ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36643—2018

信息安全技术
网络安全威胁信息格式规范

Information security technology—Cyber security threat information format

2018-10-10 发布　　2019-05-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国电子技术标准化研究院、北京赛西科技发展有限责任公司、北京天际友盟信息技术有限公司、北京奇安信科技有限公司、中国科学院信息工程研究所、公安部第三研究所、中国信息安全测评中心、国家计算机网络应急技术处理协调中心、中电长城网际系统应用有限公司、中国电子科技网络信息安全有限公司、阿里巴巴(北京)软件服务有限公司、百度在线网络技术(北京)有限公司、北京神州绿盟信息安全科技股份有限公司、北京启明星辰信息安全技术有限公司、神州网云(北京)信息技术有限公司、远江盛邦(北京)网络安全科技股份有限公司、北京君源创投投资管理有限公司、北京派网软件有限公司、深信服科技股份有限公司、中国科学院软件研究所、北京天融信网络安全技术有限公司、腾讯云计算(北京)有限责任公司、上海交通大学、北京工业大学、西安电子科技大学、北京邮电大学、北京中电普华信息技术有限公司、中国人民公安大学、武汉大学。

本标准主要起草人:蔡磊、叶润国、杨建军、刘贤刚、范科峰、闵京华、鲍旭华、刘威歆、冯侦探、金湘宇、董晓康、杨大路、杨泽明、李克鹏、李强、宋超、孙薇、贺新朋、李宗洋、孙波、梁露露、宋好好、王惠莅、刘慧晶、孙成胜、权晓文、李建华、雷晓锋、裴庆祺、易锦、刘玉岭、李衍、史博、孙朝晖、周毅、邹荣新、曾志峰、叶建伟、杨震、马占宇、翟湛鹏、曹占峰、姜政伟、杜彦辉、王丽娜。

引　言

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，并提升整体的网络安全防护效率。

网络安全威胁信息的共享和利用是实现关键信息基础设施安全防护的重要环节，有利于实现跨组织的网络安全威胁信息的快速传递，进而实现对复杂网络安全威胁的及时发现和快速响应。

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，因此它在推动网络安全威胁信息技术发展和产业化应用方面具有重要意义。

信息安全技术
网络安全威胁信息格式规范

1 范围

本标准规定了网络安全威胁信息模型和网络安全威胁信息组件，包括网络安全威胁信息中各组件的属性和属性值格式等信息。

本标准适用于网络安全威胁信息供方和需方之间进行网络安全威胁信息的生成、共享和使用，网络安全威胁信息共享平台的建设和运营可参考使用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 18336.1—2015 信息技术 安全技术 信息技术安全评估准则 第1部分：简介和一般模型

GB/T 20274.1—2006 信息安全技术 信息系统安全保障评估框架 第1部分：简介和一般模型

GB/T 25069—2010 信息安全技术 术语

GB/T 28458—2012 信息安全技术 安全漏洞标识与描述规范

3 术语和定义

GB/T 18336.1—2015、GB/T 20274.1—2006 和 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

网络安全/网络空间安全 cyber security

在网络空间中对信息保密性、完整性和可用性的保持。

[ISO/IEC 27032:2012，定义 4.20]

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原由。

[GB/T 29246—2017，定义 2.83]。

3.3

威胁信息 threat information

一种基于证据的知识，用于描述现有或可能出现的威胁，从而实现对威胁的响应和预防。

注：威胁信息包括上下文、攻击机制、攻击指标、可能影响等信息。

3.4

脆弱性 vulnerability

可能被一个或多个威胁利用的资产或控制的弱点。

[GB/T 29246—2017，定义 2.89]