



中华人民共和国国家标准

GB/T 44886.4—2026

代替 GB/T 36643—2018

网络安全技术 网络安全产品互联互通 第4部分：威胁信息格式

Cybersecurity technology—Cybersecurity product interconnectivity—
Part 4: Threat information format

2026-07-02 发布

2027-02-01 实施

国家市场监督管理总局 发布
国家标准化管理委员会

目 次

前言 III

引言 IV

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 概述 2

6 组件的结构及公共属性 5

7 组件 7

8 关系组件..... 24

附录 A（规范性） 字段类型描述 26

附录 B（规范性） 模式语言的描述 28

附录 C（规范性） 可观测数据子组件 37

附录 D（规范性） 词汇表 52

附录 E（资料性） 威胁信息封装和解析方式 68

附录 F（资料性） 威胁信息组件示例的 JSON 表示 69

附录 G（资料性） 组件关系汇总 78

附录 H（资料性） 部分攻击场景下威胁信息描述示例..... 80

附录 I（资料性） 表达式计算示例 92

参考文献 94

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是 GB/T 44886《网络安全技术 网络安全产品互联互通》的第4部分。GB/T 44886 已经发布了以下部分：

- 第1部分：框架；
- 第2部分：资产信息格式；
- 第3部分：告警信息格式；
- 第4部分：威胁信息格式；
- 第5部分：行为信息格式。

本文件代替 GB/T 36643—2018《信息安全技术 网络安全威胁信息格式规范》，与 GB/T 36643—2018 相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 增加了网络安全威胁信息互联互通典型应用场景(见 5.1)；
- b) 更改了网络安全威胁信息描述模型(见 5.2, GB/T 36643—2018 的第5章)；
- c) 增加了“组件结构及公共属性”内容(见第6章)；
- d) 删除了“安全事件”组件(见 GB/T 36643—2018 的 6.4)；
- e) 更改了“攻击方法”组件描述, 将其拆分为“攻击模式”“基础设施”“恶意软件”三个组件进行独立描述(见 7.2.1、7.2.2、7.2.5, GB/T 36643—2018 的 6.6)；
- f) 增加了“漏洞”组件实现对攻击目标的描述(见 7.2.4)；
- g) 更改了可观测数据组件描述和内容(见 7.3.1 和附录 C, GB/T 36643—2018 的 6.2)；
- h) 增加了“工具”“恶意软件分析结果”“攻击活动集”“地理位置”“报告”和“观点”6 个组件(见 7.2.3、7.2.6、7.3.4、7.4.1、7.4.2、7.4.3)。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国电子技术标准化研究院、国家计算机网络应急技术处理协调中心、北京天际友盟信息技术有限公司、北京神州绿盟科技有限公司、华为技术有限公司、天翼安全科技有限公司、中国科学院信息工程研究所、国家信息技术安全研究中心、中国信息安全测评中心、国家信息中心、中国交通通信信息中心、公安部第一研究所、北京航空航天大学、西安电子科技大学、中国科学院计算机网络信息中心、中国人民大学、安徽科技工程大学、杭州安恒信息技术股份有限公司、北京源堡科技有限公司、奇安信科技集团股份有限公司、北京天融信网络安全技术有限公司、启明星辰信息技术集团股份有限公司、北京微步在线科技有限公司、长扬科技(北京)股份有限公司、北京长亭科技有限公司、上海斗象信息科技有限公司、远江盛邦安全科技集团股份有限公司、用友网络科技股份有限公司、中广核智能科技(深圳)有限责任公司、中移动信息技术有限公司。

本文件主要起草人：王惠莅、张东举、廖剑、李琳、蔡磊、崔牧凡、翟湛鹏、张宇娜、李强、梁伟、姚叶鹏、秋阳、姚佳明、贺铮、易锦、韩一剑、耿同成、杜渐、伍前红、马文平、习宁、肖彪、秦波、曹浩、涂小毅、梁露露、白敏、晋钢、胡月、张宽、白燕妮、杨大路、赵华、陈联鉴、曾裕智、权晓文、季晟宇、姜政伟、封荣、陈伟雄、冀文、白雪。

本文件及其所代替文件的历次版本发布情况为：

- 2018 年首次发布为 GB/T 36643—2018；
- 本次为第一次修订。

引 言

GB/T 44886《网络安全技术 网络安全产品互联互通》是指导网络安全产品互联互通建设的基础性和通用性标准,拟由六个部分构成。

- 第1部分:框架。目的在于明确网络安全产品互联互通应用场景,提出互通建设思路。
- 第2部分:资产信息格式。目的在于提出网络安全产品互联互通时的资产描述。
- 第3部分:告警信息格式。目的在于有效整合网络安全产品报送的告警信息,提高告警应急处置效率。
- 第4部分:威胁信息格式。目的在于统一网络安全产品及各组织威胁信息共享格式。
- 第5部分:行为信息格式。目的在于促进网络安全产品行为信息的分析利用。
- 第6部分:功能接口。目的在于高效整合网络安全信息,促进网络安全产品功能协同。

随着网络攻防对抗博弈的日益加剧,网络攻击方式和攻击手法呈现出多样性、复杂性特点,网络安全威胁具有越来越明显的普遍性和持续性,且攻击者获取攻击工具越来越便利,导致网络攻击成本大大降低,检测网络攻击的难度却越来越大。传统的网络安全防护方案仅仅依靠各个组织独立实施垂直的防护机制,在应对这些复杂网络攻击时显得越来越低效,亟待采取新的技术手段来提升整体网络安全防护能力。

网络安全威胁信息共享和利用是提升整体网络安全防护效率的重要措施,旨在采用多种技术手段,通过采集大规模、多渠道的碎片式攻击或异常数据,集中地进行深度融合、归并和分析,形成与网络安全防护有关的威胁信息线索,并在此基础上进行主动、协同式的网络安全威胁预警、检测和响应,以降低网络安全威胁的防护成本,提升整体的网络安全防护效率。

目前威胁信息来源多样,其描述格式不尽统一。威胁信息是网络安全产品互联互通信息的6类信息之一。规范网络安全威胁信息的格式和交换方式是实现网络安全威胁信息共享和利用的前提和基础。本文件规定了一种结构化方法描述网络安全威胁信息,目的是规范网络安全威胁信息的一致性描述,提升威胁信息的共享效率、互操作性,进而提升整体的网络安全威胁态势感知能力,实现网络安全威胁管理和应用的自动化。

网络安全技术 网络安全产品互联互通

第4部分:威胁信息格式

1 范围

本文件规定了网络安全产品互联互通场景下网络安全威胁信息的格式,包括各组件的属性及组件之间的关系。

本文件适用于网络安全产品生成、使用和威胁信息处理,也为网络安全威胁信息平台的建设和运营提供参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 4754 国民经济行业分类

GB/T 17969.8 信息技术 对象标识符登记机构操作规程 第8部分:通用唯一标识符(UUIDs)的生成及其在对象标识符中的使用

GB/T 25069 信息安全技术 术语

GB/T 28458 信息安全技术 网络安全漏洞标识与描述规范

GB/T 44886.2 网络安全技术 网络安全产品互联互通 第2部分:资产信息格式

IETF RFC 1034 域名 概念和设施(Domain names—Concepts and facilities)

IETF RFC 3986 统一资源标识符(URI):通用语法[Uniform Resource Identifier(URI):Generic Syntax]

IETF RFC 5322 互联网消息格式(Internet Message Format)

IETF RFC 5646 语言识别标签(Tags for Identifying Languages)

IETF RFC 5890 面向应用的国际化域名(IDNA):定义和文档框架 [Internationalized Domain Names for Applications (IDNA):Definitions and Document Framework]

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

网络安全产品互联互通 cybersecurity product interconnectivity

通过统一的网络安全信息描述和功能接口定义,有效共享网络安全产品感知或产生的信息,协同不同网络安全产品的功能,支撑监测预警、信息共享、应急响应、态势感知等应用,提升网络安全防护能力和网络安全事件处置效率的一种机制。

[来源:GB/T 44886.1—2024,3.2]

3.2

威胁 threat

可能对系统或组织造成危害的不期望事件的潜在因素。

[来源:GB/T 25069—2022,3.628]

3.3

威胁信息 threat in formation

基于证据的、经过自动或人工处理而形成的,用于描述现有或可能出现的威胁的知识。

注:威胁信息一般包括两大类。

- a) 对可能威胁网络正常运行的行为,用于描述其意图、方法、工具、过程、结果等的信息。例如:计算机病毒、网络攻击、网络入侵、网络安全事件等。
- b) 可能暴露网络脆弱性的信息。例如:系统漏洞、网络和信息系统存在风险的情况等。

3.4

攻击链 kill chain

一个用来描述包含多个攻击步骤的多步攻击模型。

4 缩略语

下列缩略语适用于本文件。

APT:高级可持续威胁(Advanced Persistent Threat)

ATT&CK:对抗性战术、技术和常识知识库(Adversarial Tactics Techniques and Common Knowledge)

CA:证书颁发机构(Certificate Authority)

CAPEC:通用攻击模式枚举与分类(Common Attack Pattern Enumeration and Classification)

CIDR:无类别域间路由(Classless Inter-Domain Routing)

CPE:通用平台枚举(Common Platform Enumeration)

IP:互联网协议(Internet Protocol)

JSON:JavaScript 对象表示法(JavaScript Object Notation)

MAC:媒体访问控制(Media Access Control)

MIME:多用途互联网邮件扩展(Multipurpose Internet Mail Extensions)

URL:统一资源定位符(Uniform Resource Locator)

5 概述

5.1 应用场景

威胁信息互联互通典型应用场景主要包括以下两类。

- a) 威胁信息的汇聚与分析。威胁信息分析人员通过威胁信息平台从威胁信息共享门户或服务站点获取外部威胁信息,结合内部防火墙、入侵检测系统、入侵防御系统、终端安全监测等产品回传的告警及行为信息进行分析研判,生成威胁信息,如图 1 所示。

注:威胁信息平台是指根据收集到的信息进行安全分析,并生成威胁信息的系统。

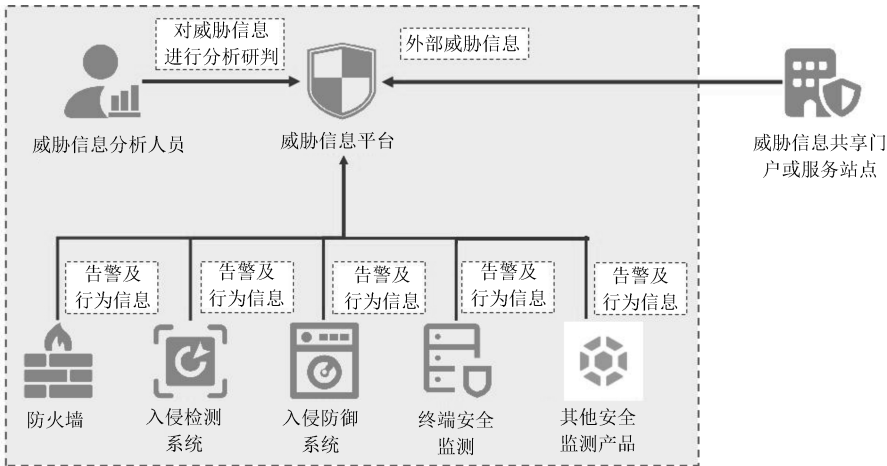


图 1 威胁信息汇聚与分析场景示意图

b) 威胁信息的共享与分发。威胁信息平台将经过分析研判的威胁信息与各级威胁信息平台共享,将相应的威胁信息通过接口分发给防火墙、入侵检测系统、入侵防御系统、终端安全监测等产品,或共享到威胁信息共享门户或服务站点。图 2 给出了一个两级威胁信息平台分发与共享威胁信息的示意图。

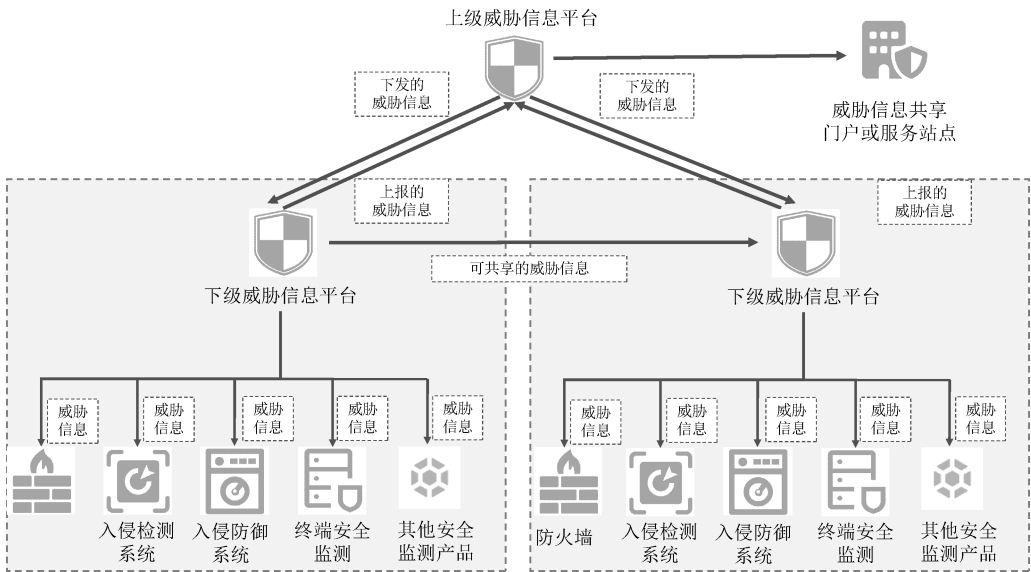


图 2 威胁信息共享与分发场景示意图

5.2 描述模型

给出了在互联互通场景下一种通用的网络安全威胁信息描述模型(以下简称“威胁信息描述模型”),包括对象、方法、事件和辅助 4 个描述域,以及 16 个网络安全威胁信息域组件(以下简称“组件”)和 1 个关系组件。

- a) 4 个描述域。
 - 1) 对象域:描述网络安全威胁主体、目标,包括“威胁主体”和“威胁目标”2 个组件。
 - 2) 方法域:描述网络安全威胁主体所使用的“攻击模式”“基础设施”“工具”“漏洞”“恶意软

- 件”“恶意软件分析结果”方法类组件,以及威胁目标所使用的“应对措施”组件。
- 3) 事件域:在不同的层面描述网络安全威胁相关的事件,包括“可观测数据”“攻击指标”“攻击活动”和“攻击活动集”4个组件。
- 4) 辅助域:用于研判网络安全威胁信息,并进行提供额外帮助决策的信息,包括“地理位置”“报告”和“观点”3个组件。
- b) 16个组件:描述威胁信息的基本组成单元,定义了“威胁主体”“威胁目标”“攻击模式”“基础设施”“工具”“漏洞”“恶意软件”“恶意软件分析结果”“应对措施”“可观测数据”“攻击指标”“攻击活动”“攻击活动集”“地理位置”“报告”和“观点”16个组件。
- c) 1个关系组件:描述不同组件之间存在的关联关系。

威胁信息描述模型描述不同域中组件及其主要的关联关系,见图3。

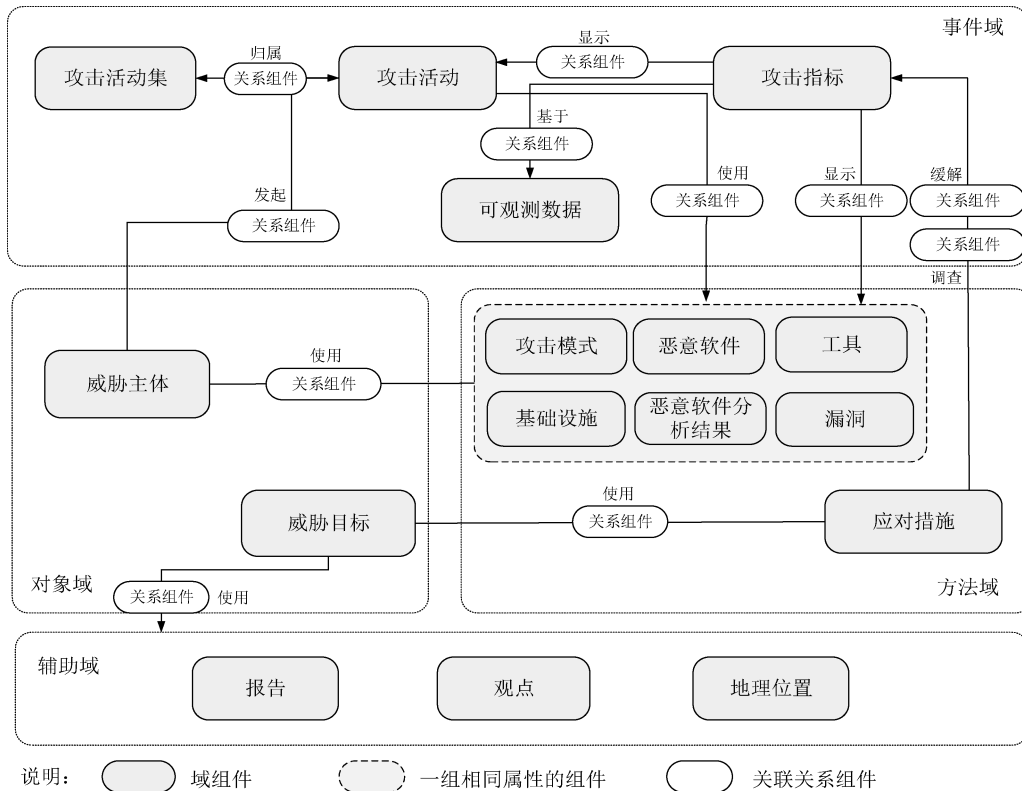


图3 威胁信息描述模型

“威胁主体”是“攻击活动”和“攻击活动集”中发起活动的主体,“威胁主体”使用相关方法(“攻击模式”“恶意软件”“漏洞”“工具”“基础设施”等攻击技术和战术)达到攻击意图。“攻击活动”和“攻击活动集”是依据对应指标(“攻击指标”)检测出的网络攻击。“攻击指标”是指在特定的网络环境中,用来识别显示“攻击活动”的综合性指标,它可能是多个“可观测数据”的组合。“可观测数据”是指与主机或网络相关的有状态的属性或可测量事件,是威胁信息描述模型中最基础的组件(见图3)。

“威胁目标”使用一定“应对措施”开展调查、缓解攻击活动,“应对措施”观测“攻击指标”,以评估措施的有效性。“威胁目标”在获得事件域信息的基础上,综合考虑不同来源和“地理位置”“报告”“观点”等信息进行研判和决策(见图3)。

6 组件的结构及公共属性

6.1 组件的结构

组件一般包括属性信息和关系信息,如图 4 所示。属性信息包括必选属性和可选属性,关系信息为可选信息。

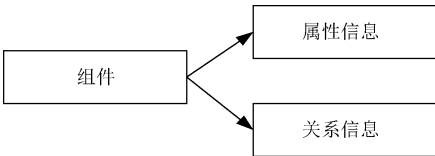


图 4 不包括子组件的组件信息构成示意图

有时组件可包括子组件(如“可观测数据”)。组件包括子组件时,子组件包括若干描述子组件的属性信息,组件包括该组件与其他组件之间的关系信息,见图 5。



图 5 包括子组件的组件信息构成示意图

关系信息使用关系组件来描述,关系组件只包括属性信息,见图 6。



图 6 关系组件的组件信息构成示意图

各个威胁信息组件都是可选的,它既可独立使用,也可任意方式组合。在不同的应用场景下,可只使用一个或几个相关的组件,而不必使用全部的组件。

附录 A 定义了字段描述,组件中使用的模式语言规则应符合附录 B 的规定,可观测数据子组件应符合附录 C 的规定,属性信息词汇应符合附录 D 的规定,威胁信息解析方式示例见附录 E,16 个网络安全威胁信息组件使用 JSON 表示的示例见附录 F,组件之间的关联关系见附录 G,部分场景下威胁信息 JSON 表示的示例见附录 H,表达式计算示例见附录 I。

6.2 公共属性

公共属性是多个组件以及关系组件都包括的具有相同含义的属性。公共属性在组件属性表中的“必选公共属性”和“可选公共属性”栏体现。对于需进一步说明的公共属性应重复列入组件属性表。

