



中华人民共和国国家标准

GB/T 47744—2026

网络安全技术 互联网恶意软件定义与描述格式

Cybersecurity technology—Definition and description of internet malware

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

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 互联网恶意软件 2

5.1 总则 2

5.2 互联网恶意软件分类 3

5.2.1 概述 3

5.2.2 蠕虫 3

5.2.3 病毒 3

5.2.4 特洛伊木马 3

5.2.5 勒索软件 4

5.2.6 黑客工具 4

5.2.7 其他互联网恶意软件 4

5.3 互联网恶意软件运行环境 4

5.4 互联网恶意软件家族 4

5.5 互联网恶意软件变种 5

5.6 互联网恶意软件风险与行为 5

5.7 互联网恶意软件通报格式 5

5.7.1 互联网恶意软件通报格式命名规则 5

5.7.2 互联网恶意软件分类编码 5

5.7.3 互联网恶意软件风险与行为标签编码 6

6 互联网恶意软件描述格式 6

6.1 互联网恶意软件描述格式结构 6

6.2 来源信息 6

6.3 基本信息 7

6.4 主机行为信息 7

6.5 网络行为信息 8

6.6 厂商自定义扩展信息 8

附录 A（规范性） 互联网恶意软件运行环境编码 9

A.1 计算机网络设备 9

A.2 移动互联网智能设备 12

附录 B（规范性） 互联网恶意软件风险与行为标签编码 13

附录 C（资料性） 恶意软件上报场景下互联网恶意软件通报描述格式完整示例 18

参考文献 22

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：国家计算机网络应急技术处理协调中心、国家计算机网络应急技术处理协调中心浙江分中心、中国移动通信集团有限公司、安天科技集团股份有限公司、恒安嘉新(北京)科技股份有限公司、三六零数字安全科技集团有限公司、北京百度网讯科技有限公司、杭州安恒信息技术股份有限公司、蚂蚁科技集团股份有限公司、国家信息技术安全研究中心、北京天融信网络安全技术有限公司、公安部第三研究所、西安邮电大学、启明星辰信息技术集团股份有限公司、西安交大捷普网络科技有限公司、武汉安天信息技术有限责任公司、国家工业信息安全发展研究中心、中国电力科学研究院有限公司、陕西省网络与信息安全测评中心、北京神州绿盟科技有限公司、新华三技术有限公司、兴唐通信科技有限公司、奇安信科技集团股份有限公司、东软集团股份有限公司、亚信科技(成都)有限公司、中国科学院软件研究所、浙江大学。

本文件主要起草人：韩志辉、严寒冰、何能强、李佳、肖新光、刘冬、兰雪、丁丽、韩耀光、季莹莹、崔牧凡、苏璞睿、杨满智、许益鑫、徐艺激、杨绍波、白晓媛、李霞、张凤羽、孙永清、张勇、赵秋鹏、何建锋、潘宣辰、余果、陈牧、马卓元、叶建伟、万晓兰、穆永恒、胡伟、石鹏飞、赵帅、梁宇、王绪国、叶佳旭、王小航、王亮。

网络安全技术

互联网恶意软件定义与描述格式

1 范围

本文件界定了互联网恶意软件的定义和分类,规定了其命名格式和关于捕获来源、行为、危害等的描述格式。

本文件适用于移动互联网设备、计算机网络设备上恶意软件的分类、命名以及共享等工作,为互联网恶意软件安全管理、安全检测、通报、预警通报等提供规范化参考。

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 25069—2022 信息安全技术 术语

GB/T 40652—2021 信息安全技术 恶意软件事件预防和处理指南

3 术语和定义

GB/T 25069—2022 和 GB/T 40652—2021 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

被专门设计用于损坏或中断系统、破坏保密性、完整性和/或可用性的软件。

注:病毒和特洛伊木马都是恶意软件。

[来源:GB/T 25069—2022,3.141]

3.2

互联网恶意软件 internet malware

通过互联网或其他网络传播或分发,通过本地运行或者网络远程执行的恶意软件(3.1)。

3.3

互联网恶意软件样本 internet malware sample

互联网恶意软件的文件实体或数据镜像,是互联网恶意软件在传播、运行过程中形成的可被捕获与分析的具体载体。

注:互联网恶意软件既能是独立的互联网恶意软件载体文件,被互联网恶意软件感染后的文件对象,也能是非文件载体恶意代码的文件镜像。互联网恶意软件样本是互联网恶意软件检测、分析和研究的对象。

3.4

病毒 virus

一种程序,即通过修改其他程序,使其他程序包含一个自身可能已发生变化的原程序副本,从而完成传播自身程序,当调用受传染的程序,该程序即被执行。

注:病毒经常造成某种损失或困扰,并可能被某一事件(诸如出现的某一预定日期)触发。

[来源:GB/T 25069—2022,3.50]

3.5

蠕虫 worm

一种通过数据处理系统或计算机网络传播自身的独立程序。

注: 蠕虫经常被设计用来占满可用资源,如存储空间或处理时间。

[来源:GB/T 25069—2022,3.494]

3.6

特洛伊木马 trojan horse

一种伪装成良性应用程序的恶意程序。

[来源:GB/T 25069—2022,3.594]

3.7

勒索软件 ransomware

采取加密或屏蔽用户操作等方式劫持用户对系统或数据的访问权,并借此向用户索取勒索金的恶意软件。

[来源:GB/T 40652—2021,3.5]

4 缩略语

下列缩略语适用于本文件。

COM:组件对象模型(Component Object Model)

ELF:可执行与可链接格式(Executable and Linkable Format)

EXE:可执行文件(Executable)

FTP:文件传输协议(File Transfer Protocol)

ID:标识符(Identifier)

IP:网际协议(Internet Protocol)

IPv4:互联网协议第4版(Internet Protocol version 4)

IPv6:互联网协议第6版(Internet Protocol version 6)

IRC:互联网中继聊天(Internet Relay Chat)

PE:可移植的可执行文件(Portable Executable)

P2P:对等式网络(Peer-To-Peer)

SMTP:简单邮件传输协议(Simple Mail Transfer Protocol)

Telnet:电传网络协议(Teletype Network)

5 互联网恶意软件

5.1 总则

互联网恶意软件主要包括通过互联网或其他网络传播扩散的恶意软件,本章从互联网恶意软件分类、运行环境、家族、变种、风险与行为、通报格式六方面描述互联网恶意软件的定义。

