CSDE

Council to Secure the Digital Economy

国际反僵尸网络指南 2018年

USTELECOM THE BROADBAND ASSOCIATION | ITI

Consumer Technology Association™

注意

《国际反僵尸网络指南》旨在通过全球互联网和通信生态系统中不同利益相关方的自愿参与和协作，促进缓解僵尸网络和其他自动化分布式威胁。《指南》向信息和通信技术利益相关者提供信息和鼓励，根据他们各自的情况和彼此之间的关系，采取消极措施为实现这一目标而采取的措施。

《指南》重点介绍了从"基准"到"高级"的信息和通信技术部门各个环节的有效自愿做法。虽然制定本指南的行业领导者认识到，没有任何组合措施可以保证消除所有威胁和风险，但他们认为，基线和先进实践均为ICT利益相关方提供了宝贵的框架，可帮助其确定和选择以下实践：自行缓解自动分布式攻击的威胁。《指南》认识到，不同的ICT利益相关者在实施安全措施时面临着不同的挑战，考虑因素和优先事项。
因此，本《指南》和《指南》确定的做法是信息和通信技术利益相关方应根据情况实施的工具；它们不是要求或强制性要求，也不以其他任何方式强制性规定。

大型企业已经在使用本文档中讨论的许多实践和技术来保护其网络和系统，从网络服务提供商的深度数据包检查（DPI）合同到禁止使用没有足够的内置安全措施。但是，在更广泛的消费者空间中实施这些功能具有更广泛的政策含义。例如：

- IP流量DPI等高级功能虽然在某些情况下有用，但如果部署在公共网络上，可能会对个人隐私产生重大影响。
- 如果政府要求满足其他政策目标，则基于IP地址和其他手段过滤公共网络流量也可能会影响信息自由流动。
- 企业拥有技术娴熟的信息技术人员，可以与供应商协商详细需求，并将成本效益分析纳入决策制定。这种动态变化在消费者空间中并不存在，因为成本效益分析与大型企业的成本效益分析可能存在显着差异。对于消费者而言，需要在不同的风险管理规模上评估成本和消费者保护问题。
- 在不考虑国际贸易影响和其他地方法规的情况下，不能简单地临时禁止在特定国家/地区禁止视为安全功能不足的设备。

内容

01 执行摘要

数字经济保护理事会（CSDE）和消费者技术协会（CTA）™成员涵盖整个复杂的全球互联网和通信生态系统，提供基础设施，软件和设备，使世界上大部分消费者受益，小型企业，大型私营企业，政府和非营利组织（统称为全球数字经济）。

为本指南做出贡献的公司是最早采用自愿方法保护生态系统免受网络威胁的公司。同时，技术领域受益于全球硬件，软件，设备和系统以及相关服务提供商的按设计安全实践，托管安全服务和生命周期支持。尽管如此，基础设施提供商，软件开发人员，设备和系统制造商，系统安装程序以及所有类型的企业仍然面临挑战。

CSDE与CTA密切合作制定的《国际反僵尸网络指南》，借鉴了这些利益相关方的不同全球视角，实践和经验，应对僵尸网络和其他自动化，分布式威胁对全球数字经济的持续不断增长的挑战。

激活共同责任确保全球数字经济。数字经济一直是全球商业增长和生活质量改善的引擎。但是，无论是公共部门还是私营部门，都没有一个利益相关者控制这个系统。相反，安全地管理这种增长所带来的机会，是信息和通信技术（ICT）社区每一位利益相关者的挑战和责任。

然而，近年来，僵尸网络对数字经济的损害越来越大，成本越来越高。僵尸网络是由受到攻击的互联网连接的计算机和设备组成的大型网络，恶意行为者可以命令进行分布式拒绝服务（DDoS）攻击，勒索软件传播，网络钓鱼攻击和虚假信息
虚假社交媒体和其他恶意行为的放大活动。1不幸的是，随着联网人员，企业和设备数量的增长，这些恶意攻击的潜力也在增加。如今，僵尸网络的破坏力呈指数级增长，因为它们攻击并利用了数十亿个物联网设备，到2020年估计将达到200亿个互联设备。全球网络犯罪成本预计将达到数万亿美元。僵尸网络是造成这些损失的工业规模驱动因素。

事实上，僵尸网络威胁今天比历史上任何时候都严重。最近已记录到对大型组织的大规模高调攻击，而规模较小，低调攻击的暗流造成了持续但未知的危害。这些发展给数字经济带来了直接的，有形的成本（总计数十亿美元）。的

无形成本同样有害，因为这些威胁破坏了对数字经济的基本信心和信任。

本指南旨在扭转这些趋势。尽管本指南的开发者强烈支持政府在建立多样化生态系统中发挥的重要作用，但实施
注重法规遵从性的规定性法规要求将抑制安全创新，这对于保持领先于当今复杂威胁的关键。此外，早期的政策努力是基于
基于针对这些威胁的乌托邦式解决方案，其前提是互联网服务提供商（ISP）可以简单地关闭所有僵尸网络，或者制造商可以确保所有设备都具有普遍安全性。
相反，以自愿共识标准为基础，以市场需求为驱动力，并在全球数字经济中由利益相关者实施的动态，灵活解决方案是应对这些不断发展的系统挑战的更好解决方案。

为实现此类解决方案并鼓励所有利益相关方分担责任，本指南提出了一系列利益相关方应实施的基线实践；
此外，它重点介绍了当前可用但未充分利用的其他高级功能。广泛实施本指南中的安全实践将大大减少僵尸网络，帮助保护全球数字经济。《指南》提供了针对全球挑战的现实，当前可用的解决方案，一个利益相关者群体或一个国家/地区或任何政府授权都无法解决。该指南得益于与多个行业和国家的公司持续合作以大幅减少僵尸网络威胁，以及对迅速发展的全球威胁和漏洞以及越来越强大和坚定的对手的分析。

本指南以下列核心安全原则为前提，并肯定地寻求推进：

- 安全需要动态，灵活的解决方案，这些解决方案必须由强大的全球市场力量驱动，并且与需要缓解的网络威胁一样灵活，适应性强，而不是根据地方或国家/地区司法管辖区不同而制定的法规遵从机制。
- 安全是互联网和通信生态系统中所有利益相关方的共同责任。政府和行业利益相关者应提倡增加所有参与者责任的解决方案，而不是在某些选定组成部分或利益相关者中寻求简便的解决方案。
- 安全依赖于政府，供应商，提供者，研究人员，企业和消费者之间的互利团队合作和伙伴关系，通过对不良行为者采取集体行动并为负责任的行为者做出贡献而获得奖励。

这些原则是环境要求的僵尸网络缓解新方法的基础。

《国际反僵尸网络指南：实践和能力摘要》。由互联网和相关的通信生态系统组成的“系统系统”的复杂性和多样性使得不可能提供一套统一适用于所有利益攸关方的指导。《指南》根据提供商，供应商和用户利益相关者的五种构成类型将这些不同的组件分类：（1）基础设施，（2）软件开发，（3）设备和设备系统，（4）家用和小型企业系统安装，以及（5）企业。对于上述每个方面，《指南》都列出了所有此类利益相关方都应渴望达到的基准实践，以及市场上目前可用的高级功能（如果未充分利用）。这些实践和功能（以下简要概述）是本指南的核心。

