计算机工程 2012, 38(2) 129-131 DOI: 10.3969/j.issn.1000-3428.2012.02.041 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

基于行为特征的恶意代码检测方法

左黎明，汤鹏志，刘二根，徐保根

(华东交通大学基础科学学院，南昌 330013)

摘要： 研究基于行为特征的恶意代码检测模型及其实现方式，并分析实现中的关键技术。使用自定义行为特征编码模板进行恶意代码匹配，将短周期内2次匹配成功作为判定恶意代码的标准，利用最大熵原理分析2次恶意代码行为的信息论特征。实验结果表明，该方法具有较低的病毒检测误报率和漏报率，并且能有效防范未知恶意代码。

关键词： 数据安全 恶意代码 行为特征 病毒检测 最大熵

Malicious Code Detection Method Based on Behavior Characteristic

ZUO Li-ming, TANG Peng-zhi, LIU Er-gen, XU Bao-gen

(School of Basic Science, East China Jiaotong University, Nanchang 330013, China)

Abstract: This paper researches the model for detection method of malicious codes based on characteristics of malicious behaviors, and analyzes the key techniques in the realization. The method uses customizing code of the malicious behavior to match and uses two malicious behaviors in short period as the decision-making standard, the information entropy characteristics of the two malicious behaviors are analyzed by the maximum entropy principle. Experimental result shows that the method works in most cases of detection and only has minor errors in few conditions, and it has very positive sense for unknown malicious code detection.

Keywords: data security malicious code behavior characteristic virus detection maximum entropy

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

DOI: 10.3969/j.issn.1000-3428.2012.02.041

基金项目:

国家自然科学基金资助项目(11061014)；江西省教育厅青年科学基金资助项目(GJJ10129)；江西省教育厅科研基金资助项目(GJJ10708)

通讯作者:

作者简介: 左黎明(1981－)，男，讲师、硕士、CCF会员，主研方向：网络与信息安全，非线性系统设计；汤鹏志、刘二根、徐保根，教授

通讯作者E-mail: limingzuo@126.com

参考文献：

[1] Cohen F. Computer Viruses: Theory and Experiments[J].Compu- ters and Security.1987, 6

(1):22-35

本刊中的类似文章

1. 郭致昌, 张平, 庞建民, 郭浩然, 崔晨.基于行为特征的BIOS Rootkit检测[J]. 计算机工程, 2011,37(2): 251-252
2. 贡晓静, 钟诚, 华蓓.基于等距变换的聚类挖掘敏感信息保护方法[J]. 计算机工程, 2011,37(19): 122-125
3. 王乾, 舒辉, 李洋, 黄荷洁.基于DynamoRIO的恶意代码行为分析[J]. 计算机工程, 2011,37(18): 139-141
4. 苗甫, 王振兴, 张连成.基于流量统计指纹的恶意代码检测模型[J]. 计算机工程, 2011,37(18): 131-133
5. 霍亚格, 黄广君.基于最大熵的汉语短语结构识别方法[J]. 计算机工程, 2011,37(16): 206-208
6. 池亚平, 许盛伟, 方勇.BIOS木马机理分析与防护[J]. 计算机工程, 2011,37(13): 122-124
7. 沙秀艳, 辛杰.基于最大熵的模糊核聚类图像分割方法[J]. 计算机工程, 2011,37(10): 187-188
8. 白莉莉;庞建民;张一弛;岳 峰.基于关键应用编程接口图的恶意代码检测[J]. 计算机工程, 2010,36(9): 139-141
9. 王丽娜;谭小彬;潘剑锋;奚宏生.恶意代码检测中的PrefixSpan*算法应用[J]. 计算机工程, 2010,36(7): 119-121
10. 岳 峰;庞建民;赵荣彩;白莉莉.反汇编过程中call指令后混淆数据的识别[J]. 计算机工程, 2010,36(7): 144-146

文章评论

反馈人		邮箱地址	
反馈标题		验证码	0288