摘要

随着万物互联时代的到来，由僵尸网络导致的 DDoS 攻击，勒索加密，钓鱼邮件，信息泄露等安全事件层出不穷。伴随大数据、物联网的发展，僵尸网络的危害涉及工控系统、IoT 设备、移动安全、云服务、电信服务等多个领域。同时，在国与国之间的网络对抗中，僵尸网络作为一种有效的网络武器能够对国家公共基础设施造成巨大的危害，在未来第五维网络空间战场中将发挥重要的作用。因此，研究僵尸网络的核心架构及关键技术，深入分析僵尸网络的行为特征及交互特点，掌握僵尸网络的进化方向及演变规律，对提升僵尸网络防护能力，保障网络空间安全有着重要的意义。

文章以僵尸网络的行为作为切入点，通过分析网络日志，识别僵尸网络在不同状态下的行为特征，结合行为时序关系，构建僵尸网络的行为识别模型。针对僵尸网络的不同行为，定义僵尸网络行为细粒度标签，结合机器学习相关算法，将散乱的行为标签加以关联，实现对僵尸网络在生存能力、攻击能力、传播能力、身份特征、活动规律和本地资产六个维度的画像。主要研究内容包括：

（1）僵尸网络行为模型研究。通过分析僵尸网络的生命周期，建立僵尸网络行为标签与周期状态之间映射关系，研究僵尸网络在感染、维护、潜伏、传播、攻击、销毁六个状态下的转换行为及时序关系，提出基于 CRF（Conditional Random Field，条件随机场）的僵尸网络检测模型。

（2）僵尸网络行为标签研究。从标签提取，标签定义和标签识别三个方面论述了行为标签技术。以 Mirai 僵尸病毒为例，提取其行为特征，结合多种病毒分析结果归纳出僵尸病毒行为的特征元数据，然后根据行为标签的属性对其进行分层，设计标签结构，最后，根据实际情况使用多种方法识别僵尸网络行为标签。

（3）僵尸网络多维画像研究。研究基于行为分析僵尸网络画像体系结构，构建基于属性、规则和实例的僵尸网络本体。针对僵尸网络行为标签，结合机器学习的相关算法，将散乱的僵尸网络行为标签进行结构化关联，实现僵尸网络在生存能力、攻击能力、传播能力、身份特征、活动规律和本地资产六个维度的画像。

（4）基于行为标签的僵尸网络画像仿真平台实现。以 ELK 日志平台作为基础架构，结合 Bro 入侵检测系统，Spark 实时计算系统以及 sklearn，tensorflow 等相关机器学习工具实现网络流量及日志的实时采集、存储、分析，实现僵尸网络画像。

关 键 字：僵尸网络， 画像， 行为标签， 机器学习