ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 37027—202X
代替GB/T 37027—2018

信息安全技术　网络攻击和网络攻击事件判定准则

Information security technology—Criteria for determinations of network attack and network attack incident

(点击此处添加与国际标准一致性程度的标识)

（征求意见稿）

2023-08-24

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 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。

本文件代替GB/T 37027—2018 《信息安全技术 网络攻击定义及描述规范》，与GB/T 37027—2018相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 调整了网络攻击的定义（见3.1）；
b) 增加了网络攻击事件的定义（见3.2）；
c) 调整了网络攻击的描述（见5.1）；
d) 调整了对安全漏洞的描述，删除“表3 安全漏洞分类表”，改为“见GB/T 30279—2020”（见5.1、5.2）；
e) 调整了对攻击方式的描述，删除“表2 攻击方式分类表”，改为与GB/T 20986—2023具有一致性的19类攻击技术手段（见5.1、6.1）；
f) 增加了网络攻击事件的描述（见5.2）；
g) 删除了对攻击严重程度的描述，增加了与GB/T 20986—2023具有一致性的事件分级描述（见5.2）；
h) 删除了对攻击后果的描述，增加了与GB/T 20986—2023具有一致性的事件影响描述（见5.2）；
i) 增加了网络攻击的判定指标（见6.1）；
j) 增加了网络攻击事件的判定指标（见6.2）；
k) 增加了网络攻击的计数标准（见7.1）；
l) 增加了网络攻击事件的计数标准（见7.2）。
m) 调整了对攻击对象分类的描述，对“表1 攻击对象分类表”的内容进行调整，并将表名改为“表A.1 攻击对象类型表”，从正文中删除，作为资料性附录（见附录B）；
n) 调整了对典型网络攻击过程的描述（见附录C）；
o) 增加了网络攻击和网络攻击事件的典型判定方法（见附录D）；

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：国家计算机网络应急技术处理协调中心北京分中心、国家计算机网络应急技术处理协调中心、中国移动通信集团有限公司、启明星辰信息技术集团股份有限公司、安天科技集团股份有限公司、北京长亭科技有限公司、国家工业信息安全发展研究中心、国能数智科技开发（北京）有限公司、郑州信大捷安信息技术股份有限公司、北京天融信网络安全技术有限公司、国家信息中心（国家电子政务外网管理中心）、中国信息通信研究院、广东省信息安全测评中心、中科信息安全共性技术国家工程研究中心有限公司、杭州安恒信息技术股份有限公司、北京升鑫网络科技有限公司、奇安信科技集团股份有限公司、中国电子信息产业集团有限公司第六研究所、北京时代新威信息技术有限公司、江苏君立华域信息安全技术股份有限公司、北京中测安华科技有限公司、中电科网络安全科技股份有限公司、北京神州绿盟科技有限公司、三六零科技集团有限公司、杭州迪普科技股份有限公司、公安部第三研究所、国家计算机网络应急技术处理协调中心黑龙江分中心、长安通信科技有限责任公司。

本文件主要起草人：赵彦、饶毓、卢卫、严寒冰、郭晶、徐剑、吕志泉、韩志辉、徐雅丽、陈亮、周莹莹、李一鸣、邱勤、杨天识、刘佳男、杨坤、张晓菲、牛月坤、刘为华、杨剑、闫桂勋、董航、甄茁、胡建勋、袁明坤、徐晓星、刘勇、赵云龙、俞政臣、刘德志、严默默、曹旭博、肖岩军、耿贵宁、刘吉林、陶源、刘琨、张洛什。

本文件及其所代替文件的历次版本发布情况为：

——2018年首次发布为GB/T 37027—2018 《信息安全技术 网络攻击定义及描述规范》。

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：网络攻击和网络攻击事件有何不同；网络攻击和网络攻击事件的界定和分类；网络攻击及网络攻击事件涉及的角色、过程、关键技术、后果评估；各类网络攻击的和网络攻击事件的判定及计数方法等内容。随着网络攻击事件的日益增多，当前各组织对网络攻击、网络攻击事件判定和计数标准不统一，导致各组织判定和统计网络攻击出现较大差异，难以有效实现网络攻击态势的共享和准确感知。面对各个层面的挑战,需对网络攻击和网络攻击事件进行准确的定义、描述，以及统一分类、判定及统计准则,提升网络攻击态势的感知效果，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　网络攻击和网络攻击事件判定准则

