计算机应用 2007 27 (06): 1371-1373 ISSN: 1001-9081 CN: 51-1307/TP

信息与网络安全

基于AEC的恶意代码检测系统的设计与实现

李晓冬[1];李毅超[2]

成都市电子科技大学[1]

收稿日期 2006-12-14 修回日期 2007-2-9 网络版发布日期 2007-6-5 接受日期

摘要 针对现有恶意代码检测技术的不足，提出了能够有效检测复杂攻击的活动事件关联（AEC）分析技术，设计并实现了一个基于AEC的全新的检测系统。该系统结合误用与异常检测技术，采用AEC的思想将网络中的单个事件进行分类，对每类事件进行纵向关联分析。同时结合一段时间内的数据流量统计结果，最终更准确地推断出可疑的攻击并在它们完成攻击前阻止，向网络管理员发出有意义的准确的报警。

关键词 误用检测 异常检测 活动事件关联检测 流量统计

分类号

DOI:

对应的英文版文章：6127704

通讯作者：
李晓冬 lixiaodong@uestc.edu.cn；xdli2005@yahoo.com.cn
作者个人主页：李晓冬 李毅超