[2017]DTB-IDS: an intrusion detection system based on decision tree using behavior analysis for preventing APT attacks

摘要

- APT攻击
  - advanced persistent threats (APT)攻击很牛逼
  - APT攻击在初始入侵时进行相对简单的攻击，如网络钓鱼，但在初始入侵后通过泄露长期信息而形成后门，并通过分析内部网络传播恶意代码
- 文章贡献
  - 文章提出了一种基于决策树的入侵检测系统，利用行为信息分析来检测入侵后智能变化的APT攻击
  - 可以通过快速响应APT攻击来检测初始入侵的可能性，并将损害最小化

1. Introduction

- APT流程
  - 开始先用技术/非技术手段，获取目标系统相关信息
  - 获取终端路由权限后，通过长期监听获得账户密码或者远程控制工具接管目标网络
  - 初始时攻击方式简单，入侵后，攻击方式极为智能，0-Day，提权，后门添加
- 入侵检测系统
  - 防止系统被破坏和长期的信息泄漏
  - 对恶意代码的行为进行分析，然后通过决策树进行规则设置
  - 通过分析可执行文件或新应用的安装文件，来对恶意状态进行分类
- 入侵检测系统分类
  - Host-based IDS
    - 关注内部系统
  - Network-based IDS
    - 关注外部接口
    - 除了APT攻击的隐藏阶段外，所有阶段都需要NIDS
  - Distributed IDS

- 检测系统
  - signature-based detection system
  - behavior-based detection system
    - system-based detection method(within the computer system)
      - integrity inspection method
      - behavior block method
    - network-based detection method(within all networks)
- 决策树
  - 收集分析历史数据
  - 用树的形式存储
  - 与其他机器学习技术相比，决策树具有非常好的准确性，这在精度是一个重要因素的IDS中具有很大的优势
- 其他检测系统
  - behavioral signature
  - labeling system

3. DTB-IDS

- 架构
  - Reporter：负责各模块间的通信。每个模块都必须给出检测信息，基于决策树的入侵检测模块以检测异常行为作为相互补充的关系
  - System behavior manager：完整性检验，进程监控，API监控，注册表监控，驱动监控
  - Network behavior manager：会话监控，出入IP监控，负载监控，协议监控，DNS监控
  - Decision tree-based intrusion detection module：规则更新，特征选取，静态分析，决策树模型，告警
  - The log manager：接受系统行为日志，网络行为日志，决策树行为日志
  - Storage：存放用于决策树的变量信息
- 行为分析
  - System behavior：
    - 文件创建，文件删除，读文件，文件复制，文件路径检查，临时文件重路由
    - 注册表键/值创建删除
    - 进程创建，进程终止，进程信息查看，命令执行
  - Network behavior：
    - 会话统计
    - IP/MAC/ARP改变次数
- 服务方案
- 实验分析