专栏：信息安全

基于大数据分析的安全威胁情报在电信运营商的落地应用

薄明霞，唐洪玉，马晨，张鉴
（中国电信股份有限公司研究院，北京 102200）

摘　要：威胁情报作为运营商应对新的攻击手段和变化多端的安全威胁的利器，也是将传统的被动防御转为主动防御的核心动力。介绍了威胁情报对于运营商的重要性，详细分析了威胁情报的生产流程，最后给出威胁情报的典型应用场景，可为电信运营商威胁情报的落地实践提供技术参考。

关键词：威胁情报；主动防御；情报生产；情报应用
中图分类号： TP309
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2020301

Application of security threat intelligence based on big data analysis in telecom operators

BO Mingxia, TANG Hongyu, MA Chen, ZHANG Jian
Research Institute of China Telecom Co., Ltd., Beijing 102200, China

Abstract: As a powerful tool for operators to deal with means of new attack and ever-changing security threats, threat intelligence is also the core power to transform traditional passive defense into active defense. The importance of threat intelligence to operators was introduced, the productive process of threat intelligence was analyzed in detail, and finally the typical application scenarios of threat intelligence were given, which could provide technical reference for telecom operators in the practice of threat intelligence.

Key words: threat intelligence, active defense, productive process of threat intelligence, application scenarios of threat intelligence

1　引言

网络安全问题一直是电信运营商面临的重要问题。随着技术的不断进步，威胁形式瞬息万变，传统防护体系受到严峻挑战。传统的网络威胁，通常以特征检测为主，而随着技术的不断演进，攻击行为逐渐呈现分布化、远程化与虚拟化等新趋势，新型威胁更多地利用“0day 漏洞”进行攻击，无法提前获知特征信息，现有检测机制基本失效。目前，高级持续性威胁攻击行为处于活跃和高发态势，攻击方式更加隐蔽、杀伤力也更强，传统防御并不敏感，难以侦测。此外，攻击工具和攻防方法的商业化与产业化使传统防御不能有效应对有组织、有预谋且花样繁多的安全威胁。目前窘境的主要原因在于攻防力量不均衡和信息的不对称。“未知攻，焉知防”，提前掌握对手尽

收稿日期：2020−08−28；修回日期：2020−11−10

可能多的信息，让战局处于相对优势。在这种背景下，建立在“知彼知己，百战不殆”思想下的威胁情报安全技术应运而生，成为应对新的攻击手段和变化多端的安全威胁的利器，也是将传统被动防御转为主动防御的核心动力。

电信运营商的防御思路需要从基于漏洞的被动防御转向基于情报驱动的主动防御来解决当前的防御困境。通过情报共享拉通安全资源，同时借助情报平台形成相关系统的协同防御机制，构建预警、检测、响应、追溯一体化的立体防御体系，实现及时发现、快速响应，应对高级威胁和未知攻击。

2 威胁情报定义

情报（intelligence）一词，源于军事领域，指“获得的他方有关情况以及对其分析研究的成果”，多带机密性质，目前在不同的领域内均有应用。

威胁情报是在网络安全领域，有狭义和广义之分。狭义的威胁情报，可单纯理解为“敌情”和“知彼”；广义的威胁情报，是一个宽泛的概念，在狭义的基础上还需要关注“我情”和“知己”，包括威胁情报、资产情报、漏洞情报、事件情报以及基础数据情报等。为了更贴合实际应用，威胁情报已经演变成一个由威胁及其相关的资产、漏洞、事件等组成的知识集合。本文的威胁情报均指广义威胁情报。

威胁情报是信息对抗的产物，本质是“减少冲突的不确定性”，是出于掌握对手动态的需求，对威胁的具象化描述。可以将其理解为通过各类方法收集获取包括漏洞、威胁、特征、行为等一系列证据的知识集合及可操作性建议，可还原已发生的、检测现在正发生、预测未来可能发生的网络攻击，为安全决策提供参考依据，帮助使用者避免或减小网络攻击带来的损失。简而言之，威胁情报是可以帮助使用者识别安全威胁并做出明确决定的知识。

