基于通信活动分析的网络威胁源行为画像模型研究

黄双[1]，龚俭[1]

（1. 东南大学网络空间安全学院，南京，210000）

摘　要：为了解决现有追踪取证系统中网络威胁源的复杂网络通信行为活动数据层次低、各追踪对象通信活动零散的问题，本文设计了一个基于通信活动分析的威胁源行为画像模型。该模型基于特定的安全事件信息，用 OpenFlow 交换机实现报文的过滤和转发，利用 PF_RING ZC 零拷贝驱动工具采集报文，使用开源入侵检测软件 Suricata 和网络流量分析工具 Zeek 离线得到原始活动日志，然后利用日志信息关联性以及连接状态和超时机制合并会话，最后从时间、空间、内容、威胁四个角度提取威胁源行为特征，得到网络威胁源的个体画像和群体画像。通过单 IP 追踪任务以及多 IP 追踪任务两个实例对行为画像模型进行了验证，结果表明了该行为画像模型的有效性。

关键词：网络威胁源；行为特征；个体画像；群体画像

Research on Behavioral Portrait Model of Network Threat Source Based on Communication Activity Analysis

Huang Shuang[1], Gong Jian[1]

(1. School of Cyber Science and Engineering, Southeast University, Nanjing, 210000)

Abstract: In order to solve the problem that the existing tracking and forensic system has low level of complex network communication activity data for network threat sources and scattered communication activities of each tracked object, this paper designs a threat source behavior portrait model based on communication activity analysis. The model is based on specific security event information, uses OpenFlow switches to filter and forward packets, uses PF_RING ZC zero-copy drive tool to collect packets, uses open source intrusion detection software Suricata and network traffic analysis tool Zeek to get the original activity log offline, and then use log information relevance, connection status and timeout mechanism to merge sessions. Finally, the behavior characteristics of the threat source are extracted from the four perspectives of time, space, content, and threat, and individual and group portraits of the cyber threat source are obtained. The behavior portrait model was verified by two instances of single-IP tracking task and multi-IP tracking task, and the results showed the effectiveness of the behavior profile model.

Key words: Network Threat Source; Behavior characteristics; Individual portraits; Group portraits

“十一五”211 工程在 CERNET（China Education and Research Network）网络中心和 38 个核心节点上建设了高性能网络管理与网络安全保障系统[1]，其重点是面向 CERNET 主干网和江苏网的网络安全态势感知，内容包含网络运行状态的实时监控，网络安全异常及隐患的检测和网络安全事件的应急响应。CHAIRS（Cooperative Hybrid Aided Incidence Response System）系统[2]是在该系统中是一个分布式应急响应协同系统，主要是为 CERNET 网络中心以及各节点的安全管理人员提供应急响应辅助功能，帮助安全人员快速有效地处理事件，提高安全事件响应的效率。

为了帮助安全分析员对 CHAIRS 系统提供的网络威胁源进行应急响应，我们设计并实现了 MONSTER 系统。当安全管理人员对网络威胁源进行调查分析时，需要对网络威胁源进行追踪取证，即 CHAIRS 系统产生待追踪的特定对象信息（一个或一组追踪 IP），并以对象信息自动生成追踪任务（包含追踪对象信息及相应控制字段等）发送给 MONSTER 系统进行追踪取证，然后 MONSTER 系统对追踪对象进行网络通信活动的追踪与相关取证，获取丰富的证据信息，达到识别网络威胁源意

作者简介：黄双，（1997-），女，硕士研究生，E-mail: shuang@njnet.edu.cn；龚俭，（1957-），男，教授，E-mail: jgong@njnet.edu.cn.

