

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

扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF](#) (359KB)

▶ [\[HTML全文\]](#) (0KB)

▶ [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](#)

相关信息

▶ [本刊中 包含“未知病毒”的 相关文章](#)

▶ 本文作者相关文章

· [王硕](#)

· [周激流](#)

· [彭博](#)