1. *基础设施。在本指南中，“基础设施”是指支持连接和可操作性的所有系统，不仅指互联网服务，骨干网络，云，网络托管，内容交付，域名系统和其他服务提供商的物理设施，而且还有软件定义的网络和其他系统，能够反映互联网从有形事物到数字概念的演变。我们建议基础设施的基准实践和高级功能包括：*
   - 检测恶意流量和漏洞
   - 缓解分布式威胁
   - 与客户和对等协调
   - 地址域占用和删除

2. *软件开发。2软件是生态系统其他各个组成部分中越来越普遍的元素。各种各样的复杂开发过程和相互依存关系推动软件创新和改进。我们建议软件通常由基准实践和高级功能组成，包括：*
   - 设计安全开发实践
   - 安全漏洞管理
   - 安全开发流程的透明度

3. *设备和设备系统。3单个连接的设备（或“端点设备”）本身可以由多个组件组成，包括硬件模块，芯片，软件，传感器或其他操作组件。除单个设备本身之外，还有多个附加的连接层，构成一个高度动态的新市场，包括安全创新。对于物联网中的端点“事物”及其附带的应用程序和服务，我们建议基准实践和高级功能包括：*
   - 设计安全开发实践
   - 信任之源
   - 产品生命周期管理，包括寿命终止
   - 以安全为重点的工具链使用

4. *家用和小型企业系统安装。4家用和小型企业可从几种类别的连接设备中受益。这些系统可以由自己动手的家庭和企业主安装，也可以由专业人员安装，例如集成商，警报承包商等。我们强烈建议您使用互联家庭安全系统，5建议采用以下基准实践和高级功能：*

   - 身份验证和凭证管理
   - 网络配置
   - 网络硬件管理
   - 安全维护

5. *企业6。作为网络设备和系统的主要所有者和用户，包括物联网设备系统数量呈指数增长，各种企业（政府，私营部门，学术界，非营利组织）在保护数字安全方面可发挥关键作用生态系统。对于企业，建议基线实践和高级功能包括：*

   - 安全更新
   - 实时信息共享
   - 安全管理流量流的网络体系结构
   - 增强的分布式拒绝服务抵御力
   - 身份和访问管理
   - 缓解传统和盗版产品问题

后续步骤和实施。发行本指南仅是第一步。接下来，我们将在战略上与广泛的利益相关者合作，包括志趣相投国家的政府，以推广《指南》的基准实践和先进能力。此外，我们将每年更新，发布和推广该指南的新版本。

数字经济一直是全球商业增长和生活质量改善的引擎，在每个大洲创造就业机会。它可能已占全球经济价值的20%。

02 引言

数字经济保护理事会（CSDE）7和消费者技术协会（CTA）™成员涵盖了整个复杂的全球互联网和通信生态系统。这些组织属于会员公司，这些公司提供的人力和技术系统可以创建，管理和安装连接功能，软件和设备，这些功能将从世界上相当大的消费者，小企业，大型私营企业，政府和非政府组织中受益。利润-全球数字经济。 CSTA与CTA密切合作制定的《国际反僵尸网络指南》借鉴了这些利益相关者的不同国际视角及其有影响力的做法和现实世界行动，应对数字经济持续不断增长的挑战：僵尸网络以及其他自动化的分布式威胁9。

挑战概述。数字经济一直是全球商业增长和生活质量改善的引擎，在每个大洲创造就业机会。据一些估计，它可能已经代表了全球经济价值的20%。10虽然仅靠国内生产总值不能完全体现数字经济对全球经济价值的贡献-并非所有数字化价值都涉及商业交易-《华尔街日报》报道2016年数字经济价值11.5万亿美元，到2025年可能增至23万亿美元，占全球GDP的近四分之一。11商业和消费者对新技术的采用不断推动数字经济的增长。12这一惊人的增长是信息和通信技术（ICT）社区每个利益相关方的挑战和责任。

然而，近年来，僵尸网络对数字经济的损害越来越大，成本越来越高。他们能够传播恶意软件，13进行拒绝服务攻击，14并在社交媒体上人工传播腐蚀性信息。15一个僵尸网络现在可以包括超过3000万个“僵尸”端点，并允许恶意行为者每月获利六位数。 16如今，由于庞大的系统数量，系统受到的攻击比以往任何时候都多。
以及数字经济本身有希望的增长，特别是数十亿个物联网设备的快速部署，预计到2020年将达到200亿个互联设备。17这种互联经济的好处正在彻底改变企业和消费者活动，造福人类以及开发本指南的公司在部署设备时正在创新新的安全措施。尽管如此，不安全的设备仍在不断涌入市场，而没有专门用于保护设备的系统。18此外，相对不熟练的恶意行为者现在有可能租用强大的僵尸网络来进行大规模的邪恶活动。19

这些发展给数字经济带来了直接的，有形的成本。例如，自2017年以来，恶意软件已遍及欧洲，亚洲和美洲，造成超过100亿美元的损失20.据估计，仅在未来五年内，网络犯罪将在全球范围内为企业造成总计8万亿美元的损失。 （罚款，业务损失，修复成本等）。21

> “建立僵尸网络需要跨界和多学科协作，创新技术方法，以及广泛部署遵循互联网基本原则的缓解措施。”
> -互联网社会

无形成本同样有害，因为这些威胁破坏了人们对数字经济的基本信心和信任。

战略姿势和目标。我们旨在扭转这些趋势。虽然我们认识到并支持政府在帮助引导生态系统中不同参与者的活动方面发挥重要的召集作用，但我们也相信基于合规性的监管要求实际上抑制了领先于当今复杂环境的安全创新。威胁。换句话说，不仅规定性监管要求很少见效，而且实际上通常与安全目标相反。22动态，灵活的解决方案由自愿共识标准提供信息，由市场需求驱动，并由利益相关方在整个全球范围内实施全球数字经济是应对不断发展的系统挑战（如威胁该复杂生态系统中所有参与者的恶意僵尸网络的最佳解决方案）。

因此，本指南旨在赋权数字经济中负责任的参与者，确保其未来并充分利用其全部潜力。我们认为，从长远来看，积极合作和集体行动将对所有利益相关者（不论大小）产生商业利益。为此，可以使用本指南来增强互联网和通信生态系统的弹性，并增强基础数字基础设施的交易完整性。指南敦促全球数字市场中的所有利益相关方实施一系列基准工具，实践和流程；此外，它重点介绍了当前可用的其他高级功能，但也许仍未充分利用。广泛实施本指南中的安全实践将大大减少僵尸网络，帮助保护全球数字经济。

方法和后续步骤。编写本指南的公司对做法和材料进行了全面审查，展示了已知有效抵御僵尸网络等自动化分布式攻击的技术和工具；他们还研究了政府和国际机构的报告，并征询了行业，学术界和民间社会的外部专家和消息来源。23但需要明确的是，发布本指南仅仅是第一步。接下来，我们将战略性地与包括政府在内的广泛利益相关方进行互动