图的目的。

然而随着安全保障系统的持续运行，其中的追踪取证部分暴露出了基础数据不完整以及缺乏高层次行为分析的问题[3]。本研究对原安全保障系统中的追踪取证部分进行了功能上的完善与增强，提高安全事件响应的准确性与及时性。具体的改进包括：1.加强通信活动后处理功能，通过日志的关联性合并使用开源入侵检测软件 Suricata[4]和网络流量分析工具 Zeek（原名为 Bro）[5]离线得到原始活动日志，利用连接状态和超时机制合并离线检测软件无状态性造成的周期分割会话，解决通信活动离散问题和数据不完整问题。2.提出一种网络威胁源行为画像模型[6]，通过对通信活动进行时间、空间、内容、威胁四个角度分析得到威胁源的个体画像和群体画像，解决复杂网络通信行为活动数据层次低的问题。

1 行为画像系统架构

根据安全保障系统的实际功能需求，基于通信活动分析的网络威胁源行为画像的分层结构如图 1 所示。数据收集层主要完成从通信活动库和 IP 基础数据库[7]中提取所需要的数据。特征提取层主要完成基于关联分析和统计分析等技术从通信活动数据中从时间、空间、内容、威胁等维度提取相关特征。行为画像层主要负责基于行为特征对追踪对象进行个体画像和群体画像，得到画像结果。

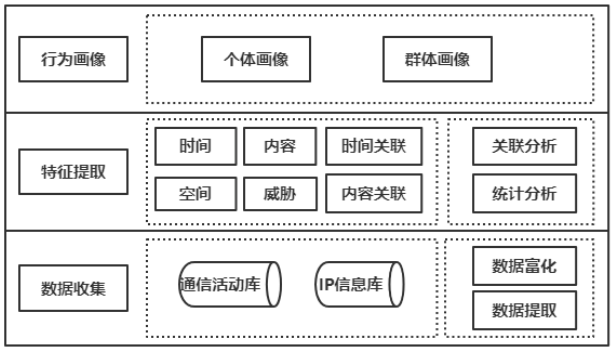

图 1 行为画像模型分层结构图

由于该模块是作为MONSTER 系统中的一个子模块，需要与其他系统协作进行，因此嵌入到安全保障系统后整个工作流程如图 2 所示。其中，HYDRA（hybrid detection response agent）为基于 SDN 技术的入侵阻隔系统[8]，该系统经过 OpenFlow[9]交换机控制网络报文的转发，可以保证在网络正常运行的同时，实现对恶意流量的阻断、对攻击流量的样本采集。其中取证采集模块利用 PF_RING ZC[10]零拷贝驱动工具进行报文采集，通信活动识别模块使用开源入侵检测软件 Suricata 和网络流量分析工具 Zeek 离线得到原始活动日志。本文主要针对通信活动识别模块中数据后处理部分以及行为画像模型进行介绍。

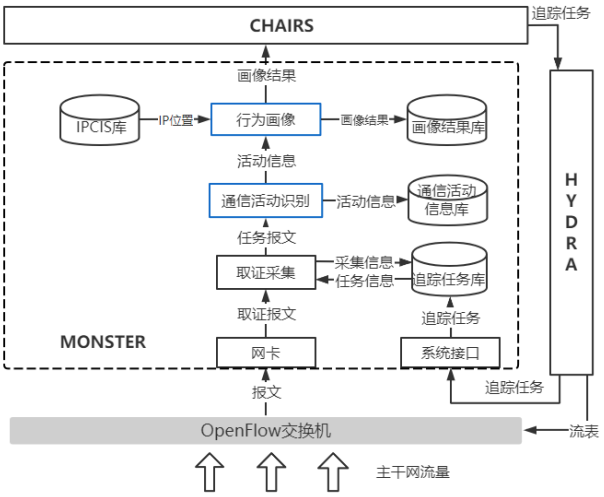

图 2 系统工作流程

2 通信活动后处理模块设计与实现

MONSTER 系统取证采集模块已经根据追踪任务的追踪条件，采集到追踪任务的网络流量并存储在磁盘中，然后基于 Suricata 和 Zeek 两种报文检测工具得到原始活动日志信息。基于当前数据完整性和有效性问题本文设计了一个通信活动后处理模型，该模块的流程图如图 3 所示。