1 范围

本文件给出了网络攻击和网络攻击事件的描述信息要素、判定指标和计数标准。

本文件适用于指导组织开展网络攻击和网络攻击事件的监测分析、态势感知、信息报送等活动。

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 20986－2023　信息安全技术　网络安全事件分类分级指南

GB/T 30279—2020　信息安全技术　网络安全漏洞分类分级指南

3 术语和定义

GB/T 20986—2023、GB/T 30279—2020界定的以及下列术语和定义适用于本文件。

3.1

网络攻击　network attack

指通过计算机、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，其目的在于窃取、篡改、破坏网络和数据设施中传输和存储的信息；或延缓、中断网络和数据服务；或破坏、摧毁、控制网络和数据基础设施。

3.2

网络攻击事件　network attack incident

网络攻击（3.1）造成或潜在造成业务损失或社会危害的网络安全事件，包括一次或多次被识别的网络攻击。

4 缩略语

下列缩略语适用于本文件。

APT：高级可持续威胁攻击（advanced persistent threat）

ARP：地址解析协议（address resolution protocol）

AS：自治域（autonomous system）

BGP：边界网关协议（border gateway protocol）

DNS：域名系统（domain name system）

IOC：失陷指标（indicators of compromise）

IP：互联网协议（internet protocol）

WLAN：无限局域网（wireless local area network）

5 描述

5.1 网络攻击的描述

描述网络攻击的基本信息要素见表1。

表1 描述网络攻击的基本信息要素

信息要素	说明
标识号	每个网络攻击应具有唯一标识号
攻击对象	被实施网络攻击的客体信息，如被攻击设备的IP地址、域名，或具体的某个网络设备或者信息系统等
攻击对象分类	攻击对象的分类描述，见附录B
攻击源	实施网络攻击的主体信息，包括攻击者身份（如攻击组织名、网络身份标识）、攻击资源（如攻击者使用的直接攻击IP、真实攻击IP、控制域名）等
攻击技术手段	网络攻击使用的技术手段，包括网络扫描探测、网络钓鱼、漏洞利用、后门利用、后门植入、凭据攻击、信号干扰、拒绝服务、网页篡改、暗链植入、域名劫持、域名转嫁、DNS污染、WLAN劫持、流量劫持、BGP劫持、广播欺诈、失陷主机、其他，共19类。 注：GB/T 20986—2023中的供应链攻击事件、APT攻击事件一般是综合使用上述技术手段和其他非技术手段的网络攻击事件，因此不在攻击技术手段中单独设置相应的类别。
攻击时间	攻击发生的时间点或时间范围

描述网络攻击的扩展信息要素见表2。

表2 描述网络攻击的扩展信息要素

信息要素	说明
网络攻击名称	简要描述网络攻击
安全漏洞	攻击过程中所利用的网络或系统的安全脆弱性或弱点
安全漏洞类型	安全漏洞的类型，见GB/T 30279—2020
攻击源详细信息	攻击源的详细信息，包括国内/国外、组织内部/组织外部等
攻击阶段	攻击所处的阶段，见附录C
攻击详细信息	详细描述攻击行为、手法或过程等
判定方法	判定网络攻击所使用的方法，见附录D
扩展信息	可根据需要增加一个或多个扩展信息要素

5.2 网络攻击事件的描述

描述网络攻击事件的基本信息要素见表3。

表3 描述网络攻击事件的基本信息要素

信息要素	说明
标识号	每个网络攻击事件应具有唯一标识号
事件时间	攻击事件发生的时间点或者时间范围
事件类型	网络攻击事件的类型，见GB/T 20986—2023
攻击对象	同表1中的相关描述

攻击对象类型	同表1中的相关描述
攻击源	同表1中的相关描述
事件影响	网络攻击事件已造成或潜在造成的影响，包括影响对象的重要程度、业务损失的具体情况、社会危害具体情况等