志趣相投的国家/地区，以推广《指南》的基准实践和先进功能。此外，我们将每年更新，发布和推广该指南的新版本。

03 僵尸网络：解决多样化互联网生态系统中的自动化分布式威胁

对全球互联网和通信生态系统的自动化，分布式威胁最突出的类别是僵尸网络，僵尸网络是指与具有命令和控制功能的服务器通信的受损互联网连接计算机和设备的大型网络。

僵尸网络通过恶意软件在全球范围内传播，恶意软件扫描互联网上的不安全网络，计算机和其他连接设备。当僵尸网络入侵了足够数量的设备后，犯罪分子和其他不良行为者可以命令他们实施各种邪恶行为，例如分布式拒绝服务（DDoS）攻击，勒索软件传播，网络钓鱼攻击和人为虚假信息操作放大虚假的社交媒体帖子24。

今天，僵尸网络威胁比历史上任何时候都更加严重。在2000年代初，犯罪分子主要使用僵尸网络进行最基本的拒绝服务攻击，使虚构的目标网站和网络活动泛滥成灾。随着时间的流逝，他们的能力不断增强。通过利用恶意软件感染大量设备，黑客发现他们能够大规模开展恶意活动。 2007年，一个名为“ Storm Worm”的僵尸网络被发现收集了近5,000万台计算机，用于进行股票价格欺诈和身份盗窃等犯罪。 2009年，发现一个僵尸网络每天发送令人难以置信的740亿封垃圾邮件。252011-2013年，攻击者利用僵尸网络发起针对北美银行的分布式拒绝服务攻击运动，向其网站发送互联网流量来自世界各地的僵尸网络节点。26

如今，罪犯使用大型僵尸网络处理各种网络犯罪，从加密货币挖掘到分布式拒绝服务攻击，例如2016年针对域名系统提供商Dyn的历史性Mirai僵尸网络攻击。 2016 Mirai僵尸网络恶意软件使用默认登录凭证列表进行传播，获得近40万个访问权限
终端设备（如闭路电视摄像机和数字视频录像机），而车主没有注意到或内部化其设备被感染的任何经济后果。27攻击-按僵尸网络驱动的流量，是先前针对设备的攻击量的四倍主要银行—暂时禁止用户访问关键的在线平台和服务，对许多依赖Airbnb，Amazon.com，BBC，CNN和Netflix等公司在线服务的用户造成严重问题。28

虽然大多数僵尸网络无法达到Mirai的规模29，但许多小型僵尸网络攻击能够关闭网站和服务，传播勒索软件，并在社交媒体上传播虚假信息。不幸的是，缺乏技术知识来构建自己的僵尸网络的犯罪分子更容易获得较小的攻击功能。在黑市发现的在线市场上，新手黑客可以购买工具包来设计满足个性化需求的独特僵尸网络，称为“恶意软件即服务”（MaaS）。如果犯罪客户不想开发或购买僵尸网络，则可以每天低至0.66美分租用一个僵尸网络。30犯罪分子只需购买功能（如分布式拒绝服务攻击），低至20.31美元。这是一个蓬勃发展的

创新市场。例如，在Mirai攻击后不久，僵尸网络的创建者在线发布了Mirai源代码，自那时以来，许多其他有抱负的黑客制作了原始Mirai代码的变体。

恶意行为者不断发现僵尸网络的新用途。例如，黑客使用僵尸网络来复兴声名狼藉的WannaCry勒索软件，使超过150个国家/地区的200,000多台计算机系统瘫痪，迫使银行，医院，大学和其他机构关闭或向罪犯支付赎金32。当安全研究人员意识到恶意软件正在查询一个未注册的域时，WannaCry爆发才停止。注册域名的后果是“僵尸开关”关闭了僵尸网络。33黑客利用“ Mirai僵尸网络的模仿者”狠狠地攻击了该域名。其目标是使暂时失败的勒索软件复活。34同时，出现了比WannaCry更复杂的勒索软件——Petya，在全球范围内造成了严重破坏，基于Petya的恶意软件（称为NotPetya）的成本更高。超过100亿美元的损失35。

恶意僵尸网络的功能有可能破坏对数字经济的基本信心和信任。

不幸的是，随着联网人员，企业和设备数量的增长，大型恶意软件的潜力，力量和利润也随之增长。攻击。如上所述，全球正在使用的连接设备总数为数十亿，并非巧合的是，全球网络犯罪成本预计将达到数万亿。僵尸网络是该问题的工业规模驱动因素。除了明显的经济损失外，恶意僵尸网络的功能还可能破坏对数字经济的基本信心和信任。这种结果不利于量化，但其负面影响却可能使人衰弱，就像对污染的担忧威胁着我们对呼吸空气和饮用水的信心一样。

在高度多样化，复杂和相互依存的全球互联网生态系统中处理僵尸网络的根本挑战在于，互联网的基本本质是非分层和高度连接的。没有任何一个利益相关者（政府或私营部门）控制该系统，但我们依靠它连接我们所有人。对抗恶意僵尸网络是典型的“公地悲剧”挑战：如果每个人都与互联网公有利益并不可避免地建立了联系，但没有人控制，那么谁负责清理威胁每个人基本功能的恶意僵尸网络依靠？

答案是，所有利益相关者必须承担责任，而不仅仅是清理公地的利他目的。生态系统中的每个实体在减少恶意僵尸网络方面都有各自的利益。僵尸网络用于攻击所有ICT产品所依赖的互联网，而参与僵尸网络攻击会直接影响执行力或损害声誉，从而损害相关公司。

应对生态系统挑战的先前努力

负责实施本指南的公司最早采用自愿措施保护生态系统免受僵尸网络侵害。例如，2012年，美国通信行业领导人制定了针对互联网服务提供商的《反僵尸网络行为守则》，采取了有意义的行动，通过教育，检测，通知，补救和协作根除僵尸网络。同时，技术部门受益于
全球硬件，软件，设备和系统以及相关服务提供商的按设计安全实践，托管安全服务和生命周期支持。

尽管如此，整个生态系统仍面临挑战：

- 许多互联网服务提供商（ISP）和其他基础设施提供商都在不断推动市场进入安全性更高的状态，以缓解僵尸网络威胁。随着僵尸网络规模和复杂性的增加，运营基础设施网络的公司已经增加了网络容量，以保护客户免受日益严重的攻击。
  但是，所有利益相关者在生态系统中高效运营还有许多工作要做，而较小的提供者通常需要指导和资源以达到基准。
- 软件对于所有全球商业和政府流程都是不可或缺的。数字经济中的不同利益相关者越来越依赖安全软件。这种依赖激励了不良行为者不断发展
  复杂的漏洞利用。作为回应，负责任的公司已经制定了软件开发安全实践并制定了基本安全目标。
  产品生命周期的每个阶段。这些是小型开发人员可以效仿的实践。
- 联网设备系统的开发，部署和使用方面的惊人创新是一把双刃剑，向世界引入了数十亿台新的互联网设备，也为网络罪犯开发了许多新切入点。如上所述，其中许多设备在设计或部署时都没有考虑到安全性，也没有部署在能够缓解各自漏洞的系统中。
- 家庭或企业中的计算机和连接的设备应在设备的整个生命周期内得到保护–也许最重要的是，在设备初始安装和配置时。正确的安装和配置仍然很少见，因此，产品通常无法达到其最佳安全性能。
- 公共和私营部门的所有类型的企业都是僵尸网络和其他自动化分布式威胁的受害者和主机传播者。这些企业采用安全解决方案（市场上越来越多的安全解决方案）可从中受益匪浅。