示例：“type”为公共属性,在“威胁主体”组件中对该属性进一步说明为必选项,取值为“threat-actor”。

公共属性的名称、类型和描述应符合表 1 的规定。

表 1 公共属性

序号	信息项	字段名称	字段类型	描述
1	类型	type	string	描述该组件或子组件的类型,取值为本文件定义的组件或子组件名称
2	版本	spec_version	string	描述该组件的版本,取值为“2.0”,表示本文件定义的格式
3	组件标识号	id	identifier	该组件的唯一标识号,符合 GB/T 17969.8 的规定
4	组件创建者标识号	created_by_ref	identifier	该组件创建者的标识号,符合 GB/T 17969.8 的规定
5	创建时间	created	timestamp	该组件的创建时间
6	修改时间	modified	timestamp	该组件最近一次被修改的时间
7	撤销标志	revoked	boolean	该组件是否已被撤销。true 表示已被撤销,false 表示未被撤销。默认为 false
8	标签	labels	list of type string	该组件的标签信息,是用于描述该组件特性的关键词,用户可自定义
9	可信度	confidence	integer	创建者对于该组件设置的可信度级别,取值为 0~100,数值越大表示可信度越高
10	语言	lang	string	该组件使用的语言,符合 IETF RFC 5646 的规定。如果组件中不包含该属性,则默认的语言为 en(英语)
11	外部信息引用	external_references	list of type external-reference	对外部信息的引用列表,可能是一个或多个 URL、描述信息、外部漏洞库漏洞号等
12	共享范围	object_marking_refs	string	该组件共享范围,取值符合 D.8 的规定
13	数据修改标志	defanged	boolean	组件中包含的数据是否被修改。true 表示被修改,false 表示未被修改。默认值为 false
14	扩展信息	extensions	dictionary	组件的扩展信息,可新增组件,也可新增已有组件的属性信息。以字典形式呈现。新增组件时,字典主键为新增组件的 id;新增属性时,字典主键为被扩展属性的组件的 id

7 组件

7.1 对象域组件

7.1.1 威胁主体

7.1.1.1 属性信息

威胁主体组件用于描述实施网络安全威胁行为的主体,及其可能的意图和历史行为,包括攻击者角色、攻击者经验、攻击目的、攻击资源级别等属性。威胁主体组件的属性应符合表 2 的规定。

表 2 威胁主体属性

必选公共属性					
type, spec_version, id, created, modified					
可选公共属性					
created_by_ref, revoked, labels, confidence, lang, external_references, object_marking_refs, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	组件类型	type	string	类型	是。取 值 为 “threat-actor”
2	名称	name	string	描述“威胁主体”的名称	是
3	详细描述	description	string	描述“威胁主体”的细节和背景,包括但不限于“威胁主体”的目的和主要特征等信息	是
4	威胁主体类型	threat_actor_types	list of type vocabulary	描述“威胁主体”的类型,取值符合 D.3	是
5	别名	aliases	list of type string	描述“威胁主体”的别名	否
6	首次观测时间	first_seen	timestamp	描述“威胁主体”首次被观测到的时间	否
7	末次观测时间	last_seen	timestamp	描述“威胁主体”最后一次被观测到的时间,如果给出 first_seen 值,那么 last_seen 的取值大于或等于 first_seen	否
8	攻击者角色	roles	list of type vocabulary	描述“威胁主体”对应的攻击者角色,取值符合 D.4 的规定	否
9	攻击目的	goals	list of type string	描述“威胁主体”的攻击目的	否
10	攻击经验	sophistication	vocabulary	描述“威胁主体”实施攻击所展现的攻击经验,取值符合 D.10 的规定	否
11	攻击资源级别	resource_level	vocabulary	描述“威胁主体”的攻击资源级别,取值符合 D.5 的规定	否

表 2 威胁主体属性（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
12	主要攻击动机	primary _ motiva- tion	vocabulary	描述“威胁主体”的主要攻击动机,取值符合 D.11 的规定	否
13	次要攻击动机	secondary _ moti- vations	list of type vocab- ulary	描述“威胁主体”的次要攻击动机,取值符合 D.11 的规定	否
14	个人攻击动机	personal _ motiva- tions	list of type vocab- ulary	描述“威胁主体”的个人攻击动机,取值符合 D.11 的规定	否

7.1.1.2 关系信息

威胁主体组件与威胁目标、攻击模式、基础设施、工具、漏洞、恶意软件、可观测数据、攻击指标、攻击活动、地理位置等组件存在关系。

7.1.2 威胁目标

7.1.2.1 属性信息

威胁目标组件用于描述网络安全威胁针对的目标主体。威胁目标组件的属性应符合表 3 的规定。

表 3 威胁目标属性

必选公共属性					
type,spec_version, id, created, modified					
可选公共属性					
created_by_ref, revoked, labels, confidence, lang, external_references, object_marking_refs, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取 值 为 “threat-target”
2	威胁目标名称	name	string	描述“威胁目标”的名称	是
3	详细描述	description	string	描述“威胁目标”的细节和背景,包括但不限于“威胁目标”的主要特征等信息	否
4	别名	aliases	list of type string	描述“威胁目标”的别名	否
5	首次观测时间	first_seen	timestamp	描述“威胁目标”首次被观测到的时间	否
6	末次观测时间	last_seen	timestamp	描述“威胁目标”最后一次被观测到的时间;如果给出 first_seen 值,那么 last_seen 的取值大于或等于 first_seen	否

表 3 威胁目标属性（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
7	所属行业信息	sectors	string	描述“威胁目标”所属的行业信息，取值符合 GB/T 4754 中分类	否
8	角色信息	roles	list of type string	描述“威胁目标”所担任的角色信息	否
9	身份类别	identity_class	vocabulary	描述“威胁目标”所对应的身份类别，取值符合 D.18 的规定	否
10	联系方式	contact_information	string	描述“威胁目标”的联系方式信息	否

7.1.2.2 关系信息

威胁目标组件与威胁主体、漏洞、基础设施、地理位置、攻击模式、攻击活动、恶意软件和工具等组件存在关系。

7.2 方法域组件

7.2.1 攻击模式

7.2.1.1 属性信息

攻击模式描述了攻击者试图攻击威胁目标的方式。攻击模式用于帮助对攻击进行分类，将特定的攻击概括为它们遵循的模式，并提供有关如何执行攻击的详细信息。攻击模式包括攻击模式的名称、描述、别名以及其所对应的攻击链阶段等属性。攻击模式组件各属性应符合表 4 的规定。

表 4 攻击模式属性

必选公共属性					
type, spec_version, id, created, modified					
可选公共属性					
created_by_ref, revoked, labels, confidence, lang, external_references, object_marking_refs, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“attack-pattern”
2	外部参考信息	external_references	list of type external-reference	描述“攻击模式”的外部参考信息。此属性可用于提供一个或多个攻击模式标识符，例如：CAPEC、ATT&CK 的技术分类等	否
3	名称	name	string	描述“攻击模式”的名称	是

表 4 攻击模式属性（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
4	详细描述	description	string	描述“攻击模式”的详细内容,包括但不限于“攻击模式”的上下文、主要特征等信息	是
5	别名	aliases	list of type string	描述“攻击模式”的别名	否
6	攻击阶段	cyber_kill_chain_phases	list of type cyber_kill-chain-phase	描述“攻击模式”对应攻击链的一个或多个阶段,当 kill_chain_name 取值为 lockheed-martin-cyber-kil-chain 时,phase_name 取值符合 D.9 的规定	否

7.2.1.2 关系信息

攻击模式组件与威胁主体、威胁目标、基础设施、工具、漏洞、恶意软件、应对措施、可观测数据、攻击指标、攻击活动、地理位置等组件存在关系。

7.2.2 基础设施

7.2.2.1 属性信息

基础设施组件描述用以支持某些目的(例如:用于攻击的命令与控制服务器、用于防御的设备或服务、作为被攻击目标的数据库服务器等)的系统、软件服务或相关物理/虚拟资源的信息。该组件包括基础设施类型、基础设施别名、基础设施所在的攻击链等属性。基础设施组件的属性应符合表 5 的规定。例如:可使用基础设施组件和 IP 地址子组件,来描述某个基础设施所关联的 IP 地址。

表 5 基础设施属性

必选公共属性					
type, spec_version, id, created, modified					
可选公共属性					
created_by_ref, revoked, labels, confidence, lang, external_references, object_marking_refs, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“infrastructure”
2	名称	name	string	描述“基础设施”的名称	是
3	详细描述	description	string	描述“基础设施”的详细内容,包括但不限于“基础设施”的上下文、主要特征等信息。涉及资产的相关描述符合 GB/T 44886.2 的规定	否

表 5 基础设施属性（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
4	基础设施的类型	infrastructure_types	list of type vocabulary	描述“基础设施”的类型，取值符合 D.12 的规定	否
5	别名	aliases	list of type string	描述“基础设施”的别名	否
6	攻击阶段	cyber_kill_chain_phases	list of type cyber_kill-chain-phase	描述“基础设施”对应攻击链的一个或多个阶段。当 kill_chain_name 取值为 lockheed-martin-cyber-kill-chain 时，phase_name 取值符合 D.9 的规定	否
7	首次观测时间	first_seen	timestamp	描述“基础设施”首次被观测到的时间	否
8	末次观测时间	last_seen	timestamp	描述“基础设施”最后一次被观测到的时间，如果给出了 first_seen 值，那么 last_seen 的取值大于或等于 first_seen	否

7.2.2.2 关系信息

基础设施组件与威胁主体、威胁目标、攻击模式、基础设施、工具、漏洞、恶意软件、可观测数据、攻击指标、攻击活动、攻击活动集、地理位置等组件存在关系。

7.2.3 工具

7.2.3.1 属性信息

工具组件是通常在系统中使用的软件，并且对高级用户、系统管理员、网络管理员甚至普通用户具有合法用途。工具组件也可被威胁主体用来进行攻击。它包括工具类型、工具别名、检测到的行为所处攻击链阶段、工具版本等属性。工具组件的属性应符合表 6 的规定。

表 6 工具属性

必选公共属性					
type, spec_version, id, created, modified					
可选公共属性					
created_by_ref, revoked, labels, confidence, lang, external_references, object_marking_refs, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“tool”
2	名称	name	string	描述“工具”的名称	是
3	工具特征	tool_features	string	描述“工具”的特征	否

表 6 工具属性（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
4	详细描述	description	string	对“工具”的详细描述,包括但不限于“工具”的上下文等信息	是
5	工具类型	tool_types	list of type vocabulary	工具类型,取值符合 D.6	否
6	别名	aliases	list of string	描述“工具”的别名	否
7	攻击链阶段	cyber_kill_chain_phases	list of type cyber_kill-chain-phase	描述“工具”对应攻击链的一个或多个阶段。当 kill_chain_name 取值为 lockheed-martin-cyber-kil-chain 时,phase_name 取值符合 D.9 的规定	否
8	版本	tool_version	string	描述“工具”的版本	否

7.2.3.2 关系信息

工具组件与威胁主体、攻击模式、基础设施、漏洞、恶意软件、应对措施、攻击指标、攻击活动、攻击活动集、地理位置等组件存在关系。

7.2.4 漏洞

7.2.4.1 属性信息

漏洞组件是指在软件和某些硬件组件(例如:固件)中发现的计算逻辑(例如:代码)中的弱点或缺陷,威胁主体可直接利用这些弱点或缺陷对系统的机密性、完整性或可用性产生负面影响。它包括外部参考信息、名称、描述等属性。漏洞组件的属性应符合表 7 的规定。

表 7 漏洞属性

必选公共属性					
type,spec_version, id, created, modified					
可选公共属性					
created_by_ref, revoked, labels, confidence, lang, external_references, object_marking_refs, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“vulnerability”

表 7 漏洞属性（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
2	外部参考信息	external_references	list of type external-reference	描述“漏洞”的外部参考信息，例如：CNVD(China National Vulnerability Database,国家信息安全漏洞共享平台)、CNNVD (China National Vulnerability Database of Information Security,国家信息安全漏洞库)、NVDB(National Vulnerability DataBase,网络安全威胁和漏洞信息共享平台)、CVE(Common Vulnerabilities & Exposures,通用漏洞披露)等	否
3	名称	name	string	描述“漏洞”的名称	是
4	漏洞编号	vul_num	string	描述“漏洞”的编号。当给出编号时，在description中给出漏洞库名称	否
5	详细描述	description	string	对“漏洞”的详细描述，包括但不限于“漏洞”的上下文、主要特征等信息。描述格式符合 GB/T 28458 的规定	是

7.2.4.2 关系信息

漏洞组件与威胁主体、威胁目标、攻击模式、基础设施、工具、恶意软件、应对措施、可观测数据、攻击活动、攻击活动集等组件存在关系。

7.2.5 恶意软件

7.2.5.1 属性信息

恶意软件组件用于描述恶意代码信息，可能属于某个恶意软件家族。它通常是指非法侵入操作系统的程序，其目的是破坏目标的数据、应用程序或操作系统的机密性、完整性或可用性，或以其他方式干扰被攻击者。它包括恶意软件类型、恶意软件所处攻击链阶段、操作系统环境、运行架构、编写语言、能力等属性。恶意软件组件的属性应符合表 8 的规定。在描述某个恶意文件属于某个恶意软件家族时，通常使用恶意软件和可观测对象中“文件信息”来组合表示。

表 8 恶意软件属性

必选公共属性					
type, spec_version, id, created, modified					
可选公共属性					
created_by_ref, revoked, labels, confidence, lang, external_references, object_marking_refs, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“malware”

表 8 恶意软件属性 (续)

序号	信息项	字段名称	字段类型	字段描述	是否必填
2	名称	name	string	描述“恶意软件”的名称	是
3	恶意软件关联样本杂凑列表	sample_refs	list of type identifier	描述与“恶意软件”相关的可观测数据 id, 一般指向“文件信息”或“字节片段信息”子组件。子组件中包含了“恶意软件”关联的杂凑列表	否
4	流行度	popularity	string	“恶意软件”的流行程度	否
5	是否和 APT 相关	is_appt	boolean	“恶意软件”是否和 APT 攻击相关。是为 true, 否则为 false	否
6	详细描述	description	string	对“恶意软件”的详细描述, 包括但不限于“恶意软件”的上下文、主要特征等信息	是
7	恶意软件类型	malware_types	list of type vocabulary	恶意软件类型, 取值符合 D.13 的规定	否
8	是否为恶意软件家族	is_family	boolean	描述“恶意软件”是否为恶意软件家族, 是为 true, 否则为 false。如果取值为 true, 则需在 description 中给出所属恶意软件家族名称	是
9	别名	aliases	list of type string	描述“恶意软件”的别名	否
10	攻击链阶段	cyber_kill_chain_phases	list of type cyber_kill_chain_phase	描述“恶意软件”对应攻击链的一个或多个阶段。当 kill_chain_name 取值为 lockheed-martin-cyber-kill-chain 时, phase_name 取值符合 D.9 的规定	否
11	首次被观测到的时间	first_seen	timestamp	描述“恶意软件”首次被观测到的时间	否
12	末次被观测到的时间	last_seen	timestamp	描述“恶意软件”最后一次被观测到的时间, 如果给出 first_seen 值, 那么 last_seen 的取值大于或等于 first_seen	否
13	操作系统信息	operating_system_refs	list of type identifier	描述可支持“恶意软件”在其上运行的操作系统信息	否
14	处理器架构	architecture_execution_envs	list of type vocabulary	描述“恶意软件”在其运行环境中涉及的处理器架构信息, 取值符合 D.15 的规定	否
15	编程语言信息	implementation_languages	list of type vocabulary	描述用于实现“恶意软件”的编程语言信息, 取值符合 D.16 的规定	否
16	能力信息	capabilities	list of type vocabulary	描述“恶意软件”具有的能力信息, 取值符合 D.17 的规定	否

7.2.5.2 关系信息

恶意软件组件与威胁主体、威胁目标、攻击模式、基础设施、工具、漏洞、恶意软件分析结果、应对措施、可观测数据、攻击指标、攻击活动、攻击活动集、地理位置等组件存在关系。

7.2.6 恶意软件分析结果

7.2.6.1 属性信息

恶意软件分析结果组件用于描述恶意软件样本的动态或静态分析结果。该组件包括分析引擎或工具、分析引擎或工具版本号、虚拟机信息、操作系统信息、软件名称、配置信息、分析模块、样本提交时间、分析时间、分析名称、分析结论、关联样本等属性。恶意软件分析结果组件的属性应符合表 9 的规定。

表 9 恶意软件分析结果属性

必选公共属性					
type,spec_version, id, created, modified					
可选公共属性					
created_by_ref, revoked, labels, confidence, lang, external_references, object_marking_refs, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“malware-analysis”
2	分析引擎或工具名称	product	string	描述出具“恶意软件分析结果”的分析引擎或工具名称,如果无法指定工具名称,则取值“anonymized”	是
3	版本信息	version	string	描述出具“恶意软件分析结果”的分析引擎或工具的版本信息	否
4	虚拟机操作系统环境	host_vm_ref	identifier	描述用于对恶意软件进行动态分析的虚拟机操作系统环境,如果此值未与 operating_system_ref 属性一起给出,则表示动态分析可能是在实体机(即非虚拟化)上执行的。此字段取值为可观测数据“软件信息”子组件 id	否
5	操作系统环境	operating_system_ref	identifier	描述用于对恶意软件进行动态分析的操作系统环境,既可描述虚拟化操作系统,也可描述实机操作系统。此字段取值为可观测数据“软件信息”子组件 id	否
6	软件信息	installed_software_refs	list of type identifier	描述用于分析恶意软件而安装在操作系统上的软件信息。此字段取值为可观测数据“软件信息”子组件 id	否

表 9 恶意软件分析结果属性（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
7	配置信息	configuration_version	string	描述用于本次分析定义的产品配置参数的配置信息	否
8	模块信息	modules	list of type string	描述本次分析运行期间在工具中使用和配置的特定分析模块信息	否
9	版本信息	analysis_engine_version	string	描述用于执行分析的分析引擎或工具版本信息	否
10	分析工具版本信息	analysis_definition_version	string	描述用于执行分析的分析工具版本信息	否
11	首次提交扫描或分析的时间	submitted	timestamp	描述恶意软件首次提交扫描或分析的时间。该值将保持不变,而扫描日期可能会发生变化	否
12	开始分析恶意软件的时间	analysis_started	timestamp	描述开始分析恶意软件的时间	否
13	恶意软件分析结束的时间	analysis_ended	timestamp	描述恶意软件分析结束的时间	否
14	分类结果或名称信息	result_name	string	描述分析引擎或工具为恶意软件定义的分类结果或名称信息	否
15	分类结果信息	result	vocabulary	描述“恶意软件分析结果”的分类结果信息,取值符合 D.14 的规定	否
16	捕获到的可观测数据 id	analysis_sco_refs	list of type identifier	描述“恶意软件分析结果”在分析中捕获到的可观测数据中相应子组件的 id	否
17	分析的可观测数据 id	sample_ref	list of type identifier	描述“恶意软件分析结果”所分析的可观测数据中相应子组件的 id	否

7.2.6.2 关系信息

恶意软件分析结果组件与恶意软件等组件存在关系。

7.2.7 应对措施

7.2.7.1 属性信息

应对措施组件用于描述应对正在进行或已发生的攻击而采取的行动。该组件包括所用措施的描述、自动化响应动作等属性。应对措施组件的属性应符合表 10 的规定。

表 10 应对措施属性

必选公共属性					
type, spec_version, id, created, modified					
可选公共属性					
created_by_ref, revoked, labels, confidence, lang, external_references, object_marking_refs, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取 值 为 “course-of-action”
2	名称	name	string	描述“应对措施”的名称	是
3	详细描述	description	string	对“应对措施”的详细描述,包括但不限于上下文、主要特征等信息	否
4	响应动作	action	string	描述“应对措施”的自动化响应动作。例如:阻断、忽略、告警等动作	否
5	外部参考信息	external _ refer-ences	list of type external-reference	描述“应对措施”的外部参考信息。此属性可用于提供一个或多个应对措施标识符,例如:ATT&CK 的缓解措施分类等	否

7.2.7.2 关系信息

应对措施组件与攻击模式、工具、漏洞、恶意软件、攻击指标等组件存在关系。

7.3 事件域组件

7.3.1 可观测数据

7.3.1.1 属性信息

可观测数据组件是威胁信息最基础的组件,用于描述在某个时间点或时间段内观测到的网络或系统中的一个或多个数据。定义了 16 类可观测数据作为子组件,各子组件属性应符合附录 C 的规定。组件属性应符合表 11 的规定。组织可根据需求增加可观测数据子组件,也可增加子组件中的属性。

可观测数据中的信息可来自告警信息和行为信息,内容见 GB/T 44886.3 和 GB/T 44886.5。

表 11 可观测数据属性

必选公共属性					
type,spec_version, id, created, modified					
可选公共属性					
created_by_ref, revoked, labels, confidence, lang, external_references, object_marking_refs, extensions					

表 11 可观测数据属性（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取 值 为 “observed-data”
2	首次观测时间	first_observed	timestamp	描述“可观测数据”的首次观测时间	是
3	最近一次观测时间	last_observed	timestamp	描述“可观测数据”的最近一次观测时间,取值大于 first_observed 属性值	是
4	观测到的总次数	number_observed	integer	描述“可观测数据”的可观测数据集合被观测到的总次数	是
5	引用的可观测数据标识符	object_refs	list of type identifier	描述“可观测数据”的引用的可观测对象标识符,每一个引用的可观测数据的属性符合附录 C 的规定	否