互联网恶意软件分类主要体现互联网恶意软件特质,结合恶意软件部署位置和传播方式,综合将互联网恶意软件分为病毒、蠕虫、特洛伊木马、黑客工具、勒索软件、其他互联网恶意软件等六类。运行环境指互联网恶意软件安装或运行所需要的环境。家族主要用于区分不同互联网恶意软件的主体功能。变种主要用于区分同一家族中不同配置的互联网恶意软件。风险与行为主要用于区分互联网恶意软件攻击目的和危害,揭示互联网恶意软件风险与行为属性。互联网恶意软件通报格式采用分段式格式,完

整命名共五段,依次包括互联网恶意软件分类、互联网恶意软件运行环境、互联网恶意软件家族、互联网恶意软件变种、互联网恶意软件风险与行为。

5.2 互联网恶意软件分类

5.2.1 概述

按照部署位置(被攻击侧、攻击侧)和传播方式(自主传播、半自主传播、被控传播、融合传播)两个维度,互联网恶意软件可分为六类。若同时具备多种分类特性,则以最主要的特性作为分类。

- a) 蠕虫,部署在被攻击侧,具有独立自主传播能力,不依赖于其他文件或程序。
- b) 病毒,部署在被攻击侧,半自主传播,应依赖其他程序。
- c) 特洛伊木马,部署在被攻击侧,被控传播,不具备自主传播能力,诱导用户下载等方式传播。
- d) 勒索软件,部署在被攻击侧,融合传播,作为一种具有重大网络安全威胁的互联网恶意软件,可能具备多种传播方式。
- e) 黑客工具,通常运行在攻击者设备侧。
- f) 其他互联网恶意软件。

5.2.2 蠕虫

蠕虫的核心特性、传播方式、主要行为、常见示例如下所示。

- a) 核心特性:蠕虫的核心特征为自我复制传播,具有不依赖于其他文件或程序、独立自我传播的能力。蠕虫能复制自身,并将复制品传播到其他计算机上,可在短时间内快速扩散到大量计算机。
- b) 传播方式:蠕虫通常利用系统或软件漏洞、弱口令、文件共享、网络共享等方式进行传播,也可通过发送恶意电子邮件、利用即时通信程序或社交媒体等途径,寻找新的目标计算机并传播自身。
- c) 主要行为:蠕虫可能会在感染的计算机上执行各种恶意操作,包括窃取敏感信息、破坏系统文件、创建僵尸网络、发起分布式拒绝服务攻击等。
- d) 常见示例:莫里斯蠕虫、震网蠕虫等。

5.2.3 病毒

病毒的核心特性、传播方式、主要行为、常见示例如下所示。

- a) 核心特性:病毒具有自我传播能力,并且需依赖其他程序完成传播自身。
- b) 传播方式:病毒以修改其他程序的方式来完成传播自身程序,通常在其他程序中插入破坏计算机功能或数据、影响计算机使用并能自我复制的计算机指令或程序代码,常见的其他程序包括但不限于磁盘文件、引导扇区及其他能达成互联网恶意软件自我传播方式的载体。
- c) 主要行为:常见的行为包括破坏宿主程序的功能和数据;占用系统资源,降低计算机性能;感染其他文件或系统区域。
- d) 常见示例:宏病毒、文件感染病毒、引导扇区病毒等。

5.2.4 特洛伊木马

特洛伊木马的核心特性、传播方式、主要行为、常见示例如下所示。

- a) 核心特性:特洛伊木马一般不会自我传播和感染其他文件,常通过伪装成良性应用程序等方式吸引用户下载执行,具有较明确的目的。
- b) 传播方式:特洛伊木马通常通过钓鱼邮件、软件捆绑、虚假下载等方式进行传播。

- c) 主要行为:包括但不限于远程监控主机、组建僵尸网络、窃取敏感信息、下载其他恶意软件并执行等。
- d) 常见示例:后门、远程控制木马、挖矿木马、间谍软件、下载者木马、僵尸网络、数据擦除器等。

5.2.5 勒索软件

勒索软件的核心特性、传播方式、主要行为、常见示例如下所示。

- a) 核心特性:勒索软件属于重大风险,以勒索赎金为目的,可能还会导致窃取数据、曝光数据(泄露或出售)、数据破坏等影响,严重危害用户网络安全和数据安全。
- b) 传播方式:勒索软件通过漏洞利用、网络钓鱼、木马下载等方式进行传播。
- c) 主要行为:常见的行为包括文件加密、提示勒索信息等,勒索软件作为一种影响较大的恶意软件,可能与蠕虫、病毒、木马、黑客工具等恶意软件组合使用。
- d) 常见示例:WannaCry、GandCrab、Ryuk 等勒索软件。

5.2.6 黑客工具

黑客工具的核心特性、传播方式、主要行为、常见示例如下所示。

- a) 核心特性:黑客工具是一类攻击者或恶意软件作者使用的工具,通常运行在攻击者设备侧,需要使用者主动操作和控制,与病毒、木马等不同,它本身一般不具备自我传播能力、感染其他文件或损害当前运行主机的能力,部分黑客工具具备自动化功能,用于加速扫描探测或攻击行为。
- b) 传播方式:常见的传播方式包括伪装成正常工具包诱导下载或集成在恶意软件中进行安装。
- c) 主要行为:主要用于分析、测试、模拟或利用系统和网络中的漏洞和弱点,通常被攻击者用于辅助非法的网络攻击、数据窃取、开发和传播恶意软件、密码破解、漏洞利用、扫描探测、社工模拟、钓鱼测试、逃避检测等。
- d) 常见示例:拒绝服务攻击工具、木马生成器、代码混淆器等。

5.2.7 其他互联网恶意软件

不在 5.2.2~5.2.6 分类内的互联网恶意软件统一归为其他互联网恶意软件。

5.3 互联网恶意软件运行环境

互联网恶意软件运行环境是指互联网恶意软件安装或运行所需要的环境,具体包括操作系统、编程语言平台和宿主格式等信息。

在对互联网恶意软件运行环境进行命名时,为保证命名的准确性和唯一性,应遵循从直接到间接的优先级原则,即优先标识最直接承载并触发恶意代码执行的运行环境层级。优先级从高到低依次为:宿主格式、编程语言平台、操作系统。对于能够在多个平台/操作系统运行的恶意软件,可使用“Multi”进行标识。

互联网恶意软件运行环境使用英文(区分大小写)或数字标识,直接使用操作系统英文名称、编程语言英文名称或宿主格式英文名称命名。取值依据附录 A 中的表 A.1 和表 A.2。

5.4 互联网恶意软件家族

互联网恶意软件家族是指具有相似恶意主体功能的软件种类,具有不同恶意主体功能的软件种类可命名为不同家族名称。

互联网恶意软件家族名称使用英文(不区分大小写)或数字标识。互联网恶意软件家族名称可使用解开安装包或压缩格式后的恶意软件主程序的可执行文件名、主要进程的名称或特征字符串命名,亦可使用主程序体中第一个可用的字符串命名。原则上应遵循使用第一个公开报告的家族名称。若无具体

