ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 37027-2025

Replacing GB/T 37027-2018

Cybersecurity technology - Criteria for determining network attack and network attack incident

网络安全技术 网络攻击和网络攻击事件判定准则

Issued on: February 28, 2025 **Implemented on: September 1, 2025**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part 1: Structure and drafting rules for standardization documents" Drafting.

This document replaces GB/T 37027-2018 "Information Security Technology Network Attack Definition and Description Specification" and GB/T 37027- Compared with 2018, in

addition to structural adjustments and editorial changes, the main technical changes are as follows.

a) The definition of cyber attack has been changed (see 3.1, 3.1 of the 2018 edition);

b) Added the definition of cyber attack incidents (see 3.2);

c) Changed the descriptions of "Attack technical means" and "Security vulnerability types" in "Cyber Attack" (see 5.1, 6.2 and 6.3 of the 2018 version);

d) Added information description of network attack incidents (see 5.2);

e) Added criteria for determining network attacks (see 6.2);

f) Added the criteria for determining network attack events (see 6.3);

g) Added counting method for network attacks (see 7.2);

h) Added the counting method for network attack incidents (see 7.3).

This document was proposed and coordinated by the National Cybersecurity Standardization Technical Committee (SAC/TC260).

This document was drafted by: National Computer Network Emergency Technical Processing Coordination Center, National Computer Network Emergency Technical Processing Coordination Center Beijing Branch, China Electronics Standardization Institute, China Mobile Communications Group Co., Ltd., Venusstar Information Technology Group Co., Ltd.

Co., Ltd., Antiy Technology Group Co., Ltd., Beijing Changting Technology Co., Ltd., National Industrial Information Security Development Research Center, Guoneng Digital Zhi Technology Development (Beijing) Co., Ltd., Zhengzhou Xindajiean Information Technology Co., Ltd., Beijing Topsec Network Security Technology Co., Ltd.

Department of Information and Communications Technology, National Information Center (National E-Government External Network Management Center), China Academy of Information and Communications Technology, Guangdong Provincial Information Security Evaluation Center, National Engineering Research Center for Information Security Common Technology Co., Ltd., Hangzhou Anheng Information Technology Co., Ltd., Beijing Shengxin Network Technology Co., Ltd.

Ltd., Qi'anxin Technology Group Co., Ltd., the Sixth Research Institute of China Electronics Information Industry Group Co., Ltd., Beijing Times New Prestige Information Technology Co., Ltd., Jiangsu Junli Huayu Information Security Technology Co., Ltd., Beijing Zhongce Anhua Technology Co., Ltd., China Electronics Technology Network Security Technology Co., Ltd., Beijing Shenzhou Green Alliance Technology Co., Ltd., 360 Digital Security Technology Group Co., Ltd., Hangzhou Deeptech Technology Co., Ltd., the Third Research Institute of the Ministry of Public Security, the Heilongjiang Branch of the National Computer

Network Emergency Response Technology Coordination Center, Changan Communications TECHNOLOGY LIMITED.

The main drafters of this document are: Yan Hanbing, Rao Yu, Guo Jing, Chen Liang, Zhao Yan, Zhou Yingying, Lu Wei, Xu Jian, Lü Zhiquan, Han Zhihui, Wen Senhao, Wang Huili, Zhu Xuefeng, Xu Yali, Li Yiming, Qiu Qin, Yang Tianshi, Liu Jianan, Yang Kun, Zhang Xiaofei, Niu Yuekun, Liu Weihua, An Gaofeng, Yan Guixun, Dong Hang, Zhen Zhuo, Hu Jianxun, Chen Yanyu, Bian Jianchao, Liu Yong, Zhao Yunlong, Wang Lianqiang, Jin Jianjun, Yan Momo, Cao Xubo, Xiao Yanjun, Geng Guining, Liu Jilin, Tao Yuan, Liu Kun, Zhang Luoshi.

The previous versions of this document and the documents it replaces are as follows.

- First published in 2018 as GB/T 37027-2018;

- This is the first revision.

Introduction

In recent years, with the popularization and rapid development of network applications, the methods and forms of network attacks have become more complex and varied, causing great challenges to network security. Serious threat.

The determination of cyber attacks and cyber attack incidents involves many factors, including. the difference between cyber attacks and cyber attack incidents;

Definition and classification of cyber attacks and network attacks; roles, processes, key technologies, and consequence assessments involved in cyber attacks and network attacks;

With the increasing number of cyber attacks and cyber attack incidents, Currently, there is no unified method for determining and counting network attacks and network attack incidents among various organizations, which leads to the fact that the methods used by various organizations to determine and count network attacks are inconsistent.

There are large differences in the network attack situation, making it difficult to effectively share and accurately perceive the network attack situation. Therefore, it is necessary to conduct a comprehensive analysis of network attacks and network attack events.

More accurate definitions and descriptions, unified classification, judgment and statistical criteria are given to lay a solid foundation for resisting network attacks and improve the network attack situation The perception effect can enhance network security protection capabilities. Cybersecurity Technology Criteria for determining cyber attacks and cyber attack incidents

1 Scope

This document establishes the information elements for describing, determining and counting cyber-attacks and cyber-attack incidents.

This document is applicable to guiding organizations in carrying out activities such as monitoring and analysis, situational awareness, and information reporting of cyber attacks and cyber attack incidents.

2 Normative references

GB/T 20986-2023

GB/T 30279-2020

3 Terms and definitions

The terms and definitions defined in GB/T 20986-2023, GB/T 30279-2020 and the following apply to this document.

3.1 network attacknetworkattack

Through information network technology and various means, the security loopholes and security defects in the network are used to interfere with, control, Any behavior that affects the normal operation of the network, such as sabotage, etc., as well as any behavior that endangers data security, such as stealing, abusing, tampering, and damaging network data.

3.2 Network attack incident network attack incident

Cyber attack (3.1) A security incident that causes or has the potential to cause business loss or harm.

4 Abbreviations

The following abbreviations apply to this document.

APT. Advanced Persistent Threat ARP. Address Resolution Protocol (addressresolutionprotocol) AS. Autonomous system BGP. Border Gateway Protocol DNS. Domain Name System (domainnamesystem) HTTP. Hypertext Transfer Protocol IOC. indicators of compromise IP. Internet Protocol WLAN. Wireless Local Area Network (wireless local area network)