描述网络攻击事件的扩展信息要素见表4。

表4 描述网络攻击事件的扩展信息要素

信息要素	说明
网络攻击事件名称	简要描述网络攻击事件
事件分级	网络攻击事件的分级描述，见GB/T 20986—2023，包括特别重大事件（一级）、重大事件（二级）、较大事件（三级）、一般事件（四级）
事件详细信息	详细描述网络攻击事件的行为、手法或过程等
安全漏洞	攻击过程中所利用的网络或系统的安全脆弱性或弱点
安全漏洞分类	安全漏洞的类别，见GB/T 30279—2020
攻击源详细信息	攻击源的详细信息，包括国内/国外、内部/外部、攻击组织等
攻击动机	可能的攻击动机，如政治、经济、兴趣、炫耀等
判定方法	判定网络攻击事件所使用的方法，见附录D
扩展信息	可根据需要增加一个或多个扩展信息要素

6 判定指标

6.1 网络攻击的判定指标

6.1.1 网络扫描探测攻击的判定指标

存在下列一种或者多种情况，判定发生网络扫描探测攻击：

a) 一定时间范围内，针对端口、路径、配置等的网络请求数量超出正常阀值范围，或网络请求内容存在遍历性和构造性；
b) 网络流量或设备/系统/软件日志中包含网络扫描软件的特征。

6.1.2 网络钓鱼攻击的判定指标

当通过网络传播的信息（如网页、网络邮件、软件、文件等）具有欺诈性、伪造性，且存在诱使访问者提交重要数据和个人信息的情况时，判定发生网络钓鱼攻击。

6.1.3 漏洞利用攻击的判定指标

存在下列一种或者多种情况，判定发生漏洞利用攻击：

a) 网络流量或设备/系统/软件日志中包含漏洞利用攻击包的特征；
b) 网络流量或设备/系统/软件日志中包含漏洞利用工具的特征。

6.1.4 后门利用攻击的判定指标

存在下列一种或者多种情况，判定发生后门利用攻击：

a) 网络流量或设备/系统/软件日志中包含后门利用攻击包的特征，如后门利用工具的特征；
b) 网络或信息系统中包含后门利用的痕迹，如后门执行文件等。

6.1.5 后门植入攻击的判定指标

存在下列一种或者多种情况，判定发生后门植入攻击：

a) 网络流量或设备/系统/软件日志中包含后门植入攻击包的特征，如后门植入工具的特征；
b) 网络或信息系统中包含后门植入的痕迹，如被植入的后门文件。

6.1.6 凭据攻击的判定指标

存在下列一种或者多种情况，判定发生凭据攻击：

a) 网络流量或者业务系统日志中包含攻击者在短时间内进行口令枚举猜解的行为特征；
b) 攻击者存在识别解析登录口令的行为。

6.1.7 信号干扰攻击的判定指标

存在下列一种或者多种情况，判定发生信号干扰攻击：

a) 通信信号质量下降，数据包丢失，通信中断等问题。通过监测信号的频谱特征、幅度变化、频率偏移等，可以检测到信号的异常表现；
b) 通信信号的信噪比下降、比特错误率增加、丢包率升高等指标的变化；
c) 通过检测与正常设备行为不一致的迹象，如未经授权的无线电发射器的存在，可以发现潜在的信号干扰攻击；
d) 过监测邻近通信链路的质量变化和异常行为。

6.1.8 拒绝服务攻击的判定指标

存在下列一种或者多种情况，判定发生拒绝服务攻击：

a) 网络流量中包含拒绝服务攻击的指令特征；
b) 网络或信息系统的流入流量或访问量超过正常阈值。

注：可通过设定或者自学习网络和信息系统的正常流量或正常访问量的阀值，并与实际流量、访问量进行比对。针对不同单位可以依据其重要程度设定不同的检测阀值。

6.1.9 网页篡改攻击的判定指标

存在网页内容被非授权恶意更改的情况时，判定发生网页篡改攻击。

6.1.10 暗链植入攻击的判定指标

存在下列一种或者多种情况，判定发生暗链植入攻击：

a) 发现存在未经授权的或异常的链接，指向恶意网站、下载恶意软件的链接或其他恶意资源；
b) 发现存在异常的访问流量模式，突然增加的访问量、来自不同地理位置或非正常的用户行为等；
c) 发现安全日志和监测出现异常行为，网站或应用程序文件被修改。