家族,使用“Generic”标识。

5.5 互联网恶意软件变种

互联网恶意软件主体功能相同,但配置不同的,则认为是同一家族的恶意软件,这时应用变种名称来区分。

互联网恶意软件变种名称根据样本发现顺序采用英文字母(均小写)依次命名。第一个发现的样本命名为 a,第二个命名为 b,第 27 个发现的样本命名为 aa,第 28 个命名为 ab,以此类推。

互联网恶意软件主体功能相同,配置也相同,但散列值不同,则认为是同一互联网恶意软件的同一变种,其家族名称及变种名称均应完全相同。

5.6 互联网恶意软件风险与行为

互联网恶意软件风险与行为主要用于补充互联网恶意软件分类、运行环境、家族和变种无法表示的关键威胁信息,细致区分互联网恶意软件攻击目的和危害,揭示互联网恶意软件风险与行为属性。常见的风险与行为包括僵尸网络、分布式拒绝服务攻击、释放恶意软件、拨号、键盘记录等。

5.7 互联网恶意软件通报格式

5.7.1 互联网恶意软件通报格式命名规则

互联网恶意软件采用分段式格式命名规则,完整命名共五段,第一段为互联网恶意软件分类、第二段为互联网恶意软件运行环境、第三段为互联网恶意软件家族、第四段为互联网恶意软件变种、第五段为互联网恶意软件风险与行为,前四段间以“.”分隔,每段使用英文(不区分大小写)或数字标识,第五段为可选扩展字段,为恶意软件行为标签字段,使用中括号“[]”标识,可使用任何 Unicode 字符。命名格式如下:

互联网恶意软件主分类.互联网恶意软件运行环境编码.互联网恶意软件家族名称.互联网恶意软件变种名称[互联网恶意软件风险与行为标签编码]

以上字段中,主分类、运行环境编码和家族名称为必填字段,其他为可选字段。

示例:

- Trojan.Win32.Photosys.a[PSW]
- Ransomware.Win32.Phobos.d[Ransom]
- Trojan.Linux.Mirai.ba[Backdoor]
- Trojan.Linux.Generic

5.7.2 互联网恶意软件分类编码

本文件将互联网恶意软件分为六类,使用英文标识,互联网恶意软件按照表 1 进行分类编码。

表 1 分类名称和编码

序号	分类名称	分类编码
1	蠕虫	Worm
2	病毒	Virus
3	特洛伊木马	Trojan
4	勒索软件	Ransomware
5	黑客工具	HackTool
6	其他恶意软件	Other

5.7.3 互联网恶意软件风险与行为标签编码

互联网恶意软件风险与行为标签兼容和吸收各业界命名中所包含的有效信息、适应新威胁的出现并增加扩展空间,可输出一种或多种风险或行为标签,分隔符使用“/”,互联网恶意软件风险与行为标签编码及说明应符合附录 B。

6 互联网恶意软件描述格式

6.1 互联网恶意软件描述格式结构

互联网恶意软件使用标签语言描述。本文件中的恶意软件描述使用五大类标签,每个大类标签可包含若干个子类标签,五大类标签按照表 2 的规定。

表 2 恶意软件描述标签

标签名称	标签说明	是否有下级子标签
〈Source〉	互联网恶意软件来源的相关信息	是
〈SampleBasic〉	互联网恶意软件文件基本信息	是
〈SampleAnalysis〉	互联网恶意软件对主机产生的注册表、文件、进程等行为信息	是
〈NetworkOperation〉	互联网恶意软件具有的网络行为信息	是
〈VendorAnalysis〉	各厂商自定义的扩展信息,一般包括恶意属性判定,流行度,是否感染其他文件等描述信息	自定义

以互联网恶意软件上报场景为例,附录 C 给出了互联网恶意软件描述格式完整示例。

6.2 来源信息

标签名称:〈Source〉

该标签描述了互联网恶意软件来源的相关信息,包含捕获时的文件名、样本文件散列值、报告来源信息、首次捕获时间、首次发现地点、攻击活动次数、攻击来源 IP、攻击目的 IP、传播互联网恶意软件的网址。

具体子标签名称以及各子标签的信息按照表 3 的规定。

表 3 〈Source〉子标签信息

子标签命名	说明	是否有下级子标签
〈FileName〉	互联网恶意软件捕获时的文件名	否
〈Hash〉	互联网恶意软件文件散列值	是
〈SourceName〉	互联网恶意软件报告来源信息,如提交厂商名称、捕获系统名称、交换来源名称等	否
〈Time〉	互联网恶意软件首次被捕获的时间,如:2020-05-31 12:32:54	否
〈Location〉	互联网恶意软件首次发现的地点,使用民政部规定的行政区划代码	否
〈AttackCount〉	监测到的互联网恶意软件攻击活动次数	否

表 3 〈Source〉子标签信息（续）

子标签命名	说明	是否有下级子标签
〈SourceIPv4〉	互联网恶意软件的攻击来源 IPv4 地址,使用点分形式	否
〈SourceIPv6〉	互联网恶意软件的攻击来源 IPv6 地址	否
〈DestIPv4〉	互联网恶意软件攻击的目标 IPv4 地址,使用点分形式	否
〈DestIPv6〉	互联网恶意软件攻击的目标 IPv6 地址	否
〈URL〉	传播互联网恶意软件的网络地址	否

6.3 基本信息

标签名称:〈SampleBasic〉

该标签描述互联网恶意软件文件基本信息,包含样本文件散列值、互联网恶意软件命名、文件实际大小、文件格式、文件创建时间、文件修改时间、壳、包裹、文件标准版本、PE 文件结构、ELF 文件结构,具体子标签名称以及各子标签的信息按照表 4 的规定。

表 4 〈SampleBasic〉子标签信息

子标签命名	说明	是否有下级子标签
〈Hash〉	互联网恶意软件文件散列值	是
〈MalwareName〉	互联网恶意软件命名,格式为:互联网恶意软件主分类.互联网恶意软件运行环境编码.互联网恶意软件名称.互联网恶意软件变种名称.[互联网恶意软件行为标签编码]	否
〈FileSize〉	互联网恶意软件文件实际大小使用十六进制表示	否
〈FileFormat〉	COM、EXE、ELF 等文件格式	是
〈FileTime〉	包括创建时间,修改时间	是
〈Packet〉	对可执行文件加壳:即预先运行一段程序,将原程序展开到内存后执行,可起到压缩或加密功能。同一可执行程序可被多次加壳	是
〈Archive〉	按照包裹的形式,可以分为静态包裹(StaticArchive)和自解压包裹(SFX)。静态包裹不具有自我执行能力,应有配套的解压程序才能解开;自解压包裹在包裹上加一个可执行的文件头,该文件头能将包裹自行解开	否
〈FileVersion〉	PE 等可执行文件标准版本	否
〈PEStruct〉	Windows 操作系统中的主要可执行文件的结构	是
〈ELFStruct〉	Linux 操作系统中的主要可执行文件的结构	是

