

网络空间威胁情报感知、共享与分析技术综述

李建华

(上海交通大学信息安全工程学院, 上海 200240)

摘要: 在大数据、云计算、物联网等新型信息技术飞速发展的背景下, 网络空间威胁也朝泛化和复杂化的趋势在发展, 各类网络攻击也更加具有持续性和隐蔽性。基于威胁情报进行网络安全防御能够及时分析已发生的入侵, 对未来威胁态势进行预判, 并据此评估潜在的安全风险以指导用户制定有效的安全决策, 系统化增强网络空间防御能力。威胁情报的范畴十分广泛, 因此, 介绍了威胁情报感知、共享和分析等方面的研究和发展。

关键词: 网络空间安全; 威胁情报感知; 威胁情报共享; 人工智能

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00028

Overview of the technologies of threat intelligence sensing, sharing and analysis in cyber space

LI Jian-hua

(School of Information Security Engineering, Shanghai Jiaotong University, Shanghai 200240, China)

Abstract: With a rapid development of information technologies including big data, cloud computing, Internet of things, etc., the threats in cyber space also become more ubiquitous and complex. Moreover, more and more persistence and hidden features present in all kinds of network attacks. Threat intelligence based network defense can analyze the undergoing attacks and predict the threat situation in the future. Furthermore, based on the potential risk, users can define efficient security policy, thus the defense capabilities of the cyber space could be enhanced systematically. Threat intelligence is a very wide research area. The research works and developments of the sensing, sharing and analysis for threat intelligence were studied and reviewed deeply.

Key words: cyber space security, threat intelligence perception, threat intelligence sharing, artificial intelligence

1 引言

在信息全球化的今天, 网络空间将具备开放性、异构性、移动性、动态性、安全性等诸多特性, 不断演化出下一代互联网、5G 移动通信网络、移动互联网、物联网等新型网络形式以及云计算、大数据、社交网络等众多新型的服务模式。网络空间已经逐步发展成为继陆、海、空、天之后的

第五大战略空间, 是影响国家安全、社会稳定、经济发展和文化传播的核心、关键和基础。在信息技术变革式和爆炸式的发展趋势下, 信息技术与传统行业的深度融合也是大势所趋。为此, 我国提出了“互联网+”、“中国制造 2025”等战略, 全面推动新型网络业态和产业的发展。其他国家也提出了相应的战略规划, 如德国已开展实施“工业 4.0”计划, 用新型信息技术推动第四次工业革

收稿日期: 2016-02-02; 修回日期: 2016-02-06。通信作者: 李建华, lijh888@sjtu.edu.cn

基金项目: 国家自然科学基金资助项目 (No. 61431008)

Foundation Item: The National Natural Science Foundation of China (No. 61431008)

命。在多元化的网络空间中，安全问题日益凸显。随着信息技术的发展与应用，信息安全的内涵在不断地延伸，从最初的信息机密性发展到信息的完整性、可用性、可控性和不可否认性，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术^[1]。传统的安全防护仅仅依靠部署于边界或特殊节点的防火墙、入侵检测系统（IDS, intrusion detection system）、入侵防御系统（IPS, intrusion prevention system）等安全设备进行的静态控制，实行以特征检测为主的网络安全监控，并基于预置规则匹配产生告警信息，这种被动式防御已不再适用于高级持续威胁（APT, advanced persist threat）、0day 攻击等新型网络安全威胁的防护^[2-16]。更为严峻的是，随着网络威胁呈泛化和持续化趋势发展，多样化的攻击切入点、高水平的入侵方式、系统化的攻击工具使网络威胁代价降低。为最大限度地保护核心系统资产安全，亟需对传统的安全防御方式进行优化和改进，形成能应对多样化和持续化威胁的安全体系。威胁情报感知、共享与分析旨在利用多种渠道采用多样化的技术手段采集大规模碎片式的异常数据以及其他相关威胁信息，并集中地进行深度挖掘、提炼、融合、归并以形成与信息系统核心资产有关的威胁线索集合，再借助机器学习、语义分析、事件关联等技术分析已发生的入侵或对未来威胁态势进行预判，在此基础上评估潜在的安全风险以指导用户制定有效的安全决策，增强信息系统防御能力。而与此同时，这些以原始威胁情报作为输入，经整合、剖析得到的包括攻击概貌、安全态势研判、解决对策等信息在内的输出又可反过来作为威胁情报的一部分，为其他信息系统安全管理者在应对相似威胁时提供借鉴。从传统的 PDR2 到 Gartner 最近提出的自适应安全体系，威胁情报的感知、共享和分析是防御、检测、响应、恢复等安全技术的核心基石。目前，“威胁情报驱动的信息安全防御”已成为业界公认的信息安全未来发展方向，备受学术界和产业界关注，甚至一些媒体将 2015 年称为“威胁情报共享元年”，同时威胁情报体系的建设已被许多企业乃至国家纳入其安全战略规划之中^[17]。

本文围绕感知、共享和分析 3 个方面对威胁情报进行讨论。在威胁情报感知方面，重点阐述了高质量威胁情报来源、获取、威胁情报预处理与存储；在威胁情报共享方面，在探讨威胁情报共享体系结构的基础上，讨论了多源异构威胁情报融合、大数据背景下威胁情报交易、共享过程的博弈论以及共享标准等问题；在威胁情报分析方面，重点讨论了威胁情报评估、关联分析、人工智能分析、分析工具等。

2 威胁情报研究现状与发展趋势

2.1 威胁情报研究现状

以威胁情报为中心的信息安全保障框架对于生活和生产关键基础设施的稳定运行、军事作战指挥能力保障及国际社会的和平稳定具有重大意义，多全球知名互联网企业、各国政府以及学术界都对其高度重视。在企业界，作为以面向用户需求提供高质量情报信息为目的的新型服务产业，威胁情报行业近几年在全球增长迅速，如 CrowdStrike、Flashpoint、iSight Partners 等威胁情报厂商通过建立的威胁情报中心可从网络犯罪、信誉库、漏洞、恶意软件等多个角度满足不同用户的特定需求。在政府工作中，美国国土安全部于 2012 年就着手开始推动建立一整套涵盖国家重要基础设施的威胁情报中心，2015 年美国众议院通过了网络安全信息共享法案（CISPA, cybersecurity information sharing act），要求加强企业与政府的情报共享以改善国家在应对网络安全事件时的决策能力。美国国家标准研究委员会制定了威胁情报分享草案，为保障政企、企企、企业与用户之间在自身利益不被损害的前提下安全、高效地共享威胁情报提供标准化的技术方案。除此之外，由斯诺登披露的美国“棱镜计划”显示，美国国家安全局早在 2007 年开始就与 Apple、Microsoft、Facebook、Twitter 等公司开展合作对全球互联网上的数据流实施动态监听以采集有用信息供情报部门分析。在学术领域，虚拟化、云计算、大数据、软件定义网络的出现正在革命性地推动着威胁情报感知、共享和利用等各个层面的全面发展。一方面，新技术为构建检测与响应能力更强大的威胁情报中心提供了有益的保障，

另一方面,新环境新场景下的安全威胁变得更加多样化,给网络空间安全防御和态势评估带来了更严峻的挑战,面对新型高级持续性威胁,传统的基于静态特征库的单纯以防御为中心的相互独立的网络空间安全防护体系难以满足大规模虚拟环境下资源分布式部署、通信集中化管控对网络安全动态检测、关联分析和实时响应的需求。

相比之下,我国威胁情报体系发展还较为落后,但却是挑战与机遇并存。在研究领域方面,各阶段所涉及领域内形成的学术成果散乱,缺乏有效、可靠的威胁情报的采集、共享与利用规范,但信息安全领域的原始积累如信息内容分析、可信计算、云安全、超级计算机、5G通信标准化等重点领域的研究已处于领先水平;在企业界,尚未建成规模化的技术完备的集数据截获、分析、转化、共享与利用为一体的现代化威胁情报中心,因而缺乏面向政府、军队、企业、设备厂商、个人或民间组织提供的威胁情报的综合服务平台,但以奇虎360为代表的服务厂商建设的威胁情报集中化管理中心已在部分区域试行;在学科建设方面,网络空间安全已被批准为国家一级学科,各高校和研究所相关科研单位积极投入,并开始建立完善信息安全人才培养体系。尽管我国网络空间安全起步较晚,仍处于发展的初级阶段,然而随着“宽带中国”、“全面上网”、“家电下乡”等政策的部署与落实及近年来智能终端的全面普及,我国已成为拥有8亿网民的网络大国。因此,在一定高度上对整个社会信息系统的安全运行实现高效管控、积极引导,尽力规避潜在漏洞对党政机关、各企事业单位和用户造成的威胁及经济损失,同时在激烈的国际竞争中扭转局面,掌握主动权,规范威胁情报采集、共享与利用等环节相关技术实施要点,实现威胁情报实时检测、安全共享、最大化利用,全面提升我国网络空间安全监测与响应能力成为各方研究的热点课题。