3 电信运营商的威胁情报生产及类型

3.1 电信运营商的威胁情报生产

电信运营商的威胁情报生产主要依托于运营商的管道资源优势，基于自有网络流量和现有业务系统数据，生产符合运营商安全业务需求的情报数据。不仅扩展情报类型，丰富情报数据，弥补外部情报厂商数据能力的不足，同时也满足运营商特色威胁情报应用场景的需求。威胁情报生产流程包括原生情报生产、情报融合、情报分析和情报管理四大部分，如图 1 所示。

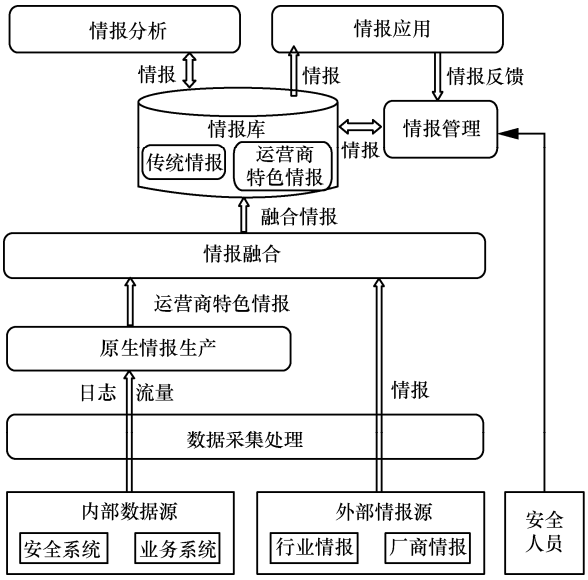

图 1 威胁情报生产流程

（1）原生情报生产

对从内部系统采集的数据进行分析处理，生成电信运营商特色的原生情报。针对安全系统的告警日志和业务系统的流量日志采用不同的处理方式，具体如下。

- 基于安全日志的情报生产。主要利用基于规则的方法对安全设备、僵木蠕系统、病毒系统、恶意网址识别监测平台等输出的告警日志进行分析，提取威胁情报。
- 基于流量的情报生产。针对大网流量和移动网络的话单、访问日志等海量基础数据，

利用大数据建模分析、智能检测算法和数据关联挖掘等方法识别恶意流量，发现新的威胁事件，生成威胁情报。

（2）情报融合

将原生情报与外部输入情报进行融合分析，生成统一情报元语言表示的标准格式情报。具体包括：

- 基于元语建模的情报理解引擎，将输入的异构内外部情报转换为平台的标准格式；
- 利用威胁情报质量量化评估算法，从准确性、全面性、时效性 3 个维度评估情报质量；
- 基于情报质量评估结果对多源威胁情报进行格式和语意层面的融合。

（3）情报分析

周期性地对本地存储的威胁情报数据进行关联和统计，丰富情报维度；并利用推理、挖掘等深度分析技术，发现隐含的威胁信息，生成情报。其中，使用基于知识图谱的关联推理、基于攻击链模型的推理、攻击者画像、资产威胁量化评估、历史情报老化处理等技术和方法。

（4）情报管理

安全人员在平台运营过程中手动录入情报，依据专业知识和情报应用过程中的用户反馈，对情报数据进行修正。

3.2　电信运营商威胁情报类型

电信运营商生产输出的原生情报主要类型如下。

- 事件情报。包括事件名称、恶意类型、攻击意图、攻击源和目标等信息。
- 恶意软件情报。包括病毒、木马、蠕虫等恶意软件的 Hash 值、恶意类型、相关事件等信息。
- IOC 情报。包括恶意软件 Hash、恶意域名等 IOC 的指标特征、恶意类型等信息。
- 信誉情报。包括 IP 地址、域名、URL、电话号码等网络资产的攻击历史、威胁类型等信息。
- 僵尸网络情报。包括僵尸网络的 C2、Bot、攻击类型等信息。
- 违规网站情报。违规网站的域名、URL、违规类型等信息。
- 骚扰电话情报。包括骚扰电话的号码、属地、运营商、频度等信息。
- 垃圾短信情报。包括发送垃圾短信的号码、属地、运营商、频度、类型等信息。