6.4 主机行为信息

标签名称:〈SampleAnalysis〉

该标签描述了互联网恶意软件对主机产生的注册表、文件、进程等行为信息,包含运行的系统平台、进程操作、文件操作、内存操作、注册表操作和其他操作,具体子标签名称以及各子标签信息见表 5。

表 5 〈SampleAnalysis〉子标签信息

子标签命名	说明	是否有下级子标签
〈Platform〉	互联网恶意软件运行的系统平台	否
〈ProcessThreadOperation〉	进程、线程的创建、终止信息等	是
〈FileOperation〉	创建、删除、重名文件及其读写特定目录	是
〈RegisterOperation〉	创建、设置、删除注册表的键和值	是
〈MemoryOperation〉	对主机内存的相关操作	是
〈OtherOperation〉	创建的互斥体和修改的系统时间	否

6.5 网络行为信息

标签名称:〈NetworkOperation〉

该标签描述互联网恶意软件具有的网络行为信息,包含网络操作的进程 ID、进程的文件映像路径、网络行为类别、远程 IPv4 地址、远程 IPv6 地址、目的端口、网络协议、主机名、访问的统一资源定位符,具体子标签名称以及各子标签信息见表 6。

表 6 〈NetworkOperation〉子标签信息

子标签命名	说明	是否有下级子标签
〈ProcessID〉	执行网络操作的进程的 ID	否
〈ImagePath〉	执行网络操作的进程的文件映像路径	否
〈Action〉	此恶意软件网络行为的类别 如: AccessNetwork: 记录网络连接的 IP 和端口 BindNetwork: 绑定一个端口,用于发起各种网络行为	否
〈IPv4Address〉	远程 IPv4 地址,使用点分形式	否
〈IPv6Address〉	远程 IPv6 地址	否
〈Port〉	网络行为的目的端口	否
〈Protocol〉	互联网恶意软件网络操作使用的网络协议	否
〈Host〉	互联网恶意软件访问的远程主机	否
〈URL〉	互联网恶意软件访问的统一资源定位符	否
〈Domain〉	互联网恶意软件回连的域名	否
〈Email〉	互联网恶意软件回连的邮箱	否

6.6 厂商自定义扩展信息

标签名称:〈VendorAnalysis〉

该标签描述各厂商自定义的扩展信息,一般包括恶意属性判定、流行度、是否感染其他文件等描述信息。子标签名称由各厂商自行定义。

附 录 A
(规范性)
互联网恶意软件运行环境编码

A.1 计算机网络设备

计算机网络设备上的恶意软件运行环境编码依据表 A.1,其字符编码采用 GB/T 1988 编码,英文字母区分大小写。

表 A.1 计算机网络设备上的恶意软件运行环境编码

序号	类型	编码	运行环境说明
1	操作系统	DOS	80 年代推出的个人操作系统,是一种行命令的单任务系统,可执行文件格式为 COM 和 DOS MZ
2		DOS32	32 位的 DOS 操作系统
3		Linux	一种开源的类 unix 系统
4		Mac	操作系统 Macintosh OS
5		NeoKylin	中标麒麟,一种基于 Linux 内核的国产操作系统
6		Unix	20 世纪 70 年代开发的一款操作系统,目前已经形成了商用 Unix 和免费 UNIX 等多个家族
7		Win16	16 位 Windows 操作系统架构,代表版本是 Windows 3.0,其主要的可执行文件是 NE (NEW EXE)格式
8		Win32	32 位 Windows 操作系统架构,代表版本有 Win95、Win2k、WinNT、WinXP 等,其主要的可执行文件结构是 PE 格式
9		Win64	64 位 Windows 操作系统架构
10		Other	其他操作系统
11	编程语言平台	ASP	Active Server Page 脚本
12		BAT	DOS 批处理命令
13		HTML	超文本标记语言
14		IRC	Internet Relay Chat 的缩写,是一种网络即时聊天应用协议,支持相关脚本语言
15		Java	Java 语言,一种具有良好的操作系统移植性的开发语言
16		JS	JavaScript 脚本
17		JSP	Java Server Pages,一种动态网页技术标准
18		Lua	一个简洁、轻量、可扩展的脚本语言,有着相对简单的 C API 而很容易嵌入应用中

表 A.1 计算机网络设备上的恶意软件运行环境编码（续）

序号	类型	编码	运行环境说明
19	编程语言平台	Macro	一些命令组织在一起,作为一个单独命令完成一个特定任务,在实际应用中往往特指微软在 office 系统中提供的宏体制
20		Matlab	一款商业数学软件,用于算法开发、数据可视化、数据分析以及数值计算的高级技术计算语言和交互式编程环境,主要包括 MATLAB 和 Simulink 两大部分
21		MEL	Maya Embedded Language(MEL),Autodesk Maya 的脚本语言,用于 3D 建模和动画工具自动化
22		MSIL	MSIL 是将 .Net 代码转化为机器语言的一个中间过程,是一种介于高级语言和基于 Intel 的汇编语言的伪汇编语言
23		Perl	一种历史悠久的脚本语言,主要用于 CGI 类技术开发
24		PHP	英文“超级文本预处理语言”(PHP:Hypertext Preprocessor)的嵌套缩写,是一种在 Linux 应用非常广泛的 CGI 类技术开发语言
25		PowerShell	运行在 Windows 操作系统上实现对系统以及应用程序进行管理自动化的命令行脚本环境
26		Python	一种跨平台的计算机程序设计语言,是一个高层次的结合了解释性、编译性、互动性和面向对象的脚本语言
27		Ruby	一种解释型的方便快捷的面向对象脚本语言,于 1993 年 2 月 24 日诞生,于 1995 年 12 月正式公开发布
28		Shell	命令解释器脚本,又称 Shell 脚本、Shell 命令稿、程序化脚本,是一种电脑程序使用的文本文件,内容由一连串的 shell 命令组成,经由 Unix Shell 直译其内容后运行
29		SQL	Structured Query Language(结构化查询语言)的缩写,用于数据库操作的脚本语言
30		VBS/ WBS	VBScript 脚本。WBS 脚本,实际上也是 VBS 脚本
31		WinINF	一种 Windows 操作系统上的描述脚本,文本格式,主要用于驱动安装描述、自动化运行等方面
32		WinREG	Windows 注册表脚本
33		XML	可扩展标记语言(Extensible Markup Language),标准通用标记语言的子集,可用于来标记数据、定义数据类型,是一种允许用户对自己的标记语言进行定义的源语言
34		Other	其他编程语言