7.3.1.2 关系信息

可观测数据组件与威胁主体、攻击模式、基础设施、漏洞、恶意软件、攻击指标、攻击活动、地理位置等组件存在关系。

7.3.2 攻击指标

7.3.2.1 属性信息

攻击指标组件用于检测可疑或恶意的网络活动。该组件包括模式语言(见附录 B)、检测到的行为所处攻击链阶段、有效时间段等属性。攻击指标组件的属性应符合表 12 的规定。

表 12 攻击指标属性

必选公共属性					
type, spec_version, id, created, modified					
可选公共属性					
created_by_ref, revoked, labels, confidence, lang, external_references, object_marking_refs					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取 值 为 “indicator”
2	名称	name	string	描述“攻击指标”的名称	否
3	详细描述	description	string	对“攻击指标”的详细描述,包括但不限于“攻击指标”的上下文、潜在的用途、关键的特点等信息	否

表 12 攻击指标属性（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
4	所属子类型	indicator_types	list of type vocabulary	描述“攻击指标”所属子类型的列表,取值符合 D.1 的规定	否
5	模式语言	pattern	string	描述“攻击指标”的模式语言,符合附录 B 的规定	是
6	模式语言的类型	pattern_type	vocabulary	描述“攻击指标”模式语言的类型,取值符合 D.2 的规定	是
7	模式语言的版本号	pattern_version	string	描述“攻击指标”模式语言的版本号	否
8	有效起始时间	valid_from	timestamp	描述“攻击指标”的有效起始时间	是
9	有效结束时间	valid_until	timestamp	描述“攻击指标”的有效结束时间,取值大于 valid_from 属性值,如未赋值,则表示“攻击指标”的有效期为无限长	否
10	攻击链阶段	cyber_kill_chain_phases	list of type cyber-kill-chain-phase	描述“攻击指标”对应攻击链的一个或多个阶段。当 kill_chain_name 取值为 lockheed-martin-cyber-kill-chain 时, phase_name 取值符合 D.9 的规定	否

7.3.2.2 关系信息

攻击指标组件与威胁主体、攻击模式、基础设施、工具、恶意软件、应对措施、可观测数据、攻击活动、攻击活动集等组件存在关系。

7.3.3 攻击活动

7.3.3.1 属性信息

攻击活动组件用于描述一系列针对特定目标的恶意活动或攻击信息。该组件包括活跃时间、攻击目的等属性。攻击活动组件的属性应符合表 13 的规定。

表 13 攻击活动属性

必选公共属性					
type, spec_version, id, created, modified					
可选公共属性					
created_by_ref, revoked, labels, confidence, lang, external_references, object_marking_refs, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“campaign”

表 13 攻击活动属性（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
2	名称	name	string	描述“攻击活动”的名称	是
3	详细描述	description	string	对“攻击活动”的详细描述,包括但不限于“攻击活动”的上下文、目的、主要特征等信息	否
4	别名	aliases	list of type string	描述“攻击活动”的别名	否
5	首次被观测到的时间	first_seen	timestamp	描述“攻击活动”首次被观测到的时间	否
6	末次被观测到的时间	last_seen	timestamp	描述“攻击活动”最后一次被观测到的时间,如果给出了 first_seen 时间值,那么 last_seen 的取值大于或等于 first_seen	否
7	主要目标	objective	string	描述“攻击活动”的主要目标、目的或预期结果	否
8	风险等级	risk	string	描述“攻击活动”的风险等级。取值符合 D.19 的规定	是

7.3.3.2 关系信息

攻击指标组件与威胁主体、威胁目标、攻击模式、基础设施、工具、漏洞、恶意软件、可观测数据、攻击指标、攻击活动集、地理位置等组件存在关系。

7.3.4 攻击活动集

7.3.4.1 属性信息

攻击活动集组件用于描述一个或多个攻击活动,一般是由同一个威胁主体发起。如无法明确威胁主体,也可将具有相似特征的活动归入一个攻击活动集。该组件包括攻击首次发现时间、末次发现时间、攻击目的、使用的攻击资源级别以及其主要攻击动机和次要攻击动机等属性。攻击活动集组件各属性应符合表 14 的规定。

表 14 攻击活动集属性

必选公共属性					
type, spec_version, id, created, modified					
可选公共属性					
created_by_ref, revoked, labels, confidence, lang, external_references, object_marking_refs, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“intrusion-set”

表 14 攻击活动集属性（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
2	名称	name	string	描述“攻击活动集”的名称	是
3	详细描述	description	string	描述“攻击活动集”的详细内容,包括但不限于“攻击活动集”的上下文、主要特征等信息	否
4	别名	aliases	list of type string	描述“攻击活动集”的别名	否
5	首次发现时间	first_seen	timestamp	描述“攻击活动集”的首次发现时间。如果接收到比首次发现时间更早的新的观测结果,则更新该属性	否
6	末次发现时间	last_seen	timestamp	描述“攻击活动集”的最后发现时间。如果接收到比最后发现时间更晚的信息,则应更新该属性。如果 last_seen 和 first_seen 都已定义,则 last_seen 大于或等于 first_seen	否
7	攻击目的	goals	list of type string	描述“攻击活动集”背后的攻击者的攻击目的	否
8	攻击资源级别	resource_level	vocabulary	描述“攻击活动集”使用的攻击资源级别,取值符合 D.5 的规定	否
9	主要攻击动机	primary _ motivation	vocabulary	描述“攻击活动集”的主要攻击动机,取值符合 D.11 的规定	否
10	次要攻击动机	secondary _ motivations	list of type vocabulary	描述“攻击活动集”的次要攻击动机,取值符合 D.11 的规定	否

7.3.4.2 关系信息

攻击活动集组件与威胁主体、攻击模式、基础设施、工具、漏洞、恶意软件、攻击指标、攻击活动、地理位置等组件存在关系。

7.4 辅助域组件

7.4.1 地理位置

7.4.1.1 属性信息

地理位置组件主要用于为其他对象提供上下文背景信息。该组件包括地理位置的经度、纬度、所属地区、所属国家、所属城市、所属街道、邮政编码以及定位的精确度等属性。涉及资产地理位置的信息也可从 GB/T 44886.2 中获取。地理位置组件的属性应符合表 15 的规定。

表 15 地理位置属性

必选公共属性					
type, spec_version, id, created, modified					
可选公共属性					
created_by_ref, revoked, labels, confidence, lang, external_references, object_marking_refs, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取 值 为 “location”
2	名称	name	string	描述“地理位置”的名称	否。名称、经度、纬度、地区字段至少一项必选
3	详细描述	description	string	描述“地理位置”的详细内容,包括但不限于“地理位置”的上下文、主要特征等信息	否
4	纬度	latitude	float	描述“地理位置”的纬度,此属性的值在 $-90.0 \sim 90.0$ 之间(包括 -90.0 和 90.0)。如果给出 longitude 值,则给出此属性值	否。名称、经度、纬度、地区字段至少一项必选
5	经度	longitude	float	描述“地理位置”的经度,此属性的值在 $-180.0 \sim 180.0$ 之间(包括 -180.0 和 180.0)。如果给出 latitude 值,则给出此属性值	否。名称、经度、纬度、地区字段至少一项必选
6	精确度	precision	float	描述“地理位置”通过其经纬度定位的精确度,以米为单位。如果给出此属性值,则给出 latitude 和 longitude 属性值	否
7	地区	region	vocabulary	描述“地理位置”所属的地区,取值符合 D.20 的规定	否。名称、经度、纬度、地区字段至少一项必选
8	国家	country	string	描述“地理位置”所属的国家	是
9	行政区域	administrative_area	string	描述“地理位置”所属的行政区域,例如:省份	否
10	城市	city	string	描述“地理位置”所属的城市	否
11	街道名称	street_address	string	描述“地理位置”所属的街道名称	否
12	邮政编码	postal_code	string	描述“地理位置”所对应的邮政编码	否

7.4.1.2 关系信息

地理位置组件与攻击模式、攻击活动、基础设施、恶意软件、威胁主体、工具等组件存在关系。

7.4.2 报告

7.4.2.1 属性信息

报告组件是集中在一个或多个主题上的威胁信息的集合,例如:对威胁组织、恶意软件或攻击技术的描述,包括上下文和相关细节。它们用于将相关威胁信息组合在一起,作为一个综合性的网络威胁信息报告呈现。该组件包括报告的名称、描述、报告类型、报告发布时间、关联对象等属性。报告组件的属性应符合表 16 的规定。

表 16 报告属性

必选公共属性					
type,spec_version, id, created, modified					
可选公共属性					
created_by_ref, revoked, labels, confidence, lang, external_references, object_marking_refs,extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取 值 为 “report”
2	名称	name	string	描述“报告”的名称	是
3	发布者	pub_name	string	描述“报告”的发布者名称	否
4	详细描述	description	string	描述“报告”的详细内容,包括但不限于“报告”的上下文、主要特征等信息	否
5	报告类型	report_types	list of type string	描述“报告”的报告类型,报告类型为其他 15 个组件中一个或多个组件的类型	否
6	发布时间	published	timestamp	描述“报告”被创建者发布时间	是
7	关 联 的 组 件 id 信息	object_refs	list of type identifier	描述“报告”关联的组件 id 信息	是

7.4.2.2 关系信息

报告组件与其他组件无明确关系。

7.4.3 观点

7.4.3.1 属性信息

观点组件用于描述对不同实体所发布组件中信息正确性的评估。该组件包括观点、观点的解释、作者、关联对象等属性。观点组件的属性应符合表 17 的规定。

表 17 观点属性

必选公共属性					
type,spec_version, id, created, modified					
可选公共属性					
created_by_ref, revoked, labels, confidence, lang, external_references, object_marking_refs, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取 值 为 “opinion”
2	解释信息	explanation	string	“观点”的解释信息,即对生产者为何持有此意见的解释	否
3	姓名信息	authors	list of type string	描述“观点”的作者姓名信息或组织名称	否
4	意见内容	opinion	enum	描述“观点”的意见内容,取值符合 D.7 的规定	是
5	关联对象	object_refs	list of type identifier	描述“观点”的关联对象	是

7.4.3.2 关系信息

观点组件与其他组件无明确关系。

8 关系组件

关系组件用于描述组成威胁信息的组件之间的各种关联关系。主要属性包括关系类型、描述、源组件标识和目标组件标识等属性。关系组件的属性应符合表 18 的规定。

表 18 关系组件属性

必选公共属性					
type, spec_version, id, created, modified					
可选公共属性					
created_by_ref, revoked, labels, confidence, lang, external_references, object_marking_refs, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取 值 为 “relationship”
2	关系类型	relationship_type	string	描述关系类型,取值见附录 G 中的关系类型	是

表 18 关系组件属性（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
3	描述	description	string	对关系的更多描述,包括用途、主要特征等	否
4	源组件标识	source_ref	identifier	源组件的标识	是
5	目标组件标识	target_ref	identifier	目标组件的标识	是
6	起始时间	start_time	timestamp	关系存在的起始时间	否
7	终止时间	stop_time	timestamp	关系终止时间。如给出了 start_time,则本属性值晚于起始时间。如未给本属性赋值,则终止时间为未知、未披露或未定义	否

附 录 A
(规范性)
字段类型描述

字段类型应遵从 JSON 语言约定。所使用的字段类型应符合表 A.1 的规定。

表 A.1 字段类型及描述

序号	字段类型	描述
1	boolean	布尔类型的值为 true 或 false,分别表示真或假
2	binary	二进制类型是一系列字节
3	hex	十六进制数据类型将八位字节数组(8 位字节)编码为十六进制形式。该字符串应由偶数个十六进制字符组成,这些字符包括数字 '0'~'9' 以及小写字母 'a'~'f'
4	integer	整数类型表示一个有符号整数。正整数省略加号 '+',负整数在前面加连字符减号 '-' 来表示
5	float	浮点类型表示双精度数。正浮点数省略加号 '+',负浮点数在前面加上连字符减号 '-' 来表示
6	string	字符串类型表示由 Unicode 编码字符集中的有效字符组成的有限长度字符串
7	timestamp	时间戳类型定义了日期和时间在本文件中的表示方式,使用 YYYY-MM-DDTHH:mm:ss[.s+]Z 格式表示。[.s+]表示亚秒,时间为 UTC 时间
8	enum	枚举类型是一组以字符串形式表示的硬编码词汇列表(见附录 D)
9	dictionary	字典类型为任意一组键/值对。键在每个字典中唯一,为 ASCII 格式,取值为字符 a-z (小写 ASCII)、A-Z(大写 ASCII)、数字 0-9、连字符(-)和下划线(_)。键的长度不超过 250 个 ASCII 字符,并且应小写。 值应是有效的字段类型
10	hashes	杂凑类型是以一组特殊的键/值对表示一个或多个杂凑值。每个杂凑算法的名称应指定为字典中的一个键,并且应标识用于生成相应值的杂凑算法的名字。 字典键在每个杂凑属性中应唯一,应为 ASCII 码格式,为字符 a-z(小写 ASCII)、A-Z (大写 ASCII)、数字 0-9、连字符(-)和下划线(_)。字典键的长度应至少为 3 个 ASCII 字符,长度不超过 250 个 ASCII 字符
11	List	列表类型定义了一系列值,这些值根据它们在列表中的显示方式进行排序。“list of type <type>”用于表示列表中的所有值都应符合指定的类型。不应使用空列表
12	cyber_kill-chain-phase	攻击链阶段描述了攻击者为实现其目标而可能采取的各个阶段。它包括 kill_chain_name 和 phase_name 两个字段,均为 string 字符类型,均为必填字段,值应全部小写,并应使用连字符作为单词分隔符

表 A.1 字段类型及描述（续）

序号	字段类型	描述
13	external-reference	外部引用类型用于描述指向其他组件信息的指针。包括： source_name（必填），字段类型为 string，定义外部引用的源的名称（系统、注册表、组织等）； description（可选），字段类型为 string，描述信息； url（可选），字段类型为 string，指向外部资源的 URL 引用； hashes（可选），字段类型为 hashes，为 url 的内容指定杂凑字典； external_id（可选）字段类型为 string，外部引用内容的标识符
14	identifier	标识符类型唯一标识组件（含子组件）。格式为“组件类型-UUID”，其中组件类型是被标识或引用的组件的类型属性的值（所有类型名称都是小写字符串）

附录 B
(规范性)
模式语言的描述

B.1 概述

模式语言是一种语法,描述识别给定网络或端点内活动的恶意代码和威胁主体的攻击特征,通过比较表达式、观测表达式、组合表达式和模式表达式进行表述。其中,模式表达式是对比较表达式、观测表达式、组合表达式等多个表达式进行运算,得出威胁匹配判定结果。

B.2 模式语言术语

模式语言中使用的术语见表 B.1。

表 B.1 在模式语言中使用的术语

名称	定义	示例
空白字符	使用的空白符号,例如换行符、回车符、制表符和空格符等	N/A
观测数据	在特定时间点观测到的有关系统或网络的数据,例如,文件信息、运行的进程信息或在两个 IP 之间传输的网络流量	N/A
比较表达式	比较表达式是观测表达式的基本组成部分。它们由一个组件路径和一个由比较运算符连接的字段类型组成	user-account;value = 'Peter'
比较运算符	比较运算符在比较表达式中使用,用于将组件路径与一个字段类型或一组字段类型进行比较	MATCHES
对象路径	组件路径为可观测数据的某个属性及其值	ipv6-addr;value
观测表达式	观测表达式由一个或多个用布尔运算符连接的比较表达式组成,并用方括号括起来。 一个观测表达式可由两个通过观测运算符连接的观测表达式组成。观测表达式后面可有一个或多个限定符,进一步约束结果集。若限定符作用于所有与观测运算符连接的观测表达式,则应使用圆括号对该组观测表达式进行分组,限定符置于右圆括号之后	[ipv4-addr; value = '203.0.113.1' OR ipv4-addr;value = '203.0.113.2'] 或 ([ipv4-addr;value = '198.51.100.5'] FOLLOWEDBY [ipv4-addr;value = '198.51.100.10']) 或 ([ipv4-addr;value = '198.51.100.5'] AND [ipv4-addr; value = '198.51. 100.10']) WITHIN 300 SECONDS
布尔运算符	布尔运算符用于在观测表达式中对比较表达式进行布尔运算	user-account; value = 'Peter' OR user-account;value = 'Mary'
限定符	限定符对被认为是有效的、与前面的观测表达式匹配的观测提供了限制条件	[file; name = 'foo.dll'] START t' 2016-06-01T00:00:00Z' STOP t' 2016-07-01T00:00:00Z'

表 B.1 在模式语言中使用的术语（续）

名称	定义	示例
观测运算符	观测运算符将两个不同的观测表达式进行观测运算	[ipv4-addr; value = '198.51.100.5'] AND [ipv4-addr; value = '198.51.100.10']
模式表达式	模式表达式表示识别出的最终结果	[file; size = 25536]

B.3 可进行运算的字段类型

比较表达式中进行运算所支持的字段类型应符合表 B.2 的规定。

表 B.2 可进行运算的字段类型

序号	字段类型	可比较字段类型
1	boolean	boolean
2	binary	binary hex string
3	hex	binary hex string
4	integer	integer float
5	float	integer float
6	string	string binary hex
7	timestamp	timestamp

B.4 表达式

表达式包括比较表达式、观测表达式、组合表达式，以及模式表达式。

a) 比较表达式：使用比较运算符对组件的单个属性的值和常量进行比较。

示例 1：

表示与 IPv4 地址进行匹配的表达式：[ipv4-addr; value = '198.51.100.1/32']

b) 观测表达式：由一个或多个由布尔运算符连接并由方括号限定的比较表达式组成。观测表达式主要明确哪一组网络可观测数据能与条件匹配。观测表达式最少由一个比较表达式组成。

示例 2：

用一个观测表达式来匹配多个 IPv4 地址和一个 IPv6 地址：

[ipv4-addr:value = '198.51.100.1/32' OR ipv4-addr:value = '203.0.113.33/32' OR ipv6-addr:value = '2001:0db8:dead:beef:dead:beef:dead:0001/128']

观测表达式后面可能有一个或多个限定符,这些限定符可对匹配出的数据集提出限制条件。

示例 3:

使用限定符来说明应重复多次观测 IP 地址:

[ipv4-addr:value = '198.51.100.1/32' OR ipv4-addr:value = '203.0.113.33/32' OR ipv6-addr:value = '2001:0db8:dead:beef:dead:beef:dead:0001/128'] REPEATS 5 TIMES

- c) 组合表达式:通过观测运算符组合两个或多个表达式,生成能在多个可观测数据组件之间匹配的表达式。

示例 4:

使用观测运算符指定特定域名的观测应紧跟在 IP 地址的观测之后,同时使用不同的限定符来声明应在特定时间窗口内观测 IP 地址和域名:

([ipv4-addr:value = '198.51.100.1/32' OR ipv4-addr:value = '203.0.113.33/32' OR ipv6-addr:value = '2001:0db8:dead:beef:dead:beef:dead:0001/128'] FOLLOWEDBY [domain-name: value = 'example.com']) WITHIN 600 SECONDS

- d) 模式表达式:比较表达式和/或观测表达式、组件路径语法(例如:ipv4-addr:value)等的组合。模式表达式满足以下规定:

- 1) 模式表达式的计算结果应为 true 或 false;
- 2) 模式表达式编码应为 Unicode 字符串;
- 3) 在运算符前后可使用空格,包括空格符、换行符和回车符;
- 4) 将一行中的多个空格视为单个空格;
- 5) 若出现语法错误,则模式表达式结果应为 false。

B.5 比较表达式

B.5.1 常用计算形式

比较表达式是模式语言最基本的表达式,由组件路径和由比较运算符连接的字段类型组成,从左到右进行运算。

布尔运算符将两个比较表达式连接在一起。在表 B.3 中,a 或 b 要么是比较表达式,要么是由两个或多个比较表达式组成的复合表达式,这些比较表达式用布尔运算符连接,并用圆括号括起来。比较表达式常用计算形式应符合表 B.3 的规定。

表 B.3 比较表达式常用计算形式

布尔运算	描述	运算次序
a AND b	a 和 b 都是比较表达式或由两个或多个比较表达式组成,若是多个比较表达式则用布尔运算符连接,并用圆括号括起来。a 和 b 在相同的观测值上都为 true 时,判断结果为匹配成功	左到右
a OR b	a 和 b 都是比较表达式或由两个或多个比较表达式组成,若是多个比较表达式则用布尔运算符连接,并用圆括号括起来。a 或 b 在相同的观测值上都为 true 时,判断结果为匹配成功	左到右

