基于随机森林的僵尸网络流量检测

肖　琦　1，苏开宇　2

(1 中国计量大学 信息工程学院，浙江 杭州 310018；

2 中国计量大学 现代教育技术中心，浙江 杭州 310018)

摘　要：近年来，僵尸网络已经成为互联网领域所面临的严重的安全威胁之一.僵尸网络的控制者使用僵尸程序进行例如 DDOS 攻击，发送垃圾邮件，盗取敏感信息等一系列恶意活动.在海量的互联网流量中，从正常流量中有效的识别出僵尸网络流量是亟待解决的问题.本文的研究目的是分析和识别僵尸网络流量.实验在真实的包含僵尸网络流量数据中提取了 9 种特征，采用随机森林算法作为训练模型，与 5 种其他机器学习算法进行比较，实验结果表明本文提出的模型在给出的评价标准下性能最优.

关键词：僵尸网络；机器学习；网络安全

Botnet traffic detection based on random forest algorithm

XIAO Qi　1，SU Kai-yu　2

(1 College of Information Engineering, China Jiliang University, Hangzhou 310018,China；

2 Modern Education Technology Center, China Jiliang University, Hangzhou 310018,China)

Abstract：In recent years,Botnets have become one of the serious security threats in the Internet field. Botnet controllers used bots process to perform a series of malicious activities, such as DDOS attacks, sending spam, stealing sensitive user information, and so on. Identification of botnet traffic from normal traffic in the massive internet traffic is an urgent problem. The purpose of this paper was to analyze and identify botnet traffic. The experiment extracted 9 features from the real botnet traffic data, used the random forest algorithm as the training model and compared it with 5 other machine learning algorithms. The experimental results show that the proposed model has the best performance under the given evaluation criteria.

Key words：botnet traffic；machine learning；network security

作者简介：

肖　琦　女，(1993-)，硕士.研究方向为网络安全、机器学习.E-mail：15751153961@163.com.

苏开宇　男，(1978-)，硕士.研究方向为计算机网络.