通过与外部接入情报的关联分析，可扩展的相关情报包括：攻击者情报、战役情报、漏洞情报、攻击模式情报、恶意软件情报、工具情报、应对措施情报、信誉情报、资产威胁评分以及报告等。

4　威胁情报在电信运营商的落地应用

运营商生产了情报，必然要将之落地应用。可落地的威胁情报才具有真正价值。本节主要介绍威胁情报如何在运营的安全防护中落地应用，将从以下几个方面分别介绍威胁情报的典型应用场景。

4.1　僵木蠕治理

电信运营商为了防范和处置木马、僵尸网络以及移动恶意代码引发的网络安全隐患，通过利用现网设备，从 DPI 镜像链路流量到僵木蠕分析系统完成威胁检测，并通过本地管理平台上报总部管理平台。经过研判后，总部下发结果到本地平台，本地平台根据研判结果进行处置。建设威胁情报平台后，僵木蠕监测系统与威胁情报平台对接，及时获取全球最新威胁信息和特征，扩展检测范围，提升检测效率，及时防护本地网络未知威胁。僵木蠕本地管理平台获取情报信誉后下发到前置检测设备及样本分析设备。僵木蠕态势感知系统获取最新的威胁情报（如僵尸网络、恶意文件等），并结合僵木蠕的传播特点，对网络上传播的僵木蠕进行识别，并追踪溯源僵木蠕的传

播路径、控制命令路径，最终追踪溯源发现命令控制服务器。通过发现命令控制服务器，再反查受控主机，最终实现对僵木蠕网络态势的感知，为后续采取行动打击僵木蠕创造条件。

借助威胁情报支撑，运维人员可以及时地对资产面临的安全威胁进行准确预警，了解最新的威胁动态，实施积极主动的威胁防御和快速响应策略，结合安全数据的深度分析全面掌握安全威胁态势，并准确地进行威胁追踪和攻击溯源。针对监测发现的僵木蠕事件，对于受控端通过客服等途径及时通知客户开展病毒查杀等处置方式、对于主控端则通过 DPI 等平台进行封堵，从大网侧切断连接。

在整个公共互联网安全监控及防御的过程中，单个节点的威胁信息是不够的。威胁情报平台实现了全网“情报共享”，将海量安全威胁情报信息汇集起来，体现了最大的防护效果和效率。基于威胁情报的协同防护，可以对重要网络出口和重要网络节点进行严密监控，及时检测危害网络安全的大规模僵尸、木马、蠕虫及移动恶意代码事件，随时掌握公共互联网安全发展趋势，深度挖掘追踪安全事件，有效降低安全事件的频度和损失。基于威胁情报的僵木蠕治理应用如图 2 所示。