表 A.1 计算机网络设备上的恶意软件运行环境编码 (续)

序号	类型	编码	运行环境说明
35	宿主格式	Acad	一种绘图的辅助工具 AutoCAD
36		ANSI	ANSI 编码格式文件
37		Boot	引导扇区
38		Boot-DOS	引导扇区和 DOS 文件
39		EML	电子邮件文件的标准格式,包含邮件头和正文信息
40		HWP	韩国的汉字处理软件的文档文件格式,类似于 Microsoft Word
41		JPG	JPEG 图像压缩标准的有损压缩格式,广泛用于数字摄影
42		MakeFile	一个工程文件的编译规则,描述了整个工程的编译和链接等规则,用于自动编译和链接
43		MP3	音频压缩编码格式,用于存储音乐和声音
44		MP4	多媒体容器格式,用于存储视频、音频和字幕等数据
45		MSAccess	复合文档格式文件,Access 是微软桌面办公软件 office 家族产品,采用 OLE2 复合结构存储,支持 VB 脚本
46		MSEExcel	复合文档格式文件,是微软桌面办公软件 office 家族产品,采用 OLE2 复合结构存储,支持 VB 脚本
47		MSOffice	复合文档格式文件,微软桌面办公系统家族 Office,其文件采用 OLE2 复合结构存储
48		MSPPoint	复合文档格式文件,Point 是微软桌面办公软件 office 家族产品,采用 OLE2 复合结构存储,支持 VB 脚本
49		MSProject	复合文档格式文件,Project 是微软桌面办公软件 office 家族产品,采用 OLE2 复合结构存储,支持 VB 脚本
50		MSVisio	复合文档格式文件,Visio 是微软桌面办公软件 office 家族产品,采用 OLE2 复合结构存储,支持 VB 脚本
51		MSWord	复合文档格式文件,Word 是微软桌面办公软件 office 家族产品,采用 OLE2 复合结构存储,支持 VB 脚本
52		Multi	具有多态性质,可能有不同类型的宿主载体
53		NSIS	NSIS (Nullsoft Scriptable Install System)是 Windows 下的一个安装程序制作工具
54		PDF	便携式文档格式(Portable Document Format),在不同设备和系统上保持文档版式、字体和图像的一致性

表 A.1 计算机网络设备上的恶意软件运行环境编码（续）

序号	类型	编码	运行环境说明
55	宿主格式	PNG	无损压缩的位图图像格式,支持透明度和高色彩深度
56		RAR/ZIP/ ARJ/HA/ BZip/GZip	流行的文件压缩格式
57		RTF	富文本格式(Rich Text Format)即 RTF 格式,又称多文本格式,是由微软公司开发的跨平台文档格式。大多数的文字处理软件都能读取和保存 RTF 文档
58		SWF	Adobe Flash 动画或应用程序的文件格式,用于网页交互内容
59		WinHLP	Windows 操作系统上的帮助文件,二进制格式文件
60		WinLNK	Windows 快捷方式文件
61		WinPIF	微软系列软件创建的 Program Information File (PIF) Windows 文件
62		Other	其他宿主格式

A.2 移动互联网智能设备

移动互联网智能设备上的互联网恶意软件运行环境编码依据表 A.2。

表 A.2 移动互联网智能设备上的互联网恶意软件运行环境编码

序号	编码	运行环境说明
1	Android	一种基于 Linux 内核(不包含 GNU 组件)的自由及开放源代码的移动操作系统,主要应用于智能手机、平板电脑等移动设备
2	BlackBerry	一种为智能手机产品 BlackBerry 开发的专用操作系统
3	Harmony-OS	鸿蒙操作系统,一种面向多设备的分布式操作系统,主要应用于手机、平板电脑、智能手表、智慧屏、打印机、智能眼镜、车机等移动设备
4	iOS	一种移动操作系统,主要应用于苹果手机、平板电脑、智能手表等移动设备
5	NucleusOS	一种嵌入式实时操作系统,使用标准 C 开发,主要用于联发科技 MTK 芯片的手机
6	Symbian	一种手机操作系统
7	Other	其他类型的平台

附 录 B
(规范性)

互联网恶意软件风险与行为标签编码

互联网恶意软件风险与行为标签编码依据表 B.1。

表 B.1 互联网恶意软件风险与行为标签编码

序号	编码	风险与行为标签	对应互联网恶意软件主分类	行为说明与危害
1	Promotion	恶意推广	特洛伊木马、其他	通过欺骗、骚扰、侵犯隐私或诱导用户进行非自愿操作等违规手段,伪装成系统相关应用、安装无图标或运行隐藏图标,实现后台请求广告链接、推送广告且无法正常关闭、后台私自下载、安装的行为
2	WebTool-bar	收集用户浏览记录	特洛伊木马、其他	在用户不知情或未授权的情况下,下载并安装浏览器工具,收集浏览记录、篡改浏览结果等
3	ArcBomb	包裹炸弹	特洛伊木马	一种针对反病毒软件的行为,利用各种方法来对抗、干扰、破坏反病毒产品的运行、检测等功能,典型的行为是使用压缩软件制作引发反病毒软件长时间扫描的文件,这种方法会被用户误认为反病毒软件“假死”。可能导致系统崩溃
4	AutoRun	自动运行	特洛伊木马	在用户不知情或未授权的情况下,利用系统各种运行机制,自动启动和运行的行为。会导致恶意软件长期驻留在系统中,无法去除
5	Backdoor	后门	特洛伊木马	在用户不知情或未授权的情况下,在被感染的系统上以隐蔽的方式运行并对被感染的系统进行远程控制的行为
6	Banker	窃取银行账号数据	特洛伊木马	窃取与网上银行系统,电子支付系统等有关的用户账户数据,将窃取的数据传输到击者手中。通常会导致用户银行账号被窃取,可能间接导致用户经济损失
7	Batch	批量操控/外挂	黑客工具	受黑客工具控制,完成自动点赞、关注、转发、评论、直播人气等僵尸粉行为和游戏外挂等
8	Bootkit	感染引导层	特洛伊木马	将恶意代码植入到计算机引导扇区或引导目录,以达到在计算机启动时执行目的的行为。可能导致系统被控等后果
9	Botnet	僵尸网络	木马、病毒、蠕虫	通过各种途径传播恶意软件感染网络上的大量主机,在控制者和被感染主机之间形成的一对多控制的网络
10	Bundler	打包隐匿	特洛伊木马	将恶意软件打包成隐藏或伪装成合法文件或应用程序的行为。目的是欺骗用户和防止恶意软件被杀毒软件或系统安全措施检测和删除,从而更容易传播和执行恶意行为
11	Clicker	点击器	特洛伊木马	自动执行鼠标点击或屏幕手势操作,常用来对网站进行多次访问来提高网站的访问量或刷数据

