基于行为特征分析的僵尸网络检测模型

曾品善

（武警警官学院信息工程系　四川·成都　610213）

摘　要　本文分析了僵尸网络所具有的明显特性，提出了一种基于行为特征分析的僵尸网络检测模型，并从预处理层、行为特征分析层、综合检测层三个层次对该模型进行了介绍，给出了每一部分的具体功能。

关键词　行为特征分析份　僵尸网络

中图分类号：TP393　　**文献标识码**：A

所有僵尸网络都具备两个主要特点：第一是都有一个命令控制信道，通过这个信道，僵尸网络控制者及其所操纵的僵尸傀儡可以进行相互间的交流以及命令的传送；第二是都具有明显的攻击性，能够依照控制者的命令进行各式各样的攻击。这两个特点恰恰是僵尸网络有别于其他恶意代码或者病毒的关键。同一僵尸网络中的所有僵尸节点均是由同一个命令控制信道联系起来的，因此其在交流行为和恶意行为上所表现出的特征也具有一定的相似性。这正是基于行为特征分析的僵尸网络检测的理论依据。

1 基于行为特征分析的僵尸网络检测流程

基于行为特征分析的僵尸网络检测可分为三个阶段进行，即流量统计分析阶段、行为特征分析阶段和关联分析阶段。每个阶段的基本过程如下：

(1)流量统计分析阶段：收集待检测的内网与其外部网络之间的所有通信流，对传输方向由内向外的流进行分析记录。

(2)行为特征分析阶段：根据流分析纪录，依据僵尸傀儡的相似性特征，使用聚类和特征模式匹配的方法，分别从交流行为特征和恶意行为特征两个方面展开分析，得出分别在这两方面具有相似性的主机群。

(3) 对交流行为特征相似主机群和恶意行为特征相似主机群进行关联分析，得出检测结果。

2 基于行为特征分析的僵尸网络检测模型

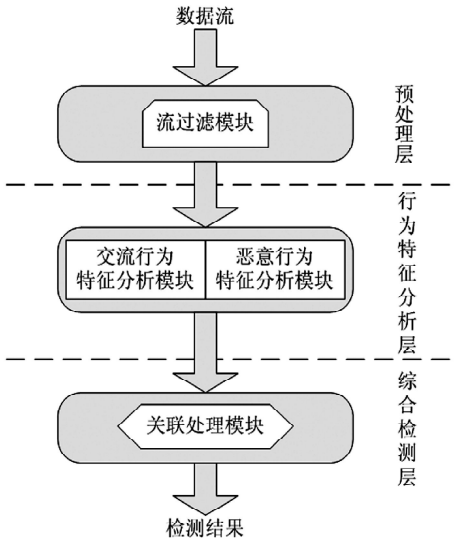

图 1: 基于行为特征分析的僵尸网络检测模型

本文提出了一种基于行为特征分析的僵尸网络检测模型，其基本结构如图 1 所示。

该模型共分为三个层次，即预处理层、行为特征分析层、综合检测层。可进一步细化为流过滤模块、交流行为特征分析模块、恶意行为特征分析模块、关联处理模块四个部分。

预处理层被安置在网络边缘，一般应部署于网关，在内、外网络的交界处。如此便能够使得内、外网之间进行信息交互的所有流量都通过该层。对于本系统而言，检测对象仅为TCP流，因此，流过滤模块的主要任务是对通过的待检测数据流进行预处理，将对于检测没有意义的其它流过滤掉，为系统整体工作减轻了压力，提高了检测效率。

行为特征分析层是本系统的核心部分，其中的交流行为特征分析模块和恶意行为特征分析模块并行工作来处理经过上一层过滤的数据流。交流行为特征分析模块按照一定规则对流经的数据流的相关信息加以记录，而后根据这些记录展开聚类分析，进而确定交流行为特征相似的主机群。恶意行为特征分析模块同样是在监控流经的数据流的过程中，探寻异常行为的存在并对其相关信息加以记录，然后从记录中分析查找出恶意行为特征相似的主机群。

综合检测层为本系统的关键一层，它的存在直接使得本系统在检测结果的准确性上有了质的飞跃，远胜于其它针对单一特征的检测手段。关联处理模块针对行为特征分析层得出的交流行为相似主机群和恶意行为相似主机群展开关联分析，找出这两个群中所存在的某种联系，进而确定某个主机是某僵尸网络的一份子，从而得出检测结果。

参考文献

[1] 王海龙,唐勇,龚正虎.僵尸网络命令与控制信道的特征提取模型研究[J].计算机工程与科学,2013,52(03):385-389.

[2] 成淑萍,谭良,黄彪等.僵尸网络传播模型分析[J].计算机工程与应用,2013,49(01):107-111.