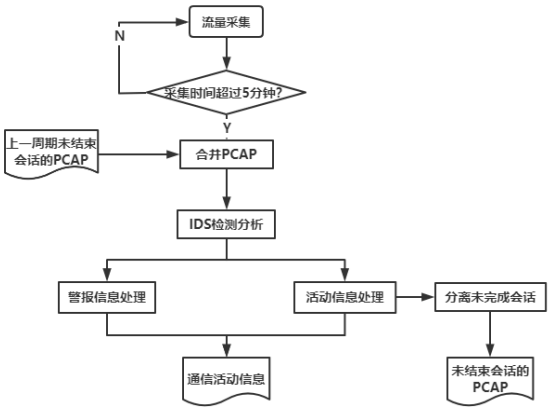

图 3 通信活动识别流程图

本文首先获取当前采集的周期报文，接着合并上一周期未结束会话的 PCAP 送入检测模块进行检测分析，然后对其中的活动日志和警报日志分别进行数据后处理，最后将结果存入通信活动信息库，作为后续分析的基础数据库。

2.1 警报数据后处理

追踪对象相关报文在经过 IDS 检测后会得到两种异构的警报日志，另外警报日志中存在会话标识信息能够直接关联到协议活动信息，因此需要对警报日志进行进一步的处理。Zeek 流量分析器对于每一条会话会自动生成一个 uid，该标识能够关联到协议活动日志，协助分析警报出现的原因。因此在对 Suricata 警报信息和 Zeek 警报信息进行合并的同时，为了使两者标识符统一，帮助定位到同一个会话，需要填充对应 Zeek 会话的 uid。除此之外，警报信息还需要包含关键信息，如时间戳，源地址，源端口，目的地址，目的端口，警报特征值，检测出该警报的 IDS 名称。最终格式如表 1 所示。

表 1 警报信息格式

字段	字段描述
ts	时间戳
uid	会话标识符
srcip	源地址
srcport	源端口
dstip	目的地址
dstport	目的端口
signature	警报特征值
sensor	检测出该警报的 IDS 名称

2.2 协议活动数据后处理

开源流量分析系统 Zeek 以及 Suricata 都支持多种应用层协议活动的识别和解析，包括域名解析协议 DNS、超文本传输协议 HTTP 等。追踪对象的周期通信报文经过 IDS 检测解析后会产生活动日志文件并存储于磁盘文件。但是由于离线检测系统是无状态性的，因此那些持续时间超过采集周期的报文会被割裂成多个会话，这会严重影响后续分析结果。另外不同流量分析系统具有不同的应用层解析机制，因此需要结合两者的结果得到最完整的应用层协议活动信息。为了解决以上几个问题，协议活动数据后处理模块需要完成以下三个处理：1. 协议日志合并。以 Zeek 解析结果为基准，对于未识别出的应用层活动从 Suricata 中查找是否被正确解析，最后统一格式存储。2. 分离未完成会话以及对应的报文，与下一周期通信报文合并后参与 IDS 检测。

2.3 会话分离与合并

分离会话主要利用的是会话日志 conn.log，其中的 history 字段包含了该会话的通信历史，各状态的含义如表 2。

表 2 history 状态含义

Letter	Meaning
s	不带 ACK 位的 SYN
h	SYN + ACK（“握手”）
a	纯 ACK
d	带有有效载荷的数据包（“数据”）
f	FIN 位置 1 的数据包
r	RST 位置 1 的数据包
t	重传有效载荷的数据包

通过连接挥手状态以及会话是否超时来作为会话结束标志，未结束的会话将会话关键信息<ts,srcip, srcport, dstip, dstport, proto>放入全局活动哈希表中，最后遍历当前周期报文，对于符合要求的报文进行分离处理，当下一周期报文到达时合并分析。

通过比较当前方案得到的识别结果、先前方案识别结果以及完整报文的识别结果可以验证当前方案的完整性和正确性，其中完整报文的识别方案指对所有报文合并后的到的完整报文识别的结果，能够作为一种理想结果来进行比较，表 3 为追踪任务验证结果。

表 3 方案结果对比

策略	先前检测方案	本文检测方案	完整报文检测方案
会话数量	14199	10702	10692

如上图所示，该方案能很好的解决之前方案带来的会话分割问题，原先的检测方案由于周期检测问题，将一条会话被分割为多条，直接导致最后得到的会话数量远远大于实际的会话数量，而本方案与理想方案结果相比，存在的部分误差在能接收的范围之内，因此说明了该方法的有效性。