B.5.2 比较运算符

表 B.4 给出了在比较表达式中使用的比较运算符,其中,a 是组件路径,b 是字段类型。如果所比较

的对象字段类型不可互相计算,则结果为 false,如果使用 $!=$ 运算符,则结果为 true。可比较的字段类型应符合表 B.2 的规定。

表 B.4 常用的比较运算符

序号	比较运算符	描述	示例
1	$a = b$	a 和 b 相等,其中 a 是组件路径,b 是与 a 指定的组件属性具有相同字段类型的值	file:name = 'foo.dll'
2	$a \neq b$	a 和 b 不相等,其中 a 是组件路径,b 是与 a 指定的组件属性具有相同字段类型的值	file:size $\neq$ 4112
3	$a > b$	a 在数值上或 ASCII 编码值大于 b,其中 a 是组件路径,b 是与 a 指定的组件属性具有相同字段类型的值	file:size > 256
4	$a < b$	a 在数值上或 ASCII 编码值小于 b,其中 a 是组件路径,b 是与 a 指定的组件属性具有相同字段类型的值	file:size < 1024
5	$a \leq b$	a 在数值上或 ASCII 编码值小于或等于 b,其中 a 是组件路径,b 是与 a 指定的组件属性具有相同字段类型的值	file:size $\leq$ 25145
6	$a \geq b$	a 在数值上或 ASCII 编码值大于或等于 b,其中 a 是组件路径,b 是与 a 指定的对象属性具有相同字段类型的值	file:size $\geq$ 33312
7	$a \text{ IN } (x,y,\dots)$	a 是组件路径,且值为 x、y…集合中枚举的值之一。集合中的值是相同字段类型的常量,且是 a 对应的组件属性的有效字段类型。如果 a 为集合中的值之一,则返回值为 true。如果 a 不等于集合中的任何值,则计算结果为 false	process:name IN ('proccy', 'proximus', 'badproc')
8	$a \text{ LIKE } b$	a 是组件路径,且与 b 中指定的模式匹配,其中“%”代表 0 个或多个字符,“_”是代表任意一个字符。字符串 b 在求值之前先进行 Unicode 编码	directory:path LIKE 'C:\\Windows\\%\\foo'
9	$a \text{ MATCHES } b$	a 是组件路径,且与 b 中指定的模式匹配,其中 b 是符合 PCRE(Perl Compatible Regular Expressions)正则表达式的字符串。如果属性类型是字符串类型,则 a 在比较之前先进行 Unicode 编码	directory:path MATCHES 'C:\\\\Windows\\w+ \$'
10	$a \text{ ISSUBSET } b$	当 a 被集合 b 包含时,计算结果为 true。a 是组件路径,其组件属性值为 ipv4-addr 或 ipv6-addr,b 是相应组件属性类型的有效字符串表示。在 a 和 b 计算结果为相同的单个 IP 地址或相同的 IP 子网的情况下,计算结果为 true	ipv4-addr:value ISSUBSET '198.51.100.0/24'
11	$a \text{ ISSUPERSET } b$	当 a 完全包含 b 指定的集合时,计算结果为 true。a 是引用 ipv4-addr 或 ipv6-addr 组件的组件路径。b 是相应组件类型的有效字符串表示形式。在 a 和 b 计算结果为相同的单个 IP 地址或相同的 IP 子网的情况下,计算结果为 true	ipv4-addr:value ISSUPERSET '198.51.100.0/24'
12	EXISTS a	a 是组件路径,表示在观测表达式中指定组件的一个属性。如存在,则计算结果为 true	EXISTS windows-registry-key:values

B.5.3 字符串比较

对于字符串比较,应将其转换为二进制进行比较。如果一个字符串比另一个字符串长,但在其他情况下相等,则较长的字符串大于较短的字符串。

B.5.4 二进制类型比较

当比较两个二进制的值时,应把值作为无符号八位字节进行比较。如果一个值比另一个值长,且在其他方面相等,则较长的值视为大于较短的值。

B.5.5 可观测数据组件的属性值比较

若可观测数据组件的属性格式的值是二进制或十六进制编码,比较前都默认转换为八位字节的格式。如果将一个二进制和一个字符串常量进行比较,则应将字符串转换为二进制进行比较;如不能转换,一般比较结果为 false;如果比较运算符为“! =”,则计算结果为 true。

B.6 观测表达式

B.6.1 观测表达式表示形式

观测表达式由通过布尔运算符连接的一个或多个比较表达式组成。由左方括号“[”,和右方括号“]”括起来的观测表达式为一个完整的表达式。在观测表达式的右方括号或右括号之后可有一个或多个观测表达式限定符。观测表达式之间由观测运算符连接。

单个观测表达式只可与单个可观测数据进行匹配运算。多个观测表达式可与多个可观测数据进行匹配运算。

例如:以下可观测数据与观测表达式不匹配,尽管这两个 IP 地址同属一个观测数据对象,但不存在在一个单独的网络流量组件同时引用这两个 IP 地址,因此不满足观测表达式中的条件。

观测表达式示例如下。

```
[ network-traffic:src_ref.value = '203.0.113.10' AND network-traffic:dst_ref.value = '198.51.100.58' ]
```

可观测数据示例如下。

```
{
  "type": "observed-data",
  "id": "observed-data-0960319a-3cab-4258-a143-4dbb25525bb1",
  "created": "2019-10-20T00:20:01.000000Z",
  "modified": "2019-10-20T00:51:01.000000Z",
  "first_observed": "2019-10-20T00:12:01.000000Z",
  "last_observed": "2019-10-20T00:30:02.000000Z",
  "number_observed": 1,
  "objects": {
    "0": {
      "type": "network-traffic",
      "src_ref": "1",
      "protocols": "tcp"
    },
  },
}
```

```

    "1": {
      "type": "ipv4-addr",
      "value": "203.0.113.10"
    },
    "2": {
      "type": "network-traffic",
      "dst_ref": "3"
    },
    "3": {
      "type": "ipv4-addr",
      "value": "198.51.100.58"
    }
  }
}

```

如果要匹配可观测数据与观测表达式,正确的可观测数据示例如下。

```

{
  "type": "observed-data",
  "id": "observed-data--0960319a-3cab-4258-a143-4dbb25525bb1",
  "created": "2019-10-20T00:20:01.000000Z",
  "modified": "2019-10-20T00:51:01.000000Z",
  "first_observed": "2019-10-20T00:12:01.000000Z",
  "last_observed": "2019-10-20T00:30:02.000000Z",
  "number_observed": 1,
  "objects": {
    "0": {
      "type": "network-traffic",
      "src_ref": "1",
      "dst_ref": "2",
      "protocols": "tcp"
    },
    "1": {
      "type": "ipv4-addr",
      "value": "203.0.113.10"
    },
    "2": {
      "type": "ipv4-addr",
      "value": "198.51.100.58"
    }
  }
}

```

B.6.2 观测表达式限定符

观测表达式可使用 INITIAL、START/STOP 和 REPEATS 关键字来表示时间约束条件和重复数量约束条件。常用的观测表达式限定符应符合表 B.5 的规定。

表 B.5 常用的观测表达式限定符使用形式

限定符使用	描述
a REPEATS x TIMES	a 是观测表达式或前置的限定符。a 至少匹配 x 次,其中每次匹配都是不同的观测数据。x 是正整数。例如:[b] FOLLOWEDBY [c] REPEATS 5 TIMES
a WITHIN x SECONDS	a 是观测表达式或前置的限定符。由 a 匹配的所有观测数据在指定的时间窗口内发生或已经被观测到。x 是正的浮点值或整数值。例如: ([file:hashes.'SHA-256' = '13987239847 ...'] AND [win-registry-key:key = 'hkey']) WITHIN 120 SECONDS
a START x STOP y	a 是观测表达式或前置的限定符。与 a 匹配的所有观测数据在 $\geq x$ 且 $\leq y$ 的观测时间内。x 和 y 是 timestamp 类型

B.6.3 观测运算符

可使用观测运算符组合两个或多个观测表达式,以便进一步约束与模式表达式匹配的观测集合。常用的观测运算符使用形式应符合表 B.6 的规定。

表 B.6 常用的观测运算符使用形式

可观测运算符使用	描述	计算次序
[a] AND [b]	a 和 b 是观测表达式,且在不同的观测数据上计算值为 true	左到右
[a] OR [b]	a 和 b 是观测表达式,且 a 或 b 中的一个在不同的观测数据上计算值为 true	左到右
[a] FOLLOWEDBY [b]	a 和 b 是观测表达式。a 和 b 值都为 true,其中与 b 关联的观测时间戳大于或等于与 a 关联的观测时间戳,且在不同的观测数据上值为 true	左到右

B.6.4 操作符计算次序

运算符的计算次序可使用括号来明确。一般运算符计算次序是从左到右的。操作符优先次序符合表 B.7 的规定。

表 B.7 操作符优先次序

操作符	计算次序	使用范围
()	左到右	观测表达式或模式表达式、观测表达式和限定符
AND	左到右	观测表达式、模式表达式

表 B.7 操作符优先次序（续）

操作符	计算次序	使用范围
OR	左到右	观测表达式、模式表达式
FOLLOWEDBY	左到右	模式表达式

B.7 组件路径语法

B.7.1 语法符号

表 B.8 规定了在模式语言中用于寻址可观测数据属性的语法符号。

表 B.8 语法符号

符合	描述
<object-type>	要匹配的可观测数据子组件类型
<property_name>	要匹配的可观测数据子组件属性名称。 嵌套的属性使用语法<property_name>.<property_name>指定,其中“.”前面的<property_name>是父属性名称,后面的是子属性名称

B.7.2 基本对象

在可观测数据子组件上指定的属性,该属性格式不是字典和列表。

语法为:<object-type>:<property_name>。

示例: file:size

B.7.3 列表对象

在可观测数据子组件上指定的属性,该属性格式是列表。

语法为:<object-type>:<property_name>[list_index].<property_name>

示例 1: file:extensions.'windows-pebinary-ext'.sections[*].entropy

示例 2: network-traffic:protocols[0]

B.7.4 字典对象

在可观测数据子组件上指定的属性,该属性格式是字典。

语法为:<object-type>:<property_name>.<key_name>

其中:<property_name>是字典的子组件属性名称,而<key_name>是字典中键的名称。

示例 1: file:hashes.ssdeep

示例 2: file:extensions.'raster-image-ext'.image_height

B.7.5 组件引用

可观测数据子组件的属性格式为 identifier 字段类型(可为单个 identifier,identifier 列表),且该属性引用了别的组件的属性。

对于单个 identifier,语法为:

<object-type>:<property_name>.<dereferenced_object_property>

其中:<property_name>是指可观测数据子组件的属性名称,<dereferenced_object_property>是被引用组件的属性名称。

示例 1: email-message:from_ref.value

对于 identifier 列表的情况,语法为:

<object-type>:<property_name>[list_index].<dereferenced_object_property>

示例 2: directory:contains_refs[*].name

附 录 C
(规范性)
可观测数据子组件

C.1 IP 地址信息

IP 地址信息描述与 IP 地址相关的观测值,包括 IP 地址、MAC 地址引用列表、自治系统引用列表等,IP 地址信息属性应符合表 C.1 的规定。可使用 IP 地址和网络流量信息两个子组件描述 IP 及其端口信息,见附录 I。

表 C.1 IP 地址信息字段

必填公共属性					
type,id					
可选公共属性					
spec_version, object_marking_refs, defanged, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“ipv4-addr、ipv6-addr”
2	地址值	value	srting	描述“IP 地址”,使用 CIDR 表示法表示一个或多个地址的值。如为 IPv4 地址类型,且表示单个 IPv4 地址,则可省略 CIDR/32 后缀,如为 IPv6 地址类型,且表示单个 IPv6 地址,则可省略 CIDR/128 后缀	是
3	MAC 地址引用列表	resolves_to_refs	list of type identifier	描述“IP 地址”解析到的一个或多个 MAC 地址的引用列表,此列表中应引用“MAC 地址信息”子组件	否
4	自治系统引用列表	belongs_to_refs	list of type identifier	描述“IP 地址”所属的一个或多个自治系统的引用列表,此列表中应引用“自治系统信息”子组件	否

C.2 域名信息

域名信息描述与网络域名信息相关的观测值,包括域名值、域名解析引用列表等,域名信息属性应符合表 C.2 的规定。

表 C.2 域名信息字段

必填公共属性					
type, id					
可选公共属性					
spec_version, object_marking_refs, defanged, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取 值 为 “domain-name”
2	值	value	string	描述“域名”的值,符合 IETF RFC 1034 的规定,域名中包含的每个域和子域均符合 IETF RFC 5890 的规定	是
3	IP 地址或域名的引用列表	resolves_to_refs	list of type identifier	描述“域名”解析到的一个或多个 IP 地址或域名的引用列表,此列表中引用的是 ipv4 addr 或 ipv6 addr 类型或域名类型	否

C.3 URL 信息

URL 信息描述与统一资源定位符相关的观测值。URL 信息字段应符合表 C.3 的规定。

表 C.3 URL 信息字段

必填公共属性					
type, id					
可选公共属性					
spec_version, object_marking_refs, defanged, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“url”
2	值	value	string	描述本项“URL”的值。此属性的值符合 IETF RFC 3986 中 1.1.3 的要求	是

C.4 电子邮件信息

电子邮件信息描述与电子邮件相关的观测值,包括电子邮件地址、显示名称、用户账户、多用途互联网邮件扩展、发送时间、发件人、收件人、抄送、密件抄送、消息 id、主题、标题、正文等,电子邮件信息字段应符合表 C.4 的规定。

表 C.4 电子邮件信息字段

必填选公共属性					
type,id					
可选公共属性					
spec_version, object_marking_refs, defanged, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取 值 为 “email-addr”或 “email-message”
2	地址值	value	string	描述本项“电子邮件”地址的值,不包括显示名称	当 type 取 值 为 “email-addr”时, 是必填
3	名称	display_name	string	描述本项“电子邮件”单个电子邮件显示名称。属性格式应符合 IETF RFC 5322 中 3.4 的要求	否
4	用户账户	belongs_to_ref	string	描述本项“电子邮件”电子邮件地址所属的用户账户	否
5	是否包含多个 MIME 部分	is_multipart	boolean	描述本项“电子邮件”正文是否包含多个 MIME 部分。值为 true 时表示为多部分,值为 false 时表示不为多部分	是
6	发送时间	date	timestamp	描述本项“电子邮件”发送的日期/时间	否
7	传输数据包头的值	content_type	string	描述本项“电子邮件”传输数据包头的值,用于描述消息主体的字段类型和编码方式	否
8	“发件人:”包头的值	from_ref	identifier	描述本项“电子邮件”的“发件人:”包头的值。“发件人:”字段为邮件的作者,即负责撰写邮件的人员或系统的邮箱。引用的子组件类型为“email-addr”	否
9	“发件人”字段的值	sender_ref	identifier	描述本项“电子邮件”的“发件人”字段的值。“发件人:”字段指定负责实际传输邮件的代理的邮箱。引用的子组件类型为“email-addr”	否
10	“收件人:”邮箱引用列表	to_refs	list of type identifier	描述本项“电子邮件”的“收件人:”邮箱引用列表,引用的子组件类型为“email-addr”	否
11	抄送的地址列表	cc_refs	list of type identifier	描述本项“电子邮件”抄送的地址列表,表明邮件抄送的全部收件人。引用的子组件类型为“email-addr”	否

表 C.4 电子邮件信息字段（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
12	密件抄送的地址列表	bcc_ref	list of type identifier	描述本项“电子邮件”密件抄送的地址列表,表明邮件密件抄送的全部收件人。引用的子组件类型为“email-addr”	否
13	消息 id	message_id	string	描述本项“电子邮件”的消息 id	否
14	主题	subject	string	描述本项“电子邮件”的主题	否
15	“已接收”标题字段列表	received_lines	list of type string	描述本项“电子邮件”标题中可能包含的一个或多个“已接收”标题字段列表,列表值应以与电子邮件中相同的顺序出现	否
16	指定字典	additional_header_fields	dictionary	将本项“电子邮件”中的任何其他包头字段 (date、received_lines、content_type、from_ref、sender_ref、to_refs、cc_refs、bcc_refs 和 subject 除外)指定为字典。字典中的每个键/值对表示单个包头字段的名称/值,或多次出现的包头字段的姓名/值。每个字典键的对应值应始终是字符串类型的列表	否
17	正文的字符串	body	string	描述本“电子邮件”正文的字符串。如果 is_multipart 为 true,则不应使用此属性	否
18	MIME 部分的列表	body_multipart	list of type email-mime-part-type	描述组成本项“电子邮件”正文的 MIME 部分的列表。如果 is_multipart 为 false,则不应使用此属性	否
19	原始二进制内容	raw_email_ref	identifier	描述本项“电子邮件”的原始二进制内容,包括标题和正文。引用子组件“字节片段信息”	否

C.5 网络流量信息

网络流量信息描述与网络流量相关的观测值,包括扩展、启动时间、结束时间、状态、来源、目的地、端口、协议、字节数、数据包、ip 字典、封装等,网络流量信息字段应符合表 C.5 的规定。

表 C.5 网络流量信息字段

必填选公共属性
type,id
可选公共属性
spec_version, object_marking_refs, defanged, extensions

表 C.5 网络流量信息字段 (续)

序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“network-traffic”
2	扩展信息	extensions	dictionary	描述本项“网络流量”扩展的其他自定义信息,可针对特定网络协议类型[例如: http(Hypertext Transfer Protocol,超文本传输协议)、tcp(Transmission Control Protocol,传输控制协议)等]增加专属特征属性	否
3	启动时间	start	timestamp	描述本项“网络流量”启动的日期/时间	否
4	结束时间	end	timestamp	描述本项“网络流量”结束的日期/时间。如果 is_active 属性为 true,则不包含 end 属性。如果此属性和 start 属性都已定义,则此属性大于或等于 start 属性中的时间戳	否
5	是否仍在进行中	is_active	boolean	描述本项“网络流量”是否仍在进行中。如果提供了 end 属性,则此属性应为 false	否
6	来源	src_ref	identifier	描述本项“网络流量”的来源,引用“IP 地址信息”“MAC 地址信息”或“域名信息”(域名的 IP 地址未知时)的子组件	否
7	目的地	dst_ref	identifier	描述本项“网络流量”的目的地,引用“IP 地址信息”“MAC 地址信息”或“域名信息”(域名的 IP 地址未知时)的子组件	否
8	源端口	src_port	integer	以整数形式指定网络流量中使用的源端口。端口值应在 0~65535 的范围内	否
9	目标端口	dst_port	integer	以整数形式指定网络流量中使用的目标端口。端口值应在 0~65535 的范围内	否
10	协议	protocols	list of type string	描述本项“网络流量”中观测到的协议及其相应状态	是
11	源发出的字节数	src_byte_count	integer	将从源发出的字节数指定为正整数	否
12	目标发回的字节数	dst_byte_count	integer	从目标发回到源的正整数字节数	否
13	源发送到目标的数据包数量	src-packets	integer	将从源发送到目标的数据包数量指定为正整数	否

表 C.5 网络流量信息字段（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
14	目标发送到源的数据包数量	dst_packets	integer	将从目标发送到源的数据包数量指定为正整数	否
15	字典	ipfix	dictionary	将本项“网络流量”的任何 IP 流信息导出 ipfix 数据指定为字典。字典中的每个键/值对表示单个 ipfix 元素的名称/值	否
16	源发送到目标的字节	src_payload_ref	identifier	描述本项“网络流量”从源发送到目标的字节。引用“字节片段信息”子组件	否
17	目标发送到源的字节	dst_payload_ref	list of type identifier	描述本项“网络流量”从目标发送到源的字节。引用“字节片段信息”子组件	否
18	链接	encapsulates_refs	identifier	与本项“网络流量”封装的其他网络流量的链接。引用“网络流量信息”子组件	否
19	网络流量链接	encapsulated_by_ref	identifier	链接到封装本项“网络流量”的另一个网络流量。引用“网络流量信息”子组件	否

C.6 MAC 地址信息

MAC 地址信息描述与硬件地址相关的观测值。MAC 地址信息字段应符合表 C.6 的规定。

表 C.6 MAC 地址信息字段

必填选公共属性					
type,id					
可选公共属性					
spec_version, object_marking_refs, defanged, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“mac-addr”
2	单个 MAC 地址的值	value	string	描述本项单个 MAC 地址的值。MAC 地址值应表示为单个冒号隔开的、小写的 MAC-48 地址	是

C.7 自治系统信息

自治系统信息描述与自治系统相关的观测值。自治系统信息字段应符合表 C.7 的规定。

表 C.7 自治系统信息字段

必填公共属性					
type, id					
可选公共属性					
spec_version, object_marking_refs, defanged, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“autonomous-system”
2	编号	number	integer	描述分配给本项“自治系统”的编号	是
3	名称	name	string	本项“自治系统”的名称	否
4	机构名称	rir	string	为本项“自治系统”分配编号的机构名称	否

C.8 字节片段信息

字节片段信息描述与发现的任意字节片段相关的观测值,包括数据类型、字节片段数据、URL、杂凑值、加密算法、解密密钥等。字节片段表示一个 base64 编码的字节数组,或一个文件内容。字节片段信息字段应符合表 C.8 的规定。

