附件 8

对抗环境下恶意代码检测系统研究成果登记公示信息

成果名称:	对抗环境下恶意代码检测系统研究
完成单位:	东莞理工学院
完成人员:	张福勇,王艺,李宽,何凯,赵铁柱,王天健,陈启超
研究起止日期:	2020-07-01 至 2022-06-30
成果应用行业:	信息传输、软件和信息技术服务业
高新技术领域:	非定向研究
评价单位:	东莞市科学技术局
评价日期:	2023-01-12
成果简介:	本项目成果的主要内容包括： （1）对抗环境下代码特征选择研究 项目组系统研究了 Windows 和 Android 平台下的恶意代码特征，通过对近 20 万恶意代码样本的实验和分析统计，认为在 Windows 平台下综合采用基于文件字节特征的静态特征和基于系统调用或 IRP 的动态行为特征可以达到较好的检测效果。Android 平台下的恶意代码检测通过提取文件描述信息及反汇编得到的 API 调用、网络地址等信息可实现较好的检测效果。 （2）基于主动学习的恶意代码检测模型 本项目采用基于代表性和不确定性相结合的选择策略，选择最具代表性的样本进行标记。提出通过提取文件描述信息及反汇编得到的 API 调用、网络地址等八种不同类别的特征集合作为检测特征，并将这些特征向量化。然后选取部分样本数据训练基于 SVM 的检测模型，最终实现对未知程序的有效检测，在只用 20%左右标记数据的情况下可达到 96.56%的检测准确率。 （3）基于迁移学习的恶意代码检测模型 本项目采用基于特征选择的迁移方法，该方法首先利用源领域以及目标领域数据的公共特征训练一个分类器；然后，提取目标领域数据的特有特征，使用这些特有的特征优化分类器；最终，得到适合于目标领域的检测模型。本项目提出的基于迁移学习的恶意代码检测模型可实现拥有少数目标领域训练数据，甚至仅拥有源领域训练数据的情况下，实现对目标领域样本的有效检测。 （4）基于主动迁移学习的检测框架 本项目将基于主动学习的检测模型和基于迁移学习的检测模型相结合，形成一个完整的检测框架，并以此框架为基础，开发了恶意代码检测工具，可自动实现对恶意代码文件的特征选择及检测过程。最终通过 ROC、AUC 等度量指标来评估模型的泛化能力和鲁棒性。