2.2 威胁情报研究发展趋势

在网络空间安全态势越来越复杂的趋势下,不管对于企业、政府部门、国家机关还是国际组织,威胁情报的研究都有至关重要的意义。参与威胁情报感知、共享和分析的各方结合自身业务流程与安全需求,针对核心资产增强威胁情报感

知能力,积极融合云计算、大数据等前沿技术,建立威胁与漏洞深度分析系统,在深度挖掘与关联融合的基础上做好安全态势评估及风险预警,动态调整安全策略,部署快速可行的安全响应战略,确保关键资产的安全,同时还应在涉及一致利益的领域,以政府主导或产业联盟等多种形式,本着“和平利用、利益均衡”的原则展开广泛而深入的协同交流,在面对共同威胁时形成合力,并在情报共享实践中持续健全相关法律法规保障体系,努力构筑和谐、健康、成熟的威胁情报生态圈。在设计高效能威胁情报感知、共享与分析体系时也朝着可见性、细粒度、完整性、准确性、实时性、协同性和智能化的方向发展。

1) 可见性。信息系统中的核心资产信息是安全防护的重点,为防止其受损或泄露,这些敏感信息在安保级别较高的系统中经常与普通数据隔离存储,其结构、分布和使用情况等被内置软件实时监控。理论上用户核心资产信息的可见度越高,网络应用的权限分配、用户认证、访问控制策略、流量状态、行为模式等情况就越容易被获取。获取信息系统可靠的威胁情报必须增强关键资产、网络流量、用户权限、行为操作、应用数据的可见性。

2) 细粒度。对于每个重要的可反映主机或网络行为的入侵指示器(IOC, indicator of compromise),应尽可能做到在细粒度的层面处理与之相关的情报信息,这样能够搜集到威胁事件的细节。一般来说,收集到的数据越具体细致,情报的可信度越高,入侵还原和攻击溯源也就越精准。

3) 完整性。威胁情报应是全天候的全网的安全事件状态信息。在某个限定的时间窗口对系统运行情况进行监控而非在整个攻击生命周期内持续采集数据,将对后期了解攻击的波动性及实施者的TTP带来困难,使利用数据子集进行局部分析可能引发误判。

4) 准确性。尽可能降低情报搜集过程中信息假阴性和假阳性的几率,确保所获威胁情报信息的准确性,以保障后续分析引擎做出的安全决策的可用性和有效性。

5) 实时性。威胁情报感知应具有尽可能小的时延,否则所收集的威胁情报的有效性就会大大

降低。只有快速感知才能对速度较高、变化较快、危害大的恶意攻击进行有效遏制。

6) 协同性。威胁情报体系建设具有协调与合作的性质，体系中各单位之间的协调、协作形成拉动效应，推动威胁情报防御体系共同前进，协同的结果使各方获益，整体加强，共同发展。

7) 智能化。在对海量威胁情报进行分析的时候，应该实现对高维数据的智能分析，从而达到对全网的威胁态势进行较为精确的预测，帮助信息系统的管理者了解当前安全态势。

3 威胁情报感知

3.1 威胁情报的来源分布

威胁情报是从多种渠道获得的用以保护系统核心资产的安全线索的总和，它涵盖了在特定场景下与某种威胁相关的上下文、指标、攻击概况、影响及应对建议。在大数据兴起及“互联网+”发展的背景下，威胁情报的采集范畴大大扩展，其获取来源、媒体形态、内容类型得到了极大的丰富，除以防火墙、IDS、IPS 为代表的传统安全设备对信息系统的监控及异常数据的拦截过程中生成的与非法接入、未授权访问、身份认证、非常规操作等事件相关的安全日志之外，威胁情报的来源还包括全面沙盒执行、端点侦测、深度包检测（DPI，deep packet inspection）、深度/动态流量检测（DFI，deep/dynamic flow inspection）、恶意代码检测、蜜罐等技术的输出结果以及安全服务厂商、漏洞发布平台、专门的威胁情报提供机构给出的警示信息。此外，威胁情报不是简单的数

据聚集，它是在原始形式之上整合而出的有价值的参考信息，它的内涵已超越了早年的特征库、黑/白名单，通常包括但不限于攻击源、目标系统、入侵动机、对手能力评估、攻击工具（如 Yara 签名）、“战术、技术和过程（TTP，tactics techniques and procedures）”、可用漏洞、攻击危害、应对策略。威胁情报的来源分布如图 1 所示。

3.2 威胁情报感知的作用

威胁情报是后续分析、预判、决策的基础，获取高质量的威胁情报对于整个网络空间安全保障体系攻击应对流程有效运作具有重要意义和明确的需求特征，如图 2 所示。在防御阶段，利用多样化分布式的威胁情报感知技术从多个场景多个维度全面收集威胁信息，进而在攻击造成危害之前组织积极防御，可以减少攻击面；在检测阶段，从所收集的海量信息中提取有价值的威胁情报，并在保障自身权益的同时积极参与威胁情报共享以支持和借鉴其他机构的经验知识，可以检测失陷主机特征、攻击源等，进而进行溯源分析、危害结果统计；在响应阶段，控制中心将分析结果及相应策略实时分发，可以将失陷主机、攻击源进行隔离，并跟踪记录整个响应过程的网络状态；在预测阶段，控制中心根据分析结果和下发的策略预判安全态势，可以评估风险并给出合理安全防护建议。

此外，威胁情报的利用价值直接取决于其供应机制的质量。云计算/大数据环境下的威胁情报采集具有数据规模大、增长速度快且质量良莠不齐的特点。威胁情报并非海量数据的堆砌，相反，垃圾信