表 B.1 互联网恶意软件风险与行为标签编码（续）

序号	编码	风险与行为标签	对应互联网恶意软件主分类	行为说明与危害
12	Client-IRC	通过 IRC 受控	其他	在用户不知情或未授权的情况下,通过一些商用或开源的 IRC 客户端软件,受远程控制端指令并进行相关操作的行为
13	Client-P2P	通过 P2P 受控	其他	在用户不知情或未授权的情况下,通过一些商用或开源的 P2P 客户端软件,受远程控制端指令并进行相关操作的行为
14	Client-SMTP	通过 SMTP 受控	其他	在用户不知情或未授权的情况下,通过一些商用或开源的 SMTP 客户端软件,受远程控制端指令并进行相关操作的行为
15	Construct	生成器	黑客工具	生成新的病毒、蠕虫、木马的功能行为,通常具备配置操作界面,提供选择生成的恶意软件类型、混淆、控制服务器地址等功能,部分生成器同时也作为木马的控制端
16	DDoS	分布式拒绝服务攻击	黑客工具、特洛伊木马	分布式拒绝服务攻击(DDoS)是危害程度极大的攻击行为,通常利用大量主机同时对目标发送数据包,导致目标网络服务中止
17	Dialer	拨号	特洛伊木马、其他	通常是指木马等恶意软件伪装成拨号程序,通过用户的计算机或设备拨打付费电话号码获利的行为。通常会给用户造成经济损失等后果
18	DoS	拒绝服务攻击	黑客工具、特洛伊木马	在用户不知情或未授权的情况下,对网络中的目标发起拒绝服务攻击的行为
19	Downloader	下载恶意软件	特洛伊木马	诱导用户到指定的 URL 地址下载更多的恶意软件并运行,使得攻击者获得更大操作权限
20	Dropper	释放恶意软件	特洛伊木马	运行时自动释放或安装单个或多个恶意软件的行为,通常为静默安装
21	Email	邮件蠕虫	蠕虫	蠕虫通过电子邮件进行自我传播的行为
22	Expense	资费消耗	特洛伊木马	在用户不知情或未授权的情况下,通过自动拨打电话、发送短信、彩信、邮件、频繁连接网络等方式,导致用户资费损失的行为
23	Exploit	漏洞利用	特洛伊木马、病毒、蠕虫、黑客工具	利用本地或远程计算上运行软件中的一个或多个漏洞,到达恶意目的的行为。可能导致用户系统瘫痪、业务中断、远程被控等后果
24	Fake	仿冒	特洛伊木马、其他	通过仿冒、伪装、重打包、篡改其他应用名称、标识、代码的形式,执行恶意行为达到不正当目的。如诈骗、窃取隐私、下载安装恶意软件等
25	FakeAV	伪装杀软	特洛伊木马	伪装成杀毒软件的行为

表 B.1 互联网恶意软件风险与行为标签编码（续）

序号	编码	风险与行为标签	对应互联网恶意软件主分类	行为说明与危害
26	Fraud	诱骗欺诈	特洛伊木马	欺诈诱骗行为,在用户不知情或未授权的情况下,通过伪造、篡改、劫持短信、彩信、通信录、通话记录、邮件、浏览器、网站、收藏夹、桌面等方式,诱导用户点击恶意链接、下载恶意附件或输入敏感信息,从而达到不正当目的行为。通常会导致用户敏感信息被窃等后果
27	GameThief	盗取游戏账号信息	特洛伊木马	盗取网络游戏账号、口令、装备和密保等信息,并通过邮件或网络传输给攻击者。通常会导致用户游戏信息被窃取
28	Illegal	非法内容	其他	伪装成正常应用,但是内容存在博彩、诈骗、赌博、色情、宗教等非法内容,以达到非法传播目的
29	IM	通过即时通信传播	蠕虫	蠕虫通过即时通信进行自我传播的行为
30	Injector	注入	特洛伊木马、蠕虫、病毒	通过特定手段将恶意代码注入到目标系统中合法运行的进程(如浏览器、系统服务、常用应用程序等)中,以隐藏自身痕迹、绕过安全检测并获得持续控制权
31	IRC	通过 IRC 传播	蠕虫	蠕虫通过 IRC 进行自我传播的行为
32	KeyLogger	键盘记录	特洛伊木马	在用户不知情或未授权的情况下,秘密监控和记录所有的键盘输入活动,常用来收集口令或财务类等敏感信息。通常会导致用户敏感信息被窃取
33	LockScreen	锁屏	特洛伊木马	通过强制界面置顶、设置口令等方式,锁定用户屏幕干扰用户设备正常使用的行为。通常会造成设备不可用等后果
34	Miner	挖矿	特洛伊木马	未经用户明确授权或知情的情况下,利用受感染设备的计算资源进行加密货币挖矿的行为。会显著降低受感染设备的性能,增加电力消耗
35	Modifier	篡改浏览器	其他	针对用户的浏览器进行篡改和修改,可能以插件、扩展、工具栏、恶意软件等形式存在,目的是控制用户的浏览器行为、篡改浏览器设置,以及导向用户访特定网站,从中获利或进行其他恶意行为
36	Monitor	监视用户信息	其他	在用户不知情或未授权的情况下对计算机活动(包括进程活动、网络活动等)进行监视,从而对用户行为或轨迹进行监视,以达到不法目的的行为。可能会造成用户隐私信息泄露等后果
37	Net	通过网络自我传播	蠕虫	蠕虫通过网络进行自我传播的行为,一般都是利用漏洞进行传播
38	Obfuscator	混淆器	黑客工具	指通过代码结构变换、控制流混淆、字符串混淆和无用代码插入等手段隐藏代码的真实目的,以逃避安全检测和分析的行为
39	Other	其他	—	其他未提及的互联网恶意软件风险或行为