表 C.8 字节片段信息字段

必填选公共属性					
type,id					
可选公共属性					
spec_version, object_marking_refs, granular_markings, defanged, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“artifact”
2	数据类型	mime_type	string	优先使用 MIME 标准定义字段类型,如不使用 MIME 可自定义	否
3	数据	payload_bin	binary	以 base64 编码字符串表示本项“字节片段”数据。如果提供了 url,则此项不应存在	否
4	url 值	url	string	描述本项“字节片段”的 url 值,应解析为未编码内容的有效 url。如提供了 payload_bin,则此项应不存在	否

表 C.8 字节片段信息字段（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
5	杂凑字典	hashes	hashes	为 url 或 payload_bin 的内容指定杂凑字典。当 url 属性存在时,此属性应存在。字典键符合 D.21	否
6	加密算法类型	encryption_algorithm	enum	如果字节片段被加密,则指定加密算法类型,符合 D.22。如果同时包含 mime_type 和 encryption_algorithm,则该字节片段表示加密的内容	否
7	解密密钥	decryption_key	string	解密密钥。当 encryption_algorithm 属性不存在时,此项不应存在	否

C.9 文件信息

文件信息描述与文件信息相关的观测值,包括扩展信息、杂凑值、文件大小、名称、编码、文件格式、MIME 类型、文件创建时间、文件修改时间、文件访问时间、父目录、引用、文件内容等,文件信息字段应符合表 C.9 的规定。

表 C.9 文件信息字段

必填选公共属性					
type,id					
可选公共属性					
spec_version, object_marking_refs, defanged, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“file”
2	扩展信息	extensions	dictionary	描述本项“文件”扩展的其他自定义信息,可针对特定文件类型(例如:linux 文件、PDF 文件等)增加专属特征属性	否
3	杂凑值	hashes	hashes	文件的杂凑值	是。至少包括 1 项杂凑类型的取值
4	文件大小	size	integer	描述本项“文件”的大小(以字节为单位)。此属性的值不应为负	否
5	名称	name	string	描述本项“文件”的名称	否
6	编码方式	name_enc	string	描述本项“文件名”所使用的编码方式	否
7	文件格式	magic_number_hex	string	本项“文件”对应的表示文件格式的十六进制常量	否

表 C.9 文件信息字段（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
8	MIME 类型名称	mime_type	string	为文件指定的 MIME 类型名称	否
9	创建时间	ctime	timestamp	描述本项“文件”创建时间	否
10	上次写文件的时间	mtime	timestamp	描述上次写本项“文件”的时间	否
11	上次访问文件的时间	atime	timestamp	描述上次访问本项“文件”的时间	否
12	父目录	parent _ directory_ref	identifier	描述本项“文件”的父目录	否
13	可观测对象的引用列表	contains_refs	list of type identifier	本项“文件”中包含的其他网络可观测对象的引用列表	否
14	所在的字节片段	content_ref	identifier	描述本项“文件”的内容所在的字节片段,引用的对象是字节片段	否

C.10 目录信息

目录信息描述与文件系统目录相关的观测值,包括目录原始路径、路径编码方式、目录创建时间、目录修改时间、目录访问时间、包含关系等,目录信息字段应符合表 C.10 的规定。

表 C.10 目录信息字段

必填公共属性					
type, id					
可选公共属性					
spec_version, object_marking_refs, defanged, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“directory”
2	原始路径	path	string	描述文件系统上目录的原始路径	是
3	编码方式	path_enc	string	描述本项“路径”的编码方式	否
4	创建时间	ctime	timestamp	描述本项“目录”创建的时间	否
5	修改时间	mtime	timestamp	描述本项“目录”上次修改的时间	否
6	访问时间	atime	timestamp	描述本项“目录”上次访问的时间	否

表 C.10 目录信息字段（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
7	引用列表	contains_refs	list of type identifier	描述对本项“目录”中包含的其他文件和/或目录对象的引用列表。此列表中引用的对象是文件或目录类型	否

C.11 互斥信息

互斥信息记录与互斥对象相关的观测值。互斥信息字段应符合表 C.11 的规定。

表 C.11 互斥信息字段

必填公共属性					
type, id					
可选公共属性					
spec_version, object_marking_refs, defanged, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“mutex”
2	名称	name	string	描述互斥对象的名称	是

C.12 进程信息

进程信息描述与进程相关的观测值,包括扩展信息、状态、进程 ID、创建时间、环境变量、网络连接、列表、用户、文件引用、父进程、子进程等,进程信息字段应符合表 C.12 的规定。

表 C.12 进程信息字段

必填公共属性					
type, id					
可选公共属性					
spec_version, object_marking_refs, defanged, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“process”
2	扩展信息	extensions	dictionary	描述本项“进程”扩展的其他自定义信息,可针对特定进程类型(例如:windows进程)增加专属特征属性	否

表 C.12 进程信息字段（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
3	是否隐藏	is_hidden	boolean	描述本项“进程”是否隐藏	否
4	进程 ID	pid	integer	描述本项“进程”的进程 ID 或 PID	否
5	创建时间	created_time	timestamp	本项“进程”创建的时间	否
6	当前工作目录	cwd	string	描述本项“进程”的当前工作目录	否
7	命令行	command_line	string	执行本项“进程”时使用的完整命令行	否
8	环境变量值	environment_variables	dictionary	将与进程关联的环境变量列表描述为字典。字典中的每个键都应是环境变量名称的大小写版本,每个对应的值都应是字符串形式的环境变量值	否
9	网络连接列表	opened_connection_refs	list of type identifier	本项“进程”打开的网络连接列表,此列表中引用的组件是“网络流量”类型	否
10	用户	creator_user_ref	identifier	创建本项“进程”的用户	否
11	二进制文件	image_ref	identifier	作为进程映像执行的可执行二进制文件,此属性中引用的组件应是“文件信息”类型	否
12	父进程	parent_ref	identifier	生成本项“进程”的另一个进程(即其父进程),此属性中引用的组件是“进程”类型	否
13	子进程	child_refs	list of type identifier	描述由本项“进程”(即其子进程)生成的其他进程,此列表中引用的组件是“进程”类型	否

C.13 用户信息

用户信息描述与用户相关的信息,包括扩展信息、用户标识、凭据、登录账户、显示名称、进程关联、特权、时间要素等,用户信息字段应符合表 C.13 的规定。

表 C.13 用户信息字段

必填公共属性					
type,id					
可选公共属性					
spec_version, object_marking_refs, defanged, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“user-account”

表 C.13 用户信息字段（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
2	扩展信息	extensions	dictionary	描述本项“用户”扩展的其他自定义信息,可针对特定用户类型(例如:UNIX 用户)增加专属特征属性	否
3	标识符	user_id	hashes	指定账户的标识符。标识符可为数字 ID、GUID、账户名、电子邮件地址等,但应是所属系统的唯一标识符字段	是
4	明文凭据	credential	string	明文凭据	否
5	账户登录名	account_login	string	描述账户登录时实际输入的字符串,用于在 user_id 属性所指定的内容与用户实际输入的登录信息不一致的情况下使用。例如,对于 user_id 为 0 的 Unix 账户,其 account_login 可能是“root”	否
6	账户类型	account_type	string	账户类型,例如:windows 账户、微信账户等	否
7	账户名称	display_name	string	在用户界面中显示的账户的名称	否
8	关联关系	is_service_account	boolean	账户与网络服务或系统进程(守护进程)的关联关系,true 表示有关联关系,false 表示无关联关系	否
9	是否为特权账户	is_privileged	boolean	账户是否为特权账户,true 表示是,false 表示否	否
10	是否具有升级权限	can_escalate_privs	boolean	账户是否具有升级权限,true 表示是,false 表示否	否
11	是否禁用该账户	is_disabled	boolean	是否禁用该账户,true 表示是,false 表示否	否
12	创建时间	account_created	timestamp	创建账户的时间	否
13	到期日期	account_expires	timestamp	账户的到期日期	否
14	更改账户凭据时间	credential _ last _ changed	timestamp	上次更改账户凭据的时间	否
15	首次访问时间	account_first_login	timestamp	首次访问账户的时间	否
16	末次访问时间	account_last_login	timestamp	上次访问账户的时间	否

C.14 注册表信息

注册表信息描述与注册表相关的观测值,包括注册表项、时间、账户、子键等,注册表信息字段应符合表 C.14 的规定。

表 C.14 注册表信息字段

必填公共属性					
type,id					
可选公共属性					
spec_version, object_marking_refs,defanged, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“win-dows-registry-key”
2	键值	key	string	描述完整的注册表路径,包括根键	是
3	值	values	list of type win-dows-registry-v	描述在本项“注册表”中与键值对应的值	是
4	修改时间	modified_time	timestamp	上次修改注册表项的时间	否
5	用户账户	creator_user_ref	identifier	创建注册表项的用户账户	否
6	子键数量	number_of_sub-keys	integer	描述本项“注册表”项下包含的子键数量	否

C.15 软件信息

软件信息描述与软件相关的观测值,包括软件名称、CPE 条目、软件标识、语言、供应商、版本等,软件信息字段应符合表 C.15 的规定。

表 C.15 软件信息字段

必填公共属性					
type, id					
可选公共属性					
spec_version, object_marking_refs, defanged, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取值为“soft-ware”
2	名称	name	string	描述本项“软件”的名称	是

表 C.15 软件信息字段（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
3	CPE 条目	cpe	string	描述本项“软件”的 CPE 条目	否
4	标识	swid	string	描述本项“软件”的软件标识	否
5	语言	languages	list of type string	描述本项“软件”支持的语言,取值符合 IETF RFC 5646 的规定	否
6	供应商名称	vendor	string	描述本项“软件”供应商的名称	否
7	版本值	version	string	描述本项“软件”的版本号	否

C.16 CA 证书信息

CA 证书信息描述与 CA 证书相关的观测值,包括杂凑值、编码证书版本、序列号、签名、颁发机构、公钥、算法等,CA 证书信息字段应符合表 C.16 的规定。

表 C.16 CA 证书信息字段

必填公共属性					
type, id					
可选公共属性					
spec_version, object_marking_refs, defanged, extensions					
序号	信息项	字段名称	字段类型	字段描述	是否必填
1	类型	type	string	类型	是。取 值 为 “x509-certificate”
2	是否自签名	is_self_signed	boolean	证书是否是自签名的,true 表示是,false 表示否	否
3	杂凑值	hashes	hashes	证书的杂凑值	是
4	版本	version	string	证书的编码版本	否
5	序列号	serial_number	string	由特定证书颁发机构颁发的证书的唯一标识符	否
6	签 名 算 法 名称	signature _ algo-rithm	string	用于对证书进行签名的算法名称	否
7	机构名称	issuer	string	颁发证书的机构名称	否
8	有效期开始日期	validity_not _ be-fore	timestamp	证书有效期开始的日期	否
9	有效期结束日期	validity_not_after	timestamp	证书有效期结束的日期	否

表 C.16 CA 证书信息字段（续）

序号	信息项	字段名称	字段类型	字段描述	是否必填
10	实体名称	subject	string	证书中公钥关联的实体的名称	否
11	加密算法名称	subject_public_key_algorithm	string	发送给实体的用于加密数据的算法名称	否
12	模数部分	subject_public_key_modulus	string	实体的 RSA 公钥的模数部分	否
13	指数部分	subject_public_key_exponent	integer	实体的 RSA 公钥的指数部分, 类型为整数	否

附 录 D
(规范性)
词汇表

D.1 攻击指标类型词汇 Indicator Type Vocabulary

攻击指标类型对攻击指标进行分类,具体内容应符合表 D.1 的规定。

表 D.1 攻击指标类型词汇

词汇表总结	
anomalous-activity, anonymization, benign, compromised, malicious-activity, attribution, unknown	
词汇表值	描述
anomalous-activity	异常活动,表示意外的或异常的活动,不一定是恶意的,也不一定表示存在危害。此类活动可能包括类似侦测的行为,例如端口扫描或版本识别、网络行为异常以及资产和/或用户行为异常
anonymization	匿名,表示可疑的匿名化工具或基础设施(代理、TOR、VPN 等)
benign	良性,表示活动本身并不可疑或恶意,但与其他活动结合使用时可能表示可疑或恶意行为
compromised	失陷,表示疑似失陷的资产
malicious-activity	恶意活动,表示可疑恶意对象或活动的模式
attribution	归因,表示指示特定威胁主体或攻击活动的行为模式
unknown	未知

D.2 模式类型词汇 Pattern Type Vocabulary

模式类型描述攻击指标所使用的模式语言,具体内容应符合表 D.2 的规定。

表 D.2 模式类型词汇

词汇表总结	
stix, pcre, sigma, snort, suricate, yara	
词汇表值	描述
stix	STIX 模式语言
pcre	Perl 兼容正则表达式
sigma	SIGMA 日志检测规则语言

表 D.2 模式类型词汇 (续)

词汇表值	描述
snort	SNORT 流量检测规则语言
suricate	SURICATE 流量检测规则语言
yara	YARA 文件检测规则语言

D.3 威胁主体类型词汇 Threat Actor Type Vocabulary

威胁主体类型描述个人或团体所属类型,具体内容应符合表 D.3 的规定。

表 D.3 威胁主体类型词汇

词汇表总结	
activist, competitor, crime-syndicate, criminal, hacker, insider-accidental, insider-disgruntled, nation-state, sensationalist, spy, terrorist, unknown	
词汇表值	描述
activist	激进分子。试图破坏组织的商业模式或损害其形象的个人或组织
competitor	商业竞争对手
crime-syndicate	犯罪集团
criminal	罪犯
hacker	黑客
insider-accidental	内部人员。无意中使组织受到损害的内部人员
insider-disgruntled	内部不满人员。内部人员(包括在职的和已离职的)发起的报复性的攻击活动
nation-state	国家级组织
sensationalist	追求轰动效应的个人或组织
spy	间谍
terrorist	恐怖分子
APT	APT 组织
ransomware-group	勒索集团
cybercrime-syndicate	黑产组织
unknown	未知

D.4 威胁主体角色词汇 Threat Actor Role Vocabulary

威胁主体角色描述威胁主体承担的不同角色,具体内容应符合表 D.4 的规定。

表 D.4 威胁主体角色词汇

词汇表总结	
agent, director, independent, infrastructure-architect, infrastructure-operator, malware-author, sponsor	
词汇表值	描述
agent	代理人。威胁主体代表自己或在其他人的指导下执行攻击
director	指挥者。指导恶意活动的活动、目标和目的的威胁主体
independent	独立攻击者。独立行动的威胁主体
infrastructure-architect	基础设施设计者。设计基础设施的架构师
infrastructure-operator	基础设施操作者。提供和操作用于实施攻击的基础设施(僵尸网络提供商、云服务等)的威胁主体
malware-author	恶意软件编写者。编写恶意软件或其他恶意工具的威胁主体
sponsor	资助者。资助恶意活动的威胁主体

D.5 攻击资源级别词汇 Attack Resource Level Vocabulary

攻击资源级别描述威胁主体、攻击活动集或活动可能访问的资源的级别,包括个人可调用的,到政府可调用的资源级别。具体内容应符合表 D.5 的规定。

表 D.5 攻击资源级别词汇

词汇表总结	
individual, club, contest, team, organization, government	
词汇表值	描述
individual	个人。资源仅限于普通个人,或威胁主体独立实施攻击
club	兴趣小组或俱乐部。非正式的社会团体,自愿互动
contest	临时组织。非正式的、短暂的且可能是匿名的活动,当参与者实现了一个单一目标时结束
team	正式团体。一个正式组织起来的团体,长期存在,通常在单一地域内活动
organization	大规模组织。比团队规模更大、资源更丰富的组织,例如犯罪集团。通常在多个地理区域运行,并长期持续
government	政府。可使用辖区内的公共资产和职能,资源充足并长期提供

D.6 工具类型词汇 Tool Type Vocabulary

工具类型描述了可用于执行攻击的工具类别,具体内容应符合表 D.6 的规定。

表 D.6 工具类型词汇

词汇表总结	
denial-of-service, exploitation, information-gathering, network-capture, credential-exploitation, remote-access, vulnerability-scanning, unknown	
词汇表值	描述
denial-of-service	拒绝服务类。用于执行拒绝服务攻击或 DDoS 攻击的工具,例如:Low Orbit Ion Cannon (LOIC)和 DHCPig
exploitation	软件或系统利用。用于利用软件和系统漏洞的工具,例如:sqlmap 和 Metasploit
information-gathering	信息收集。用于枚举系统和网络信息的工具,例如:NMAP
network-capture	网络抓包。用于捕获网络流量的工具,例如:Wireshark、Kismet
credential-exploitation	密码/证书破解。用于在本地或远程破解口令数据库或以其他方式利用/发现凭据的工具,例如:John the Ripper、NCrack
remote-access	远程访问。用于远程访问计算机的工具,例如:VNC、远程桌面
vulnerability-scanning	漏洞扫描。用于扫描系统和网络漏洞的工具,例如:Nessus
unknown	未知

D.7 观点枚举词汇 Opinion Enumeration

观点枚举描述了创建者对所引用观点的认可程度。具体内容应符合表 D.7 的规定。

表 D.7 观点枚举词汇

词汇表总结	
strongly-disagree, disagree, neutral, agree, strongly-agree	
词汇表值	描述
strongly-disagree	强烈不同意。如果使用数值表示,可使用“1”
disagree	不同意。如果使用数值表示,可使用“2”
neutral	中立。如果使用数值表示,可使用“3”
agree	同意。如果使用数值表示,可使用“4”
strongly-agree	强烈同意。如果使用数值表示,可使用“5”

D.8 TLP 标记对象枚举词汇 TLP Marking Object Enumeration

TLP 标记对象限定共享范围。具体内容应符合表 D.8 的规定。

表 D.8 TLP 标记对象枚举词汇

词汇表总结	
TLP:RED, TLP:AMBER+STRICT, TLP:AMBER, TLP:GREEN, TLP:CLEAR	
词汇表值	描述
TLP:RED	小范围个人共享
TLP:AMBER+STRICT	有限共享。对象仅限组织及其客户中有知情权的个人
TLP:AMBER	组织内部共享
TLP:GREEN	团体内共享
TLP:CLEAR	共享没有限制

D.9 网络攻击链阶段词汇 Cyber Kill Chain Phases Vocabulary

网络攻击链阶段描述网络攻击所处于的阶段信息，具体内容应符合表 D.9 的规定。

表 D.9 网络攻击链阶段词汇

词汇表总结	
reconnaissance, weaponization, delivery, exploitation, installation, command and control, actions on objective	
词汇表值	描述
reconnaissance	侦察跟踪,攻击者通过互联网收集目标的信息,包括网站、邮箱、电话和社会工程学等手段,以确定攻击对象
weaponization	武器构建,攻击者根据侦察阶段收集的信息,构建攻击武器,通常使用自动化工具或手动构建恶意软件
delivery	载荷投递,攻击者通过钓鱼邮件、网页、USB 等方式将构建好的网络武器投递到目标系统
exploitation	漏洞利用,攻击者利用目标系统的漏洞启动恶意代码
installation	安装植入,在目标系统中安装木马或后门,以便长期潜伏和控制
command and control	命令与控制,攻击者建立控制路径,通过自动和手工方式控制目标系统
actions on objective	目标达成,执行攻击行为,如窃取信息、篡改信息等

D.10 威胁主体经验词汇 Threat Actor Sophistication Vocabulary

威胁主体经验描述威胁主体的经验水平，具体内容应符合表 D.10 的规定。

表 D.10 威胁主体经验词汇

词汇表总结	
none, minimal, intermediate, advanced, expert, innovator, strategic	
词汇表值	描述
none	无。此类人员会使用工具进行攻击,计算机专业水平能力一般
minimal	极小。此类人员懂得攻击系统弱点,会使用常见脚本和工具,了解工具的基本用途
intermediate	中等。此类人员会熟练使用公开的攻击框架和漏洞利用工具
advanced	高级。此类人员能自行开发漏洞利用等攻击工具
expert	专家。此类人员能自行开发利用已知和未知漏洞的攻击工具
innovator	创新者。此类人员能利用已知和未知漏洞,开发针对 0-day 漏洞的攻击利用框架,创造新的攻击模式
strategic	战略者。此类攻击者可利用供应链进行攻击,设计针对任何系统的攻击,可发动 APT(高级可持续化)攻击

D.11 攻击动机词汇 Attack Motivation Vocabulary

攻击动机描述攻击者的攻击动机信息,具体内容应符合表 D.11 的规定。

表 D.11 攻击动机词汇

词汇表总结	
accidental, coercion, dominance, ideology, notoriety, organizational-gain, personal-gain, personal-satisfaction, revenge, unpredictable	
词汇表值	描述
accidental	非故意行为。非恶意行为,无意中造成损害
coercion	被胁迫。被他人胁迫而进行攻击
dominance	控制资源。展示自身技术优越性
ideology	意识形态原因。因意识形态原因进行攻击,借此表明自身立场、态度
notoriety	扩大影响。为了追求声望或获取知名度而进行攻击
organizational-gain	寻求竞争优势。为使组织获得竞争优势而进行攻击,经常涉及窃取知识产权或供应链协议信息
personal-gain	获取个人经济利益。出于改善个人经济状况目的进行攻击,经常使用欺诈、窃取知识产权等手段