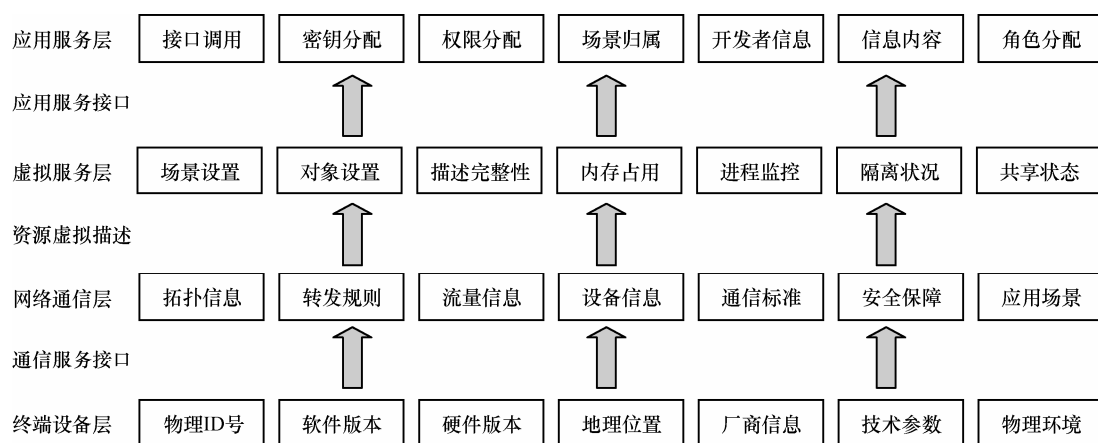


图1 威胁情报分布模型

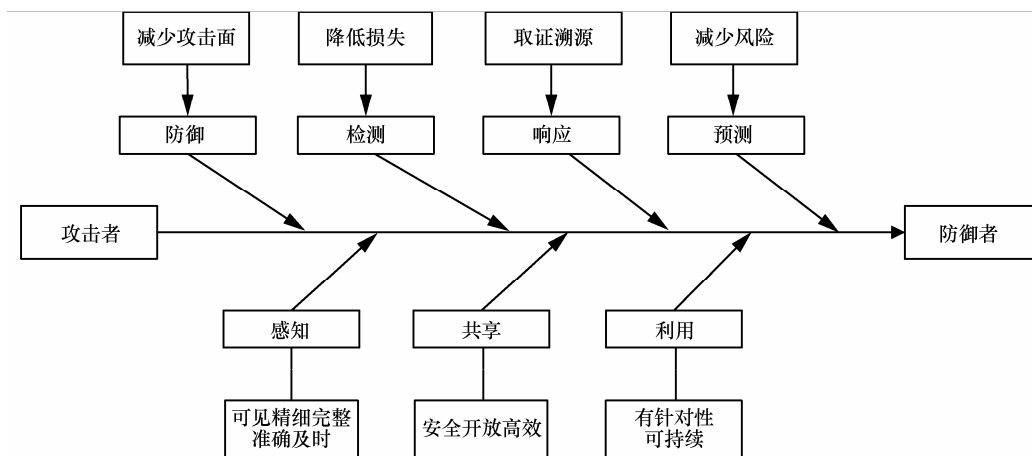


图2 获取威胁情报的意义和需求特征

息的泛滥往往会导致真正有用的信息被淹没，难以从庞大冗杂的信息集合中筛选出有效的情报。

3.3 威胁情报感知技术发展

近年来，为保障网络空间可靠运行，主机异常检测、流量监控、安全态势评估、多元异构数据处理、恶意代码检测等相关安全技术都有不同程度的进步。随着由计算机通信网络技术的发展而衍生出的“互联网+”概念在各领域深度融合，移动互联网、智能电网、智慧城市、工业 4.0 等将网络空间安全威胁推向更加广泛的基础设施，

使得威胁情报感知更加复杂化、规模化。随着信息与通信技术的发展，威胁情报感知的发展进程如图 3 所示。

在传统网络方面，GREECH 等^[18]针对基于主机的入侵检测系统提出一种采用连续非连接的语义分析法。MA 等^[19]提出一种基于混沌分析熵的 DDoS 网络流量的检测方法将网络流量进行可视化处理，使安全人员可以实时观察到全网数据流的动态状况从而及时发现网络安全异常。荆涛等^[20]针对当前网络中多连接通信日益增多、难以

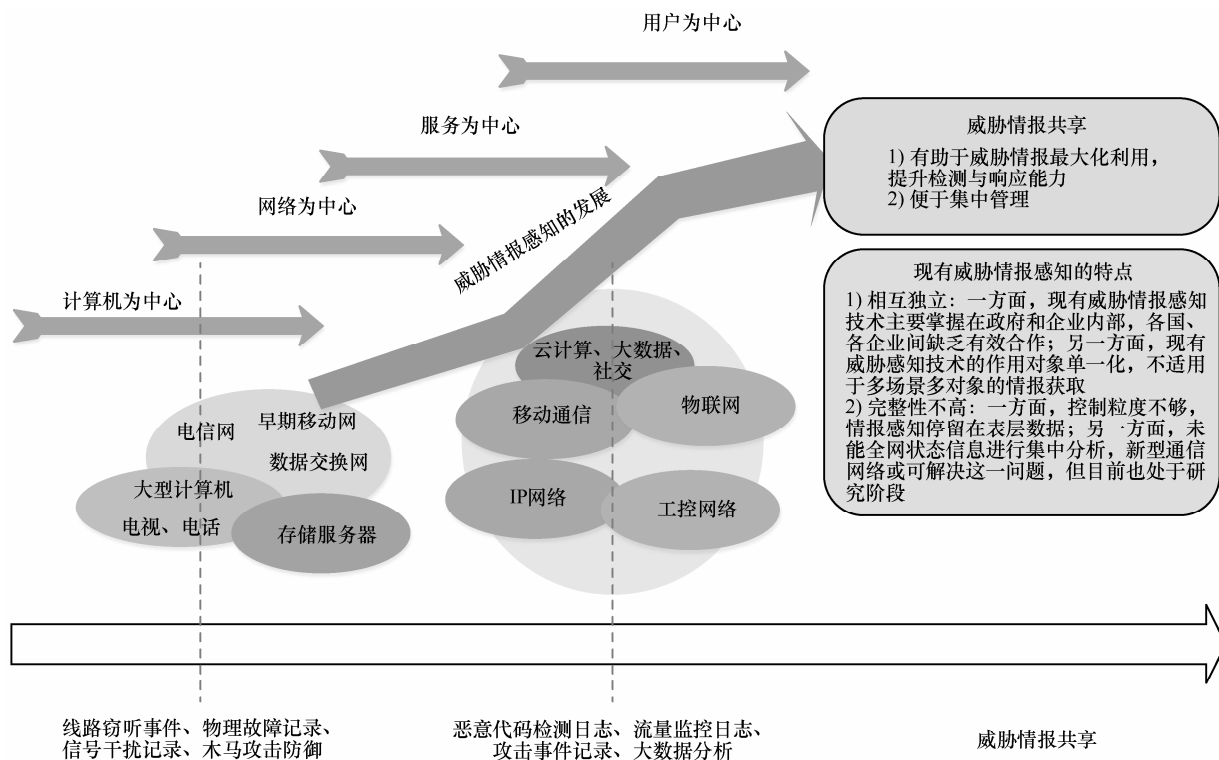


图3 威胁情报感知技术的发展

监管的问题,利用 NetFlow 网管数据实现了一种基于相异度分析网络通信异常行为识别方法,但当网络中新增应用服务时会出现误报。文献[21]和文献[22]提出了一种网络态势感知的分层模型,首先从传感器中选取 NetFlow、SNMP、日志、服务类数据等有代表性且具有互补性的数据源,收集网络流量、IDS 报警信息等安全状态数据,然后利用遗传神经算法(GA-BPNN, BP neural network with genetic algorithm)、支持向量机(SVM, support vector machine)、模糊聚类(FC, fuzzy cluster)3种分类器以及基于 DS 证据理论(Dempster-Shafer theory)的融合器将其提取和转化为与系统安全态势相关的情报。为了实现对攻击行为的实时监控,帮助安全管理人员了解攻击者的攻击方式,分析其目的和动机,此外,研究者设计实现了蜜罐,然而蜜罐技术的使用会引入其他风险,使用不当可能会导致“引狼入室”的相反效果^[23]。基于沙箱的虚拟执行技术在恶意程序检测方面十分有效,恶意程序被重定向至虚拟沙箱下执行,因此能够实现对整个攻击过程的实时监控,既保护了物理主机又便于监控人员了解攻击原理。

传统网络中威胁情报感知技术的作用对象单一、相互之间独立、粒度不够,给威胁情报的精确、完整、高效感知带来诸多不便。云计算虚拟化技术的出现极大地扩展了网络的规模,增加了信息系统的复杂性,给威胁情报感知带来了新的挑战。

新型通信网络架构尤其是软件定义网络利用南向接口将控制逻辑从数据层分离出来,实现了网络的集中控制,开放的可编程接口更增加了网络部署与监控的灵活性和可扩展性。新型网络结构下威胁情报的感知已经成为学术网络安全领域的的前沿方向之一。BRAGA 等^[24]通过获得 OpenFlow 交换设备的流表信息并提取出流表项速率、单流表项率、流表特征熵等特性对待测样本进行检测以确定是否发生了分布式拒绝服务(DDoS, distributed denial of service)攻击。FlowTags^[25]对传统中间件进行很小的改动以使其可以通过 FlowTags 的 API 与 SDN 控制器交互,当出现可疑流时实现对指定流的追踪和路由控制。针对 SDN 下的云平台,文献[26]提出了一种

分布式的、基于事件的、层级化的入侵检测架构,在该架构下,分管不同交换机的子控制器从数据平面收集流量统计数据并将其以“发布—订阅”机制通过事件总线上传至事件处理引擎(EPE, event processing engine)中的事件处理代理(EPA, event processing agent),使网络管理员可以使用专门的事件处理语言(EPL, event processing language)为 EPA 定义基于策略的入侵检测规则,EPE中的一系列EPA可根据制定的策略共同针对接收到的统计数据进行分析,并将多个攻击检测结果与相应的告警事件相关联以实现可疑事件的整合。OpenTM 框架提出数据转发设备将各自所在区域的网络负载状况周期性地发送给 SDN 控制器,然后由控制器根据网络中的路由信息建立全网流量分布矩阵^[27]。

