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

司成祥1,孙波1,杨文瀚2,张慧琳2,薛晓楠2.基于分布式的僵尸网络主动探测方法研究[J].通信学报,2013,(Z1):197~206

基于分布式的僵尸网络主动探测方法研究

Active-probing based distributed malware master detection system

投稿时间： 2013-07-30

DOI：10.3969/j.issn.1000-436x.2013.Z1.026

中文关键词：僵尸网络 控制端 主动探测 分布式 协议分析

英文关键词:botnet server active probe distributed system protocol analysis

基金项目:国家242信息安全计划基金资助项目（2011A40）；国家自然科学基金资助项目（61003127）

作者	单位
司成祥1，孙波1，杨文瀚2，张慧琳2，薛晓楠2	1. 国家计算机网络应急技术处理协调中心，北京 100029；2. 北京大学 计算机科学技术研究所，北京100871

摘要点击次数:**110**

全文下载次数:**44**

中文摘要:

僵尸网络是当前互联网上存在的一类严重安全威胁。传统的被动监控方法需要经过证据积累、检测和反应的过程，只能在实际恶意活动发生之后发现僵尸网络的存在。提出了基于僵尸网络控制端通信协议指纹的分布式主动探测方法，通过逆向分析僵尸网络的控制端和被控端样本，提取僵尸网络通信协议，并从控制端回复信息中抽取通信协议交互指纹，最后基于通信协议指纹对网络上的主机进行主动探测。基于该方法，设计并实现了ActiveSpear主动探测系统，该系统采用分布式架构，扫描所使用的IP动态变化，支持对多种通信协议的僵尸网络控制端的并行扫描。在实验环境中对系统的功能性验证证明了方法的有效性，实际环境中对系统扫描效率的评估说明系统能够在可接受的时间内完成对网段的大规模扫描。

英文摘要:

Nowadays, botnet is still a kind of severe threat on the Internet. It wastes lots of time for traditional passive monitoring approaches to collect enough evidence, to detect and react. Only after real malicious activities occur can we find the existence of botnet. An active probing approach was proposed based on botnet controller’s communication protocol fingerprint. Botnet samples including client and server were analyzed and the command and control protocol of the botnet were collected. The communication protocol fingerprint was also extracted from controller’s response message and the host on the Internet was scanned with the communication protocol fingerprint. Active Spear active probing system was designed and implemented based on the approach. The system employs distributed architecture and IP used in the scanning is dynamic. The system supports to scan many botnets owning different types of protocols as their command and control protocols. The functional verification in the testing environment proves the effectiveness of the approach and the evaluation to scanning efficiency in the real network environment shows the ability that the system can finish task of scanning a large scale of IP section in an acceptable time.

查看全文 查看/发表评论 下载PDF阅读器

关闭

版权所有：《通信学报》
地址：北京市丰台区成寿寺路11号邮电出版大厦8层 电话：010-81055478，81055479
81055480，81055482 电子邮件：xuebao@ptpress.com.cn
技术支持：北京勤云科技发展有限公司