表 D.11 攻击动机词汇（续）

词汇表值	描述
personal-satisfaction	获取个人满足感。出于满足个人目标或欲望的目的进行攻击,如:满足好奇心、寻求刺激和乐趣
revenge	报复。出于对某些组织或个人行为实施报复的目的而进行攻击
unpredictable	不可预期。在没有明确理由或目的的情况下进行攻击

D.12 基础设施类型词汇 Infrastructure Type Vocabulary

基础设施类型描述基础设施类型信息,具体内容应符合表 D.12 的规定。

表 D.12 基础设施类型词汇

词汇表总结	
amplification, anonymization, botnet, command-and-control, exfiltration, hosting-malware, hosting-target-lists, phishing, reconnaissance, staging, unknown	
词汇表值	描述
amplification	用于实施放大攻击的基础设施
anonymization	用于进行匿名化的基础设施
botnet	用于组成僵尸网络的基础设施
command-and-control	用于进行命令与控制的基础设施
control-system	控制系统,如 IoT, HMI, RTU, PLC 等 ICS 设施
exfiltration	用于进行数据窃取的基础设施
firewall	防火墙
hosting-malware	在终端运行的恶意软件
hosting-target-lists	用于执行有针对性攻击的基础设施
phishing	用于进行钓鱼攻击的基础设施
reconnaissance	用于进行目标识别的基础设施
routers-switches	用于将设备连接到网络的基础设施
staging	用于实施多阶段攻击的基础设施
malicious-scanning	用于恶意扫描的基础设施
brute-force-attack	用于暴力破解的基础设施
lateral-movement	用于横向移动的基础设施
workstation	与业务相关需要进行保护的终端设施
unknown	未知

D.13 恶意软件类型词汇 Malware Type Vocabulary

恶意软件类型描述恶意软件的类型信息,类型之间并无互斥关系,具体内容应符合表 D.13 的规定。

表 D.13 恶意软件类型词汇

词汇表总结	
adware, backdoor, bot, bootkit, ddos, downloader, dropper, exploit-kit, keylogger, ransomware, remote-access-trojan, resource-exploitation, rogue-security-software, rootkit, screen-capture, spyware, trojan, unknown, virus, webshell, wiper, worm	
词汇表值	描述
adware	广告软件。可展示广告,同时也经常搜集系统上的用户敏感信息
backdoor	后门程序。攻击者用来访问远程系统的恶意软件,一般可传输文件、获取口令或执行软件命令
bot	僵尸网络。组成僵尸网络并驻留在受害者系统上的程序
bootkit	引导后门病毒。可篡改攻击目标主引导信息的恶意程序
ddos	Ddos 工具。执行分布式拒绝服务攻击的程序
downloader	Downloader。用来下载并执行其他文件的木马程序
dropper	投放工具。用来部署恶意负载的木马程序
exploit-kit	漏洞利用工具。针对某种漏洞进行利用的工具套件
keylogger	键盘记录器。可记录键盘行为并发送到信息收集终端的恶意程序
ransomware	勒索软件。可加密受害者系统上的文件并索要赎金以解锁文件的恶意程序
remote-access-trojan	远程控制木马。远程攻击者控制计算机系统的软件
resource-exploitation	资源盗用软件。盗用计算机系统资源的恶意软件,比如挖矿软件
rogue-security-software	流氓安全软件。假冒安全产品的恶意程序
rootkit	Rootkit。可挂起系统特定功能,以隐藏系统内核级调用信息,实现在受害者系统长期驻留的高隐藏性恶意程序
screen-capture	抓屏软件。可截取系统屏幕,发送给命令与控制系统的恶意软件
spyware	间谍软件。可在受害者未注意时收集并回传敏感信息至特定终端的恶意软件
trojan	木马。可入侵受害者系统并隐藏真实目的的恶意程序
virus	病毒。可修改并繁殖自身的恶意软件
webshell	Webshell 恶意脚本。可在受害者系统上执行的恶意脚本
wiper	擦除破坏。可删除受害者系统或磁盘上文档的恶意程序
worm	蠕虫。可自我复制、自动传播的恶意软件
unknown	未知

D.14 恶意软件分析结果词汇 Malware Result Vocabulary

恶意软件分析结果描述恶意软件的分析结果信息，具体内容应符合表 D.14 的规定。

表 D.14 恶意软件分析结果词汇

词汇表总结	
malicious, suspicious, benign, unknown	
词汇表值	描述
malicious	恶意
suspicious	可疑
benign	非恶意
unknown	未知

D.15 处理器架构词汇 Processor Architecture Vocabulary

处理器架构描述恶意软件运行环境中涉及的处理器架构信息，具体内容应符合表 D.15 的规定。

表 D.15 处理器架构词汇

词汇表总结	
alpha, arm, ia-64, mips, risc-v, powerpc, sparc, x86, x86-64	
词汇表值	描述
alpha	Alpha 架构
arm	ARM 架构
ia-64	64 位 IA 架构
mips	MIPS 架构
risc-v	Risc V 架构
powerpc	PowerPC 架构
sparc	SPARC 架构
x86	32 位 x86 架构
x86-64	64 位 x86 架构

D.16 编程语言词汇 Implementation Language Vocabulary

编程语言描述用于实现恶意软件实例的语言信息，具体内容应符合表 D.16 的规定。

表 D.16 编程语言词汇

词汇表总结	
applescript, bash, c, c ⁺⁺ , c#, go, java, javascript, lua, objective-c, perl, php, powershell, python, ruby, scala, swift, typescript, visual-basic, x86-32, x86-64	
词汇表值	描述
applescript	AppleScript 程序语言
bash	Bash 程序语言
c	C 程序语言
c ⁺⁺	C ⁺⁺ 程序语言
c#	C# 程序语言
go	Go 程序语言
java	Java 程序语言
javascript	JavaScript 程序语言
lua	Lua 程序语言
objective-c	Objective-C 程序语言
perl	Perl 程序语言
php	PHP 程序语言
powershell	Windows Powershell 程序语言
python	Python 程序语言
ruby	Ruby 程序语言
scala	Scala 程序语言
swift	Swift 程序语言
typescript	TypeScript 程序语言
visual-basic	Visual Basic 程序语言
x86-32	x86 32 位汇编程序语言
x86-64	x86 64 位汇编程序语言

D.17 恶意软件能力词汇 Malware Capabilities Vocabulary

恶意软件能力描述恶意软件或家族所具备的能力信息,具体内容应符合表 D.17 的规定。

表 D.17 恶意软件能力词汇

词汇表总结	
accesses-remote-machines, anti-debugging, anti-disassembly, anti-emulation, anti-memory-forensics, anti-sandbox, anti-vm, captures-input-peripherals, captures-output-peripherals, captures-system-state-data, cleans-traces-of-infection, commits-fraud, communicates-with-c2, compromises-data-availability, compromises-data-integrity, compromises-system-availability, controls-local-machine, degrades-security-software, degrades-system-updates, determines-c2-server, emails-spam, escalates-privileges, evades-av, exfiltrates-data, fingerprints-host, hides-artifacts, hides-executing-code, infects-files, infects-remote-machines, installs-other-components, persists-after-system-reboot, prevents-artifact-access, prevents-artifact-deletion, probes-network-environment, self-modifies, steals-authentication-credentials, violates-system-operational-integrity	
词汇表值	描述
accesses-remote-machines	能访问一个或多个远程机器
anti-debugging	能防止被调试和/或在调试器中运行,或能增加其难度
anti-disassembly	能防止被反汇编或能增加其难度
anti-emulation	能防止其在模拟器中的执行,或能增加其难度
anti-memory-forensics	能防止内存取证,或能增加其难度
anti-sandbox	能防止基于沙箱的行为分析或能增加其难度
anti-vm	能防止基于虚拟机(VM)的行为分析或能增加其难度
captures-input-peripherals	能从系统的输入外设设备(如键盘或鼠标)捕获数据
captures-output-peripherals	能捕获发送到外设设备的数据
captures-system-state-data	能捕获关于系统状态的信息
cleans-traces-of-infection	能从系统中清理其感染的痕迹
commits-fraud	能实施欺诈行为
communicates-with-c2	能与命令和控制服务器进行通信
compromises-data-availability	能破坏其正在执行的本地系统上的数据可用性
compromises-data-integrity	能破坏其正在执行的系统上的数据完整性
compromises-system-availability	能消耗系统资源以实现其恶意目的,从而破坏系统的可用性
controls-local-machine	能控制其正在执行的机器
degrades-security-software	能绕过或禁用系统(包括移动设备)上的安全程序或操作系统安全功能
degrades-system-updates	能禁用系统更新和补丁的下载和安装
determines-c2-server	能确定一个或多个与其通信的命令和控制服务器
emails-spam	能发送垃圾邮件
escalates-privileges	能提升其正在执行的权限

表 D.17 恶意软件能力词汇 (续)

词汇表值	描述
evades-av	能逃避防病毒工具的检测
exfiltrates-data	能收集、整理数据并将其传输到外泄点
fingerprints-host	能对正在执行的主机系统的配置进行指纹识别或探测,以便根据此环境更改其行为
hides-artifacts	能隐藏其程序组件
hides-executing-code	能通过破坏引导程序、内核模块、虚拟机监视器等来隐藏其代码
infects-files	能感染其正在执行的系统上的一个或多个文件
infects-remote-machines	能自我传播到远程机器或用与自身不同的恶意软件感染远程机器
installs-other-components	能安装额外的组件
persists-after-system-reboot	能在其所在的系统重启后继续执行
prevents-artifact-access	能防止其组件(例如,文件、注册表项等)被访问
prevents-artifact-deletion	能防止其组件(例如,文件、注册表项等)被删除
probes-network-environment	能探测其网络环境的属性
self-modifies	能自修改
steals-authentication-credentials	能窃取认证凭证
violates-system-operational-integrity	能破坏其正在执行的系统/一个或多个远程系统的运行完整性

D.18 身份类别词汇 Identity Class Vocabulary

身份类别描述身份组件所代表的实体类型,具体内容应符合表 D.18 的规定。

表 D.18 身份类别词汇

词汇表总结	
individual, group, system, organization, class, unknown	
词汇表值	描述
individual	个人
group	团体
system	系统,指一类计算机系统,例如:SIEM(Security Information and Event Management,安全信息和事件管理)
organization	正式组织,例如:国家、公司等

表 D.18 身份类别词汇（续）

词汇表值	描述
class	某类实体,例如:所有医院、某团体成员或系统管理员等
unknown	未知

D.19 风险等级词汇 Risk Level Vocabulary

风险等级描述攻击活动风险等级的信息,具体内容应符合表 D.19 的规定。

表 D.19 风险等级词汇

词汇表总结	
critical,high,medium,low,minimal	
词汇表值	描述
critical	极高
high	高
medium	中
low	低
minimal	极低

D.20 地域词汇 Region Vocabulary

地域描述地理位置所处区域的信息,具体内容应符合表 D.20 的规定。

表 D.20 地域词汇

词汇表总结	
africa (eastern-africa, middle-africa, northern-africa, southern-africa, western-africa), americas (caribbean, central-america, latin-america-caribbean, northern-america, south-america), asia (central-asia, eastern-asia, southern-asia, south-eastern-asia, western-asia), europe (eastern-europe, northern-europe, southern-europe, western-europe), oceania (antarctica, australia-new-zealand, melanesia, micronesia, polynesia)	
词汇表值	描述
africa	非洲
eastern-africa	东非
middle-africa	中非
northern-africa	北非
southern-africa	南非

表 D.20 地域词汇（续）

词汇表值	描述
western-africa	西非
americas	美洲
caribbean	加勒比
central-america	中美洲
latin-america-caribbean	拉丁美洲-加勒比地区
northern-america	北美洲
south-america	南美洲
asia	亚洲
central-asia	中亚
eastern-asia	东亚
southern-asia	南亚
south-eastern-asia	东南亚
western-asia	西亚
europe	欧洲
eastern-europe	东欧
northern-europe	北欧
southern-europe	南欧
western-europe	西欧
oceania	大洋洲
antarctica	南极洲
australia-new-zealand	澳大利亚-新西兰群岛
melanesia	美拉尼西亚
micronesia	密克罗尼西亚
polynesia	波利尼西亚

D.21 杂凑算法词汇 Hashing Algorithm Vocabulary

杂凑算法描述常用的杂凑算法，具体内容应符合表 D.21 的规定。

表 D.21 杂凑算法词汇

词汇表总结	
MD5, SHA-1, SHA-256, SHA-512, SHA3-256, SHA3-512, SSDEEP, SM3, TLSH, OTHERS	
词汇表值	描述
MD5	MD5 消息摘要算法
SHA-1	SHA-1(安全杂凑算法 1)加密杂凑函数
SHA-256	SHA-256 加密杂凑函数(属于 SHA-2 算法族)
SHA-512	SHA-512 加密杂凑函数(属于 SHA-2 算法族)
SHA3-256	SHA3-256 加密杂凑函数
SHA3-512	SHA3-512 加密杂凑函数
SSDEEP	SSDEEP 模糊杂凑算法
SM3	SM3 密码杂凑算法
TLSH	TLSH 模糊杂凑算法
OTHERS	其他

D.22 加密算法词汇 Encryption Algorithm Enumeration

加密算法描述常用的加密算法,具体内容应符合表 D.22 的规定。

表 D.22 加密算法词汇

词汇表总结	
AES-128-GCM, AES-256-GCM, AES-128-CCM, AES-256-CCM, AES-128-OCB, AES-256-OCB, ChaCha20-Poly1305, RSA-OAEP, RSA-PSS, RSA-SHA256, SM1-ECB, SM1-CBC, SM2-1, SM2-2, SM2-3, SM4-ECB, SM4-CBC, SM4-CFB1, SM4-CFB8, SM4-CFB128, SM4-OFB, SM4-CTR, SM4-WRAP, SM4-GCM, SM4-OCB, SM4-XTS, SM4-FFX, SM7-ECB, SM7-CBC, SM7-CFB, SM7-OFB, SM9-1, SM9-2, SM9-3, SM9-4, ZUC, OTHERS	
词汇表值	描述
AES-128-GCM	AES-128-GCM 密码算法
AES-256-GCM	AES-256-GCM 密码算法
AES-128-CCM	AES-128-CCM 密码算法
AES-256-CCM	AES-256-CCM 密码算法
AES-128-OCB	AES-128-OCB 密码算法
AES-256-OCB	AES-256-OCB 密码算法
ChaCha20-Poly1305	ChaCha20-Poly1305 流密码算法

表 D.22 加密算法词汇 (续)

词汇表值	描述
RSA-OAEP	RSA-OAEP 加密算法
RSA-PSS	RSA-PSS 签名算法
RSA-SHA256	RSA-SHA256 签名算法
SM1-ECB	SM1 分组密码算法-电子码本模式
SM1-CBC	SM1 分组密码算法-密码块链模式
SM2-1	SM2 椭圆曲线公钥密码算法-数字签名算法
SM2-2	SM2 椭圆曲线公钥密码算法-密钥交换协议
SM2-3	SM2 椭圆曲线公钥密码算法-公钥加密算法
SM4-ECB	SM4 分组密码算法-电子码本模式
SM4-CBC	SM4 分组密码算法-密码块链模式
SM4-CFB1	SM4 分组密码算法-1 比特密码反馈模式
SM4-CFB8	SM4 分组密码算法-8 比特密码反馈模式
SM4-CFB128	SM4 分组密码算法-128 比特密码反馈模式
SM4-OFB	SM4 分组密码算法-输出反馈模式
SM4-CTR	SM4 分组密码算法-计数器模式
SM4-WRAP	SM4 分组密码算法-密钥封装模式
SM4-GCM	SM4 分组密码算法-伽罗瓦/计数器模式
SM4-OCB	SM4 分组密码算法-偏移码本模式
SM4-XTS	SM4 分组密码算法-全磁盘加密模式
SM4-FFX	SM4 分组密码算法-保留格式加密模式
SM7-ECB	SM7 分组密码算法-电子码本模式
SM7-CBC	SM7 分组密码算法-密码块链模式
SM7-CFB	SM7 分组密码算法-密码反馈模式
SM7-OFB	SM7 分组密码算法-输出反馈模式
SM9-1	SM9 标识密码算法-公钥加密算法
SM9-2	SM9 标识密码算法-数字签名算法
SM9-3	SM9 标识密码算法-密钥建立协议
SM9-4	SM9 标识密码算法-密钥封装算法
ZUC	祖冲之序列密码算法
OTHERS	其他

附 录 E
(资料性)
威胁信息封装和解析方式

威胁信息通常采用 Bundle 模式进行封装,该模式是一种将任意威胁信息组件内容打包在一起的包装机制,其目的为提升威胁信息的解析效率。Bundle 模式的描述见表 E.1,Bundle 示例见附录 H。

表 E.1 Bundle 模式描述表

名称	描述	格式	是否必填
id	标识号	string	是
type	类型	string	是。取值为“bundle”
spec_type	威胁信息标准类型	string	是。取值范围为“STIX”或“威胁信息国家标准”
spec_version	威胁信息标准版本信息	string	是。与上面威胁信息标准类型对应的版本信息。例如当标准类型为 STIX,取值为 2.0、2.1 或其他版本;当标准类型为威胁信息国家标准时,取值为 1.0 或者 2.0,其中 1.0 代表 2018 年发布的威胁信息国家标准,2.0 代表本文件
created	Bundle 创建时间	string	是
creator	Bundle 创建者	string	是
count	Bundle 集合中包含威胁信息组件的条目数	integer	否
objects	Bundle 集合中包含的组件	list of type object	否。object 是本文件定义的一个或多个组件

附录 F

(资料性)

威胁信息组件示例的 JSON 表示

F.1 可观测数据

```

{
  "type": "observed-data",
  "spec_version": "2.0",
  "id": "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf",
  "created": "2016-04-06T19:58:16.000Z",
  "modified": "2016-04-06T19:58:16.000Z",
  "first_observed": "2015-12-21T19:00:00Z",
  "last_observed": "2015-12-21T19:00:00Z",
  "number_observed": 50,
  "object_refs": [
    "ipv4-addr--efcd5e80-570d-4131-b213-62cb18eaa6a8",
    "domain-name--ecb120bf-2694-4902-a737-62b74539a41b"
  ]
}

{
  "type": "domain-name",
  "id": "domain-name--ecb120bf-2694-4902-a737-62b74539a41b",
  "value": "example.com",
  "resolves_to_refs": ["ipv4-addr--efcd5e80-570d-4131-b213-62cb18eaa6a8"]
}

{
  "type": "ipv4-addr",
  "id": "ipv4-addr--efcd5e80-570d-4131-b213-62cb18eaa6a8",
  "value": "198.51.100.3"
}

```

F.2 攻击指标

```

{
  "type": "indicator",
  "spec_version": "2.0",
  "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
  "created": "2016-04-06T20:03:48.000Z",

```

```
    "modified": "2016-04-06T20:03:48.000Z",
    "indicator_types": ["malicious-activity"],
    "name": "Poison Ivy Malware",
    "description": "This file is part of Poison Ivy",
    "pattern": "[ file:hashes.'SHA-256' = '4bac27393bdd9777ce02453256c5577cd02275510b22
27f473d03f533924f877' ]",
    "valid_from": "2016-01-01T00:00:00Z"
  }
```

F.3 攻击活动

```
{
  "type": "campaign",
  "spec_version": "2.0",
  "id": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
  "created": "2016-04-06T20:03:00.000Z",
  "modified": "2016-04-06T20:03:00.000Z",
  "name": "Green Group Attacks Against Finance",
  "risk": "high",
  "description": "Campaign by Green Group against a series of targets in the financial services
sector."
}
```

F.4 应对措施

```
{
  "type": "course-of-action",
  "spec_version": "2.0",
  "id": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
  "created": "2016-04-06T20:03:48.000Z",
  "modified": "2016-04-06T20:03:48.000Z",
  "name": "Add TCP port 80 Filter Rule to the existing Block UDP 1434 Filter",
  "description": "This is how to add a filter rule to block inbound access to TCP port 80 to the
existing UDP 1434 filter ..."
}
```

F.5 威胁主体

```
{
  "type": "threat-actor",
  "spec_version": "2.0",
  "id": "threat-actor--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
  "created": "2016-04-06T20:03:48.000Z",
  "modified": "2016-04-06T20:03:48.000Z",
}
```

```

    "threat_actor_types": [ "crime-syndicate"],
    "name": "Evil Org",
    "description": "The Evil Org threat actor group",
    "aliases": [ "Syndicate 1", "Evil Syndicate 99"],
    "roles": [ "director"],
    "goals": [ "Steal bank money", "Steal credit cards"],
    "sophistication": "advanced",
    "resource_level": "team",
    "primary_motivation": "organizational-gain"
  }

