通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

闫健恩1,袁春阳2,许海燕1,张兆心1.基于多维流量特征的IRC僵尸网络频道检测[J].通信学报,2013,(10):49~55

基于多维流量特征的IRC僵尸网络频道检测

Method of detecting IRC Botnet basedon the multi-features of traffic flow

投稿时间： 2013-04-28

DOI：10.3969/j.issn.1000-436x.2013.10.006

中文关键词：IRC协议 僵尸网络 数据流 聚类分析

英文关键词:IRC protocol Botnet traffic flow cluster analysis

基金项目:国家高技术研究发展计划(“863”计划)基金资助项目(2007AA010503)；国家自然科学基金资助项目(61100189，61003261)；国家科技支撑计划基金资助项目(2012BAH45B01)；山东省中青年科学家奖励基金资助项目(BS2011DX001)；威海市科技攻关基金资助项目(2010-3-96)；哈尔滨工业大学科研创新基金资助项目(HIT.NSRIF.2011119)

作者	单位
闫健恩1，袁春阳2，许海燕1，张兆心1	1. 哈尔滨工业大学 计算机科学与技术学院，黑龙江 哈尔滨 150001；2. 国家计算机网络应急技术处理协调中心，北京 100029

中文摘要:

针对IRC僵尸网络频道的检测问题，提出一种基于流量特征的检测方法。分析了僵尸网络频道数据流在不同周期内流量的聚类性、相似性、平均分组长度、流量高峰和协同流量高峰等特征，并以此作为僵尸网络频道检测的依据。检测过程中，采用改进的最大最小距离和k-means聚类分析算法，改善了数据聚类的效果。最后经过实验测试，验证了方法的有效性。

英文摘要:

To resolve the problem of detecting IRC Botnet, a method based on traffic flow characteristics was proposed. The characteristics of Botnet channel traf?c were analyzed in different periods such as data-clustering, data-similarity, the average length of packet, peak of synchronized traf?c, and peak of collaborative synchronized traf?c, and these cha-racteristics were used to detect the botnet. In analyzing, improved max-min distance means and k-means cluster analysis algorithm were also presented to promote the efficiency of data clustering. At last, the availability of the method was verified by experiment.

查看全文 查看/发表评论 下载PDF阅读器

关闭