除了上述直接面向网络本身、相关基础设施和流量监控的威胁情报感知外,移动终端和社交媒体如微博、论坛、Facebook、Instagram 等社交化网络媒体的盛行,使威胁情报的搜集边界朝着面向用户和服务的信息内容分析方向快速发展。从社会化网络媒体中搜寻攻击者或与其有关的核心人物的资料可为情报分析工作提供更广阔的视角。用户在网络上的搜索、浏览、讨论、交流等行为可在整理归并后作为判断该用户是否有可能实施攻击的重要依据。且通过黑客论坛、黑产交易网站等方式获取情报也可很大程度上提高情报获取效率、降低成本。IBM 2015 X-Force 威胁情报报告显示,在系统遭到的所有入侵中,由外部人员造成的攻击占安全事件总数的 45%,而其余的 55%则均与内部人员有关,这一事实给系统管理者传达了一个信息——应同时关注内部和外部可能存在的威胁源,外防内控两头抓,才能得到较为全面的情报。外部威胁情报可通过特定行业的共享社区、业务合作伙伴、公开情报源、业界同行、情报服务提供商等途径获得,利用诸如 OSINT、Dell SecureWorks、RSA NetWitness Live、CyberUnited、CrowdStrike、IBM QRadar 等安全分析产品也可实现不同粒度及规模的安全监控需求下的智能网络情报感知。内部情报来源则包括系统部署的入侵检测和防护系统,安全信息和事件管理产品,恶意软件检测工具,文件完整性检

测软件的警报,操作系统、网络、服务和应用程序的日志等,另外,定期对整个系统进行安全等级测评以分析和评估其脆弱性及潜在威胁同样不容忽视。通过对系统合理部署已成熟的安全感知产品,并根据具体安全需求融合运用多种检测技术,从多个维度进行信息的搜集与整合,进而可在全景视角的高度上实现有效的威胁情报感知。

4 威胁情报共享

面对当前日益严峻的威胁形势,各自为政地分头开展情报采集工作不仅易形成信息孤岛从而增大情报搜集成本,而且限制了情报在各组织之间的积极流动,不利于形成健康高效的威胁情报生态系统。打破藩篱,加强各信息系统协同互助,构筑宽共享、全联通的信息共享环境可使威胁情报价值最大化,进而提高参与共享各方的威胁检测与应急响应能力。

4.1 情报共享体系结构

情报共享平台以多种形式存在。根据参与情报共享各方的组织形式不同,可将共享模式分为系统内部共享、平行机构共享、政企共享、国际共享。

1) 系统内部共享。信息系统内部各个部门从各自的业务需求出发,独立地从可用渠道采集情报很容易造成情报内容存在较高的重叠率,导致资源和成本的浪费。较好的做法是以系统核心资产为中心,对情报搜集和研究工作进行统筹规划、合理部署,增强部门之间的沟通协作,同时,寻求一个有效、快速的情报流通、发布机制,尽力克服信息在多部门之间传递时存在的滞后问题,

从而增进整个系统对威胁的了解与感知能力。以攻击溯源为例,该工作需要多来源的数据支持以及跨部门的协作分析,面向攻击溯源的需求,一个定制化的轻量型威胁情报共享利用框架(LWTISUF, light weight threat intelligence sharing and using framework)被建立,在实现攻击情报共享、交换的同时为攻击溯源提供协同化处理机制。系统内部的情报共享是提升整体情报工作的效率及对安全事件的应急响应能力的关键^[28]。

2) 平行机构共享。以产业联盟的方式促进互联网公司、云安全公司、传统安全公司、安全研究人员的情报共享以及金融、银行等具有较高相似度行业中各机构的情报交换可增进企业之间的互信互补,促进参与方对攻击者 TTP 及总体战略的理解,使参与方有机会获取因自身视野存在盲点或信息渠道狭窄而无法搜集到的情报。由 AlienVault 发起的公开威胁交换(OTX, open threat exchange)平台以安全社区的形式为众多组织机构及个人用户提供社交网络框架以共同参与到情报数据及防御方案的交换中。作为国内首个比较正式的情报共享平台,奇虎 360 威胁情报查询中心的发布引起了广泛关注;2015 年 10 月,由天际友盟、WebRAY 等 8 家公司率先发起的“烽火台”安全威胁情报联盟正式成立,这些重要事件推动了国内威胁情报生态圈的发展^[29]。

3) 政企共享。在与公共安全息息相关的關鍵基础设施和国家重点行业的网络安全保障领域注重强化政企合作,开展充分的对话和交流对于提升基础设施、公共服务的安全水平和恢复能力具

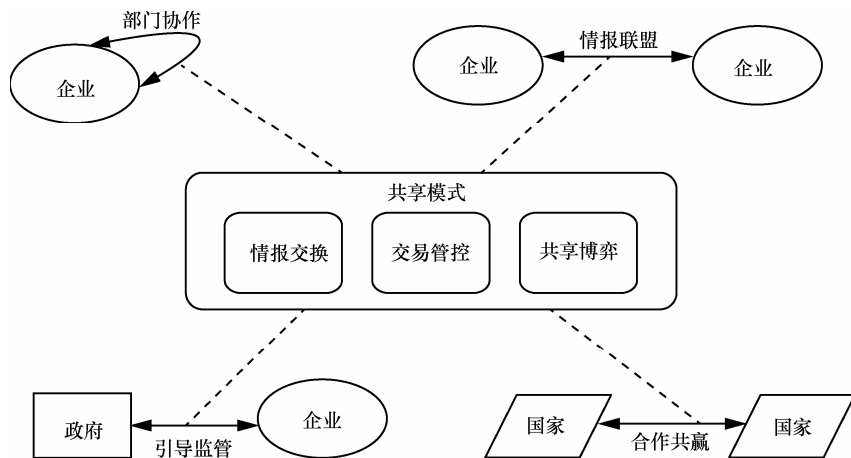


图4 威胁情报共享的层次模型

有重要意义。近几年陆续有国家的关键性基础设施成为安全威胁的指向目标, 业界普遍认为这类状况正有愈演愈烈之势。政府相关部门在应对此类危害公共安全的攻击事件时的防御及相应能力亟待提升。2008年4月, 美国国家情报局推出《美国情报界信息共享战略》, 作为美国出台的关于信息共享的第一份战略报告, 它标志着美国已将情报界共享变革提上国家战略的重要日程^[30]。2015年2月, 白宫宣布成立网络威胁与情报整合中心 (CTIIC, Cyber Threat Intelligence Integration Center) 以调动整合国土安全部、联邦调查局等政府部门与民间企业的情报力量。相比之下, 我国在情报共享领域起步较晚, 2015年6月, 由国家互联网应急中心 (CNCEERT, China National Computer Emergency Response Team) 牵头, 32家单位共同签署了《中国互联网协会漏洞信息披露和处置自律公约》, 这是国内在相关领域的有益尝试。我国应借鉴美国等发达国家的实践经验, 尽快着手建立适合本国国情的紧密合作的政企伙伴关系。

4) 国际情报共享。恐怖组织伊斯兰国 (ISIS, the Islamic State) 通常使用社交网站、网络论坛等互联网媒介传播极端思想并招募成员, 据统计, ISIS 每天在网络上释放多达 9 万多条信息。2015年1月, ISIS 支持者还成功入侵美国中央司令部的 YouTube 和 Twitter 账户导致该机构大量内部文件泄露。犯罪团伙及恐怖主义组织已能够较为熟练地利用互联网进行联络。更为糟糕的是, 由于基础设施对于网络攻击活动的敏感性, 一旦恐怖组织选择利用“数字化武器”实施针对发电站等重要能源系统的网络攻击活动, 那么将会导致天然气、石油、汽油、供水等供应链瘫痪, 对公众生活造成极大不便, 甚至可能造成人员伤亡等严重后果, 从而对目标国家造成比传统恐怖活动更巨大的破坏。政府部门应慎重考虑其日常运作体系可能面临的攻击威胁, 及时做好相关情报的发掘与共享工作。2015年12月16日, 习近平主席在第二届世界互联网大会上发表重要讲话时指出, “各国应加强沟通, 扩大共识, 深化合作, 共同构建网络空间命运共同体”。面对人类共同的威胁, 各国应在相互尊重信任的基础上, 就反恐、打击跨国犯罪等相关事项进行建设性对话, 推动