```

F.6 威胁目标

```

{
  "type": "threat-target",
  "spec_version": "2.0",
  "id": "threat-target--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
  "created": "2016-04-06T20:03:48.000Z",
  "modified": "2016-04-06T20:03:48.000Z",
  "name": "××证券机构公司",
  "description": "××证券是中国首批综合类券商之一,总部位于××省××市,专注于中国优质企业
及富裕人群,拥有行业领先创新能力的资本市场综合服务商。",
  "aliases": [ "××证券"]
}

```

F.7 攻击模式

```

{
  "type": "attack-pattern",
  "spec_version": "2.0",
  "id": "attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5",
  "created": "2016-05-12T08:17:27.000Z",
  "modified": "2016-05-12T08:17:27.000Z",
  "name": "Spear Phishing as Practiced by Adversary X",
  "description": "A particular form of spear phishing where the attacker claims that the target
had won a contest, including personal details, to get them to click on a link.",
  "external_references": [
    {
      "source_name": "capec",
      "external_id": "CAPEC-163"
    }
  ]
}

```

F.8 基础设施

“Poison Ivy C2”远控服务器及其 IP 地址为基础设施，恶意软件“Poison Ivy”使用其 IP 地址 198.51.100.3 和 198.52.200.4 进行远程控制。

```
{
  "type": "infrastructure",
  "spec_version": "2.0",
  "id": "infrastructure--38c47d93-d984-4fd9-b87b-d69d0841628d",
  "created": "2016-05-07T11:22:30.000Z",
  "modified": "2016-05-07T11:22:30.000Z",
  "name": "Poison Ivy C2",
  "infrastructure_types": ["command-and-control"]
},
{
  "type": "relationship",
  "spec_version": "2.0",
  "id": "relationship--7aebe2f0-28d6-48a2-9c3e-b0aaa60266ed",
  "created": "2016-05-09T08:17:27.000Z",
  "modified": "2016-05-09T08:17:27.000Z",
  "relationship_type": "controls",
  "source_ref": "infrastructure--38c47d93-d984-4fd9-b87b-d69d0841628d",
  "target_ref": "malware--16f4f3f9-1b68-4abb-bb66-7639d49f1e30"
},
{
  "type": "malware",
  "spec_version": "2.0",
  "id": "malware--16f4f3f9-1b68-4abb-bb66-7639d49f1e30",
  "created": "2016-05-08T14:31:09.000Z",
  "modified": "2016-05-08T14:31:09.000Z",
  "is_family": true,
  "malware_types": [
    "remote-access-trojan"
  ],
  "name": "Poison Ivy"
},
{
  "type": "relationship",
  "spec_version": "2.0",
  "id": "relationship--7aebe2f0-28d6-48a2-9c3e-b0aaa60266ef",
  "created": "2016-05-09T08:17:27.000Z",
  "modified": "2016-05-09T08:17:27.000Z",
```

```

    "relationship_type": "consists-of",
    "source_ref": "infrastructure--38c47d93-d984-4fd9-b87b-d69d0841628d",
    "target_ref": "ipv4-addr--b4e29b62-2053-47c4-bab4-bbce39e5ed67"
  },
  {
    "type": "relationship",
    "spec_version": "2.0",
    "id": "relationship--b82b2819-3b86-4bd5-afb3-fa36cfbc3f18",
    "created": "2016-05-09T08:17:27.000Z",
    "modified": "2016-05-09T08:17:27.000Z",
    "relationship_type": "consists-of",
    "source_ref": "infrastructure--38c47d93-d984-4fd9-b87b-d69d0841628d",
    "target_ref": "ipv4-addr--84445275-e371-444b-baea-ac7d07a180fd"
  },
  {
    "type": "ipv4-addr",
    "id": "ipv4-addr--b4e29b62-2053-47c4-bab4-bbce39e5ed67",
    "value": "198.51.100.3"
  },
  {
    "type": "ipv4-addr",
    "id": "ipv4-addr--84445275-e371-444b-baea-ac7d07a180fd",
    "value": "198.52.200.4"
  }
}

```

F.9 攻击活动集

```

{
  "type": "intrusion-set",
  "spec_version": "2.0",
  "id": "intrusion-set--4e78f46f-a023-4e5f-bc24-71b3ca22ec29",
  "created": "2016-04-06T20:03:48.000Z",
  "modified": "2016-04-06T20:03:48.000Z",
  "name": "Bobcat Breakin",
  "description": "Incidents usually feature a shared TTP of a bobcat being released within the building containing network access, scaring users to leave their computers without locking them first. Still determining where the threat actors are getting the bobcats.",
  "aliases": ["Zookeeper"],
  "goals": ["acquisition-theft", "harassment", "damage"]
}

```

F.10 恶意软件

恶意软件“Poison Ivy”使用 2 个 IP 地址为 198.51.100.3 和 198.52.200.4 的基础设施作为远控服务

器的示例。

```
{
  "type": "malware",
  "spec_version": "2.0",
  "id": "malware--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",
  "created": "2016-05-12T08:17:27.000Z",
  "modified": "2016-05-12T08:17:27.000Z",
  "name": "Cryptolocker",
  "description": "A variant of the cryptolocker family",
  "malware_types": ["ransomware"],
  "is_family": false
}
```

F.11 恶意软件分析结果

模拟了一个名为“Cuckoo Sandbox”的自动化沙箱对一个勒索软件样本进行深度分析的威胁信息表示。

```
{
  "type": "bundle",
  "id": "bundle--7a923456-e29b-41d4-a716-446655440001",
  "spec_type": "威胁信息国家标准",
  "spec_version": "2.0",
  "count": "3",
  "objects": [
    {
      "type": "malware-analysis",
      "spec_version": "2.0",
      "id": "malware-analysis--df7c3400-1234-41d4-a716-abcdef123456",
      "created": "2026-01-13T10:00:00.000Z",
      "modified": "2026-01-13T10:30:00.000Z",

      // --- 产品与引擎信息 ---
      "product": "Cuckoo Sandbox",
      "version": "2.0.7",
      "analysis_engine_version": "Cuckoo-Monitor-v1.4",
      "analysis_definition_version": "Community-Ruleset-2026-01-13",
      "configuration_version": "Anti-Ransomware-Profile-v4",
      "modules": ["network", "yara", "behavior", "screenshot", "memory_dump"],

      // --- 分析状态与结论 ---
      "submitted": "2026-01-13T09:45:00.000Z",
      "analysis_started": "2026-01-13T09:46:00.000Z",
    }
  ]
}
```

```

"analysis_ended": "2026-01-13T09:55:00.000Z",
"result_name": "WannaCry-Variant Behavioral Match",
"result": "malicious",

// --- 环境引用 (SCO Refs) ---
"sample_ref": "file--8e82c442-98fc-1c14-9afb-f4c8996fb924",
"host_vm_ref": "software--virtualbox-6-1",
"operating_system_ref": "software--windows-7-spl-x64",
"installed_software_refs": [
  "software--adobe-reader-11",
  "software--office-2010"
],

// --- 分析产出的可观测对象 (SCOs) ---
"analysis_sco_refs": [
  "ipv4-addr--1.2.3.4",
  "domain-name--ransom-c2-com",
  "windows-registry-key--run-key-entry"
],

// --- 元数据与外部文档 ---
"external_references": [
  {
    "source_name": "Cuckoo Internal Report",
    "description": "View the full dynamic analysis report in Cuckoo Dashboard.",
    "url": "https://cuckoo.local/analysis/45678/summary"
  }
],
"object_marking_refs": [
  "marking-definition--613f2e3d-d103-4646-81da-b8473d0a793d"
]
},

// --- 环境背景对象 ---
{
  "type": "software",
  "id": "software--virtualbox-6-1",
  "name": "Oracle VirtualBox",
  "version": "6.1.x"
},
{

```

```

    "type": "software",
    "id": "software--windows-7-spl-x64",
    "name": "Windows 7 Professional",
    "version": "Service Pack 1",
    "swid": "x64-platform"
  }
]
}

```

F.12 漏洞

```

{
  "type": "vulnerability",
  "spec_version": "2.0",
  "id": "vulnerability--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",
  "created": "2016-05-12T08:17:27.000Z",
  "modified": "2016-05-12T08:17:27.000Z",
  "name": "CVE-2016-1234",
  "external_references": [
    {
      "source_name": "cve",
      "external_id": "CVE-2016-1234"
    }
  ]
}

```

F.13 工具

```

{
  "type": "tool",
  "spec_version": "2.0",
  "id": "tool--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
  "created": "2016-04-06T20:03:48.000Z",
  "modified": "2016-04-06T20:03:48.000Z",
  "tool_types": [ "remote-access" ],
  "name": "VNC"
}

```

F.14 地理位置

```

{
  "type": "location",
  "spec_version": "2.0",
  "id": "location--a6e9345f-5a15-4c29-8bb3-7dcc5d168d64",

```

```

    "created": "2016-04-06T20:03:00.000Z",
    "modified": "2016-04-06T20:03:00.000Z",
    "region": "south-eastern-asia",
    "country": "xx",
    "administrative_area": "xxx",
    "postal_code": "63170"
  }

```

F.15 观点

```

{
  "type": "opinion",
  "spec_version": "2.0",
  "id": "opinion--b01efc25-77b4-4003-b18b-f6e24b5cd9f7",
  "created": "2016-05-12T08:17:27.000Z",
  "modified": "2016-05-12T08:17:27.000Z",
  "object_refs": ["campaign--16d2358f-3b0d-4c88-b047-0da2f7ed4471"],
  "opinion": "strongly-disagree",
  "explanation": "This doesn't seem like it is feasible. We've seen how PandaCat has attacked
xxx-country infrastructure over the last 3 years, so this change in targeting seems too great to be via-
ble. The methods used are more commonly associated with the FlameDragonCrew."
}

```

F.16 报告

```

{
  "type": "report",
  "spec_version": "2.0",
  "id": "report--84e4d88f-44ea-4bcd-bbf3-b2c1c320bcb3",
  "created": "2015-12-21T19:59:11.000Z",
  "modified": "2015-12-21T19:59:11.000Z",
  "name": "The Black Vine Cyberespionage Group",
  "description": "A simple report with an indicator and campaign",
  "published": "2016-01-20T17:00:00.000Z",
  "report_types": ["campaign"],
  "object_refs": [
    "indicator--26ffb872-1dd9-446e-b6f5-d58527e5b5d2",
    "campaign--83422c77-904c-4dc1-aff5-5c38f3a2c55c"
  ]
}

```

附 录 G
(资料性)
组件关系汇总

16 个组件之间的关系可细化为多种,常见关系见表 G.1。

表 G.1 组件关系汇总

序号	源组件	关系类型(中文/英文)	目标组件
1	攻击模式	投递/delivers	恶意软件
2	攻击模式	目标/targets	地理位置、漏洞
3	攻击模式	使用/uses	恶意软件、工具
4	攻击活动	归属/attributed-to	攻击活动集、威胁主体
5	攻击活动	攻陷/compromises	基础设施
6	攻击活动	来自/originates-from	地理位置
7	攻击活动	目标/targets	地理位置、漏洞
8	攻击活动	使用/uses	攻击模式、基础设施、恶意软件、工具
9	应对措施	调查/investigates	攻击指标
10	应对措施	缓解/mitigates	攻击模式、攻击指标、恶意软件、工具、漏洞
11	攻击指标	显示/indicates	攻击模式、攻击活动、基础设施、攻击活动集、恶意软件、威胁主体、工具
12	攻击指标	基于/based-on	可观测数据
13	基础设施	通信/communicates-with	基础设施,可观测数据中的 IP 地址、域名、URL
14	基础设施	包括/consists-of	基础设施、可观测数据
15	基础设施	控制/controls	基础设施、恶意软件
16	基础设施	投递/delivers	恶意软件
17	基础设施	具有/has	漏洞
18	基础设施	部署/hosts	工具、恶意软件
19	基础设施	位于/located-at	地理位置
20	基础设施	使用/uses	基础设施
21	基础设施	归属/attributed-to	威胁主体
22	基础设施	攻陷/compromises	基础设施
23	基础设施	部署/hosts,拥有/owns	基础设施

表 G.1 组件关系汇总 (续)

序号	源组件	关系类型(中文/英文)	目标组件
24	基础设施	来自/originates-from	地理位置
25	基础设施	目标/targets	地理位置、漏洞
26	基础设施	使用/Uses	攻击模式、基础设施、恶意软件、工具
27	恶意软件	被授权/authored-by	威胁主体、攻击活动集
28	恶意软件	回连/beacons-to, 回传/exfiltrate-to	基础设施
29	恶意软件	通信/communicates-with	可观测数据中的 IP 地址、域名、URL
30	恶意软件	控制/controls	恶意软件
31	恶意软件	下载/downloads, 释放/drops	恶意软件、工具、可观测数据中的文件
32	恶意软件	利用/exploits	漏洞
33	恶意软件	来自/originates-from	地理位置
34	恶意软件	目的/targets	基础设施、地理位置、漏洞
35	恶意软件	使用/uses	攻击模式、基础设施、恶意软件、工具
36	恶意软件	变种/variant-of	恶意软件
37	恶意软件分析结果	特征/characterizes	恶意软件
38	恶意软件分析结果	分析/analysis-of	恶意软件
39	恶意软件分析结果	静态分析/static-analysis-of	恶意软件
40	恶意软件分析结果	动态分析/dynamic-analysis-of	恶意软件
41	威胁主体	攻陷/compromises	基础设施
42	威胁主体	部署/hosts, 拥有/owns	基础设施
43	威胁主体	发起/initiate	攻击活动
44	威胁主体	位于/located-at	地理位置
45	威胁主体	目标/targets	地理位置、漏洞
46	威胁主体	使用/uses	攻击模式、基础设施、恶意软件、工具
47	工具	投递/delivers	恶意软件
48	工具	释放/drops	恶意软件
49	工具	拥有/has	漏洞
50	工具	目标/targets	基础设施、地理位置、漏洞

附 录 H

(资料性)

部分攻击场景下威胁信息描述示例

H.1 常用威胁信息使用的组件组合

常用的威胁信息使用的组件组合见表 H.1。

表 H.1 常用的威胁信息使用的组件组合

序号	威胁信息类型	组件
1	IP 类	攻击指标、可观测数据中 IP 地址子组件
2	域名类	攻击指标、可观测数据中域名信息子组件
3	漏洞类	漏洞组件、可观察对象中的软件子组件
4	恶意软件类	1. 恶意软件的一次攻击行为:攻击指标、攻击活动 2. 恶意软件的样本信息:恶意软件、可观测数据 3. 恶意软件的沙箱分析结果:恶意软件分析结果、可观测数据
5	安全事件类	攻击活动、攻击指标、可观测数据
6	APT 类	威胁主体、威胁目标、攻击指标、攻击活动、攻击模式、攻击活动集

H.2 关于 wannacry 事件的检测示例

本示例为一次 wannacry 攻击活动的描述示例,构建的威胁信息组件之间的关系如图 H.1 所示。

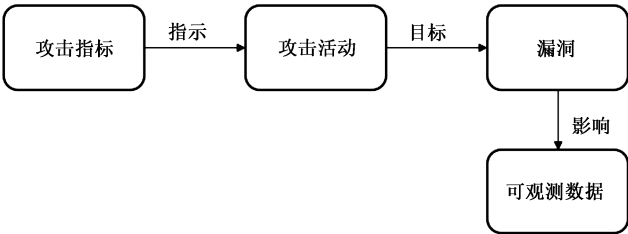


图 H.1 wannacry 事件示例

JSON 格式示例如下。

```
{
  "id": "bundle--3a1bcbb1-540b-4609-b1d2-684e7123ab1f",
  "type": "bundle",
  "spec_type": "威胁信息国家标准",
  "spec_version": "2.0",
  "count": "7",
  "objects": [
```

```

{
  "type": "indicator",
  "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
  "spec_version": "2.0",
  "created": "2016-04-06T20:03:48.000Z",
  "modified": "2016-04-06T20:03:48.000Z",
  "indicator_types": ["malicious-activity"],
  "name": "wannacry 相关的攻击指标",
  "description": "这是关于 wannacry 事件检测的攻击指标",
  "pattern": "[ file:hashes.'SHA-256' = 'ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa' ]",
  "valid_from": "2017-05-13T00:00:00Z"
},
{
  "type": "campaign",
  "id": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
  "spec_version": "2.0",
  "created": "2017-05-13T00:00:00Z ",
  "modified": "2017-05-13T00:00:00Z ",
  "name": "wannacry 勒索事件",
  "risk": "critical",
  "description": "北京时间 5 月 12 日,大量企业和教育机构的网站感染了 wannacry 勒索病毒,导致系统宕机。该勒索病毒对系统内的文件进行加密,当用户支付赎金之后才能获取口令恢复文件。同时,亚洲、欧洲等地的一些高等教育机构也受到了影响"
},
{
  "type": "vulnerability",
  "spec_version": "2.0",
  "id": "vulnerability--4a1bcbb1-540b-4609-b1d2-684e7123ab1f",
  "created": "2017-3-14T00:00:00Z",
  "modified": "2017-8-16T00:00:00Z",
  "name": "Microsoft Windows SMB 输入验证错误漏洞",
  "description": "Windows 是一套个人设备使用的操作系统。Windows Server 是一套服务器操作系统。Server Message Block(SMB)Server 是其中的一个为计算机提供身份验证用以访问服务器上打印机和文件系统的组件。Windows 中的 SMBv1 服务器存在远程代码执行漏洞。远程攻击者可借助特制的数据包利用该漏洞执行任意代码。以下版本受到影响:Windows Vista SP2,Windows Server 2008 SP2 和 R2 SP1,Windows 7 SP1,Windows 8.1,Windows Server 2012 Gold 和 R2,Windows RT 8.1,Windows 10 Gold,1511 和 1607,Windows Server 2016。"
  "external_references": [
    {
      "source_name": "cve",

```

```

        "external_id": "CVE-2017-0143",
        "url": "https://cve.mitre.org/cgi-bin/cvename.cgi? name=CVE-2017-0143"
    }
]
},
{
    "type": "software",
    "spec_version": "2.0",
    "id": "software--5a1bcbb1-540b-4609-b1d2-684e7123ab1f",
    "name": "windows SMB",
    "version": "1.0"
},
{
    "type": "relationship",
    "spec_version": "2.0",
    "id": "relationship--7a1bcbb1-540b-4609-b1d2-684e7123ab1f",
    "created": "2017-3-14T00:00:00Z",
    "modified": "2017-3-14T00:00:00Z",
    "relationship_type": "targets",
    "source_ref": "vulnerability--4a1bcbb1-540b-4609-b1d2-684e7123ab1f",
    "target_ref": "software--5a1bcbb1-540b-4609-b1d2-684e7123ab1f"
},
{
    "type": "relationship",
    "spec_version": "2.0",
    "id": "relationship--53a55c73-f2c8-47b9-8e50-ae34d8c5da4d",
    "created": "2017-05-13T00:00:00Z",
    "modified": "2017-05-13T00:00:00Z ",
    "relationship_type": "indicates",
    "source_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "target_ref": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f "
},
{
    "type": "relationship",
    "spec_version": "2.0",
    "id": "relationship--54a55c73-f2c8-47b9-8e50-ae34d8c5da4d",
    "created": "2017-05-13T00:00:00Z",
    "modified": "2017-05-13T00:00:00Z ",
    "relationship_type": "targets",
    "source_ref": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "target_ref": "vulnerability--4a1bcbb1-540b-4609-b1d2-684e7123ab1f "
}

```

```
}  
]  
}
```

H.3 一个 APT 组织的一组攻击活动的示例

本示例为某 APT 组织的攻击活动集合使用威胁信息格式描述的示例。此 APT 组织由“A”国家资助,他们的目标是“B”国家的某组织 BPP。该入侵活动由针对 BPP 网站的几个复杂活动和攻击模式组成。一个活动试图在 BPP 的网页中插入虚假信息,而另一个活动则是针对 BPP Web 服务器的 DDoS 攻击。基于掌握的威胁信息组件集合,构建的威胁信息组件之间的关系如图 H.2 所示。