6.1.11 域名劫持攻击的判定指标

当域名的解析结果被非域名所有者指向非预期的IP地址的情况时，判定发生域名劫持攻击。

6.1.12 域名转嫁攻击的判定指标

当域名的解析结果被域名所有者指向了不属于所有者或者利益相关方所拥有的IP地址情况时，判定发生域名转嫁攻击。

6.1.13 DNS 污染攻击的判定指标

当网络中存在错误的DNS数据包，把域名的解析结果指向不正确的IP地址时，判定发生DNS污染攻击。

6.1.14 WLAN 劫持攻击的判定指标

存在下列一种或者多种情况，判定发生WLAN劫持攻击：

a) 无线网络大量的数据流量被重定向到未知的目标、数据包被篡改或通信被中断；
b) 频繁断连、连接到未知的或可疑的无线网络等；
c) 未经授权的无线接入点的出现、频繁的信道切换、无线信号干扰等。

6.1.15 流量劫持攻击的判定指标

存在下列一种或者多种情况，判定发生流量劫持攻击：

a) 实际流入流量与对端发出流量存在差别；
b) 实际流出流量与达到对端流量存在差别。

6.1.16 BGP 劫持攻击的判定指标

存在下列一种或者多种情况，判定发生BGP劫持攻击：

a) 攻击者使用伪造或篡改等手段污染BGP边界网关协议的路由数据，欺骗其他AS将流量引向攻击者指定的AS，此种情况下攻击者正在发送污染包劫持路径；
b) AS实际网络通信路由路径与合理的网络路由通信路径存在差别，此种情况下攻击者已经劫持了路径，并将流量引向其指定的AS。

6.1.17 广播欺诈攻击的判定指标

存在下列一种或者多种情况，判定发生广播欺诈。

a) ARP表中IP地址与MAC地址的映射与正常情况不一致或存在重复映射；
b) 网络中的数据流量和通信模式发现大量的冲突通信、数据包丢失、通信中断等异常情况；
c) 频繁地发送ARP请求、自动更新ARP表、重置网络接口等。

6.1.18 失陷主机攻击的判定指标

存在下列一种或者多种情况，判定发生失陷主机攻击：

a) 被控设备对外发送心跳包、控制指令响应包或开启非授权端口服务；
b) 被控设备中包含具有远程控制功能的恶意代码或者相关感染痕迹，例如特洛伊木马文件等；

6.1.19 其他网络攻击的判定指标

采取其他攻击技术手段的网络攻击行为。

6.2 网络攻击事件的判定指标

判定网络攻击事件需同时满足两个条件：一是已判定单个或多个相关的网络攻击；二是已判定的网络攻击造成或潜在造成业务损失或社会危害。

针对网络扫描探测、网络钓鱼、漏洞利用、后门利用、后门植入、凭据攻击、信号干扰、拒绝服务、网页篡改、暗链植入、域名劫持、域名转嫁、DNS污染、WLAN劫持、流量劫持、BGP劫持攻击、广播欺诈、失陷主机以及其他网络攻击事件，如存在已判定的使用相应攻击技术手段的网络攻击，且网络攻击造成或潜在造成业务损失或社会危害，则判定发生相应类型的网络攻击事件。