有关威胁情报的共享, 协同构建和平、开放、稳定的国际环境。

4.2 共享平台建设中的技术性问题

在情报共享时, 要对各方提供的来自各种渠道的海量数据进行整合, 这一过程中需考虑一些技术性问题。首先, 不可避免地会存在情报数据的多源异构性。各共享参与方所提供的威胁情报可能通过各种渠道, 由计算机、安全设备、移动终端等多种类型的传感器产生, 这些情报存在格式差异较大的问题, 除了结构化数据, 它们之中往往还包含大量的非结构化及半结构化数据, 而转化和整合这些多源异构数据无论对于“中心共享式”还是“点对点共享式”平台, 都是较大的挑战。使用可扩展标记语言 (XML, extensible markup language) 是一种比较常见的解决思路, 将从多种传感器获取的异构数据先统一成 XML 数据模型再进行传输, 可简化上层系统的处理开销^[31]。对于“点对点”模式下的情报共享, 不仅存在数据不统一问题, 研究怎样在各组织的分布式异构数据库 (DHD, distributed heterogeneous database) 之间实现高效的情报交互也极为重要。采用 XML 数据读取技术和分布式操作扩展之后的 Unix 事务 (TUXEDO, transaction for unix has been extended for distributed operation) 系统异步传输机制可较好地实现孤岛情报的整合共享^[32], 这种技术也可以用来处理多源异构的威胁情报数据。以 XML 为数据交换格式, XML schema 作为公共模型, Mediator 为集成模式的异构数据库集成中间件可以较好地为用户提供透明的访问接口。但这些方案都无法为威胁情报的共享提供统一的规则, 为解决这一问题, 亟需制定一个开放、标准化的情报共享标准。其次, 大数据背景下威胁情报的规模巨大, 普通的存储技术难以满足其需求, 需寻求新的存储平台来实现对多源共享数据的储存与管理。对于未转化为统一格式的异构情报, 使用非关系数据库 (NoSQL, not only SQL), 将数据分片之后存储在多个 MongoDB 数据库集群节点中^[33]。这样可为系统处理威胁情报提供一定的负载均衡能力, 同时保证可扩展的存储空间, 但不足之处是该数据库技术无法通过 SQL 语言操作且缺乏严格的访问控制机制, 在情报共享这

一应用场景下存在一些问题。云存储大大提升了传统存储技术的容量和性能,为大规模数据的存储提供了新的思路,Hadoop 可以作为威胁情报处理平台,对海量大数据威胁情报进行存储^[34]。但云存储系统的传统构建方法存在提高性能和能耗增长呈线性关系的不足,故亟需设计一种新的架构平衡两者之间的矛盾。

4.3 威胁情报共享的相关标准

标准化的数据格式和统一的传输协议是高效威胁情报共享体系中必不可少的部分。基于结构化的规范情报描述标准和固定的传输协议可降低参与情报共享机构、存储库进行情报交换和数据格式转化的成本,提高所交换情报的效率和准确性,同时简化参与方的连接管理,促进各成员资源共享、协同交流。

为满足情报共享市场的需求,业界已制定了一系列相关标准用于威胁情报的交换。结构化威胁情报表述(STIX, structured threat information expression)基于 XML 语法实现了对威胁情报具体内容的描述,可较清晰地勾勒出威胁因素、威胁走向等相关细节。指示器可信自动交换(TAXII, rusted automated exchange of indicator information)提供了威胁情报信息的安全传输与交换,可兼容多种传输格式的数据。网络可观察对象描述(CybOX, cyber observable expression)对计算机可观察对象及网络动态和实体的表征进行了规范。目前比较主流的情报共享平台的做法是在 STIX 规范框架下,借助 CybOX 提供的词汇描述威胁情报,并利用 TAXII 进行传输^[35]。可机读威胁情报以安全设备可读的方式描述,可被防护系统自动读取与执行,极大提升了对威胁的响应能力。MANDIANT 公司开发的开放威胁指示器(OpenIOC, open indicator of compromise)共享规范可通过灵活建立威胁指示器(IOC, indicator of compromise)的逻辑分组将情报表示成可机读的形式,实现情报的快速共享。

4.4 威胁情报共享的管控

共享过程中的技术性保障的实现及相关交换标准的拟定为情报共享打下了基础,但相互信任的共享关系的形成作为推进情报共享圈发展的重要问题之一仍未得到解决。在这一问题上,应寻

求有效的共享情报预处理机制以保护情报贡献者的隐私,并采取措施限制威胁情报的合理使用。

信任关系形成的前提是保护情报共享方的隐私,同时对威胁情报中涉及到的组织信息也应进行适度的屏蔽。在情报共享过程中,应根据情报提供方的要求,允许其在公开参与信息共享的情况下仍可保持匿名,对其分享的情报应先进行某些脱敏处理,比如:钓鱼邮件样本中不包括与响应攻击事件无关的涉事者敏感信息;提交的捕获数据分组不能泄露登陆凭据、Web 表单提交数据、贡献方的财务信息等;流量统计数据中不包含与威胁无关的员工网络行为(如访问了什么网站)。烽火台等一些情报共享联盟启用了专门的动态数据脱敏引擎对收到的威胁情报自动进行脱敏处理。2015 年 4 月美国众议院通过的情报共享法案中要求在分享信息之前先筛除其中的敏感信息以为参与者提供隐私保护。但在保护贡献者隐私的同时应注意拿捏一定的度,否则可能因情报的原始背景等信息不够全面限制其利用价值。

为避免共享平台的威胁信息被不法分子用于线下黑产交易,防范共享情报的不当传播,应尊重贡献者的意愿并依据共享平台的相关规定,对每个情报进行标记,事先约定其使用范围。US-CERT 开发了红绿灯协议(TLP, traffic light protocol),参与情报共享的组织可用该协议对其产生的、可能被共享的情报的使用范围予以控制。该协议对情报进行分层,每层对应一个颜色,其中,红色表示该情报不能共享;黄色表示该情报只能在组织内部各部门间共享;绿色表示该情报可在组织外部共享,但存在范围限制;白色表示该情报可被共享联盟的任何成员无限制使用。情报共享方可对威胁情报的共享及使用范围进行自定义的管理。

对情报共享联盟成员的身份进行认证和授权控制可为共享系统建立紧密的保护层。只有在共享平台登记并核实了真实身份的组织或个人才可在严格的访问控制下获取到相应权限范围内的情报,这一举措对于保证共享情报的安全性具有重要作用。

4.5 威胁情报共享中的博弈

在威胁情报共享体系中,参与方既是情报提供者,同时也是情报接收者,每个情报持有方在决定是否以双向互动的情报流动链与其他各方进

行情报资源的交换之前, 将结合对共享体系中其他参与者信息的评估并基于自身需求, 对情报交换成本与收益的预期进行权衡, 做出共享或不共享的决策。因此, 在情报共享背后, 实质上是各参与方相互制约、相互影响的完全信息动态博弈过程。

在这一博弈中, 情报持有者一方面希望吸收其他共享参与方提供的异质知识并对其内化整合以提高自身威胁情报存量, 但另一方面又往往出于对情报共享后的利益分配不均、他方提供情报数目及质量与己方不对等、威胁信息的滥用等顾虑, 倾向于在情报共享过程中持消极保留态度, 从而导致整个共享协作圈陷入“囚徒困境”, 阻碍情报共享生态的健康发展。

事实上, 解决情报共享中各参与方缺乏情报共享动力的问题可等价于寻求博弈决策制定过程中的均衡点, 通过对各方共享或不共享情报决策下的收益及成本关系进行讨论, 求解出相关参数的取值范围, 也就得到了促使情报持有者参与共享的条件, 进而根据分析结果进行情报共享机制的建设与完善。

目前, 在学术界已开展了一些针对知识共享博弈分析的探讨, 这些博弈论方法都为高效地实现威胁情报共享提供了良好支撑。朱建明等^[36]采用博弈论方法, 提出了对信息安全技术进行评价的模型, 该模型对威胁情报共享效率的评估提供了很好的借鉴。宁焯等^[37]基于完全信息动态博弈方法, 以自学/共享净收益及其他损失为参数构造不等式求得子博弈纳什均衡值, 给出了知识共享条件, 即共享净收益大于自学净收益, 但未对相关影响因素进行讨论。类似地, LARSSON 等^[38]指出参与方的怀疑心态以及共享过程中不对称的学习资源将阻碍联盟中知识的共享进程, 为尽量避免这一情形的出现应加强各方深入交流并敦促参与方提供各自情报共享能力。杨威等^[39]提出了一个不可转移支付的联盟构造博弈模型, 解决了协作感知系统的多目标非线性优化问题, 对优化威胁情报共享中的协同感知提供了很好的支持。Lane 等^[40]针对知识共享活动提出了 IJV 模型, 探讨了共享圈中信任关系及接收实体学习能力对其他参与方所共享知识的吸收能力的影响。由于大部分关于知识共享模式的研究是从组织层面出发