现在仅包含一个僵尸网络

不仅仅是

3千万

“僵尸”端点并允许恶意行为者牟利每月六位数

> 安全需要动态，灵活的解决方案，这些解决方案必须由强大的全球市场力量驱动，并且与需要缓解的网络威胁一样灵活敏捷。

在这种背景下，过去的政策努力的常见错误在于，他们只专注于生态系统的一两个组成部分。结果很可能是一片仍然布满病树的森林。同样，缓解僵尸网络也需要更周全，整体的方法。为了个人和集体的利益，这个复杂生态系统的各个部分必须加深和加深对自身责任以及与他人责任的互补理解。而且，如果目前尚不清楚或不清楚这些界限，则利益相关者必须共同努力澄清这些界限。如果没有此类工作，打击僵尸网络的策略将恢复为只关注一两个方面的乌托邦政策解决方案的谬误
难题之谜–例如，互联网服务提供商（ISP）应仅关闭所有僵尸网络，或者使数十亿台设备具有通用安全性，或者使消费者成为无所不知的技术用户。

到目前为止，这种简单的解决方案失败了，将来也不太可能成功。取而代之的是，这个复杂的系统由遍布全球私营部门消费者和企业市场，学术界，民间社会和各国政府的数十亿人力和自动化组件组成，必须在各个级别实施缓解措施以提高其安全性。这就是本《国际反僵尸网络指南》的目标。

现在有什么不同？

本指南提供了针对当今市场挑战的现实，当前可用的解决方案，任何政府要求或单个国家都无法满足。我们正与多个行业的跨国公司合作，大幅减少僵尸网络威胁。我们通过分析快速演变的全球威胁，生态系统范围的脆弱性以及日益强大的实力和坚定的对手，制定了本《指南》，同时牢记以下共识指导原则：

- 安全需要动态，灵活的解决方案，这些解决方案必须由强大的全球市场力量驱动，并且与需要缓解的网络威胁一样灵活，适应性强，而不是根据地方或国家/地区司法管辖区不同而制定的法规遵从机制。
- 安全是互联网和通信生态系统中所有利益相关方的共同责任。各国政府和行业利益相关者应提倡增加所有参与者责任的解决方案，而不是在某些选定组成部分或利益相关者中寻求简便的解决方案。
- 安全依赖于政府，供应商，提供者，研究人员，企业和消费者之间的互利团队合作和伙伴关系，建立在对不良行为者采取集体行动并奖励负责任行为者的贡献的框架上。

04 全球互联网和通信生态系统概述

如上所述，数字经济在一个复杂的全球互联网和通信生态系统上运行，并使之成为可能，这个生态系统由许多系统组成，每个系统本身就高度复杂，彼此高度依赖。所有这些不同组成部分构成了生态系统抵御僵尸网络和其他自动化分布式攻击所构成威胁的脆弱性及其抵御能力的一部分。

由互联网和相关通信生态系统组成的“系统系统”的复杂性和多样性使得不可能提供一套统一适用于所有利益攸关方的指导。各种著名的政府和私营部门报告都有定义和描述了互联网和通信生态系统

2016年数字经济规模为11.5万亿美元，到2025年可能增至23万亿美元，占全球GDP的近四分之一

这些定义并非互为对生态系统的理解方式，而是相互补充和加强。

本指南也不例外。我们以有助于识别和实施反僵尸网络在利益相关者组成团体中实践。具体而言，本指南围绕以下五类提供商，供应商和用户进行组织：

1. 基础设施
2. 软件开发
3. 设备和设备系统
4. 家庭和小型企业系统安装
5. 企业

可以肯定的是，任何定义这个复杂生态系统的努力都可能以某种方式（无论是实际的还是感知的）包容各方。例如，经验可能表明，以上列出的五个类别中的任何一个都无法合理地容纳一些涉及类别组合的无处不在的平台（例如大型社交媒体平台）。因此，应灵活对待这一分类法，并期望系统之间的界限不断发展。

05 生态系统组成部分的实践和能力

A. 基础设施

在本指南中，“基础设施”是指支持连接和可操作性的所有系统，不仅指互联网服务，骨干网络，云，网络托管，内容交付，域名系统和其他服务提供商的物理设施，而且还有软件定义的网络和其他系统，能够反映互联网从有形事物到数字概念的演变。对于现代互联网和通信生态系统中的各种基础设施，我们建议基准实践和高级功能。

基础设施类型

互联网服务提供商

互联网服务提供商（ISP）是一个为客户提供使用诸如电缆，DSL（数字用户线），拨号和无线等技术接入互联网的组织。互联网服务提供商（ISP）通过网络接入点（互联网骨干网上的公共网络设施）相互连接。互联网服务提供商（ISP）使用这些庞大的相互连接的骨干网系统，在几秒钟内长距离传输信息。互联网服务提供商可能会提供互联网访问以外的服务，包括网站托管，域名注册，虚拟托管，软件包和电子邮件帐户。许多ISP提供旨在减少僵尸网络数量的服务，包括托管安全解决方案，使提供商在缓解对客户的威胁方面发挥积极作用。大多数宽带互联网服务提供商（ISP）都将防病毒软件作为其服务的一部分，而且许多互联网服务提供商通知被感染的客户无需额外付费。

互联网骨干网提供商

互联网的骨干网是一个庞大的，相互连接的计算机网络的集合，通常由商业，政府，学术和其他网络接入点托管。这些组织通常可以控制大型高速网络和光纤干线，本质上是为提高容量而捆绑在一起的各种光纤电缆。它们可以实现更快的数据速度和更长距离的更大带宽，并且不受电磁干扰。骨干网提供商向ISP提供互联网访问权限，并使ISP之间相互连接，从而允许ISP为客户提供高速互联网访问。最大的骨干网提供商称为“第一层”提供商。这些提供商不仅限于国家或地区，而且拥有连接世界各国的庞大网络。一些一级骨干网络提供商本身也是互联网服务提供商（ISP），由于规模大，这些组织将服务出售给小型互联网服务提供商（ISP）。

域名系统提供商

域名系统（DNS）本质上是一个与IP地址相关的域名地址簿，该地址复制并存储在全球数百万台服务器上。当用户希望访问网站并在搜索栏中键入域名时，计算机会将信息发送到域名系统（DNS）服务器。此服务器（也称为解析器）通常由用户的ISP运行。然后，解析程序将域名与IP地址进行匹配，然后将相应的IP地址发送回用户浏览器，由浏览器打开与网络服务器的连接。

域名系统提供商是提供此类域名解析服务的组织。它们提供最常见的域名系统功能，例如域转换，域查找和域名系统转发。域名系统（DNS）提供商还定期更新其域名服务器以提供最新信息。