供应链攻击事件、APT攻击事件一般是综合使用多种攻击技术手段和非技术手段的网络攻击事件。

针对供应链攻击事件，通过分析相关攻击行为，如确认攻击方通过利用合法软件产品或网络服务的供应链中的脆弱性来实现其攻击意图，则判定发生供应链攻击事件。

针对APT攻击事件，存在下列一种或者多种情况，则判定发生APT攻击事件：

a）网络攻击中的IOC（失陷指标，即在网络或设备上发现的可作为系统疑遭入侵的证据，一般以结构化的方式记录）或者技战术属于已知APT组织；

b）攻击活动存在针对性、持久性和高隐蔽性，且攻击目标是重要信息系统或高价值个人，且攻击目的是窃取情报、破坏或者潜伏等待指令。

7 计数标准

7.1 网络攻击的计数标准

7.1.1 单次网络攻击

单次网络攻击指在一个时间点或一段时间范围内，依据6.1判定的网络攻击。

7.1.2 网络攻击的计数方法

网络攻击的计数指对包含特定要素信息的单次网络攻击进行统计，得到网络攻击的次数。

网络攻击的典型计数方法包括：

a) 使用特定技术手段的网络攻击计数：对要素信息中包含特定技术手段的单次网络攻击进行统计；

b) 特定攻击目标遭受的使用特定技术手段的网络攻击计数：对要素信息中同时包含特定攻击目标、特定技术手段的单次网络攻击进行统计；

c) 特定攻击源对特定攻击目标使用特定技术手段的网络攻击计数：对要素信息中同时包含特定攻击源、特定攻击目标、特定技术手段的单次网络攻击进行统计。

7.1.3 多个网络攻击计数结果的合并计算条件

多个网络攻击计数结果满足可比较或可累加条件时可合并计算。

满足以下条件的多个网络攻击计数结果可进行比较：多个网络攻击计数结果是使用完全相同的网络攻击判定指标、网络攻击计数方法得到的。

满足以下条件的多个网络攻击计数结果可进行累加：多个网络攻击计数结果是使用完全相同的网络攻击判定指标、网络攻击计数方法得到的，且不存在单次网络攻击被重复计数的情况。

除上述情况外，多个网络攻击计数结果不宜进行合并计算。

7.2 网络攻击事件计数标准

7.2.1 单个网络攻击事件

单个网络攻击事件指在一个统计周期内，依据6.2判定的相关网络行为，需要具有一个或多个相同要素信息的一次或者多次网络攻击。

一个统计周期一般为一个自然日，或者一个持续的攻击时间段，也可依据统计的实际情况设定。

针对各事件类型，单个网络攻击事件中包括的相关网络攻击宜具有的相同要素信息见表5。

表5 单个网络攻击事件中包括的相关网络攻击宜具有的相同要素信息

事件类型	单个网络攻击事件中包括的相关网络攻击宜具有的相同要素信息（以下均指一个统计周期内）	单个网络攻击事件的典型情况（以下均指一个统计周期内）
网络扫描探测事件	攻击源、攻击目标	一个攻击目标遭受一个攻击源的网络扫描探测攻击
网络钓鱼事件	攻击源	一个具有网络钓鱼功能的、可访问的钓鱼链接或文档
漏洞利用事件	攻击源、攻击目标	一个攻击源单次或多次成功利用一个攻击目标的漏洞
后门利用事件	攻击源、攻击目标	一个攻击源单次或多次成功利用一个攻击目标的后门
后门植入事件	攻击源、攻击目标	一个攻击源向一个攻击目标单次或多次成功植入后门
凭据攻击事件	攻击源、攻击目标	一个攻击源向一个攻击目标发起单次或多次凭据攻击，并成功获取正确的凭据
信号干扰事件	攻击目标	一个设备（如通信设备、雷达系统、导航设备等）遭受信号干扰攻击的影响
拒绝服务事件	攻击目标	一个攻击目标的业务遭受拒绝服务攻击的影响
网页篡改事件	攻击目标	一个网页的内容被单次或多次成功篡改
暗链植入事件	攻击目标	一个网页被成功植入单个或多个暗链
域名劫持事件	攻击目标	一个域名被单次或多次成功劫持
域名转嫁事件	攻击目标	一个域名被单次或多次成功转嫁
DNS污染事件	攻击目标	一个域名遭受单次或多次 DNS 污染
WLAN劫持事件	攻击目标	一个无线局域网遭受 WLAN 劫持攻击的影响
流量劫持事件	攻击目标	一个攻击目标被单次或多次成功流量劫持
BGP劫持攻击事件	攻击目标	一个攻击目标遭受 BGP 劫持攻击的影响
广播欺诈事件	攻击目标	一个局域网遭受广播欺诈攻击的影响
失陷主机事件	攻击源、攻击目标	一个攻击目标被一个攻击源成功远程控制
供应链攻击事件	攻击目标	一个攻击目标发生供应链攻击事件
APT事件	攻击源、攻击目标	一个攻击源对一个攻击目标的 APT 攻击事件
其他网络攻击事件	宜根据具体情况确定	宜根据具体情况确定

