe”（PID：1320）	未启动其他进程
网络通信分析	向 1 个 IP 地址（192.168.1.235：2012）发送了 1 次连接请求	未发送连接请求
危险等级	高	低

通过表 1 中数据可以看出：1）检测系统能够在木马的传播、启动、安装、运行、网络通信五个过程中采集被检测文件的行为数据；2）每个被检测文件的检测信息存在差异；3）每个状态过程中行为数据的权重也是不同的；4）被检测文件的行为数据之间存在逻辑关联。基于被检测文件的行为数据，挖掘木马与正常文件的差异信息，结合自定义的判定规则和算法，第一个样本文件的检测结果为高危险等级，第二个样本文件的检测结果为低危险等级。

在检测准确率方面，本检测系统存在一定的误报现象。虽然误报率指标不如采用特征码扫描技术的杀毒软件，但是，在检测未知木马、变种木马、捆绑木马等新型木马方面，本检测系统又占有优势。

4　结语

本检测系统与其他采用行为分析技术检测系统的区别是：本检测系统在木马运动轨迹选择上不是单方面的，而是选择了五个重要方面，同时提出了木马生命周期的细粒度研究方法；其次，本检测系统建立了自己的木马行为特征库和判定算法，从而提高了检测准确率。下一步的工作方向：1）完善木马行为特征库。木马特征是区别于正常文件的差异信息，提取的特征信息越多检测就越准确。2）加入静态检测技术。静态检测技术不仅可以检测潜伏木马，还能有效降低误报率和漏报率。动态检测技术和静态检测技术的结合，必将推进本检测系统的实用化。

参考文献：

[1] JIN Q, WU G, LI D. Research of anti-virus engine and automatic extraction of computer virus signatures[J]. Computer Engineering and Design, 2007, 28(24): 5863 -5866.(金庆, 吴国新, 李丹. 反病毒引擎及特征码自动提取算法的研究[J]. 计算机工程与设计, 2007, 28(24): 5863 -5866.)

[2] LI H, LIU Z, QIN Z, *et al*. Technique of detecting malicious executables via behavioral and binary signatures[J]. Application Research of Computers, 2011, 28(3): 1127 -1129.(李华, 刘智, 覃征, 等. 基于行为分析和特征码的恶意代码检测技术[J]. 计算机应用研究, 2011, 28(3): 1127 -1129.)

[3] XIE B, YU S. Application layer real-time proactive defense system based on application layer protocol analysis[J]. Chinese Journal of Computers, 2011, 34(3): 452 -463.(谢柏林, 余顺争. 基于应用层协议分析的应用层实时主动防御系统[J]. 计算机学报, 2011, 34(3): 452 -463.)

[4] WANG F, ZHOU D. Design and implementation of active defense system based on white list[J]. Computer Engineering and Design, 2011, 32(7): 2241 -2244.(汪锋, 周大水. 白名单主动防御系统的设计与实现[J]. 计算机工程与设计, 2011, 32(7): 2241 -2244.)

[5] CHEN X, WANG Z, REN J, *et al*. Novel virus active defense technique and detection algorithm[J]. Application Research of Computers, 2010, 27(6): 2338 -2340.(陈项颖, 王志英, 任江春, 等. 一种新型病毒主动防御技术与检测算法[J]. 计算机应用研究, 2010, 27(6): 2338 -2340.)

[6] ZHAO H, ZHOU C, ZHAI P, *et al*. Study of intrusion deception system based on network proactive defensive security model[J]. Journal of Air Force Engineering University: Natural Science Edition, 2010, 11(3): 76 -79.(赵洪静, 周创明, 翟平利, 等. 基于网络主动防御安全模型的入侵诱骗系统[J]. 空军工程大学学报: 自然科学版, 2010, 11(3): 76 -79.)

[7] TANG Z, ZHONG M, LI H, *et al*. Design of heuristic identification system for file transfer based on network data stream[J]. Computer Engineering and Design, 2011, 32(9): 2929 -2933.(唐彰国, 钟明全, 李焕洲, 等. 基于数据流的启发式文件传输识别系统设计[J]. 计算机工程与设计, 2011, 32(9): 2929 -2933.)

[8] TANG Z, LI H, ZHONG M, *et al*. Heuristic trojan identification system based on network communication fingerprint[J]. Computer Engineering, 2011, 37(17): 119 -121.(唐彰国, 李焕洲, 钟明全, 等. 基于网络通信指纹的启发式木马识别系统[J]. 计算机工程, 2011, 37(17): 119 -121.)

[9] ZENG X, ZHANG Z, ZHANG Z. Heuristic skill of computer virus analysis based on virtual machine[J]. Computer Applications and Software, 2005, 22(9): 125 -126.(曾宪伟, 张智军, 张志. 基于虚拟机的启发式扫描反病毒技术[J]. 计算机应用与软件, 2005, 22(9): 125 -126.)

[10] LIU S, YANG X, CHEN J, *et al*. Design and implementation of tool for dynamical detecting program assertion[J]. Application Research of Computers, 2009, 26(11): 4140 -4142.(刘树锟, 阳小华, 陈继锋, 等. 程序断言动态检测工具的设计与实现[J]. 计算机应用研究, 2009, 26(11): 4140 -4142.)