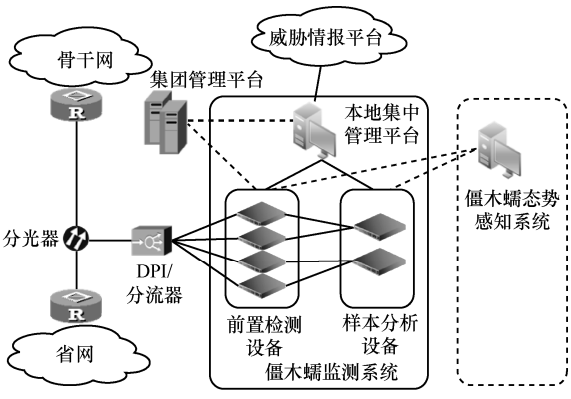

图 2　基于威胁情报的僵木蠕治理应用

4.2　DDoS 攻击治理

传统抗 DDoS 设备依赖于规则对异常流量进行清洗。运营商通过对网络中的流量数据进行采集和分析，检测互联网出口、重要业务、特定子网、关键服务器等网络资源的使用情况。设备发现 DDoS 攻击后通知清洗中心，清洗中心与核心路由基于配置好的BGP邻居关系宣告路由更新条目，流量经过清洗中心清洗后注入回核心路由，清洗结果形成汇总报告。建设威胁情报平台后，流量清洗设备（ADS）和流量检测设备（NTA）结合威胁情报平台的情报数据，形成了 ADS 的 IP 地址信誉云过滤以及NTA的威胁情报平台查询功能，丰富了抗 DDoS 方案的智慧性与高效性。

抗 DDoS 系统与威胁情报平台联动，可将最新的威胁情报转化成防护能力，利用 IP 地址信誉数据快速甄别恶意 IP 地址提高异常流量的清洗速度和性能。针对加密流量和私有协议流量的 DDoS 攻防场景，提供无须解密和深度解析协议的攻击源信任机制进行防护。针对“肉鸡”数量庞大且单个“肉鸡”流量无明显异常的防护场景，可提供百万级“肉鸡”源识别过滤的技术能力。同时，运营商安全攻防团队通过大数据分析提炼攻击威胁情报，及时发现新的 DDoS 攻击，并将情报信息与业务防护结合，提升 DDoS 攻击防护的智能性与先进性。威胁情报平台与现有的清洗平台组成一个智慧高效的清洗方案，减少了运维人员分析攻击的压力，提高了发现僵尸的效率；缩短了设备验证僵尸源的时间，提高了设备清洗的效率；简化了功能启用的配置操作，丰富了告警数据的分类，对于保障业务系统的运行连续性和完整性有着重要的意义。基于威胁情报的 DDoS 攻击治理如图 3 所示。

4.3　不良信息治理

不良信息治理对于运营商来说并不是一个陌生的课题，通过垃圾短信传播的钓鱼网站、恶意软件数量居高不下，给运营商带来了不小的挑战。通过引入运营商本地化威胁情报系统，可以弥补恶意 URL 研判能力、恶意文件研判能力，情报系统引入了文件信誉情报，包括文件信誉黑白、等级、类别、同源等信息，可以与现有的垃圾短信