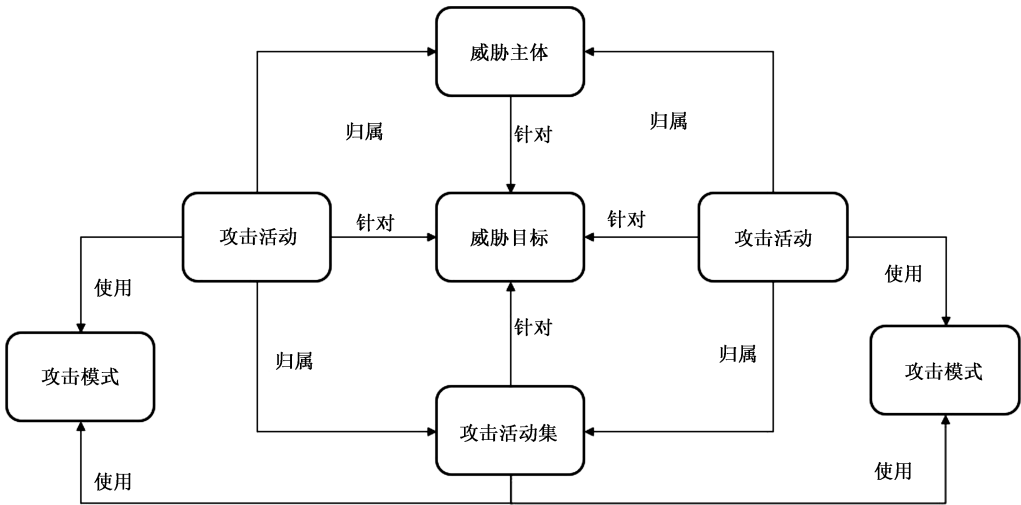


图 H.2 APT 攻击示例

JSON 格式示例如下。

```
{  
  "type": "bundle",  
  "id": "bundle-97b40f76-c1b8-4407-b050-ff177f3d67ed",  
  "spec_type": "威胁信息国家标准",  
  "spec_version": "2.0",  
  "created": "2016-08-09T15:50:10.983Z ",  
  "creator": "××公司",  
  "count": "25",  
  "objects": [  
    {  
      "type": "threat-actor",  
      "spec_version": "2.0",  
      "id": "threat-actor-56f3f0db-b5d5-431c-ae56-c18f02caf500",  
      "created": "2016-08-08T15:50:10.983Z",  
      "modified": "2016-08-08T15:50:10.983Z",  
      "name": "A 国××组织 ",  
      "threat_actor_types": [  

```

```

        "nation-state"
    ],
    "roles": [
        "director"
    ],
    "goals": [
        "Influence the election in xxx country"
    ],
    "sophistication": "strategic",
    "resource_level": "government",
    "primary_motivation": "ideology",
    "secondary_motivations": [
        "dominance"
    ]
},
{
    "type": "threat-target",
    "id": "threat-target--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "spec_version": "2.0",
    "created": "2016-04-06T20:03:48.000Z",
    "modified": "2016-04-06T20:03:48.000Z",
    "name": "B 国的某组织(BPP)",
    "description": " B 国的某组织(BPP),专注于 B 国优质企业及富裕人群,拥有行业领先创新能力的资本市场综合服务商。",
    "identity_class": "organization",
    "external_references": [
        {
            "source_name": "website",
            "url": "http://www.bpp.bn"
        }
    ]
},
{
    "type": "attack-pattern",
    "spec_version": "2.0",
    "id": "attack-pattern--19da6e1c-71ab-4c2f-886d-d620d09d3b5a",
    "created": "2016-08-08T15:50:10.983Z",
    "modified": "2017-01-30T21:15:04.127Z",
    "name": "Content Spoofing",
    "external_references": [
        {

```

```

        "source_name": "capec",
        "url": "https://capec.mitre.org/data/definitions/148.html",
        "external_id": "CAPEC-148"
    }
]
},
{
    "type": "attack-pattern",
    "spec_version": "2.0",
    "id": "attack-pattern--f6050ea6-a9a3-4524-93ed-c27858d6cb3c",
    "created": "2016-08-08T15:50:10.983Z",
    "modified": "2017-01-30T21:15:04.127Z",
    "name": "HTTP Flood",
    "external_references": [
        {
            "source_name": "capec",
            "url": "https://capec.mitre.org/data/definitions/488.html",
            "external_id": "CAPEC-488"
        }
    ]
},
{
    "type": "campaign",
    "spec_version": "2.0",
    "id": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
    "created": "2016-08-08T15:50:10.983Z",
    "modified": "2016-08-08T15:50:10.983Z",
    "name": "Operation Bran Flakes",
    "description": "A concerted effort to insert false information into the BPP's web pages.",
    "aliases": [
        "OBF"
    ],
    "first_seen": "2016-01-08T12:50:40.123Z",
    "objective": "Hack www.bpp.bn"
},
{
    "type": "campaign",
    "spec_version": "2.0",
    "id": "campaign--1d8897a7-fdc2-4e59-afc9-becbe04df727",
    "created": "2016-08-08T15:50:10.983Z",
    "modified": "2016-08-08T15:50:10.983Z",

```

```

    "name": "Operation Raisin Bran",
    "description": "A DDOS campaign to flood BPP web servers.",
    "aliases": [
        "ORB"
    ],
    "first_seen": "2016-02-07T19:45:32.126Z",
    "objective": "Flood www.bpp.bn"
},
{
    "type": "intrusion-set",
    "spec_version": "2.0",
    "id": "intrusion-set--ed69450a-f067-4b51-9ba2-c4616b9a6713",
    "created": "2016-08-08T15:50:10.983Z",
    "modified": "2016-08-08T15:50:10.983Z",
    "name": "APT BPP",
    "description": "An advanced persistent threat that seeks to disrupt the xx country's election
with multiple attacks.",
    "aliases": [
        "Bran-teaser"
    ],
    "first_seen": "2016-01-08T12:50:40.123Z",
    "goals": [
        "Influence the xx country's election",
        "Disrupt the BPP"
    ],
    "resource_level": "government",
    "primary_motivation": "ideology",
    "secondary_motivations": [
        "dominance"
    ]
},
{
    "type": "relationship",
    "spec_version": "2.0",
    "id": "relationship--98765000-efdf-4a86-8681-36481ceae57f",
    "created": "2020-02-29T17:41:44.938Z",
    "modified": "2020-02-29T17:41:44.938Z",
    "relationship_type": "attributed-to",
    "source_ref": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
    "target_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
},

```

```

{
  "type": "relationship",
  "spec_version": "2.0",
  "id": "relationship--53a55c73-f2c8-47b9-8e50-ae34d8c5da4d",
  "created": "2020-02-29T17:41:44.938Z",
  "modified": "2020-02-29T17:41:44.938Z",
  "relationship_type": "attributed-to",
  "source_ref": "campaign--1d8897a7-fdc2-4e59-afc9-becbe04df727",
  "target_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
},
{
  "type": "relationship",
  "spec_version": "2.0",
  "id": "relationship--5047c2c0-524b-4afd-9cd6-e197efe59495",
  "created": "2020-02-29T17:41:44.939Z",
  "modified": "2020-02-29T17:41:44.939Z",
  "relationship_type": "attributed-to",
  "source_ref": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
  "target_ref": "intrusion-set--ed69450a-f067-4b51-9ba2-c4616b9a6713"
},
{
  "type": "relationship",
  "spec_version": "2.0",
  "id": "relationship--9cc131ca-b64d-4ab1-a300-5e4a0073280a",
  "created": "2020-02-29T17:41:44.939Z",
  "modified": "2020-02-29T17:41:44.939Z",
  "relationship_type": "attributed-to",
  "source_ref": "campaign--1d8897a7-fdc2-4e59-afc9-becbe04df727",
  "target_ref": "intrusion-set--ed69450a-f067-4b51-9ba2-c4616b9a6713"
},
{
  "type": "relationship",
  "spec_version": "2.0",
  "id": "relationship--c171fd27-2a8a-42b7-8293-34016b70c1c8",
  "created": "2020-02-29T17:41:44.939Z",
  "modified": "2020-02-29T17:41:44.939Z",
  "relationship_type": "attributed-to",
  "source_ref": "intrusion-set--ed69450a-f067-4b51-9ba2-c4616b9a6713",
  "target_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
},
{

```

```

    "type": "relationship",
    "spec_version": "2.0",
    "id": "relationship--554e3341-d7b1-4b3c-a522-28ef52fbb49b",
    "created": "2020-02-29T17:41:44.939Z",
    "modified": "2020-02-29T17:41:44.939Z",
    "relationship_type": "targets",
    "source_ref": "intrusion-set--ed69450a-f067-4b51-9ba2-c4616b9a6713",
    "target_ref": "identity--ddfe7140-2ba4-48e4-b19a-df069432103b"
  },
  {
    "type": "relationship",
    "spec_version": "2.0",
    "id": "relationship--06964095-5750-41fe-a9af-6c6a9d995489",
    "created": "2020-02-29T17:41:44.940Z",
    "modified": "2020-02-29T17:41:44.940Z",
    "relationship_type": "uses",
    "source_ref": "intrusion-set--ed69450a-f067-4b51-9ba2-c4616b9a6713",
    "target_ref": "attack-pattern--19da6e1c-71ab-4c2f-886d-d620d09d3b5a"
  },
  {
    "type": "relationship",
    "spec_version": "2.0",
    "id": "relationship--4fe5dab1-fd6d-41aa-b8b1-d3118a708284",
    "created": "2020-02-29T17:41:44.940Z",
    "modified": "2020-02-29T17:41:44.940Z",
    "relationship_type": "uses",
    "source_ref": "intrusion-set--ed69450a-f067-4b51-9ba2-c4616b9a6713",
    "target_ref": "attack-pattern--f6050ea6-a9a3-4524-93ed-c27858d6cb3c"
  },
  {
    "type": "relationship",
    "spec_version": "2.0",
    "id": "relationship--d8b7932d-0ecb-4891-b021-c78ff2b63747",
    "created": "2020-02-29T17:41:44.940Z",
    "modified": "2020-02-29T17:41:44.940Z",
    "relationship_type": "targets",
    "source_ref": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
    "target_ref": "identity--ddfe7140-2ba4-48e4-b19a-df069432103b"
  },
  {
    "type": "relationship",

```

```

    "spec_version": "2.0",
    "id": "relationship--96cfbc6f-5c08-4372-b811-b90fbb2ec180",
    "created": "2020-02-29T17:41:44.940Z",
    "modified": "2020-02-29T17:41:44.940Z",
    "relationship_type": "targets",
    "source_ref": "campaign--1d8897a7-fdc2-4e59-afc9-bebbe04df727",
    "target_ref": "identity--ddfe7140-2ba4-48e4-b19a-df069432103b"
  },
  {
    "type": "relationship",
    "spec_version": "2.0",
    "id": "relationship--33c22977-d104-45d8-be19-273f7ab03de1",
    "created": "2020-02-29T17:41:44.940Z",
    "modified": "2020-02-29T17:41:44.940Z",
    "relationship_type": "uses",
    "source_ref": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
    "target_ref": "attack-pattern--19da6e1c-71ab-4c2f-886d-d620d09d3b5a"
  },
  {
    "type": "relationship",
    "spec_version": "2.0",
    "id": "relationship--8848cba9-4c7b-4695-bc09-5033a6f20ff4",
    "created": "2020-02-29T17:41:44.941Z",
    "modified": "2020-02-29T17:41:44.941Z",
    "relationship_type": "uses",
    "source_ref": "campaign--1d8897a7-fdc2-4e59-afc9-bebbe04df727",
    "target_ref": "attack-pattern--f6050ea6-a9a3-4524-93ed-c27858d6cb3c"
  },
  {
    "type": "relationship",
    "spec_version": "2.0",
    "id": "relationship--a97b3ea5-4ca1-46a0-a7ad-f10143ce22b2",
    "created": "2020-02-29T17:41:44.941Z",
    "modified": "2020-02-29T17:41:44.941Z",
    "relationship_type": "impersonates",
    "source_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500",
    "target_ref": "identity--ddfe7140-2ba4-48e4-b19a-df069432103b"
  },
  {
    "type": "relationship",
    "spec_version": "2.0",

```

```

    "id": "relationship--4292a6df-fb16-43d1-805d-dc1b33946fdf",
    "created": "2020-02-29T17:41:44.941Z",
    "modified": "2020-02-29T17:41:44.941Z",
    "relationship_type": "targets",
    "source_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500",
    "target_ref": "identity--ddfe7140-2ba4-48e4-b19a-df069432103b"
  },
  {
    "type": "relationship",
    "spec_version": "2.0",
    "id": "relationship--4bd67b9e-d112-4ea6-98bb-080a051667c7",
    "created": "2020-02-29T17:41:44.941Z",
    "modified": "2020-02-29T17:41:44.941Z",
    "relationship_type": "attributed-to",
    "source_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500",
    "target_ref": "identity--8c6af861-7b20-41ef-9b59-6344fd872a8f"
  },
  {
    "type": "relationship",
    "spec_version": "2.0",
    "id": "relationship--1f4ee02a-7f6e-45a6-aedd-c1492af5e179",
    "created": "2020-02-29T17:41:44.942Z",
    "modified": "2020-02-29T17:41:44.942Z",
    "relationship_type": "targets",
    "source_ref": "campaign--1d8897a7-fdc2-4e59-afc9-becbe04df727",
    "target_ref": "identity--ddfe7140-2ba4-48e4-b19a-df069432103b"
  },
  {
    "type": "relationship",
    "spec_version": "2.0",
    "id": "relationship--ba30893a-400a-43f3-b193-69d65d2a8f40",
    "created": "2020-02-29T17:41:44.942Z",
    "modified": "2020-02-29T17:41:44.942Z",
    "relationship_type": "uses",
    "source_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500",
    "target_ref": "attack-pattern--19da6e1c-71ab-4c2f-886d-d620d09d3b5a"
  },
  {
    "type": "relationship",
    "spec_version": "2.0",
    "id": "relationship--70880ead-0b19-4785-be52-a69064d4cb6c",

```

```
    "created": "2020-02-29T17:41:44.942Z",
    "modified": "2020-02-29T17:41:44.942Z",
    "relationship_type": "uses",
    "source_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500",
    "target_ref": "attack-pattern--f6050ea6-a9a3-4524-93ed-c27858d6cb3c"
  }
]
}
```

从以上威胁信息分析其攻击路径如图 H.3 所示。

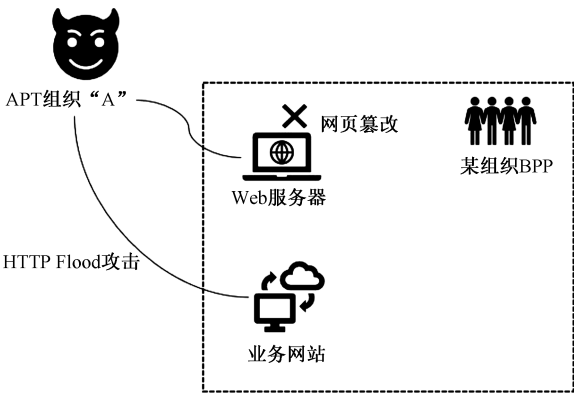


图 H.3 攻击路径示意图

附 录 I

(资料性)

表达式计算示例

下面给出多个表达式计算示例,以帮助理解附录 B 中规范的表达式。

- a) 匹配具有 SHA-256 杂凑的文件:
`[file:hashes:SHA-256 = 'aec070645fe53ee3b3763059376134f058cc337247c978add178b6ccdfb0019f']`
- b) 使用正则表达式将电子邮件与特定发件人电子邮件地址和附件文件名匹配:
`[email-message:from_ref.value MATCHES '.+\\@example\\.com$' AND email-message:body_multipart[*].body_raw_ref.name MATCHES '~Final Report.+\\.exe$']`
- c) 匹配具有 SHA-256 杂凑和 PDF MIME 类型的文件:
`[file:hashes:SHA-256 = 'aec070645fe53ee3b3763059376134f058cc337247c978add178b6ccdfb0019f' AND file:mime_type = 'application/x-pdf']`
- d) 匹配具有 SHA-256 或 SM3 杂凑值的文件,以及具有不同 SHA-256 杂凑值的不同文件:
`[file:hashes:SHA-256 = 'bf07a7fbb825fc0aae7bf4a1177b2b31fcf8a3feef7092761e18c859ee52a9c' OR file:hashes:SM3 = '66c7f0f462eedd9d1f2d46bdc10e4e24167c4875cf2f2b18c7a8578d2e751' AND [file:hashes:SHA-256 = 'aec070645fe53ee3b3763059376134f058cc337247c978add178b6ccdfb0019f']`
- e) 用 SM3 杂凑匹配一个文件,然后在 5 min 内匹配一个与某个值匹配的注册表信息子组件:
`([file:hashes:SM3 = '66c7f0f462eedd9d1f2d46bdc10e4e24167c4875cf2f2b18c7a8578d2e751'] FOLLOWEDBY [windows-registry-key:key = 'HKEY_LOCAL_MACHINE\\foo\\bar']) WITHIN 300 SECONDS`
- f) 匹配三个不同但特定的 Unix 用户账户:
`[user-account:account_type = 'unix' AND user-account:user_id = '1007' AND user-account:account_login = 'Peter'] AND [user-account:account_type = 'unix' AND user-account:user_id = '1008' AND user-account:account_login = 'Paul'] AND [user-account:account_type = 'unix' AND user-account:user_id = '1009' AND user-account:account_login = 'Mary']`
- g) 匹配字节片段信息子组件 PCAP 载荷头:
`[artifact:mime_type = 'application/vnd.tcpdump.pcap' AND artifact:payload_bin MATCHES '\\xd4\\xc3\\xb2\\xa1\\x02\\x00\\x04\\x00']`
- h) 匹配文件信息子组件与 Windows 文件路径:
`[file:name = 'foo.dll' AND file:parent_directory_ref.path = 'C:\\Windows\\System32']`
- i) Windows PE 文件的高值熵匹配:
`[file:extensions:windows-pebinary-ext.sections[*].entropy > 7.0]`
- j) 文件信息子组件 magic number 和 mime 类型不匹配时的匹配:
`[file:mime_type = 'image/bmp' AND file:magic_number_hex = hffd8']`
- k) 将网络流量与特定目标进行匹配:
`[network-traffic:dst_ref.type = 'ipv4-addr' AND network-traffic:dst_ref.value = '203.0.113.33/32']`
- l) 将恶意软件通信流量与域名进行匹配:

- [network-traffic:dst_ref.type = 'domain-name' AND network-traffic:dst_ref.value = 'example.com'] REPEATS 5 TIMES WITHIN 1 800 SECONDS
- m) 匹配 IPv4 解析的域名:
[domain-name:value = 'www.5z8.info' AND domain-name:resolves_to_refs[*].value = '198.51.100.1/32']
- n) URL 上的匹配:
[url:value = 'http://example.com/foo' OR url:value = 'http://example.com/bar']
- o) X509 证书上的匹配:
[x509-certificate:issuer = 'CN=WEBMAIL' AND x509-certificate:serial_number = '4c:0b:1d:19:74:86:a7:66:b4:1a:bf:40:27:21:76:28']
- p) 在 Windows 注册表项上匹配:
[windows-registry-key:key = 'HKEY_CURRENT_USER\\Software\\CryptoLocker\\Files' OR windows-registry-key:key = 'HKEY_CURRENT_USER\\Software\\Microsoft\\CurrentVersion\\Run\\CryptoLocker_0388']
- q) 在具有一组属性的文件上匹配:
[(file:name = 'pdf.exe' OR file:size = 371712) AND file:created = t'2014-01-13T07:03:17Z']
- r) 在电子邮件中匹配特定发件人和主题:
[email-message:sender_ref.value = 'jdoe@example.com' AND email-message:subject = 'Conference Info']
- s) 在自定义 USB 设备上匹配:
[x-usb-device:usbdrive.serial_number = '575833314133343231313937']
- t) 在特定时间窗口内使用一组特定的命令行参数启动的两个进程进行匹配:
[process:command_line MATCHES '^.+>-add GlobalSign.cer -c -s -r localMachine Root \$'] FOLLOWEDBY [process:command_line MATCHES '^.+>-add GlobalSign.cer -c -s -r localMachineTrustedPublisher \$'] WITHIN 300 SECONDS
- u) 匹配属于特定子网的网络流量 IP:
[network-traffic:dst_ref.value ISSUBSET '2001:0db8:dead:beef:0000:0000:0000:0000/64']
- v) 匹配恶意软件字节流的几种不同组合:
([file:name = 'foo.dll'] AND [windows-registry-key:key = 'HKEY_LOCAL_MACHINE\\foo\\bar']) OR [process:image_ref.name = 'fooproc' OR process:image_ref.name = 'procfoo']
- w) 匹配特定 IP 的特定端口回连流量:
[ipv4-addr:value = '192.168.1.1' AND network-traffic:dst_port = 12345]

参 考 文 献

- [1] GB/T 28517 网络安全事件描述和交换格式
 - [2] GB/T 30279 信息安全技术 网络安全漏洞分类分级指南
 - [3] GB/T 36643—2018 信息安全技术 网络安全威胁信息格式规范
 - [4] GB/T 37027 网络安全技术 网络攻击和网络攻击事件判定准则
 - [5] GB/T 44886.1—2024 网络安全技术 网络安全产品互联互通 第1部分:框架
 - [6] GB/T 44886.3 网络安全技术 网络安全产品互联互通 第3部分:告警信息格式
 - [7] GB/T 44886.5 网络安全技术 网络安全产品互联互通 第5部分:行为信息格式
 - [8] ECMA-404:2017, *The JSON Data Interchange Syntax*, 2nd Edition, ECMA International, December 2017
 - [9] OASIS. STIX™ Version 2.1. OASIS Standard. 28 June 2021. [Online]. Available: <https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html>
-