3 行为画像模块设计与实现

本文的行为画像模型是基于通信活动分析构建的，网络威胁源通信活动是指基于应用层协议分析技术，从原始网络报文中识别出的通信活动信息，主要包含会话信息、应用层协议信息和异常行为信息，一组或者一个追踪 IP 相关的所有通信活动就构成了追踪对象的行为特征分析依据。从追踪对象的角度分析，如果追踪内容只包含一个追踪 IP，那么该追踪 IP 的行为特征就构成了一个追踪对象的行为特征；如果追踪内容包含了一组追踪 IP，就还需要结合分析这些追踪 IP 之间的关联关系来反映一个追踪对象的行为特征。基于以上分析，本文的威胁源行为画像将得到两个方面的结果，即个体画像和行为画像。

3.1 行为特征提取

行为特征顾名思义描述的是行为的特征，为了全方位的挖掘追踪对象的行为特征，本文将从时间、空间、内容和威胁四个维度进行分析。由于追踪对象内容的特殊性，追踪对象包含一个或多个追踪 IP，那么行为特征应该包含单个追踪 IP 行为的行为特征以及多个追踪 IP 间关联关系的行为特征，本文中将这两种特征分别命名为本体特征和关联特征，本文将对这两种行为特征分别进行提取。本体特征从四个维度进行特征提取，包括活跃度、影响范围、服务类型和威胁程度，关联特征主要从时间和内容上进行追踪 IP 关联特征挖掘。

3.1.1 活跃度

在构建追踪对象的行为画像时，有必要对该对象的通信活跃度进行描述，在本文中，用追踪对象的活动数量来衡量通信活动的活跃程度。由于不同的活动触发的会话数量不同，为了更合理的对活跃度进行描述，本文将多条源宿 IP 相同且时间相近的会话进行合并，以小时为单位统计会话集的数量来描述不同时间段内的活跃度，活跃度划分情况如表 4。其中 Sum 为画像周期内所有通信活动数，为了表达出不同时间段的活动数量分布，通过与平均每小时活动总数进行比较，确定某小时在一天内的活跃位置。

表 4 活跃度划分

活跃等级	不活跃	低活跃	中活跃	高活跃
活动数量	0	0~Sum/48	Sum/48~ Sum/24	>Sum/24

3.1.2 影响范围

影响范围主要是通过追踪对象的通信 IP 地理位置分布来反映，当追踪对象属于网内，那么对端可能分布于不同的国家、不同省份或者不同城市，当追踪对象属于网外，那么对端就将分布于不同省份或者不同城市。为了更加准确的获得追踪对象的影响范围描述，本文融合 IP 基础数据库中位置信息，从国家、省份、城市三个维度进行聚类得到结果。

3.1.3 服务类型

本文的服务类型包括两层，一个是应用层协议类型，一个是应用类型。服务类型是使用 Zeek 分析器基于应用层协议分析得到，然而当追踪对象为服务器时，对于其提供服务类型，为了加强对追踪对象角色发现，还需要对其可能承载的应用进行进一步分析。下面主要以 HTTP 协议为例进行分析。

Zeek 能对 http 报文头部进行解析得到 http 协议细节信息，另外网络流量解析器 Zeek 还能对基于 http 协议传输的文件进行解析，得到文件类型。不同的应用类型除了在流量数据上存在差异性之外，在传输内容或者报文头部特征值上会存在差异性，如信息浏览类服务，主要是提供信息量较小的数据供用户浏览，例如文字或者图片信息，从文件类型上主要表现为 text/html、image/jpeg 等，通信行为上表现为大部分以五元组<srcip, srcport, dstip, dstport, proto>的会话中存在文档或者图片的传输；如资源共享类服务，主要提供视频/音频类下载，从文件类型上主要表现为 video/mp4 、audio/x-mp4a-latm 等，通信行为上表现为大部分以五元组的会话中存在文件传输；对于代理服务器和 tracker 服务器，基于报文头部特征值能进行一定程度的区分。基于以上分析，下面列举几种应用识别规则。其中 direction=1 表示追踪 IP 为宿，proxied 表示 http 代理内容，conncount 方法表示统计包含某种规则的通信数量，connsum 表示通信活动总数。