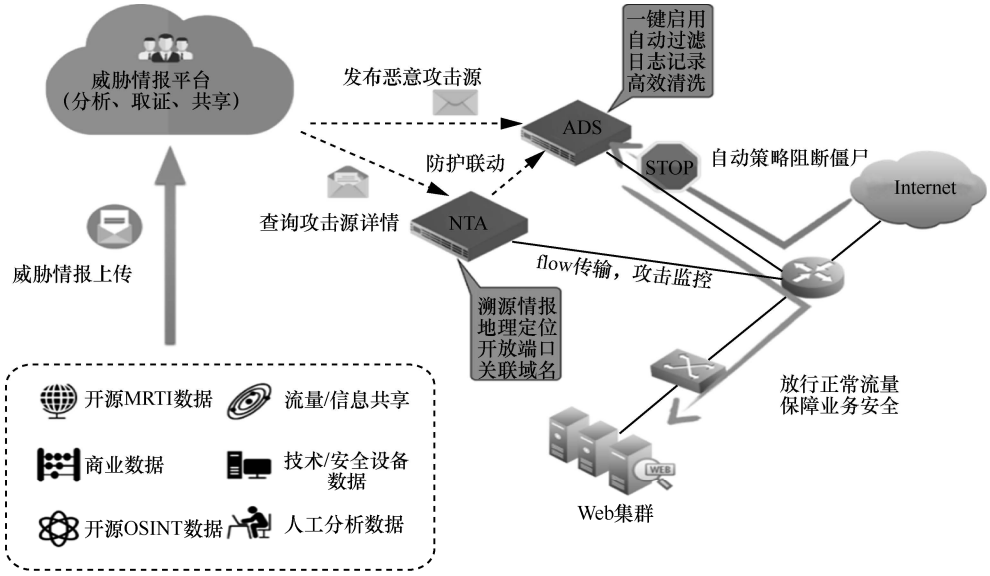

图 3　基于威胁情报的 DDoS 攻击治理

治理系统产生联动，形成能力弥补，及时对含有下载链接的恶意短信进行研判。

基于威胁情报的垃圾短信的业务治理流程在原有流程的基础上，增加了本地化情报消费的一系列流程，当垃圾短信治理系统发现携带下载 URL 时，可以将下载后的文件（或者文件 Hash）发送至运营商本地威胁情报系统，系统会将该文件情报信息发送至治理系统。此外，当用户使用网络访问恶意网址，进行文件下载时，可以通过短信闪信提示、号码过滤等方式对终端用户进行即时提醒，各类高频骚扰电话被直接拦截，从而大大缩短了原先的运营流程，其速率与成效有着明显提升，并且让运营商获得治理该类问题的一个新抓手。基于威胁情报的不良信息治理如图 4 所示。

4.4　精确定位失陷主机

失陷主机是指被攻击者成功侵入“受控制 " 的主机。权威机构研究表明，在主机数量超过 5 000 台的大型企业网络中，超过 90%的企业均存在活跃的失陷主机。威胁造成的恶性破坏或重大损失往往发生在目标主机失陷之后，而失陷主机从被侵入、到受控、再到发起恶意访问行为，往

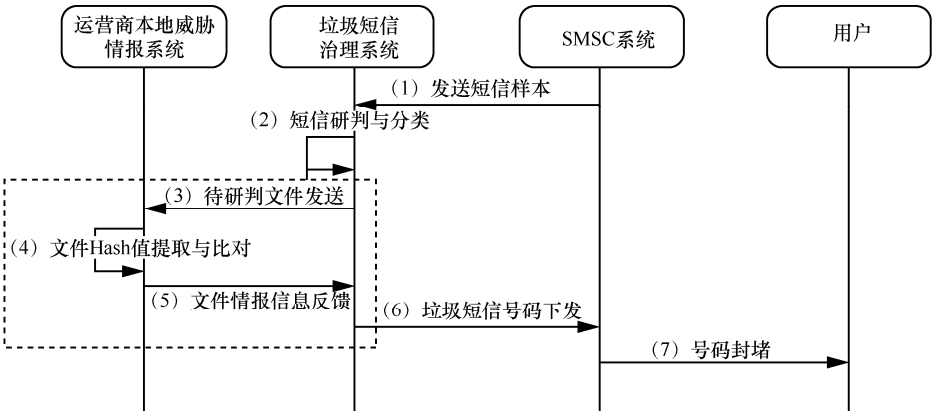

图 4　基于威胁情报的不良信息治理

往发生在几分钟、几小时、几天甚至更长的时间里。由于失陷主机受控或发起恶意行为往往难寻规律、隐蔽性极强，如果能及时发现失陷主机是防范重大损失的关键。

失陷检测是目前威胁情报比较成熟的应用。通过威胁情报可获取及时、准确的失陷情报数据，包括 APT 攻击团伙、僵尸网络、木马后门、勒索软件等的远程访问控制服务器情报、流行 DGA 家族域名情报等。通过将这些实时更新的威胁情报信息与企业网络流量、终端文件、资产库等进行碰撞关联，第一时间锁定内部被 APT 团伙、木马后门、僵尸网络控制的失陷主机，并根据情报标签，对失陷主机进行分类告警。