的而忽略了共享过程中各参与方自身对顺利共享进程的作用, SOEKIJAD 等^[41]通过对几个案例进行分析比对, 指出除了单纯的知识交换, 各参与方对知识的获取及发展能力对于成功的共享也至关重要。伍佐福^[42]基于博弈论的方法, 从能源消费的角度, 对 2 个实力大致相当的国家之间的战略互动进行研究, 并建立了“能源博弈自主合作模型”, 该模型对国家之间实现威胁情报共享的战略互动提供了很好的参考。

从以上研究中, 可得到关于建立健全情报共享机制的一些有益启示。首先, 从各参与方自身来说, 应在保证情报质量的同时努力提升情报存量, 并增强对于新获得威胁信息的转化利用能力, 缩小与其他各方在威胁情报技术上的差距, 只有拥有足够强的实力才能吸引水平相当的情报持有方与己方进行知识共享; 其次, 为充分保障情报共享者的权益, 应设立强有力的奖惩制度, 调动各方共享情报的积极性, 并严厉打击“搭便车”行为以防止其对健康共享环境造成的负面影响; 另外, 在已建立的共享关系中引导道德舆论, 形成共享实体之间的心理契约, 达成共享圈中共同的价值观对于促进协同合作, 约束投机者的行为也具有重要意义。

5 威胁情报分析

威胁情报分析工作可为安全态势评估和防御系统整改提供有益的支持, 且该评估结果与优化方案又可反过来作为威胁情报的一部分以促进对威胁的认识。只有将分析结论与常规决策流程相结合, 把情报落实为具体的安全措施, 才能改善企业安全状况, 增强国家应对突发安全事件的响应能力。

5.1 威胁情报分析的内涵

获取到大量多源情报后, 若要真正让其发挥价值, 用于信息系统的安全态势评估与研判, 辅助安全人员了解整体威胁态势、攻击组织动向, 进行实现对现有防御体系的评估与高危事故的预警, 并为特定威胁下的安全决策活动提供支持, 则必须对所掌握到的情报进行谨慎分析, 否则情报信息数目再多、搜集渠道再广泛也难以从未处理的威胁信息中“看清”其背后隐含的重要信息。实现威胁情报分析, 需要融入威胁情报分析的空

间完备性和时间连续性,从“内、外”2个空间角度出发,沿“过去、现在、将来”一条时间主线,借用多源信息融合技术,融合来自一个系统的具有相似或不同特征模式的多源检测信息,综合、准确地分析当前网络威胁状态及演化趋势,在此基础上预测威胁的未来状态,即利用网络安全属性的历史记录,为用户提供一个准确的网络威胁状态评判和网络威胁发展趋势,以便管理员了解当前、过去及未来的安全状况,使网络管理者能够有目标地进行决策和防护准备,为采取适当的系统策略提供保障。同时威胁情报分析的结构还能有力支撑网络安全的防御、检测、响应、恢复,有助于形成一个闭环的安全保护系统。

5.2 威胁情报评估

安全威胁评估是情报分析工作的重要组成部分,它根据威胁信息对信息系统现存或潜在危险及其可能带来的后果进行预测,帮助用户理解当前安全态势,有针对性地制定响应措施,提高应对突发事件的能力。王永杰等^[43]基于攻击图模型给出了一种可进行攻击序列成功概率和系统损失风险分析的安全评估方法。肖道举等^[44]采用插件技术,结合漏洞威胁信息建立了对系统安全状况进行定量分析的评估模型。BASS^[45]利用多传感器数据融合技术对分布式的异构网络设备中采集的原始数据进行处理,从而识别出攻击源、威胁危险程度、目标系统等信息以对网络的安全态势进行评估,但未提出实际应用模型。陈秀真等^[46]通过IDS的报警信息和网络性能指标提出了层次化网络安全威胁态势评估模型以实现网络安全定量评估,但该模型不适合大规模网络系统的评估。王卓君^[47]针对军事情报分析的应用场景利用ID3决策树算法和Boltzmann机神经网络算法对数据进行分类以用于军情威胁评估。

5.3 威胁情报关联分析

将关联融合、时间序列、流数据分类等技术运用于大数据环境下的威胁情报分析能够提高从繁杂的海量信息中提取出高价值威胁特征的能力,有助于对看似不相关的多方位情报进行横向、纵向关联,深度挖掘多维线索之间隐藏的内在联系,进而对系统的整体威胁态势进行清晰的描述。目前相关技术已被运用于情报研究工作中。已经

有相关研究使用决策树和聚类等相关分析方法来实现系统的入侵检测^[48,49]。卿斯汉等^[50]基于网络蠕虫攻击行为的特征给出了基于网状关联分析预警网络蠕虫的算法,但其中的预警机制对各组件的协同能力要求较高。

5.4 威胁态势智能推演

采用人工智能的方法可以实现对威胁情报的智能分析,并对其发展的态势进行推演,这将有效提升整个系统的防御能力。伍军等^[49]提出了采用强化学习结合分层学习的思想来实现无线传感网络的攻击预测。孙钦东等^[51]基于流链接密度事件序列分析检测方法,通过机器学习中的支持向量机模型对DDoS攻击实现了有效检测及确认。但传统机器学习在威胁情报规模较大的情况下可能存在处理性能的问题,对新的机器学习算法进行研究以适应大数据环境的处理需求具有重要意义^[52]。拒绝服务的分形维检测(FDD-DoS, fractal dimension detect-denial of service)算法综合运用基于熵的属性分类挖掘和分形技术同样可以较高准确率从众多通信流量中完成对异常DoS流量的鉴别^[53]。已有很多研究把智能学习算法用于对计算机系统的潜在威胁预测^[54-57]。此外,在交通、视频通信、社交网络等其他领域已经有较为成熟的智能分析模型^[58-63],其设计思路也可以为实现威胁情报智能推演提供很好的参考。

5.5 大数据背景下的威胁情报分析

当对大规模网络进行全网的威胁情报分析时,其威胁情报共享系统将形成大数据系统。大数据威胁情报的特点有体量巨大、有价值信息的密度低,因此,需要采用大数据分类技术,对海量数据进行分类整理,为此MapReduce等体系架构可以引入到威胁情报分析中来。同时,为了提高分析的精度,可以采用一些新型的智能技术,如类脑学习。此外,对原始的威胁情报大数据进行精简提炼的预处理之后,原来的决策树、聚类分析技术依然可以得到有效的使用。总之,如何在大数据环境下实现威胁情报的关联分析,是值得进一步探讨的问题。

5.6 分析工具

为实现智能情报分析,已出现了许多相关的情报分析工具。Solera DeepSee将可疑信息以时

间顺序排列, 可实现对 APT 攻击源的快速定位。Narus 公司开发的 Narus nSystems 工具可通过多维度信息融合并基于机器学习方法为不同攻击行为生成相应的签名。Fluke 网络时光机 (Fluke network time machine) 可追溯导致网络异常的根本原因, 同时它也可实现全流量分析存储。信息系统的管理人员可根据组织安全需求灵活部署相关产品辅助情报的分析。另外, 处理大数据的相关工具, 如 Hadoop、Spark、MapReduce 等, 经过定制设计, 也能用来对海量威胁情报进行分析。

6 结束语

威胁情报体系的出现革新了以往的安全防御思路, 它以威胁情报为核心, 通过多维度、全方位的情报感知, “协同合作、和平利用”的情报共享以及对所掌握信息的深度挖掘与分析, 帮助信息系统的管理者了解当前安全态势, 对威胁动向做出合理的预判, 从而将传统的“被动防御”转变为积极的“主动防御”, 提高系统的应急响应能力。但目前, 威胁情报领域在发展过程中仍存在一些障碍。比如搜集情报后的有用信息筛选, 情报共享过程中相关法律法规框架的制定以及各方利益的平衡, 大数据等分析技术在情报研究工作中应用不够深入等。这些问题将随着研究的进一步推进和经验积累而取得突破。

面对当前复杂的威胁形势, 不管对于企业、政府部门、国家机关还是国际组织, 威胁情报体系的构建都有至关重要的意义。各方应结合自身业务流程与安全需求, 针对核心资产增强威胁情报感知能力, 积极融合云计算、大数据等前沿技术, 建立威胁与漏洞深度分析系统, 在深度挖掘与关联融合的基础上做好安全态势评估及风险预警, 动态调整安全策略, 部署快速可行的安全响应战略, 确保关键资产的安全。同时还应在涉及一致利益的领域, 以政府主导或产业联盟等多种形式, 本着“和平利用、利益均衡”的原则展开广泛而深入的协同交流。在面对共同威胁时形成合力, 并在情报共享实践中持续健全相关法律法规保障体系, 努力构筑和谐、健康、成熟的威胁情报生态圈。随着威胁情报技术的不断成熟及相关规范、框架的日渐完善, 在安全问题日益严峻