表 B.1 互联网恶意软件风险与行为标签编码（续）

序号	编码	风险与行为标签	对应互联网恶意软件主分类	行为说明与危害
40	P2P	通过 P2P 传播	蠕虫	蠕虫通过 P2P 进行自我传播的行为
41	Packed	加壳	特洛伊木马	恶意软件附加一层伪装使其改变原有数据形态,从而绕过一些安全软件检测的行为
42	Patched	破解软件	黑客工具	被破解/修改的非原版程序
43	Payment	恶意扣费	特洛伊木马	在用户不知情或未授权的情况下,通过隐蔽执行、欺骗用户点击等手段,订购各类收费业务或使用移动终端支付,导致用户经济损失的行为
44	Phishing	钓鱼	特洛伊木马	以虚假的身份和形象骗取他人账号口令等信息或诱使执行危险操作的行为。通常会造成敏感信息被窃取等后果
45	PSW	窃取口令	特洛伊木马	窃取用户账号和口令的行为,窃取口令的范围非常广泛,如网络游戏、即时聊天工具(QQ)、E-mail、网站登录凭证等。通常导致用户计算机账号信息泄露,后续导致系统被控、经济损失等后果
46	Ransom	勒索	勒索软件	修改用户计算机上存储的数据,使用户无法继续使用这些数据,或阻止计算机正常运行,当数据被“劫持”(封锁或加密)后,会向用户提出赎金(勒索)要求,赎金要求通常包含恶意汇款方式和地址。通常会直接导致用户经济损失、数据不可用甚至业务中断等后果
47	RAT	远程访问	特洛伊木马	指在用户不知情或未授权的情况下,受远程控制端指令并进行相关操作的行为。被控的计算机等设备会成为控制者的肉鸡,完全被对方控制
48	Rootkit	隐藏自身或其他恶意程序	特洛伊木马	在安装目标上隐藏自身及指定的文件、进程和网络链接等信息的行为。一般通过加载特殊的驱动,修改系统内核,进而达到隐藏信息的目的。可能导致系统被控等后果
49	Server-Ftp	通过 FTP 控制	其他	FTP 服务功能,攻击者通过一些商用或开源的 FTP 工具来控制受感染的机器或传播恶意软件
50	Server-Telnet	通过 Telnet 控制	其他	Telnet 服务功能行为,攻击者来利用攻击者通过一些商用或开源的 Telnet 工具来控制受感染的机器或传播恶意软件
51	Server-Web	通过 Web 控制	其他	Web 服务功能行为,攻击者利用攻击者通过一些商用或开源的 Web 服务软件控制受感染的机器或传播恶意软件
52	SMS	通过恶意短信传播	蠕虫	在用户不知情或未授权的情况下,发送或拦截短信的行为
53	Sniffer	网络监听	黑客工具	利用被动侦听技术,监视网络的状态、数据流动情况以及网络传输信息,以达到不法目的的行为。可能会造成数据泄露等后果

表 B.1 互联网恶意软件风险与行为标签编码（续）

序号	编码	风险与行为标签	对应互联网恶意软件主分类	行为说明与危害
54	Spammer	发送垃圾邮件	黑客工具、蠕虫	自动化发送大量包含营销信息、诈骗信息等无用信息的垃圾邮件的行为,常用于辅助其他攻击,可能被攻击者用于远程控制攻击第三方
55	Spoof	欺骗攻击	黑客工具	伪造数据、身份、来源等信息欺骗用户、系统或应用程序的行为。可能导致信息泄露或系统被控等后果
56	Spread	恶意传播	特洛伊木马	自动通过复制、感染、投递、下载等方式将自身、自身的衍生物或其他恶意软件进行扩散的行为。如通过短信、彩信、邮件、蓝牙通信技术、红外通信技术、无线网络技术等向其他设备发送恶意软件
57	Spy	间谍软件	特洛伊木马	在用户不知情或未授权的情况下,获取涉及用户个人信息、工作信息、保密信息、其他非公开信息或监视用户(跟踪键盘数据,屏幕截图,检索正在运行的应用程序),并将收集到的信息通过网络传输给攻击者的行为。通常会直接导致设备被控、信息被窃等后果
58	System	系统破坏	特洛伊木马	通过感染、劫持、篡改、删除、终止进程等手段导致系统部分或全部功能、用户文件等无法正常使用,干扰、破坏、阻断通信网络、网络服务或其他合法业务正常运行的行为
59	VirTool	病毒工具	黑客工具	生成或修改病毒的行为
60	Wipe	数据擦除	特洛伊木马	擦除设备上的数据,引发数据不可恢复的情况,导致不可逆的数据损失

附 录 C

(资料性)

恶意软件上报场景下互联网恶意软件通报描述格式完整示例

如下为某互联网恶意软件的完整描述格式示例：

```

<? xml version="1.0" ?>
<MalwareDescription>
  <Source>
    <FileName>Example.exe</FileName>
    <SourceName>VDS</SourceName>
    <Time>2020-05-31 12:32:54</Time>
    <Location>北京市</Location>
    <AttackCount>128</AttackCount>
    <SourceIPv4>222.112.*.*</SourceIPv4>
    <DestIPv4>222.1.*.*</DestIPv4>
  </Source>
  <SampleBasic>
    <Hash>
      <SM3>1AB21D8355CFA17F8E61194831E81A8F22BEC8C728FEFB747ED035EB5082AA2B</SM3>
      <SHA256>9feed0c7fa8c1d32390e1c168051267df61f11b048ec62aa5b8e66f60e8083af</SHA256>
    </Hash>
    <MalwareName>Ransomware.Win32.LockBit.e.[Ransom]</MalwareName>
    <FileSize>0xEFE00L</FileSize>
    <FileFormat>
      <FormatDesc>EXE</FormatDesc>
      <FormatID>001</FormatID>
    </FileFormat>
    <FileTime>
      <CreateTime>2023-10-19 12:50:00</CreateTime>
      <Modifytime>2023-10-19 12:50:00</Modifytime>
    </FileTime>
    <Packet>
      <ShellInfo></ShellInfo>
    </Packet>
    <Archive></Archive>
    <FileVersion>14.16</FileVersion>
    <PESturct>
      <FileHeader>
        <Machine>0x014c</Machine>
        <NumberOfSections>0x3</NumberOfSections>
        <NumberOfSymbols>0x0</NumberOfSymbols>
        <PointerToSymbolTable>0x0</PointerToSymbolTable>
      </FileHeader>
    </PESturct>
  </SampleBasic>
</MalwareDescription>