内容交付网络

内容交付（或分发）网络（CDN）是数据中心和代理服务器在地理上分散的网络。 CDN是一个术语，用于描述许多不同类型的内容交付服务，例如：软件下载，网络和移动内容加速以及视频流。 CDN供应商也可能会跨领域进入其他行业，如具有分布式拒绝服务保护和网络应用防火墙（WAF）的网络安全。 CDN旨在解决延迟问题，这是从用户请求网页到屏幕上显示内容之间发生的延迟。延迟的持续时间通常取决于最终用户与托管服务器之间的距离。为缩短此持续时间，CDN通过将内容缓存版本存储在多个位置（称为接入点或PoPs）来缩短物理距离并提高站点渲染速度和性能。每个PoP在其内部连接最终用户
靠近负责内容交付的缓存服务器。通过一次在多个地方存储网站内容，公司可以为遥远的最终用户提供优质服务。

云和托管提供商

互联网托管服务使客户能够使全世界的个人和组织访问互联网上的内容。近年来，越来越多地采用云托管服务，即使用在线托管的远程服务器代替本地服务器或个人设备。

某些基准实践已被证明可以减少以下影响：僵尸网络驱动的攻击（如分布式拒绝服务攻击）应在整个生态系统中实施。

使客户能够访问可扩展且更安全的托管解决方案。
可以按订阅访问托管在云上的软件，基础设施和平台，并使客户能够执行各种计算功能。因为云网络是
在分散的情况下，它们通常可以承受众多网络组件的中断。这种架构功能使云对高度分散的僵尸网络更具弹性，并提供其他缓解功能。本质上，云服务在ISP提供的基础设施之外提供了额外的安全层。随着僵尸网络攻击规模的扩大，这一保护层变得越来越有用。
因为云相对于ISP目标而言是ISP的上游
攻击时，可以在更靠近攻击源的位置缓解问题。云安全服务补充但不会削弱僵尸网络缓解中互联网服务提供商的作用。

基础设施的基准实践和高级功能

CSDE成员采取关键步骤来提高自身网络，客户网络和全球生态系统对僵尸网络的抵御能力。政府和行业专家观察到，由于生态系统的复杂性，没有单一的工具能够始终有效地缓解威胁，37意味着行业必须保留足够的灵活性以适应新兴威胁和新技术和新工具。但是，某些
基线实践已被证明可减少僵尸网络驱动的攻击（如分布式拒绝服务攻击）的影响，应在整个生态系统中实施。38下面，我们确定基线实践以及行业领导者用来保护生态系统免受分布式攻击的更高级功能。威胁。

1. 检测恶意流量和漏洞

缓解僵尸网络等分布式威胁的第一步是，确定需要防御攻击的资产以及可能暴露这些资产的潜在漏洞（即攻击面）。此外，公司应及时了解每个已识别漏洞的最新漏洞利用（即攻击媒介）。

供应商可以在其行业内和跨部门利用可信赖的第三方数据馈送和信息共享机制。此外，许多国家/地区的政府信息共享机制使信息能够以机器速度迅速在公共部门和私营部门之间共享。39

基线检测实践摘要：提供商检查定期更新的数据库中已知类型的恶意软件。负责任的公司可以通过与安全供应商和研究人员及时共享有关新恶意软件的信息，为检测工作做出贡献。

高级检测功能汇总：有权使用更多资源的公司可能会拥有专门的安全研究人员，可以分析启发式和异常行为以检测恶意软件。研究人员的发现可以与其他利益相关方分享。

a) 签名分析

当安全专家遇到恶意软件时，会搜索唯一的特征码或“签名”（例如，恶意软件代码和漏洞利用代码的一部分）。任何能够访问恶意软件签名更新数据库的人都可以使用基于签名的分析，从而无论在哪里遇到威胁都可以识别威胁。这种分析在防病毒软件和入侵检测系统中很常见，可用于检测网络上大多数恶意威胁。尽管通常使用签名分析，但更老练的恶意行为者可以通过在每次恶意软件传播时更改其细节来限制这种技术的有效性。就像真正的病毒一样，恶意软件可以在主机之间移动并适应和发展。40签名分析的一个更明显的局限性在于，需要先知恶意软件，这意味着
签名分析的有效性取决于整个生态系统的及时更新和信息共享。理想情况下，签名分析应与其他类型的分析（如下面讨论的启发式或行为分析）结合使用，以克服这种技术的固有局限性41。

基准实践：提供商应确保其特征库为最新版本，并应为恶意软件信息共享做出贡献。

高级功能：提供商可以将签名分析与代码启发式分析（如下所述）和网络流量行为（也如下所述）相结合，以获得更好的结果。

b) 启发式分析

启发式分析通过检查代码中已知的故障迹象来检测恶意软件。代码不必完全匹配已知恶意软件即可将其标记为潜在恶意软件。启发式
分析在确定代码是否可疑时寻找许多不同的线索。在静态启发式分析中，将潜在恶意代码与数据库中恶意软件代码进行比较，如果有足够相似之处，则对代码进行标记。尽管存在误报的可能性，但启发式分析在应对未知和不断发展的威胁方面远比签名分析有效。有时，为了安全地解构代码，科学家将被认为是恶意软件的可疑代码存储在称为“沙盒”的虚拟机中，从而防止其传播到其他主机。这就是所谓的动态启发式分析。42

高级功能：提供商可以结合使用静态和动态启发式分析来检测以前未知的威胁。具有研究人员团队的提供商可以分析沙箱中的可疑代码，确定有效的缓解策略，这些策略可以与生态系统中的其他利益相关方共享。

c) 行为分析

签名分析和启发式分析都针对恶意软件代码，而行为分析则针对恶意软件感染的“症状”。当网络流量指示异常行为时，起初可能不清楚导致行为更改的原因。但是，有已知迹象表明某软件可能是恶意软件，例如，当某软件试图
获得提升的特权或与系统上的其他软件或文件异常交互。通常，行为分析类似于医学专业：即使在确切知道问题出在哪里，医生也常常可以分辨出某人何时生病。行为分析通过发现尚未识别的未知威胁，因此没有已知特征，补充其他类型的分析43。

高级功能：提供商可以使用算法检测异常流量模式并利用机构知识，或者在必要时雇用外部安全专家诊断异常流量的根本原因。

d) 数据包采样

为了理解流经网络的大量数据，许多领先的提供商使用了一种称为数据包采样的技术。这项技术需要从路由器捕获的网络流量样本中获得丰富的流量视图。通过减少需要检查的数据量，数据包采样可以使大型网络运营商分析流量，即使现代网络规模和速度不断提高。

基准实践：提供商至少应以伪随机抽样数据包，使数据包有机会被选中进行检查。该采样可以在内容中立的基础上执行。

高级功能：提供商可以使用更为复杂的采样技术，权衡概率并响应流量变化做出响应。供应商可以检查与恶意软件威胁相关的特定内容。

e) 蜜罐和数据级诱饵

除了上述网络级解决方案之外，提供商还可以利用蜜罐等数据级诱饵"诱饵"攻击者。蜜罐通常是数据或网络中的系统，对于恶意行为者而言似乎很有价值，然后当他们试图访问时，将受到阻止或监控。值得注意的是，第三方可以部署蜜罐和其他诱饵，提供商可能会与此类实体合作发现潜在的犯罪活动或其他网络攻击。由于蜜罐可用于发现犯罪主动行为，因此被用于执法行动。