的未来, 它将进一步在社会、国家乃至全球的各个层面发挥越来越大的作用。

参考文献:

- [1] 李建华, 徐婧. 信息安全内涵属性的系统性分析[J]. 信息网络安全, 2007(2): 70-78.
LI J H, XU J. Systemic analysis of the connotation attributes of information security[J]. Netinfo Security, 2007(2): 70-78.
- [2] MITCHELL R, CHEN I R. Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems[J]. IEEE Transactions on Dependable and Secure Computing, 2015, 12(1): 16-30.
- [3] SHAKSHUKI E M, KANG N, SHELAMI T R. EAACK-a secure intrusion-detection system for MANETs[J]. IEEE Transactions on Industrial Electronics, 2013, 60(3): 1089-1098.
- [4] 陈华山, 皮兰, 刘峰, 等. 网络空间安全科学基础的研究前沿及发展趋势[J]. 信息网络安全, 2015(3): 1-5.
CHEN H S, PI L, LIU F, et al. Research on frontier and trends of science of cybersecurity[J]. Netinfo Security, 2015(3): 1-5.
- [5] HE H, LI R, DONG X, et al. Secure, efficient and fine-grained data access control mechanism for P2P storage cloud[J]. IEEE Transactions on Cloud Computing, 2014, 2(4): 471-484.
- [6] LIN Y D, LIN P C, YE H C H, et al. An extended SDN architecture for network function virtualization with a case study on intrusion prevention[J]. IEEE Network, 2015, 29(3): 48-53.
- [7] LIU A X, KHAKPOUR A R. Quantifying and verifying reachability for access controlled networks[J]. IEEE/ACM Transactions on Networking, 2013, 21(2): 551-565.
- [8] VALENZANO A. Industrial cybersecurity: improving security through access control policy models[J]. IEEE Industrial Electronics Magazine, 2014, 8(2): 6-17.
- [9] THIMMA M, LIU F, LIN J, et al. HyXAC: hybrid XML access control integrating view-based and query-rewriting approaches[J]. IEEE Transactions on Knowledge and Data Engineering, 2015, 27(8): 2190-2202.
- [10] CHEMINOD M, DURANTE L, SENO L, et al. Semiautomated verification of access control implementation in industrial networked systems[J]. IEEE Transactions on Industrial Informatics, 2015, 11(6): 1388-1399.
- [11] MITCHELL R, CHEN I R. Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications[J]. IEEE Transactions on Systems, Man, and Cybernetics Systems, 2014, 44(5): 593-604.
- [12] HAN S, XIE M, CHEN H H, et al. Intrusion detection in cyber-physical systems: techniques and challenges[J]. IEEE Transactions on Dependable and Secure Computing, 2015, 12(1): 16-30.
- [13] CHEN F, BRUHadeshwar B, LIU A X. Cross-domain privacy-preserving cooperative firewall optimization[J]. IEEE/ACM Transactions on Networking, 2013, 21(3): 857-868.
- [14] THIMMA M, LIU F, LIN J, et al. HyXAC: hybrid XML access control integrating view-based and query-rewriting approaches[J]. IEEE Transactions on Knowledge and Data Engineering, 2015, 27(8): 2190-2202.
- [15] 王腾, 王江, 焦虹阳, 等. 一种基于 OpenFlow 的 SDN 访问控制策略实时冲突检测与解决方法[J]. 计算机学报, 2015, 38(4): 872-883.

- WANG J, WANG J, JIAO H Y, et al. A method of OpenFlow-based real-time conflict detection and resolution for SDN access control policies[J]. Chinese Journal of Computers, 2015, 38(4): 872-883.
- [16] 沈昌祥, 张焕国, 冯登国, 等. 信息安全综述[J]. 中国科学(E辑: 信息科学), 2007, 37(2): 129-150.
- SHEN C X, ZHANG H G, FENG D G, et al. Overview of cyber security[J]. Science in China (Series E), 2007, 37(2): 129-150.
- [17] 中国信息通信研究院. 网络与信息安全产业白皮书[R/OL]. <http://www.catr.cn/kxyj/qwfb/bps/201512/P020151223329544210421.pdf>.
- China Academy of Information and Communication Technology. White paper of network and information security industry[R/OL]. <http://www.catr.cn/kxyj/qwfb/bps/201512/P020151223329544210421.pdf>.
- [18] GREECH J, HU J. A semantic approach to host-based intrusion detection systems using contiguous and discontiguous system call patterns[J]. IEEE Transactions on Computers, 2014, 63(4): 807-819.
- [19] MA X, CHEN Y. DDoS detection method based on Chaos analysis of network traffic entropy[J]. IEEE Communications Letters, 2014, 18(1): 114-117.
- [20] 荆涛, 李俊. 基于相异度分析的网络通信异常行为识别方法[J]. 微电子学与计算机, 2014(6): 12-15.
- JING T, LI J. An identification method based on analysis of dissimilarity degree for network communication behavior[J]. Microelectronics & Computer, 2014(6): 12-15.
- [21] 王慧强, 赖积保, 胡明明, 等. 网络安全态势感知关键实现技术研究[J]. 武汉大学学报: 信息科学版, 2008(10): 995-998.
- WANG H Q, LAI J B, HU M M, et al. Research on the key realization technologies of network security situation awareness[J]. Spectroscopy and Spectral Analysis, 2008(10): 995-998.
- [22] 赖积保, 王颖, 王慧强, 等. 基于多源异构传感器的网络安全态势感知系统结构研究[J]. 计算机科学, 2011, 38(3): 144-149.
- LAI J B, WANG Y, WANG H Q, et al. Research on network security situation awareness system architecture based on multi-source heterogeneous sensors[J]. Computer Science, 2011, 38(3): 144-149.
- [23] 唐勇, 卢锡城, 胡华平, 等. Honeypot 技术及其应用研究综述[J]. 小型微型计算机系统, 2007(8): 1345-1351.
- TANG Y, LU X C, HU H P, et al. Honeypot technique and its applications: a survey[J]. Journal of Chinese Computer Systems, 2007(8): 1345-1351.
- [24] BRAGA R, MOTA E, PASSITO A. Lightweight DDoS flooding attack detection using NOX/OpenFlow[C]//The 38th Annual IEEE Conference on Local Computer Networks, Sydney. c2010: 408-415.
- [25] FAYAZBAKHSH S K, SEKAR V, YU M, et al. FlowTags: enforcing network-wide policies in the presence of dynamic middlebox actions[C]//The Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, Hong Kong, China. c2013: 19-24.
- [26] HU Y L, SU W B, WU L Y, et al. Design of event-based intrusion detection system on OpenFlow network[C]//The 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Budapest. c2013: 1-2.
- [27] TOOTOONCHIAN A, GHOBADI M, GANJALI Y. OpenTM: traffic matrix estimator for OpenFlow networks[C]//The 11th International Conference on Passive and Active Measurement, Zurich. c2010: 201-210.
- [28] 杨泽明, 李强, 刘俊荣, 等. 面向攻击溯源的威胁情报共享利用研究[J]. 信息安全研究, 2015(1): 31-36.
- YANG Z M, LI Q, LIU J R, et al. Research on the using of threat intelligence sharing facing attacking source[J]. Journal of Information Security Research, 2015(1): 31-36.
- [29] 2015 年网络安全威胁的回顾与展望[EB/OL]. http://www.antiy.com/response/2015_Antiy_Annual_Security_Report.html#. Retrospect and prospect of network security threat in 2015[EB/OL]. http://www.antiy.com/response/2015_Antiy_Annual_Security_Report.html#.
- [30] Intelligence community information sharing strategy[EB/OL]. http://www.odni.gov/retorts/IC_Information_Sharing_Strategy.pdf.
- [31] LI J, LIU C, ZHOU R, et al. Quasi-SLCA based keyword query processing over probabilistic XML data[J]. IEEE Transactions on Knowledge and Data Engineering, 2014, 26(4): 957-969.
- [32] 李玉翠. 多源异构数据集成技术研究[D]. 西安: 西安电子科技大学, 2009.
- LI Y C. Research on multi-source heterogeneous data integration technologies[D]. Xi'an: Xidian University, 2009.
- [33] PADHYE V, TRIPATHI A. Scalable transaction management with snapshot isolation for NoSQL data storage systems[J]. IEEE Transactions on Services Computing, 2015, 8(1): 121-135.
- [34] LUO S, ZHANG G, WU G, et al. Boafft: distributed deduplication for big data storage in the cloud[J]. IEEE Transactions on Cloud Computing, 2015(12): 1.
- [35] 威胁情报共享的相关规范和标准[EB/OL]. http://www.secpulse.com/archives/34801.html?utm_source=tuicool&utm_medium=referral. Related specifications and standards of threat intelligence sharing[EB/OL]. http://www.secpulse.com/archives/34801.html?utm_source=tuicool&utm_medium=referral.
- [36] 朱建明, RAGHUNATHAN S. 基于博弈论的信息安全技术评价模型[J]. 计算机学报, 2009, 32(4): 828-834.
- ZHU J M, RAGHUNATHAN S. Evaluation model of information security technologies based on game theoretic evaluation model of information security technologies based on game theoretic[J]. Chinese Journal of Computers, 2009, 32(4): 828-834.
- [37] 宁辉, 樊治平, 冯博. 知识联盟中知识共享的博弈分[J]. 东北大学学报(自然科学版), 2006, 27(9): 1046-1049.
- NING Y, FAN Y P, FENG B. Game analysis of knowledge sharing in knowledge alliances[J]. Journal of Northeastern University(Natural Science), 2006, 27(9): 1046-1049.
- [38] LARSSON R, SPARKS J. The interorganizational learning dilemma: collective knowledge development in strategic alliances[J]. Organization Science, 1998, 9(3): 285-305.
- [39] 杨威, 班冬松, 管东林, 等. 基于联盟构造博弈的认知无线网络分布式多目标协作感知算法[J]. 计算机学报, 2012, 35(4): 730-740.
- YANG W, BAN D S, GUAN D L, et al. Coalition formation based distributed algorithm for multi-objective cooperative sensing in cognitive radio networks[J]. Chinese Journal of Computers, 2012, 35(4): 730-740.
- [40] LANE P J, SALK J E, LYLES M A. Absorptive capacity, learning, and performance in international joint ventures[J]. Strategic Management Journal, 2001, 22(12): 1139-1161.
- [41] SOEKIJAD M, ANDRIESEN E. Conditions for knowledge sharing in competitive alliances[J]. European Management Journal, 2003, 21(5): 578-587.
- [42] 伍佐福. 能源消费国家间的能源国际合作: 一种博弈的分析[D]. 上海: 复旦大学, 2007.
- WU Z F. A kind of game analysis of energy international cooperation

