恶意软件网络协议的语法和行为语义分析方法

- 1 相关工作
- 2 分析方法
  - 2.1 问题描述 — 本文以常见的文本型协议为分析目标，针对不同的字段分割方式，识别和提取协议中的不同字段.
  - 2.2 协议规范分析 — 主要是完成协议字段的识别和划分工作
  - 2.3 行为语义分析 — 行为语义分析的目的是在协议字段和软件行为之间建立起对应关系，揭示不同字段所蕴含的程序行为含义
  - 2.4 结果归并 — 在完成单个消息的语法分析和语义分析之后，我们尝试着关联多个不同消息的分析结果，将相似的消息归 为一类，以便利用多条消息结果相互验证，确认某些特殊字段的含义.
- 3 实验评估
  - 3.1 实现 — 原型系统由虚拟运行环境构建模块、分析控制模块和数据分析引擎3个模块组成
  - 3.2 实例分析
    - 样本一： win32／Agobot3．BJ
    - 样本二： Win32／FT P-Mini．A
  - 3.3 讨论
- 4 总结 — 本文提出了一种利用动态程序分析技术进行网络协议逆向分析的方法，该方法通过在可控的虚拟执行环境中 运行和监视恶意软件执行过程，跟踪恶意软件对网络数据的处理流程，识别和划分通信协议字段，提取协议语法 信息，并关联协议字段到对应的程序行为