除了直接碰撞关联发现失陷主机，还可以基于威胁情报、结合大数据分析，挖掘蛛丝马迹，发现更多隐蔽的失陷主机。将威胁情报中的威胁类型（僵尸网络、木马、勒索软件、网络蠕虫等）、攻击团伙信息（名称、背景、攻击工具、攻击过程）、目前状态（活跃、非活跃等）、目前攻击链环节（遭受入侵、受到控制、发起恶意行为等）、影响设备信息（区域、设备类型、IP 地址、版本等）进行比对分析，再结合关联分析、机器学习、行为建模等技术，对网络流量、设备日志进行挖掘分析，可进一步发现资产是否遭受网络钓鱼、漏洞利用、暴力破解等形式的攻击，是否与远端的 C&C 服务器建立连接，是否作为跳板对内网或外网新的目标展开扫描攻击、拒绝服务（DoS/DDoS）攻击、恶意网址访问、漏洞入侵、间谍软件植入、数据窃取等潜伏很深的系列破坏活动，第一时间产生响应告警、消除隐患，及时遏制损失。基于威胁情报定位失陷主机如图 5 所示。

4.5 过滤告警噪声

运营商安全运营人员面临着最苦恼的问题就是被淹没在海量的告警之中无从下手。原因之一是威胁告警没有鉴别的依据，如果没有经历专业的培训，很难区分一次报警到底是突击性的扫描还是有针对性的攻击行为，导致安全团队每天有成百上千的报警。威胁情报可以为安全运营人员提供告警筛选处理依据，从而得到高质量的威胁告警，大大减轻了运维压力。

将威胁情报与安全管理平台进行联动，威胁情报可以提供异常告警相关的上下文信息和准确性，将告警数据与情报数据自动化地进行碰撞、验证，进行告警的降噪和上下文关联，把海量的告警信息大幅度缩减到人工运营能力范围之内。通过清除误报和重复警报，运维人员可以集中精力到缓解真实安全事件上，从而极大地提高安全检测的效率，避免因为不必要的告警而浪费时间，也不至于忽略重点而错过最佳防御时机。基于威胁情报过滤告警噪声如图 6 所示。

5 结束语

近几年，国内威胁情报行业发展迅速，引起了越来越多的企业和机构的重视，运营商也陆续

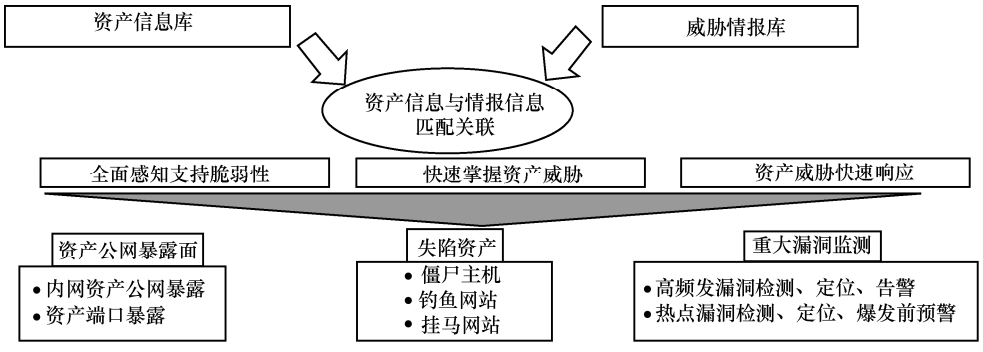

图 5 基于威胁情报定位失陷主机

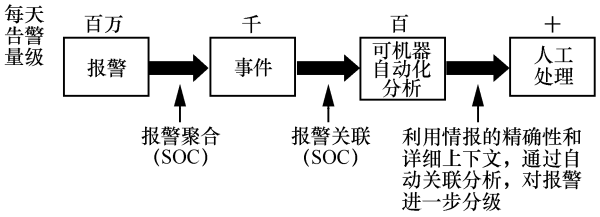

图 6　基于威胁情报过滤告警噪声

建设完成威胁情报平台，并在事前、事中、事后都有相应的应用尝试。但目前，威胁情报仍然是一个新兴的技术，运营商在落地实践中存在着大量问题需要进一步解决：首先，由于目前国内威胁情报标准还不完善，没有太多可参考的；其次，情报共享途径有限，共享难度较大；再者，威胁情报的价值发掘不足，通用威胁情报占比较大，运营商针对性的威胁情报占比少，威胁情报应用效果不理想等。为了弥补以上不足，建议国家推动威胁情报的标准化和规范化工作、构建良性发展的威胁情报生态圈、促进威胁情报共享机制建立，使国内的威胁情报体系趋于成熟，促进整个威胁情报行业的健康发展。运营商业也能从中获益，使威胁情报能在安全防护中大范围推广应用，成为运营商应对复杂安全形势的可靠利器。