7.2.2 网络攻击事件的计数方法

网络攻击事件的计数指对包含特定要素信息的单个网络攻击事件进行统计，得到网络攻击事件的个数。

网络攻击事件的典型计数方法包括：

a) 特定类型的网络攻击事件计数：对要素信息中包含特定事件类型的单个网络攻击事件进行统计；

b) 特定攻击目标的特定类型网络攻击事件计数：对要素信息中同时包含特定攻击目标、特定事件类型的单个网络攻击事件进行统计；

c) 特定攻击源、特定攻击目标的特定类型网络攻击事件计数：对要素信息中同时包含特定攻击源、特定攻击目标、特定事件类型的单个网络攻击事件进行统计。

7.2.3 多个网络攻击事件计数结果的合并计算条件

多个网络攻击事件计数结果满足可比较或可累加条件时可合并计算。

满足以下条件的多个网络攻击事件计数结果可进行比较：多个网络攻击事件计数结果是使用完全相同的网络攻击事件判定指标、网络攻击事件计数方法得到的。

满足以下条件的多个网络攻击事件计数结果可进行累加：多个网络攻击事件计数结果是使用完全相同的网络攻击判定事件指标、网络攻击事件计数方法得到的，且不存在单个网络攻击事件被重复计数的情况。

除上述情况外，多个网络攻击事件计数结果不宜进行合并计算。

附 录 A
（资料性）
网络攻击概述

网络攻击为利用网络存在的漏洞和安全缺陷对网络系统的硬件、软件及其系统中的数据进行的攻击。网络攻击具有动态和迭代性，随着攻击过程的进行，攻击者对目标的掌握和控制程度不断深入，可实施的攻击面越大，可能造成的安全影响也越大。根据网络攻击实施步骤的粗细层次及复杂程度，网络攻击又可分为单步攻击和组合攻击。单步攻击是具有独立的、不可分割的攻击目的的简单网络攻击，组合攻击是单步攻击按照一定逻辑关系或时空顺序进行组合的复杂网络攻击。通常情况下，一个典型的复杂网络攻击过程包括侦查、资源开发、初识访问、执行、持久化、提权、防御规避、凭证访问、发现、横向移动、收集、命令与控制、数据渗出、影响等步骤。典型网络攻击过程的详细描述参见附录C。

从生命周期角度看，一次网络攻击涉及的角色（包括参与者和利益相关者）包括4类：

a) 网络攻击者：利用网络安全的脆弱性，以破坏、窃取或泄露信息系统或网络中的资源为目的，危及信息系统或网络资源可用性的个人或组织，如某黑客组织。
b) 网络攻击受害者：在网络攻击的活动中,信息、资源或财产受到侵害的一方，如某互联网应用提供商。
c) 网络攻击检测者：对网络运行和服务、网络活动进行监视和控制,具有对网络攻击进行安全防护职责的组织。
d) 网络服务提供者：为网络运行和服务提供基础设施、信息和中介、接入等技术服务的网络服务商和非营利组织，如云服务提供商、电信运营商等。

