doi:10.1631/FITEE.1601745

题目：恶意代码行为描述与分析综述

概要：基于行为的分析是恶意代码自动分析和检测过程中的一项重要技术，近年来得到学术界和工业界极大关注。恶意代码行为分析技术，能够避免传统静态分析技术遇到的恶意代码混淆的障碍，也能够通过行为描述规范表达恶意代码样本多样化的行为类型。目前，虽有一些关注恶意代码行为分析的工作，但基于行为的恶意代码分析技术仍未成熟，目前尚未发现介绍当前研究进展和发展挑战的综述。本文从 3 个方面对恶意代码的行为描述和分析进行综述：恶意代码行为描述，恶意代码行为分析模型，可视化。首先，全面梳理了现有行为分析技术的分析目标、原则、特点和分类，包括现有行为数据类型和描述方法；其次，从多方面分析恶意代码分析的不足和挑战；最后，探讨了潜在研究热点。

关键词：恶意代码行为；静态分析；动态分析；行为数据表示；行为分析；机器学习；基于语义的分析；行为可视化；恶意代码演化