[11] ZHONG M, LI H, TANG Z, *et al*. Auto-detection system of suspicious file based on virtual machine technology[J]. Journal of Computer Applications, 2010, 30(12): 3357 -3359.(钟明全, 李焕洲, 唐彰国, 等. 基于虚拟机技术的可疑文件自动检测系统[J]. 计算机应用, 2010, 30(12): 3357 -3359.)

[12] CHEN J, LI H, TANG Z, *et al*. Analysis on trojan operational mechanism and behavior[J]. Computer Security, 2009, 10: 108 -110.(陈婧婧, 李焕洲, 唐彰国, 等. 木马运行机制及行为特征分析[J]. 计算机安全, 2009, 10: 108 -110.)

[13] LIU L. Research and application of the malicious code behavior analysis technology[D]. Hefei: Hefei University of Technology, 2009.(刘磊. 恶意代码行为分析技术研究与应用[D]. 合肥: 合肥工业大学, 2009.)

[14] GAO Y, FAN M. Process analyzing method based on virtual machine[J]. Journal of Computer Applications, 2010, 30(5): 1327 -1330.(高勇, 范明钰. 基于虚拟机技术的进程分析方法[J]. 计算机应用, 2010, 30(5): 1327 -1330.)

[15] LI H, CHEN J, ZHONG M, *et al*. Design of trojan horse detection model based on the behavioral library[J]. Journal of Sichuan Normal University: Natural Science, 2011, 34(1): 123 -127.(李焕洲, 陈婧婧, 钟明全, 等. 基于行为特征库的木马检测模型设计[J]. 四川师范大学学报: 自然科学版, 2011, 34(1): 123 -127.)

(上接第 750 页)

[4] THEODORAKOPOULOS G, BARAS J S. On trust models and trust evaluation metrics for Ad-Hoc networks [J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 318 -328.

[5] TONG X, ZHANG W, LONG Y. Transitivity of Agent subjective trust [J]. Journal of Software, 2012, 23(11): 2862 -2870.(童向荣,张伟,龙宇. Agent 主观信任的传递性[J]. 软件学报, 2012, 23(11):2862 -2870.)

[6] LONG Y, TONG X. Property of trust-based recommender systems [J]. Journal of Computer Applications, 2014, 34(1):222 -226.(龙宇,童向荣.结合信任的推荐系统的性质[J].计算机应用, 2014, 34(1):222 -226.)

[7] JØSANG A, POPE S. Semantic constraints for trust transitivity [C]// Proceedings of the 2nd Asia-Pacific Conference on Conceptual Modeling. Brisbane: Australian Computer Society, 2005, 43: 59 -68.

[8] CHEN Y, ZHANG M, ZHU H, *et al*. Average transitive trustworthy degrees for trustworthy networks [C]// Proceedings of the 4th International Conference on Rough Sets and Knowledge Technology. Berlin: Springer, 2009: 682 -689.

[9] MASSA P, AVESANI P. Trust-aware recommender systems [C]// Proceedings of the 2007 ACM Conference on Recommender Systems. New York: ACM, 2007: 17 -24.

[10] TONG X, HUANG H, ZHANG W. Prediction and abnormal behavior detection of Agent dynamic interaction trust [J]. Journal of Computer Research and Development, 2009, 46(8):1364 -1370.(童向荣, 黄厚宽, 张伟. Agent 动态交互信任预测与行为异常检测模型.计算机研究与发展, 2009, 46(8):1364 -1370.)

[11] JIANG L, ZHANG K, XU J, *et al*. Research on trust transitivity and aggregation in evidential trust model [J]. Journal on Communications, 2011,32(8):91 -100.(蒋黎明,张琨,徐建,等.证据信任模型中的信任传递与聚合研究[J].通信学报,2011,32(8):91 -100.)

[12] TIAN J, LU Y, LI N. Trust chain management model based on recommendation [J]. Journal on Communications, 2011,32(10):1 -9.(田俊峰,鲁玉臻,李宁.基于推荐的信任链管理模型[J].通信学报,2011,32(10):1 -9.)

[13] ZHANG L, WANG R, WANG H. Trust transitivity algorithm based on multiple influencing factors for grid environment [J]. Journal on Communications, 2011,32(7):161 -168.(张琳,王汝传,王海艳.基于多影响因素的网格信任传播算法[J].通信学报,2011,32(7):161 -168.)

[14] LI F, SHEN L, SI Y, *et al*. Dynamic adaptive trust evaluation model based on interaction-aware [J]. Journal on Communications, 2012,33(10):60 -70.(李峰,申利民,司亚利,等.基于交互感知的动态自适应的信任评估模型[J].通信学报,2012,33(10):60 -70.)

[15] QIN Y, WU X, GAO J. Research on selective trust-path search and aggregation in distributed environment [J]. Journal on Communications, 2012,33(Z1):148 -156.(秦艳琳,吴晓平,高键鑫.分布式环境下信任路径选择性搜索及聚合研究[J].通信学报,2012,33(Z1):148 -156.)