基准实践：提供商可以部署低交互蜜罐，该蜜罐具有有限的功能和信息收集功能，但风险低，因为没有实际入侵。蜜罐模拟对傻瓜攻击者的成功入侵，并收集有关他们的信息。

高级功能：提供商可以通过部署高交互蜜罐来了解有关攻击者的更多信息。在这种情况下，攻击者通常与提供商的实际系统进行交互而不是模仿，通常会暴露以前未知的攻击媒介。由于受到攻击的可能性增加，高互动蜜罐本来具有较高的风险，但更能揭示攻击者的方法。

---

†*"伪随机"数或过程具有与真正随机数或过程类似的不可预测特征，但实际上在数学上并不是随机或不可预测的。在无法产生真正随机性的系统中，使用伪随机性。*

2. 缓解分布式威胁

如果检测到恶意流量和潜在威胁，基础设施提供商还可以应用各种缓解方法（如下所述）应对这些挑战。

基线缓解实践摘要：提供商应使用入口过滤-即，应用可以限制入站流量速率的过滤器。提供商还应做出合理的努力来调整网络流量，并使用黑洞和沉洞作为网络管理工具。

高级缓解功能摘要：有权访问更多资源的公司除可以使用入口过滤外，还可以使用出口过滤，从而限制出站和入站流量的速率。他们可能使用访问控制列表（ACL）来减少攻击手段。公司可能会在整形流量时采取措施，最大限度地减少服务中断，例如，通过部署选择性黑洞。他们可能会使用BGP flowspec等技术来增加流量管理选项。他们能够与政府和行业合作，拆除恶意僵尸网络。它们还可能提供商业服务，例如清理流量和分布式拒绝服务保护。

a) 过滤

缓解僵尸网络的复杂性之一是，恶意行为者会使用IP欺骗技术，使不良流量似乎来自其实际起源位置之外的其他地方。44

> 通过过滤不良流量进入提供商网络时，提供商会降低欺骗的有效性，从而使分布式拒绝服务攻击更难以实施。

进入提供商网络时出现不良流量（例如，入口过滤，BCP38和BCP84）45，提供商可以降低欺骗的有效性，因此使分布式拒绝服务攻击更加难以实施。由于这种做法的好处显而易见，因此互联网工程任务组（IETF）将入口过滤视为最佳实践。46值得注意的是，入口过滤在网络入口点（如客户端）的效果更好。在网络交换点更困难。

此外，尽管提供商通常处于过滤恶意流量的有利位置，但运营企业自己的IP地址空间的任何实体（包括企业）都应采用BCP38等技术。提供者如由于ISP为客户端分配了许多IP地址，客户端可能会运行自己的过滤功能，也需要遵循BCP38。

此外，通过在网络边缘部署过滤器，提供商可以监控来自其生态系统角落的流量，并减少对其他方的伤害。出口过滤不是入口过滤的替代品，而是一种补充解决方案。入口和出口过滤相结合是提供商提高弹性的最佳途径47。

最后，在网络设置中，ACL用于根据流量源和目的地，IP协议，端口，EtherType和其他特征等参数识别流量。一个常见的例子是，来自较低安全接口的流量无法访问较高安全接口。48在某些情况下，可以配置ACL来考虑单个用户的访问权限，以进一步限制恶意软件渗透网络的攻击媒介。

基准实践：提供商应在网络入口点过滤入站流量（入口过滤），以减少进入其网络的恶意流量。过滤器应该能够在可能淹没网络资源的攻击中限制入站流量。

高级功能：理想情况下，提供商应过滤入站流量之外的出站流量（出口过滤），并且无论流量是出站还是入站，都应能够限制流量速率。这种混合解决方案可提供更多数量保护提供商，并使提供商与生态系统中的他人负责任。此外，提供商可以使用ACL减少攻击手段。

b) 流量整形

当识别出潜在恶意流量时，提供商可以通过使用通常会导致流量丢弃的技术或在数据速率异常高时延迟流量来安全管理流量。这两种技术在特定情况下可能有用，并且可能是综合流量管理策略的一部分49。

基准实践：提供商应做出合理的努力来调整网络流量。提供商至少应能够部署一个"黑洞"，阻止流量到达目标。应努力通过重定向流量或仅在定义的地理区域内丢弃流量来减少对合法服务的中断。

高级功能：拥有更多资源的提供商可以调整流量，而不会造成对合法流量的多次中断。例如，商业清理中心可以通过过滤恶意元素并将合法流量发送到其清理流量目的地。小型提供商可以与大型提供商建立伙伴关系，向其客户提供这些服务。

c) 黑洞

黑洞技术是一种将所有流量都流向特定在线目的地的技术。这种技术的常见版本是远程触发的基于目的地的黑洞（RTDBH），上游网络通常最接近攻击源，在恶意流量到达潜在受害者之前就将其丢弃。

尽管黑洞可以有效阻止恶意流量到达目的地，但一个明显的缺点是合法流量也无法到达目的地，这可能是恶意行为者的明确目标。为了最大程度地减少此问题，提供商可以采用称为选择性黑洞技术，将来自选定地理区域（如国家或大洲）的流量丢弃，同时允许其他地区的流量到达目的地。

基准实践：提供商应利用黑洞来保护其网络。理想情况下，提供商应尽量减少对合法流量的干扰，但至少应在没有更精细的工具或无法正常运行的情况下部署基本RTDBH。

高级功能：提供商可以利用与其他提供商的伙伴关系，在传感器和过滤存在点上提高黑洞的有效性。此外，提供商可以针对特定地理区域部署选择性黑洞，最大限度地减少对合法流量的干扰。

d) 沉孔

Sinkholing是一种将特定IP范围内的流量发送到指定服务器（“污水池”），而超出该IP范围的流量照常继续的技术。宿醉攻击的目的是为研究和缓解目的捕获僵尸网络。50宿醉攻击通常是通过策略路由或其他路由方法完成的，这些方法将构成僵尸网络的恶意软件捕获在宿坑中，执法机构可以通过这种方法进行研究。研究人员。当陷入困境的恶意软件试图与命令和控制服务器通信时，安全专家可以跟踪恶意软件向其馈送信息的机器的IP地址，从而深入了解犯罪活动。提供者还可以完全切断恶意软件与命令和控制服务器之间的通信。污水池对于大规模拆除僵尸网络至关重要，僵尸网络在全球多个国家/地区使用成千上万个启用互联网的系统。

基准实践：提供商应使用宿位作为网络管理工具，重定向入站恶意流量并收集对提供商网络威胁的信息，以进行分析或信息共享。

高级功能：行业领导者可以与其他提供商和执法机构合作，利用漏洞破坏和收集有关整个生态系统威胁的情报。提供商还可以通过与众多司法管辖区的主管部门和利益相关方进行有效协调，协助国际执法行动。

e) 擦洗

清理解决方案通常由专用的清理中心实施，这些中心分析网络流量并清除其中的恶意流量，包括分布式拒绝服务。由于与其他解决方案相比，清理是资源密集型项目，因此有多家大型提供商将清理作为一项商业服务提供。通过将流量重定向到中心（而不是将流量丢弃），清理可以使合法流量高度成功地到达目的地。因此，对于许多企业而言，擦洗是替代黑洞和水槽的首选替代方案。

