ICS 35.040
L 80

中华人民共和国国家标准

GB/T 37027—2018

信息安全技术　网络攻击定义及描述规范

Information security technology—Specifications of definition and description for network attack

2018-12-28 发布　　2019-07-01 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:北京大学软件与微电子学院、中国电子技术标准化研究院、中国科学院软件研究所、中国科学院信息工程研究所、上海众人网络安全技术有限公司、蓝盾信息安全技术有限公司、北京永信至诚科技股份有限公司、北京奇安信科技有限公司、国家计算机网络与信息安全管理中心、北京神州绿盟信息安全科技股份有限公司、国云科技股份有限公司、北京时代新威信息技术有限公司、启明星辰信息技术集团股份有限公司、贵州省公共大数据重点实验室、海南大学信息科学技术学院、重庆邮电大学网络空间安全与信息法学院、沈阳东软系统集成有限公司、阿里云计算有限公司、北京天际友盟信息技术有限公司、北京天融信网络安全技术有限公司、新华三技术有限公司、黑龙江省网络空间研究中心、百度在线网络技术(北京)有限公司、北京鼎普科技股份有限公司。

本标准主要起草人:卿斯汉、刘贤刚、叶润国、胡影、王利明、谈剑峰、鲍旭华、蔡晶晶、季统凯、李雪莹、徐震、吴汉炜、周由胜、陈驰、张大江、吕志泉、严寒冰、杨辰钟、韩炜、李佳、杨大路、翟湛鹏、罗锋盈、王新杰、彭长根、马杰、路娜、孙建坡、李文瑾、陈景妹、谢安明、徐雨晴、王希忠、方舟、王海洋、周启明、沈晴霓、文伟平、张泉、孙松儿、吴槟、姜伟鹏。

引　言

近年来，随着网络应用的普及和迅猛发展，网络攻击也日渐增多，攻击的方法更加先进和复杂，攻击的形式更是多种多样，无孔不入，对网络安全造成了严重威胁。

网络攻击涉及多方面的问题，包括网络攻击的界定、网络攻击涉及的角色、网络攻击的目的、网络攻击的分级和分类、网络攻击的过程、网络攻击的关键技术、网络攻击常用的方法、网络攻击后果的评估等内容。面对网络攻击各个层面的挑战，对网络攻击进行准确的定义和描述，增强网络安全保障，为抵御网络攻击夯实基础。

信息安全技术　网络攻击定义及描述规范

1　范围

本标准界定了网络攻击的定义、属性特征和多维度描述方法。

本标准适用于网络运营者进行网络建设、运维和管理时对安全的设计与评估。

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 5271.8—2001　信息技术　词汇　第8部分：安全

GB/T 7408—2005　数据元和交换格式　信息交换　日期和时间表示法

GB/T 25068.3—2010　信息技术　安全技术　IT网络安全　第3部分：使用安全网关的网间通信安全保护

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 5271.8—2001、GB/T 25069—2010和GB/T 25068.3—2010界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 5271.8—2001、GB/T 25069—2010、GB/T 25068.3—2010中的某些术语和定义。

3.1

网络攻击　network attack

通过计算机、路由器等计算资源和网络资源，利用网络中存在的漏洞和安全缺陷实施的一种行为。

3.2

访问控制[列]表　access control list

由主体以及主体对客体的访问权限所组成的列表。

[GB/T 25069—2010，定义2.2.1.43]

3.3

安全级别　security level

有关敏感信息访问的级别划分，以此级别加之安全范畴能更精确地控制对数据的访问。

[GB/T 25069—2010，定义2.2.1.6]

3.4

逻辑炸弹　logic bomb

一种恶性逻辑程序，当被某个特定的系统条件触发时，造成对数据处理系统的损害。

[GB/T 25069—2010，定义2.2.1.87]

3.5

特洛伊木马　trojan horse

一种表面无害的程序，它包含恶性逻辑程序，可导致未授权地收集、伪造或破坏数据。