计算机应用 2007 27 (08): 1942-1943 ISSN: 1001-9081 CN: 51-1307/TP

网络与信息安全

基于API序列分析和支持向量机的未知病毒检测

王硕[1];周激流[2];彭博[3]

四川大学 计算机学院[1]
成都信息工程学院 网络工程系[2]
四川大学计算机学院[3]
西南石油大学 计算机科学学院[4]

收稿日期 2007-1-31 修回日期 网络版发布日期 2007-8-27 接受日期

摘要 提出了一种在Windows平台下检测未知病毒的新方法,以PE文件调用的WinAPI序列为特征，运用支持向量机分类来检测未知病毒。实验结果表明，所实现BK 50系统对未知病毒具有较好的识别效果。

关键词 未知病毒 API序列分析 支持向量机

分类号

DOI:

对应的英文版文章:A7020627

通讯作者:
王硕 gamefox@163.com
作者个人主页: 王硕 周激流 彭博