高级功能：清理中心可以过滤多种类型的攻击，不仅限于容量泛洪攻击，还可以为提供商或客户防御添加重要的保护层。例如，中心可以集成防止基于SSL（加密链接）的攻击的技术。

f) BGP flowspec

边界网关协议（BGP）流规范（flowspec）是一项动态技术，使提供商可以快速部署各种不同的缓解方案，从而使专家可以根据情况做出判断。与仅支持黑洞路由的路由器不同，flowspec路由器允许其他选项，例如宿流量，因此可以由专家研究，也可以整形流量并允许其以定义的速率进行传输51。

高级功能：提供商可以使用BGP flowspec开发边界路由器的自定义指令，而不是传统的"一刀切"式所有解决方案。借助BGP flowspec，可以指示路由器丢弃数据流，重新路由流量或在flowspec发起方进行适当验证的情况下限制流量速率。

3. 与客户和同行协调

补救僵尸网络或其他分布式威胁可能会要求提供商通知其发展动态以保护其合作伙伴客户或同伴。显然，用户通知的有效性很大程度上取决于用户。由M3AAWG委托进行的一项研究发现，电话和邮政是与用户联系的最有效方法。52其他可以（也应该使用）的可用方法包括电子邮件和网页通知。联系用户的另一种方法是"围墙花园"，这种方法会限制用户访问在线服务，直到他们采取由提供商确定的特定步骤。在某些国家/地区，这种后继方法会引发法律或公共政策关注。53可以通过许多与客户相同的方法通知对等方。如果存在已建立的关系，则通知将更有效。对于提供商而言，与他们所在行业的关键参与者建立熟悉度非常有用，这样在紧急情况下不必首次进行介绍。

基准实践：提供商应通知违反可接受使用政策或从事有害活动的客户或同行。如果来自客户或对等方的流量被阻止，请同时提供（1）文本或电话消息和（2）电子邮件/用户帐户网页通知。应向客户或对等方提供明确的指示，说明如何通过不受阻碍的通信渠道联系提供商。

先进的能力：具有受过训练的人员和专用资源的提供商可以大大降低误报率，使客户在以合法方式使用服务时很少会受到干扰。

4. 地址域设置和删除

执法部门拥有可用的特定工具，近年来已成功用于成功缓解恶意僵尸网络和犯罪行为者。如果有充分的证据表明犯罪网络正在使用特定域名进行恶意目的（例如，僵尸网络攻击），提供商可以与（通常在强制性指导下）执法部门合作，拆除域名。根据相关法律。导致恶意行为者现实生活中的后果的执法行动是唯一解决僵尸网络和分布式拒绝服务攻击原因而非症状的解决方案。这种执法行动需要大量资源，通常需要进行广泛的法庭分析。大规模领域

缉获也可能需要国际协调努力。54例如，2016年，提供商与30多个国家的政府官员合作，关闭了雪崩僵尸网络，并控制了分散在全球互联网和通信生态系统中的800,000多个域。55

基准实践：提供商应为执法和安全研究人员提供一个易于查找的联络点列表。服务提供商还应该有定义明确的政策，描述他们如何支持和不支持执法工作。

高级功能：通常，行业领导者将拥有更多支持执法的程序和技术。他们还将针对特定的执法策略制定明确的政策和法律立场。他们可能会进行全球风险评估，以满足全球法律要求。除了与执法部门合作外，提供商还可能具有在特殊事件中与竞争对手合作的流程。

B. 软件开发

在本指南中，软件已成为生态系统其他各个组成部分中越来越普遍的元素。正如本指南中所讨论的那样，《指南》（基础设施，设备和设备系统，系统安装程序和企业）中强调的主要软件系统用户有多种复杂的开发流程和相互依存关系，推动软件创新和改进。因此，本节不试图捕获
与生态系统各部分专用软件开发相关的各种基准安全实践和高级功能。相反，其目的是强调安全软件在该生态系统中及整个系统中至关重要。如果在本指南的其他地方未特别说明，则软件开发通常应由这些实践组成。

软件的基准实践和高级功能：

1. 按安全设计开发实践

软件和应用程序已越来越多地集成到我们的商业和基础设施流程和产品中，以提高效率。但这使它们成为黑客的主要攻击目标。全球经济，关键基础设施和政府运营增加了对软件的依赖。

遵循最佳实践的组织将安全作为质量要素，开展一系列安全开发实践，包括在风险管理基础上的整个开发生命周期中进行开发人员培训，静态应用程序安全扫描，威胁建模，动态应用程序安全测试和手动渗透测试。可公开获得帮助开发人员采用这些最佳实践的资源。例如，致力于促进软件保证的领先组织SAFECode（代码卓越软件保证论坛）发布免费向公众提供的安全软件开发培训资源，包括安全软件开发基本实践56。

基准实践：按设计安全开发至少应包括以下内容：

- 对静态和传输中的数据进行高度加密：如果数据被盗或访问不当，加密会阻止数据可见。无论数据是静止（即存储）还是传输中，加密都是保护信息的重要工具。虽然有不同的加密选项可满足特定组织和产品的需求，但加密通常应使用强大的算法，在特定用例的情况下不能轻易破解。算法的强度可能会因上下文而异，具体取决于各种因素，例如，所讨论的攻击类型以及对某些特定类型攻击的需求服务正常运行。例如，强加密可能会阻止大多数防火墙和其他安全数据包检查服务正常工作。
- 默认情况下安全：软件的默认配置设置应高度重视安全性。应该有意更改设置，以使软件降低防御能力，允许更多选项。该原则减少了恶意行为者可以利用的攻击媒介。
- 可补丁程序和更新设计：软件设计时应考虑有必要补丁程序和更新，以防止恶意行为者不断发展和日益复杂的攻击。修补程序和更新应以最少快速的手动干预以合理快速，安全的方式交付给安装了软件的系统。
- 最小特权原则：通过将用户和应用程序访问限制为仅执行必要任务所需的基本特权，软件开发人员可以减少产品的攻击面。在设计阶段应用最小特权原则可减少恶意行为者或被泄露服务获得系统管理访问和控制的机会。
- 软件组成分析：此分析的目的是创建产品中开源和其他第三方组件的清单。这样，即使不能保证第三方和开源组件的安全，软件开发人员也可以保持警惕，以防万一出现问题时自己没有开发组件。盘点产品中使用了哪些组件，以及应用程序还可以帮助开发组织跟踪和识别相关的已知漏洞。
- 软件安全意识和教育：意识应扩展到软件开发过程中的所有人员，包括开发人员，产品经理和其他人员。应提供具有成本效益的教育机会或培训练习。

高级功能：领先的安全设计做法包括：

- 动态应用程序安全测试（DAST）：这项先进技术使用渗透测试（模拟攻击）发现应用程序运行时的漏洞。这种测试在物联网环境中尤其有用。但是，这需要可管理的配置选项，并需要雇用高技能专家。