参考文献：

[1] 陈曦, 冯梅, 李青. 当前网络威胁情报分类和实用性研究[J]. 信息系统工程, 2019(4).
CHEN X, FENG M, LI Q. Classification and practical research of current Cyber threat intelligence[J]. China CIO News, 2019(4).

[2] 兰昆, 喻显茂, 唐林. 威胁驱动的网络安全防护模型及应用研究[J]. 电力信息与通信技术, 2020, 18(10): 20-27.
LAN K, YU X M, TANG L. Research on threat-driven cyber security protection model and its application[J]. Electric Power Information and Communication Technology, 2020, 18(10): 20-27.

[3] 陶昱玮. 网络威胁情报活动模型建构与解析[J]. 保密科学技术, 2017(8): 21-28.
TAO Y W. Modeling and analysis of cyber threat intelligence activities [J]. Secrecy Science and Technology, 2017(8): 21-28.

[4] 荣晓燕, 宋丹娃. 基于大数据和威胁情报的网络攻击防御体系研究[J]. 信息安全研究, 2019, 5(5): 25-29.
RONG X Y, SONG D W. Research on cyber gattack defense system based on big data and threat intelligence[J]. Journal of Information Securyity Research, 2019, 5(5): 25-29.

[5] 黄凯. 基于威胁情报的数据分析和自动决策[C]//首届网络安全分析与情报大会. 2017.
HUANG K. Data analysis and automatic decision making based on threat intelligence[C]//Proceedings of 1st Conference on Cybersecurity Analysis and Intelligence. 2017.

[6] 肖鹏, 苏永东, 张睿, 等. 电网信息安全威胁情报自动化应用技术研究[J]. 网络安全技术与应用, 2016(12).
XIAO P, SU Y D, ZHANG R, et al. Research on application technology of Power grid information security Threat Intelligence automation[J]. Network Security Technology & Application, 2016(12).

[7] 张卓, 陈毓端, 唐伽佳, 等. 基于威胁的网络安全动态防御研究[J]. 保密科学技术, 2020(6): 22-31.
ZHANG Z, CHEN Y R, TANG J J, et al. Research on dynamic defense of network security based on threat[J]. Secrecy Science and Technology, 2020(6):22-31.

[8] 薄明霞, 唐洪玉, 冯晓冬. 基于大数据的安全威胁情报分析与共享平台技术架构研究[J]. 电信技术, 2019(11).
BO M X, TANG H Y, FENG X D. Research on security threat intelligence analysis and sharing platform technology architecture based on big data [J]. Telecommunications Technology, 2019(11).

[9] 刘汉生, 唐洪玉, 薄明霞, 等. 基于机器学习的多源威胁情报质量评价方法[J]. 电信科学, 2020, 36(1): 119-126.
LIU H S, TANG H Y, BO M X, et al. A multi-source threat intelligence confidence value evaluation method based on machine learning[J]. Telecommunications Science, 2020, 36(1): 119-126.

[作者简介]

薄明霞（1978− ），女，博士，中国电信股份有限公司研究院高级工程师，主要研究方向为威胁情报、态势感知、云网融合安全等。

唐洪玉（1977− ），男，中国电信股份有限公司研究院运营支撑部主任，主要研究方向为云安全、威胁检测、态势感知。

马晨（1993− ），男，中国电信股份有限公司研究院工程师，主要研究方向为云安全、威胁检测、态势感知。

张鉴（1976− ），男，中国电信股份有限公司研究院高级工程师，主要研究方向为云安全、安全攻防、5G 安全。