计算机工程 2011, 37(24) 1-3 DOI: 10.3969/j.issn.1000-3428.2011.24.001 ISSN: 1000-3428 CN: 31-1289/TP

博士论文

基于序列模式发现的恶意行为检测方法

王新志，孙乐昌，张 旻，陈 韬

(解放军电子工程学院网络系，合肥 230037)

摘要： 为有效预防变形病毒和新出现的恶意软件，提出一种基于序列模式发现的恶意行为静态检测方法。将恶意代码转换为汇编代码，对其进行预处理，采用类Apriori算法完成序列模式发现，并去除正常模式，得到可用于未知恶意代码检测的模式集合。实验结果表明，该方法的正确率较高、漏报率较低。

关键词： 恶意行为检测 序列模式发现 软件行为 汇编指令 静态检测

Malicious Behavior Detection Method Based on Sequential Pattern Discovery

WANG Xin-zhi, SUN Le-chang, ZHANG Min, CHEN Tao

(Network Department, Electronic Engineering Institute, Hefei 230037, China)

Abstract: To prevention metamorphism and new malware effectly, a static detection method based on data mining is proposed and its key technique is discussed. Melware code is disassembled and preprocessed into sequential data, an Apriori-like algorithm is used to discover sequential pattern and remove normal pattern, the result pattern set can be used to detect unknown malware. Experimental result shows that the method has high accuracy rate and low false positive rate.

Keywords: malicious behavior detection sequential pattern discovery software behavior assembly instruction static detection

收稿日期 2011-07-08 **修回日期** **网络版发布日期** 2011-12-20

DOI: 10.3969/j.issn.1000-3428.2011.24.001

基金项目:

国家自然科学基金资助项目(60972161)

通讯作者:

作者简介: 王新志(1978－)，男，博士研究生，主研方向：可信计算，网络安全；孙乐昌、张 旻，教授；陈韬，硕士研究生

通讯作者E-mail: xinzhi_wang@163.com

参考文献：

[1] Nwokedi I, Mathur A P. A Survey of Malware Detection Tech- niques[EB/OL]. (2007-02-

扩展功能

本文信息

Supporting info

PDF(262KB)

[HTML] 下载

参考文献[PDF]

参考文献

服务与反馈

把本文推荐给朋友

加入我的书架

加入引用管理器

引用本文

Email Alert

文章反馈

浏览反馈信息

本文关键词相关文章

恶意行为检测

序列模式发现

软件行为

汇编指令

静态检测

本文作者相关文章

王新志

孙乐昌

张旻

陈韬

PubMed

Article by Wang, X. Z.

Article by Sun, L. C.

Article by Zhang, M.

Article by Chen, T.

02). http://www.cs.purdue.edu/homes/ nidika/serc-tr286.pdf.

[6] 王丽娜, 谭小彬, 潘剑锋, 等. 恶意代码检测中的PrefixSpan*算法应用[J].计算机工程.2010, 36(7):119-121 浏览

[8] 王 成, 庞建民, 赵荣彩, 等. 基于可疑行为识别的PE病毒检测方法[J].计算机工程.2009, 35(15):132-134 浏览

本刊中的类似文章

1. 钟明全, 李焕洲, 唐彰国, 张健.基于动静特征加权的木马检测系统[J]. 计算机工程, 2012,38(2): 153-155
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

文章评论

反馈人		邮箱地址	
反馈标题		验证码	0662

Copyright by 计算机工程