ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 40652—2021

信息安全技术
恶意软件事件预防和处理指南

Information security technology—
Guide to malware incident prevention and handling

2021-10-11 发布　　2022-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

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。

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。

本文件由全国信息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：中国科学院大学、西安电子科技大学、国家计算机病毒应急处理中心、中国科学院信息工程研究所、奇安信科技集团股份有限公司、北信源软件股份有限公司、中国航空综合技术研究所。

本文件主要起草人：张玉清、何远、刘奇旭、王鹤、杨毅宇、王文杰、王基策、陈建民、付安民、李学俊、钟力、刘兴安、张翀斌、张永印、林玥、孙鸿宇、刘新建。

信息安全技术
恶意软件事件预防和处理指南

1 范围

本文件在GB/T 20985.1—2017和GB/T 20985.2—2020的基础之上，针对恶意软件事件的预防和处理过程给出了进一步指南。

本文件适用于计算机系统管理人员、网络管理人员、安全事件响应小组等预防和处理恶意软件事件。

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 20985.1—2017 信息技术 安全技术 信息安全事件管理 第1部分：事件管理原理

GB/T 20985.2—2020 信息技术 安全技术 信息安全事件管理 第2部分：事件响应规划和准备指南

GB/T 25069 信息安全技术 术语

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

恶意软件 malware

被专门设计用来损害或破坏系统，对保密性、完整性或可用性进行攻击的软件。

注：病毒和木马是恶意软件的例子。

[来源：ISO/IEC 27033-1：2015，3.22]

3.2

恶意软件事件 malware incident

由恶意软件引起，并造成保密性、完整性或可用性破坏的信息安全事件。

3.3

防病毒软件 antivirus software

监控主机和网络的程序，通过恶意软件的特征、白名单和异常行为等检测恶意软件，并能识别和清除恶意软件。

注：防病毒软件又称为反病毒软件、杀毒软件。

3.4

病毒 virus

在计算机程序中插入破坏计算机功能或者数据，影响计算机使用并且能自我复制的一组计算机指令或程序代码。

[来源：GB/T 31499—2015，3.6]