对于其他无法识别的应用类型，认为它属于其他类。

表 5 识别规则定义

编号	特征	规则	类型
1	客户端请求报文中包含 Proxy-Connection:Keep-Alive[11]	direction=1 and lower(proxied).contains(“proxy-connection:keep-alive”)	代理服务器
2	客户端请求地址中包含 get 方法，且 uri 中包含 GET/announce?”、“info_hash”等字符串[12]	direction=1 and lower(uri).startWith(“/announce?info_hash=”)	tracker 服务器
3	80%以上通信活动基于 http 协议传输的文件为文本或者图片类型	direction=1 and proto=”http” and conncount(file_type.contains(“text”) or file_type.contains(“image”))/connsum > 80%	信息浏览类服务器
4	80%以上通信活动基于 http 协议传输的文件包含视频、音频或者其他应用类型	direction=1 and proto=”http” and conncount(file_type.contains(“video”) or file_type.contains(“audio”) or file_type.contains(“application"))/connsum > 80%	资源共享类服务器

3.1.4 威胁程度

经过网络入侵检测后，可能得到大量警报信息，标识活动的威胁性，然而某次攻击一般是由多次单步攻击构成，另外对于相同活动可能引发多条警报信息。本文用警报数量和警报类型对威胁程度进行衡量，另外本文中认为两个单步攻击的发生时间间隔一般不会超过时间间隔 T，因此在计算警报数量时，将 T 时间间隔内的多条警报信息进行合并计算。

3.1.5 时间关联特征

追踪 IP 的时间关联性主要关注用户并发访问多台服务器的行为，如网络访问，完成一个网页渲染之前需要将所有资源和网页加载完毕，包含静态图片以及脚本资源等，引入分布式静态资源后，用户将并发访问多台服务器获取这些资源，最终在浏览器进行渲染。这种服务器集在行为上表现为用户会并发访问多台服务器，再结合服务器的应用类型可以判定这一组服务器是属于相同应用还是不同应用，以此区分这一组服务器的协作关系是集群还是分布式。

3.1.6 内容关联特征

多个服务器之间除了时间上的关联关系，还表现为内容上的关联关系。同一组织相关服务在使用域名进行访问时一般会使用相同二级域名或者更高级别域名，因此本文主要关注服务器是否存在相同层级域名来反映内容关联关系。从形式上看，域名是由点分隔的一组标签构造而成，这些标签具有分层结构的特点，本文将基于域名与追踪 IP 的关联，同时建立域名森林，通过寻找所有叶子节点的最低公共祖先来判定是否存在具有相同层级域名的服务器。

3.2 行为画像模型构建

基于行为特征得到的不同范围取值会得到不同的语义描述，这些语义整体上就构成了网络威胁源行为画像。由于本文的数据来源于主干网边界相关追踪 IP 全报文抓取的流量，另外网络流量分析器能对流量的应用层活动进行解析，可以直接将应用层活动提供者定义为服务器，对于不能解析的应用层活动，由于全报文抓取的特点，可以获取完整的网络连接，那么服务的提供者即为服务器。

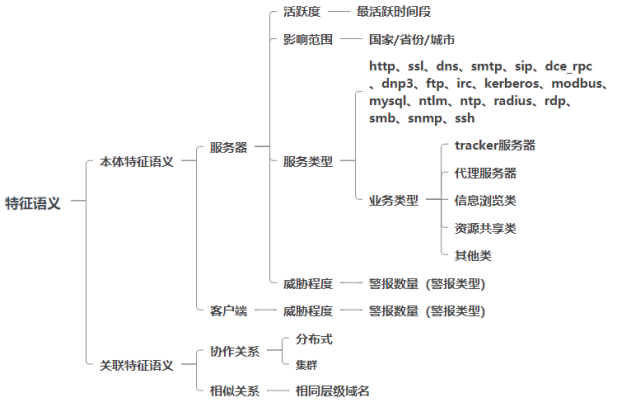

图 4 行为特征语义体系

4 实验结果与分析

本文的研究工作是为了根据追踪对象的通信活动分析，得到多维度的行为画像结果，协助安全管理员理解追踪对象意图。因此本文将通过单 IP 追踪任务以及多 IP 追踪任务两个实例对行为画像模型进行验证。

