计算机工程 2012, 38(2) 153-155 DOI: 10.3969/j.issn.1000-3428.2012.02.050 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

基于动静特征加权的木马检测系统

钟明全，李焕洲，唐彰国，张 健

(四川师范大学网络与通信技术研究所，成都 610066)

摘要： 传统木马检测方法的漏报率较高。为此，结合木马的动态特征与静态特征，设计并实现一个基于动静特征加权的木马检测系统。研究木马工作机制，建立自定义的木马特征库，介绍木马检测思路和系统工作逻辑，分析木马特征的提取过程，并给出权值分配方法。实验结果表明，该系统的检测准确率较高。

关键词： 木马特征 动态检测 静态检测 加权算法

Trojan Detection System Based on Weighting of Dynamic and Static Characteristics

ZHONG Ming-quan, LI Huan-zhou, TANG Zhang-guo, ZHANG Jian

(Institute of Network and Communication Technology, Sichuan Normal University, Chengdu 610066, China)

Abstract: In allusion to the shortage of high unreported rate of current detection method for Trojan, using dynamic and static characteristics of Trojan, Trojan detection system based on weighting of dynamic and static characteristics is designed and realized. By in-depth research of work mechanism of Trojan, custom characteristic library for Trojan is built. Detection idea for Trojan and work logic of detection system is introduced, pick-up procedure of Trojan characteristic is analyzed, and distribution method of weight for Trojan characteristic is given. Experimental result proves that the Trojan detection system has high accurate rate.

Keywords: Trojan characteristic dynamic detection static detection weighting algorithm

收稿日期 2011-07-04 **修回日期** **网络版发布日期** 2012-01-20

DOI: 10.3969/j.issn.1000-3428.2012.02.050

基金项目:

四川省教育厅基金资助项目(08ZA043)

通讯作者:

作者简介: 钟明全(1975－)，男，讲师、硕士，主研方向：网络与信息安全，网络监控；李焕洲，副教授、博士；唐彰国，讲师、硕士；张 健，讲师、博士研究生

通讯作者E-mail: mqzhong@sina.com

参考文献：

[1] 李晓东, 罗 平, 曾志峰. 利用木马的自启动特性对其进行监控[J].计算机应用研究.2007, 24(5):141-143

[7] 钟明全, 李焕洲, 唐彰国, 等. 基于网络驱动技术的木马通信检测系统[J].计算机工程.2010, 36(9):150-152 浏览

本刊中的类似文章

1. 王新志, 孙乐昌, 张旻, 陈韬.基于序列模式发现的恶意行为检测方法[J]. 计算机工程, 2011,37(24): 1-3
2. 马丽丽, 吕涛, 李华伟, 张金巍, 段永颢.用于RTL设计验证的静态错误检测方法[J]. 计算机工程, 2011,37(12): 279-281,284
3. 周雷, 陈克非.基于符号运算的归纳变量识别与约化[J]. 计算机工程, 2010,36(24): 71-73
4. 黄玉文;刘春英;李肖坚;.基于可执行文件的缓冲区溢出检测模型[J]. 计算机工程, 2010,36(2): 130-131
5. 夏 超;邱卫东.二进制环境下的缓冲区溢出漏洞动态检测[J]. 计算机工程, 2008,34(22): 187-188
6. 李 冰;金志刚;张明阳;.MANET分簇节点组通信功能的设计与实现[J]. 计算机工程, 2008,34(19): 98-100
7. 葛 瑶;李晓风;孔德光.基于红黑树的堆内存泄漏动态检测技术[J]. 计算机工程, 2008,34(16): 159-161

文章评论

反馈人		邮箱地址	
反馈标题		验证码	4928