```

```

        <SizeOfOptionalHeader>0xe0</SizeOfOptionalHeader>
        <TimeStamp>0x60fe6569</TimeStamp>
    </FileHeader>
    <OptionalHeader />
    <DirectoryEntryImport>
        <DLL>
            <DllName>SHLWAPI.dll</DllName>
            <APIName>PathAppendW</APIName>
        </DLL>
        <DLL>
            <DllName>KERNEL32.dll</DllName>
            <APIName>CreateProcessW</APIName>
            <APIName>GetSystemTime</APIName>
            <APIName>lstrlenW</APIName>
            <APIName>LocalFree</APIName>
        </DLL>
        <DLL>
            <DllName>ADVAPI32.dll</DllName>
            <APIName>CheckTokenMembership</APIName>
            <APIName>CreateWellKnownSid</APIName>
        </DLL>
        <DLL>
            <DllName>ole32.dll</DllName>
            <APIName>CoCreateInstance</APIName>
            <APIName>CoSetProxyBlanket</APIName>
        </DLL>
    </DirectoryEntryImport>
    <Section>
        <Name>.text</Name>
        <VirtualAddress>0x1000</VirtualAddress>
        <MiscVirtualSize>0xdfe63</MiscVirtualSize>
        <SizeOfRawData>0xe0000</SizeOfRawData>
    </Section>
</PEStruct>
</SampleBasic>
<SampleAnalysis>
    <Platform>Win32</Platform>
    <ProcessThreadOperation>
        <Time ID="1" LogTime="2020-5-31 19:35:10">
            <ProcessID />1564<ProcessID />
            <ImagePath>c:\virus\63dcf75ad743b292e4a6cd067ffc2c18.3F6D2C67.exe</ImagePath>
            <Action>RUN_PROCESS</Action>
        </Time>

```

```

    <Time ID="37" LogTime="2020-5-31 19:37:17">
      <ProcessID>1564</ProcessID>
      <ImagePath>C:\Windows\System32\cmd.exe</ImagePath>
      <Action>CREATE_PROCESS</Action>
    </Time>
    <Time ID="2" LogTime="2020-5-31 19:35:12">
      <ProcessID />1564<ProcessID />
      <ImagePath>c:\virus\63dcf75ad743b292e4a6cd067ffc2c18.3F6D2C67.exe</ImagePath>
      <Action>CreateThread</Action>
    </Time>
  </ProcessThreadOperation>
  <FileOperation>
    <Time ID="3" LogTime="2020-5-31 19:35:11">
      <ProcessID>1564</ProcessID>
      <ImagePath>c:\virus\63dcf75ad743b292e4a6cd067ffc2c18.3F6D2C67.exe</ImagePath>
      <Action>CREATE_FILE</Action>
      <FileFullPath>C:\2ED873D4.lock</FileFullPath>
    </Time>
    <Time ID="4" LogTime="2020-5-31 19:39:16">
      <ProcessID>1564</ProcessID>
      <ImagePath>c:\virus\63dcf75ad743b292e4a6cd067ffc2c18.3F6D2C67.exe</ImagePath>
      <Action>Renamefile</Action>
      <FileFullPath>C:\program files\microsoft games\hearts\zh-cn\hearts.exe.mui
    </FileFullPath>
    </Time>
    <Time ID="17" LogTime="2020-5-31 19:37:11">
      <ProcessID>1564</ProcessID>
      <ImagePath>c:\virus\63dcf75ad743b292e4a6cd067ffc2c18.3F6D2C67.exe</ImagePath>
      <Action>Writefile</Action>
      <FileFullPath>C:\windows\SysWOW64\2ED873.ico</FileFullPath>
    </Time>
  </FileOperation>
  <RegisterOperation>
    <Time ID="0" LogTime="2020-5-31 20:32:7">
      <ProcessID>1564</ProcessID>
      <ImagePath>c:\virus\63dcf75ad743b292e4a6cd067ffc2c18.3F6D2C67.exe</ImagePath>
      <Action>CREATE_KEY</Action>
      <KeyName>HKEY_LOCAL_MACHINE\SOFTWARE\Classe\.lockbit</KeyName>
    </Time>
    <Time ID="1" LogTime="2020-5-31 20:32:7">
      <ProcessID>1564</ProcessID>
      <ImagePath>c:\virus\63dcf75ad743b292e4a6cd067ffc2c18.3F6D2C67.exe</ImagePath>
      <Action>SET_KEY_VALUE</Action>

```

```

<KeyName>\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Run</KeyName>

      <KeyValueName>63dcf75ad743b292e4a6cd067ffc2c18.3F6D2C67</KeyValueName>

      <ValueType>REG_SZ</ValueType>
<Value>C:\Users\ASUS\Desktop\63dcf75ad743b292e4a6cd067ffc2c18.3F6D2C67.exe</Value>
  </Time>
</RegisterOperation>
<MemoryOperation>
  <Time ID="1" LogTime="2020-5-31 20:32:6">
    <ProcessID>1564</ProcessID>
    <ImagePath>c:\virus\63dcf75ad743b292e4a6cd067ffc2c18.3F6D2C67.exe</ImagePath>
    <Action>WRITE_OTHER_PROCESS_VM</Action>
    <WriteProcess>C:\Windows\System32\cmd.exe</WriteProcess>
  </Time>
</MemoryOperation>
<OtherOperation>
  <Time ID="28" LogTime="2020-5-31 19:35:17">
    <ProcessID>1564</ProcessID>
<ImagePath>C:\virus\fl55de334e036c12393103bc14c99025a1b37bc902f6cbe02cba8ace696ceb67.6A4AE6E0
</ImagePath>
    <Action>CREATE_MUTANT</Action>
    <MutexName>DefaultTabtip-MainUI</MutexName>
  </Time>
</OtherOperation>
</SampleAnalysis>
<NetworkOperation>
  <ProcessID>1564</ProcessID>
  <ImagePath>c:\virus\63dcf75ad743b292e4a6cd067ffc2c18.3F6D2C67.exe</ImagePath>
  <Action>ACCESS_NETWORK</Action>
  <IPv4Address>20.101. *.9</IPv4Address>
  <Port>443</Port>
  <URL>time.windows.com</URL>
  <Domain>aaaaaaazb.xyz.org< Domain>
  <Email>aaaaa@gmail.com< Email>
</NetworkOperation>

```

参 考 文 献

- [1] GB/T 1988—1998 信息技术 信息交换用七位编码字符集
 - [2] GB/T 25068.1—2020 信息技术 安全技术 网络安全 第1部分:综述和概念
 - [3] GB/T 36643—2018 信息安全技术 网络安全威胁信息格式规范
 - [4] YD/T 2383—2011 互联网主机恶意程序描述格式
 - [5] YD/T 2439—2012 移动互联网恶意程序描述格式
 - [6] YD/T 2707—2014 互联网主机网络安全属性描述格式
-