案例 1：案件号为 NJR-2019014610，该案件的类型为疑似 C&C 域名，追踪对象为 ilzvb-aeact-wo-mni.info，该追踪任务包含的追踪 IP 为 35.**.36.248。由于追踪对象只包含 1 个对象，因此该追踪对象经过行为画像后只得到个体画像结果。

表 6 NJR-2019014610 的个体画像

server	type	active_time	peerip_range	service_type	application_type	alert_num (alert_type)	domain
35.**.36.248	server	09:00-19:00	中国江苏省不同城市	http、ssl、unknown	tracker 服务器	1192(5)	jblconnect.app、torrentclub.tech、tracker.x4w.co

基于个体画像可以得到该追踪 IP 为 tracker 服务器，同时在 09:00-19:00 点最活跃，对端的 IP 都分布在江苏省，表明该服务具有区域性，警报数达到了 1192，但警报类型只有 5 种，因此需要对威胁性进行进一步的判断。其中 tracker 服务器的识别符合应用识别规则 2，由追踪 IP 的 HTTP 通信活动细节图 5 可知不同客户端使用多种 BT 客户端对该服务器进行访问，行为特征表现为客户端与 tracker 服务器之间的通信，因此明显 35.**.36.248 是一个 tracker 服务器，同时也证明了应用识别规则 2 的准确性。

图 5 通信活动细节

案例 2：案件号为 NJR-2020014670 的案件，该案件的类型为疑似 C&C 域名，追踪对象为 baijiayun.com，追踪任务包含的追踪 IP 集为 47.**.161.13 、 114.**.163.15 、 39.**.3.165 、 39.**.7.123 、 39.**.7.124 、 114.**.231.49 、 47.**.164.49 、 47.**.43.123 、 47.**.71.244 、 47.**.160.109，一共 10 个 IP。由于该追踪对象为多 IP 追踪任务类型，因此该追踪对象经过行为画像后得到的个体画像和群体画像两个结果，结果如表 7,8。

基于表 7 中群体画像结果可以发现所有追踪 IP 存在内容上的关联性，即都具有相同的二级域名 baijiayun.com，从时间关联性看，部分追踪 IP 具有分布式协作关系；基于表 8 中个体画像结果可以得出追踪 IP 们的活跃时间大都分布在 19:00-22:00，对端的 IP 都分布在江苏省，具有区域性，主要提供的服务类型为 http 和 ssl，警报数量较少；基于以上分析，可以认为该组服务器共同提供一种分布式 baijiayun 服务。

表 7 NJR-2020014670 的群体画像

编号	servers	type
1	39.**.3.165；39.**.7.124；47.**.160.109；47.**.161.13；47.**.71.244	分布式
2	114.**.231.49；47.**.43.123；47.**.160.109；47.**.164.49；47.**.71.244	分布式
3	114.**.163.15；39.**.3.165；39.**.7.123；47.**.160.109；47.**.71.244	分布式
4	114.**.163.15；39.**.3.165；39.**.7.123；39.**.7.124；47.**.160.109；47.**.161.13；47.**.71.244；114.**.231.49；47.**.43.123；47.**.164.49	*.baijiayun.com