- tion between energy consumption countries[D]. Shanghai: Fudan University, 2007.
- [43] 王永杰, 鲜明, 刘进, 等. 基于攻击图模型的网络安全评估研究[J]. 通信学报, 2007, 28(3):29-34.
WANG Y J, XIAN M, LIU J, et al. Study of network security evaluation based on attack graph model[J]. Journal on Communications, 2007, 28(3):29-34.
- [44] 肖道举, 杨素娟, 周开锋, 等. 网络安全评估模型研究[J]. 华中科技大学学报(自然科学版), 2002, 30(4):37-39.
XIAO D J, YANG S J, ZHOU K F, et al. A study of evaluation model for network security[J]. Journal of Huazhong University of Science and Technology (Nature Science), 2002, 30(4):37-39.
- [45] BASS T. Multisensor data fusion for next generation distributed intrusion detection systems[C]//The Iris National Symposium on Sensor & Data Fusion. c1999: 24-27.
- [46] 陈秀真, 郑庆华, 管晓宏, 等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报, 2006, 17(4):885-897.
CHEN X Z, ZHENG Q H, GUAN X H, et al. Research on a data classifying algorithm in threat assessment[J]. Journal of Intelligence, 2006, 17(4):885-897.
- [47] 王卓君. 一种用于情报威胁评估的数据分类算法研究[J]. 情报杂志, 2011, 30(10):156-162.
WANG Z J. Research on a data classifying algorithm in threat assessment[J]. Journal of Intelligence, 2011, 30(10):156-162.
- [48] WU J, SHIMAMOTO S. Integrated UCON-based access control and adaptive intrusion detection for wireless sensor networks[C]//The IEEE Global Communications Conference, Miami. c2010: 1-5.
- [49] WU J, LIU S, ZHOU Z, et al. Toward intelligent intrusion prediction for wireless sensor networks using three-layer brain-like learning[J]. International Journal of Distribute Sensor Networks, 2012, 27(3): 327-352.
- [50] 卿斯汉, 文伟平, 蒋建春, 等. 一种基于网状关联分析的网络蠕虫预警新方法[J]. 通信学报, 2004, 25(7):62-70.
QING S H, WEN W P, JIANG J C, et al. A new approach to forecasting internet worms based on netlike association analysis[J]. Journal of China Institute of Communications, 2004, 25(7):62-70.
- [51] 孙钦东, 张德运, 高鹏. 基于时间序列分析的分布式拒绝服务攻击检测[J]. 计算机学报, 2005, 28(5):767-773.
SUN Q D, ZHANG D Y, GAO P. Detecting distributed denial of service attacks based on time series analysis[J]. Chinese Journal of Computers, 2005, 28(5):767-773.
- [52] 何清, 李宁, 罗文娟, 等. 大数据下的机器学习算法综述[J]. 模式识别与人工智能, 2014(4):327-336.
HE Q, LI N, LUO W J, et al. A survey of machine learning algorithms for big data[J]. Pattern recognition and artificial intelligence, 2014(4):327-336.
- [53] 谢方军, 唐常杰, 元昌安, 等. 基于流数据分类和分形维分析的DoS攻击检测[J]. 四川大学学报(工程科学版), 2004, 36(6):87-92.
XIE F J, TANG C J, YUAN C A, et al. DoS attack detection based on classification of stream data and fractal dimension analysis[J]. Journal of Sichuan University (Engineering Science Edition), 2004, 36(6):87-92.
- [54] LIU M, MIAO L, ZHANG D. Two-stage cost-sensitive learning for software defect prediction[J]. IEEE Transactions on Reliability, 2014, 63(2): 676-686.
- [55] SHEPPERD M, BOWES D, HALL T. Researcher bias: the use of machine learning in software defect prediction[J]. IEEE Transactions on Software Engineering, 2014, 40(6): 603-616.
- [56] YANG X, TANG K, YAO X. A learning-to-rank approach to software defect prediction[J]. IEEE Transactions on Reliability, 2015, 64(1): 234-246.
- [57] HUANG W, SONG G, HONG H, et al. Deep architecture for traffic flow prediction: deep belief networks with multitask learning[J]. IEEE Transactions on Intelligent Transportation Systems, 2014, 15(5): 2191-2201.
- [58] JUANG C F, CHEN C Y. An interval type-2 neural fuzzy chip with on-chip incremental learning ability for time-varying data sequence prediction and system control[J]. IEEE Transactions on Neural Networks and Learning Systems, 2014, 25(1): 216-228.
- [59] CHAN K Y, DILLON T S. On-road sensor configuration design for traffic flow prediction using fuzzy neural networks and Taguchi method[J]. IEEE Transactions on Instrumentation and Measurement, 2013, 62(1): 50-59.
- [60] DING T, HIROSE A. Fading channel prediction based on combination of complex-valued neural networks and chirp Z-transform[J]. IEEE Transactions on Neural Networks and Learning Systems, 2014, 25(9): 1686-1695.
- [61] LOPEZ-GARIA P, ONIEVA E, OSABA E, et al. A hybrid method for short-term traffic congestion forecasting using genetic algorithms and cross entropy[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(2): 557-569.
- [62] 刘云龙, 李人厚. 发现和学习不可复位动态系统的预测状态表示的一种新算法[J]. 电子学报, 2009, 37(1): 126-131.
LIU Y L, LI R H. A new algorithm for discovery and learning of predictive state representations in dynamical systems without reset[J]. Acta Electronica Sinica, 2009, 37(1): 126-131.
- [63] LUO X, LV Y, CHEN Y. Web service QoS prediction based on adaptive dynamic programming using fuzzy neural networks for cloud services[J]. IEEE Access, 2015, 3: 2260-2269.

作者简介:



李建华(1965-), 男, 江西九江人, 博士, 上海交通大学信息安全工程学院院长、教授, 主要研究方向为网络与信息安全技术包括网络信息安全管理理论及应用、内容安全管理理论及应用、电子政务理论及应用、网络攻防和信息系统安全评测理论及应用等。