附 录 B
（资料性）
典型攻击对象类型

典型攻击对象类型如0所示。

表 B.1 攻击对象类型表

一级分类	二级分类	说明
计算机	移动终端	如智能手机、平板（Pad）等
	PC	个人电脑，如台式机、笔记本等
	服务器	为客户端提供特定应用服务的计算机系统
	其他	
工控设备	SCADA	数据采集与监视控制系统
	PLC	可编程逻辑控制器
	DCS	分布式控制系统
	其他	
网络设备	路由器	基于路由协议机制和算法选择路径或路由，建立和控制不同网络间数据流的网络设备
	交换机	利用内部交换机制来提供连通性的设备
	网关	除路由器、交换机之外的其他网关类产品，如防火墙等
	集线器	主要功能是对接收到的信号进行再生整形放大，以扩大网络的传输距离，同时把所有节点集中在以它为中心的节点上
	其他	
操作系统	Windows 系列	
	Unix 系列	
	MacOS 系列	
	IOS系列	
	Android系列	
	其他	
服务软件	数据库服务	包括关系型和非关系型数据库，对存放在库中的数据进行统一管理和处理等，并对外提供服务访问接口
	电子邮件服务	包括支持POP3协议、IMAP协议、SMTP协议等的email服务端
	FTP服务	文件传输服务，包括服务端的文件浏览、下载、上传等
	Web服务	支持处理浏览器等Web客户端的请求并返回相应处理结果，也可以放置网站、数据文件，供Web客户端浏览、下载
中间件 包括如COM、CORBA、J2EE、Docker、tomcat 、weblogic、jboss等	中间件	提供系统软件和应用软件之间连接的软件,以便于软件各部件之间的沟通,特别是应用软件对于系统软件的集中的逻辑
	其他	
用户软件	办公软件	如文档编辑、图表编辑类工具软件等

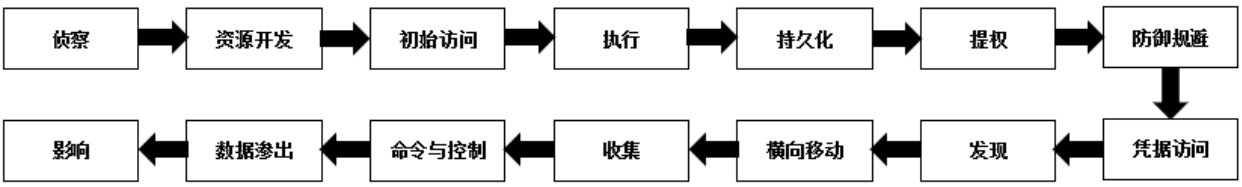
表 B.1 攻击对象类型表（续）

一级分类	二级分类	说明
	社交软件	通过网络来实现社会交往目的的软件
	支付软件	直接支持金融支付功能的软件
	其他	
网络基础设施	电信网	包括固网和移动通信网（如3G、4G和5G等）
	DNS	域名服务设施
	云计算平台	IaaS/PaaS/SaaS类型的云计算平台
	CA	证书颁发机构
	其他	

附 录 C
（资料性）
典型网络攻击过程

C.1 概述

网络攻击的典型过程如图B.1所示：



图B.1 网络攻击的典型过程

C.2 侦察

在实施网络攻击前，攻击者通过主动或被动信息收集技术，收集可以用来规划未来攻击行动的信息，包括受害组织信息、基础设施信息、人员详细情况信息等，攻击者能够利用收集的信息为实施网络攻击进行准备，为全生命周期其它阶段提供帮助。

C.3 资源开发

根据收集到的详细信息，攻击者通过创建、购买或破坏/窃取可用于支持目标定位的资源的技术，建立可用于支持行动的资源，包括基础架构、受害者账户等资源，攻击者能够利用开发的资源为全生命周期其它阶段提供帮助。

C.4 初始访问

攻击者通过使用鱼叉式网络钓鱼、利用Web服务器上漏洞等技术在目标网络中获得初始立足点。通过初始访问获得的立足点能够允许攻击者在目标网络中继续访问或攻击。

C.5 执行

攻击者在本地或远程系统上控制恶意代码执行，执行恶意代码技术通常与网络搜索、窃取数据等其它策略的技术结合使用。例如，攻击者使用远程访问工具来运行执行远程系统发现的PowerShell脚本等。