表 8 NJR-2020014670 的个体画像

server	type	active_time	peerip_range	service_type	application_type	alert_num (alert_type)	domain
114.**.163.15	server	15:00-16:00 19:00-22:00	中国江苏省 不同城市	http、ssl	其他	0(0)	video-rs-hz.baijiayun.com
114.**.231.49	server	19:00-21:00	中国江苏省 不同城市	http、ssl	其他	8(3)	qs.baijiayun.com
39.**.3.165	server	19:00-21:00	中国江苏省 不同城市	http、ssl	其他	0(0)	video-ms.baijiayun.com
39.**.7.123	server	19:00-22:00	中国江苏省 不同城市	http、ssl	其他	0(0)	video-cs02.baijiayun.com
39.**.7.124	server	14:00-15:00 19:00-21:00	中国江苏省 不同城市	http、ssl	其他	0(0)	video-cs.baijiayun.com
47.**.43.123	server	19:00-22:00	中国江苏省 不同城市	ssl	其他	0(0)	pro-video-cs.baijiayun.com
47.**.160.109	server	09:00-16:00 18:00-22:00	中国江苏省 不同城市	http、ssl	信息浏览类	11(5)	www.baijiayun.com、 www.baijiacloud.com...
47.**.161.13	server	14:00-15:00 19:00-21:00	中国江苏省 不同城市	http、ssl	其他	3(2)	video-rs.baijiayun.com
47.**.164.49	server	19:00-22:00	中国江苏省 不同城市	ssl	其他	0(0)	pro-video-rs.baijiayun.com
47.**.71.244	server	12:00-15:00 19:00-21:00	中国江苏省 不同城市	http、ssl	信息浏览类	16(3)	click.baijiayun.com

为了验证该结论的准确性，下面通过表 7 中编号为 1 的协作关系进行分析，这里选择通信对象 42.**.63.130 进行分析。

图 6 42.**.63.130 的活动图

由图 6 可以发现，通信对象几乎同一时间与 5 个服务器进行了通信。通信对象分别访问 39.**.3.165 服务器资源 video-ms.baijiayun.com/、47.**.161.13 服务器资源 video-rs.baijiayun.com/agent-bj/295、39.**.7.124 服务器资源 video-cs.baijiayun.com/chat、47.**.160.109 服务器资源 chengla.at.baijiayun.com、47.95.71.244 服务器资源 click.baijiayun.com。另外我们通过对报文负载分析，判断这组 IP 是否确实具有协作关系。由于 http 流量未进行加密，因此主要通过 http 流量负载进行分析。

图 7 39.**.3.165 报文负载

由图 7 可以发现，39.**.3.165 返回数据中包含了后续两个资源的地址信息，即多个服务器具有不同的分工来完成某一种服务，且通过报文负载可以发现这是一种 cdn 直播服务。因此这也证明了追踪对象是提供一种分布式 baijiayun 服务。

基于以上两个实例证明了本文的网络威胁源行

为画像模型的有效性，首先利用个体画像对追踪 IP 的行为特征进行描述，然后利用群体画像对追踪 IP 间的关联关系进行发现，紧密联系了追踪对象涉及到的追踪 IP，使得结果更为明确，协助安全分析人员更快、更有效地处理案件。

参考文献

[1] 朱礼智, 龚俭. 分布式网络应急响应管理系统 CHAIRS 的设计与实现[D]. 南京: 东南大学计算机科学与工程学院, 2015

[2] 吴福怀, 龚俭. 网络安全事件应急响应管理系统设计与实现[D]. 东南大学, 2017.

[3] 郑飞飞. 基于多源数据关联分析的攻击意图推断[D]. 东南大学, 2019.

[4] Suricata. Suricata open source IDS/IPS/NSM engine[EB/OL]. https://suricata.ids.org/, 2016-06-10.

[5] Nick Buraglio. Overview of the Bro intrusion detection system[EB/OL]. https://fasterdata.es.net/assets/20150522-Buraglio-Bro.pptx, 2016-06-10.

[6] 王祖俪. 网络安全中攻击者画像的关键技术研究[J]. 信息技术与信息化, 2018(08):143-145.

[7] 李亚明. IPCIS 系统中的 IPv4 地址使用位置库的改进研究[D]. 东南大学, 2015.

[8] 李成明. 基于 SDN 技术的网络入侵追踪与响应系统的研究与实现[D]. 东南大学, 2018.

[9] ONF. OpenFlow Switch Specification v1.3[EB/OL]. https://www.opennetworking.org/.

[10] Ntop. PF_RING ZC(zero copy)[EB/OL]. https://www.ntop.org/products/packet-capture/pf_ring/pf_ring-zc-zero-copy/, 2016-06-10.

[11] 侯向宁, 刘华春. 基于 Snort 的代理服务器检测[J]. 北京联合大学学报(自然科学版), 2015, 29(04):8-12.

[12] 钱鸣, 陈永生. 基于规则的 BitTorrent 流量探测[J]. 计算机工程与设计, 2008(02):357-359.