C.6 持久化

攻击者通过使用当出现重启、更改凭证、其它可能切断其访问的情况时，在中断期间保持对目标系统访问的技术，保障攻击者立足点。

C.7 提权

攻击者利用系统漏洞、错误配置等，在目标系统或网络上获得更高级别权限；通过提升权限，攻击者才能达成更多目的。提权技术通常与持久化技术重叠。

C.8 防御规避

攻击者利用卸载/禁用安全软件、混淆/加密数据和脚本等技术，以及通过利用受信任进程隐藏/伪装恶意软件等，避免在入侵目标网络过程中被发现。

C.9 凭证访问

攻击者通过键盘记录、凭证转储等技术窃取账户名和密码等。攻击者利用合法凭证访问目标系统，难于被发现，并提供了创建更多账户以帮助实现攻击目标的机会。

C.10 发现

攻击者搜索其可以控制的内容以及切入点周围的内容，获取有关系统和内部网络的知识，帮助在行动之前观察目标环境并确定行动方向。

C.11 横向移动

攻击者利用进入和控制网络远程系统的技术搜索整个网络以找到最终目标，攻击者可能会安装自己的远程访问工具，也可能将合法凭证与本机网络和操作系统工具一起使用来完成横向移动。

C.12 收集

攻击者利用收集信息相关技术在目标网络中收集其感兴趣的数据，收集目标源包括各种驱动器类型、浏览器、音频、视频和电子邮件等，收集方式包括截图、键盘输入等。

C.13 命令与控制

攻击者利用网络通信技术与受感染的系统通信并对其进行控制，通常攻击者会尝试模仿正常的预期流量以避免被发现，以及根据目标网络结构和防御情况建立具有隐蔽功能的命令和控制。

C.14 数据渗出

攻击者收集到目标数据后，通常采用压缩、加密等方式将数据打包以避免在渗出数据时被发现。从目标网络渗出数据技术包括通过命令和控制通道或备用通道传输数据、对传输设置大小限制等。

C.15 影响

攻击者利用破坏、篡改数据等技术，通过操纵业务和操作流程来破坏网络可用性或损害完整性，攻击者使用相关技术实现最终目的或为机密数据泄露提供掩护。

附 录 D
（资料性）
网络攻击和网络攻击事件的典型判定方法

D.1 网络攻击的典型判定方法

网络或信息系统运营者、安全厂商、行业主管机构、监管机构等可使用以下方法中的一种或者多种判定网络攻击：

a) 通过在网络安全设备或软件系统中发现和判定网络攻击的行为。如在流量监测设备中发现典型的漏洞利用攻击包特征，进而可判定发现漏洞利用攻击。网络安全设备或软件系统包括但不限定于防火墙、入侵检测设备、入侵防御设备、流量分析设备、蜜罐、APT检测设备、日志审计设备等。

b) 通过人工查看分析终端主机、交换机、服务器、软件等设备的日志、状态等信息，结合正常操作规律，对信息进行主观分析，从而发现和判定网络攻击。

c) 通过威胁信息共享或者其他外部途径，从个人或组织处获取关于网络攻击的指标或者其他关联线索，从而判定网络攻击行为。

D.2 网络攻击事件的典型判定方法

网络或信息系统运营者、安全厂商、行业主管机构、监管机构等可使用如下方法中的一种或者多种判定网络攻击事件：

a) 首先判定网络攻击，然后确认网络攻击已造成或潜在造成业务损失或社会危害；

b) 首先确认业务损失或社会危害已发生或潜在发生，然后判定造成业务损失或社会危害的网络攻击。

存在下列一种或者多种情况，可确认业务损失或社会危害已发生或潜在发生：

a) 网络安全设备或软件系统判定网络攻击已经成功；

b) 通过对终端、交换机等设备取证分析，确认存在非授权的操作行为；

c) 通过受害方核实或外部线索佐证，确认业务损失或社会危害已发生或潜在发生。

参 考 文 献

[1] GB/T 5271.8—2001 信息技术 词汇 第8部分:安全

[2] GB/T 7408—2005 数据元和交换格式 信息交换 日期和时间表示法

[3] 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

[4] GB/T 25069—2010 信息安全技术 术语

[5] GB/T 20985.1 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

[6] GB/T 37027—2018 信息安全技术 网络攻击定义及描述规范