- 静态应用程序安全测试（SAST）：利用这项先进技术，开发人员可以扫描源代码或二进制文件并识别漏洞。仅限于支持的语言和平台。对于物联网领域的许多产品，这可能不是一个选择。但是，可以使用特别敏感组件的仔细对等代码审阅来提高安全性。
- 威胁建模和体系结构风险分析：与政府合作或运营高度敏感的公司可以聘请专家团队，以确定恶意行为者假想如何创建或利用系统漏洞来达到邪恶目的。威胁模型可能考虑多种类型的风险，包括涉及自动分布式攻击的风险。
- 以安全为中心的工具链：开发人员可以利用以安全为中心的工具链创建新软件。工具链是促进软件开发的软件或硬件工具的集合。当工具链优先考虑安全性时，编码错误的发生频率就会降低，提供商可以强制执行质量控制。公司可以将新的漏洞和经验教训整合到开发工具中。
- 保护第三方和开源组件：领先公司将确保所使用的第三方组件和开源库没有已知漏洞。
- 此外，公司可能会向客户提供有关安全软件开发流程要素的证明，并寻求符合国际标准的认证。

2. 安全漏洞管理

为了补救新发现的漏洞，产品交付后为客户提供安全修补程序的时间和持续时间，全球不同的公司都有不同的政策。虽然主要产品制造商倾向于更定期地发布其产品补丁，但规模较小的制造商通常不太可能投入足够的资源来开发和提供安全补丁。57

基准实践：提供商应优先处理关键任务应用程序中的关键漏洞。

高级功能：更高级的提供商可以修复几乎所有已知漏洞，尤其是在风险评估期间确定优先级的漏洞。他们能够为从公司购买软件或通过应用程序与公司交互的用户提供安全保证。

3. 安全开发过程的透明性

以上每种做法在安全软件和硬件的开发中均起着重要作用。软件开发组织和私营部门已着手开发基于市场的安全开发流程评估。58然而，
政府和行业利益相关方合作开发的框架可以帮助

标准化术语和流程，增强市场信心。 NIST目前正在与SAFECode和其他利益相关方合作，开发有关安全软件开发流程和实践的特别出版物。 NTIA正在召集多方利益相关方流程，探讨组织如何交流有关第三方软件组件的信息并提高透明度。 59

基准实践：向购买软件的公司提供安全态势证明。

高级功能：为从公司购买软件并通过应用程序与公司互动的用户提供安全保证。

C. 装置和设备系统

单个连接的设备（或“端点设备”）本身可以由多个组件组成，包括硬件模块，芯片，软件，传感器或其他操作组件。成千上万的公司和数百万的开发人员可能为全球部署的数十亿个单独设备做出贡献。除单个设备本身之外，还有多个附加的连接层，构成一个高度动态的新市场，包括安全创新。简单地说，连接的设备不再仅仅是单个设备。相反，考虑到这种复杂性，本指南针对设备系统：互联端点设备（即，物联网中的一个“物”）及其相关支持元素（包括应用程序和云服务）的结合.60

设备和设备系统的基准实践和高级功能

1. 按安全设计开发实践

如果安全是早期开发流程的一部分，并且是整个流程中的关键因素，则安全性是最高，最高效的。某些类别的最佳实践已被普遍认为是确保最终产品具有基本机密性的必要工具，
完整性和可用性。61僵尸网络可以利用设备和系统实施中的弱点，因此只有在产品开发的早期和各个阶段就包括安全规划，才能避免此类弱点。

a) 安全开发生命周期流程

基准实践：应建立安全的开发生命周期（SDL）流程。在SDL流程中，每个开发阶段都有安全活动，可以手动或自动完成62。

高级功能：在建立了安全的开发生命周期流程之后，这家先进的公司正在评估和增强流程功能。衡量SDL能力是BSIMM项目（在“成熟度模型中建立安全性” 63）的一部分。 BSIMM材料是开源的，可以作为此项工作的资源。

b) 安全设计要素

本节列出了产品设计中开发人员级别的实践。

(1) 旨在保护静态数据和传输数据

此类主要涉及保护设备上存储的数据和加密数据通信。实施此类保护可能涉及有关安全硬件元素，安全启动过程等方面的决策；另请参阅高级功能：信任根源。

基准实践：数据通信应加密。敏感数据应加密存储。无论使用什么协议，如果可以使用身份验证，则应使用身份验证。通常，无论采用哪种系统，都应采用可用的安全机制。使用的加密技术应避免使用不建议使用的方法。

高级功能：应使用最新版本的协议和安全机制。安全存储器可以代替存储信息的加密。应使用与NIST FIPS 140-2或ISO / IEC 24759相适应的加密密钥方法。64

(2) 限制未经授权的访问的手段

基准实践：IoT产品通常需要本地或远程管理服务。在产品开发和制造期间，可能需要其他类型的对存储器，处理器，外围设备或控制流的低级别访问，而设备终端用户则不需要或无法使用这些访问。这些附加功能必须仔细保护。

此级别的典型步骤包括：每台设备唯一的“管理员”凭证或更改密码的首次启动要求；防止暴力破解密码猜测的限速技术；在产品交付之前保护或禁用开发人员级别的端口和服务；删除未使用或不安全的本地和远程管理服务，如远程登录。

高级功能：应支持多因素身份验证用户访问控制。

此外，终端设备和路由器开发人员应考虑新兴标准，专门帮助防止僵尸网络未经授权的访问和使用。例如，IETF制造商使用描述符（提议建议）或“ MUD” 65可能适用于许多用例。 MUD是“由IETF定义的嵌入式软件标准，允许IoT设备制造商发布设备规格，包括设备连接到网络时的预期通信模式。” 66如果设备和路由器均遵守MUD要求，路由器具有将设备限制为制造商指定用途的机制。超出目的的活动（例如，参与大规模分布式拒绝服务攻击）可由本地路由器识别和阻止。其他标准，如IEEE 802.1AR67和设备标识符组合引擎（DICE）68架构，可以提高IoT设备及其MUD组件的安全性。

(3) 使用混淆

基线实践：设备制造商不应仅使用混淆来保护机密（例如设备密钥，敏感数据），但可以使用混淆来增加攻击者定位秘密的难度。尽管如此，仍应通过访问控制和加密等其他手段保护机密。

高级功能：实施基线。

(4) 用户输入验证和系统输出编码

基准实践：必须管理从系统外部接收的任何输入，以使外部对手无法利用意外后果。应验证输入的长度，字符类型以及可接受的值或范围；另请参阅白名单
过滤。还应过滤从一个子系统到另一个子系统或到另一个站点的输出；请参阅“字符规范化”。

高级功能：实施基线。

(5) 密码学与产品需求相称

基准实践：需要使用加密方法来确保数据完整性和机密性，权限验证和请求不可否认性。应选择与评估的风险匹配的密码技术，但应使用开放的，经过同行评审的方法和算法。在可行的情况下，加密方法可以更新。

高级功能：使用开放的，经过同行评审的方法和算法，强大，可靠的，可更新的加密技术。确保加密技术能够支持对称量子加密后抗量子密钥长度。

2. 信任根源

各种类型的攻击都依赖于模仿另一个实体。例如，设备新软件的可信来源通常是原始硬件制造商。显然可以防止安装受到恶意软件破坏的软件。这就引出了如何区分差异的问题。

解决方案是建立一个信任系统。信任链是硬件和软件元素的链接，其中每个元素添加到链中时都会经过验证。链的起点是信任根，由权威实体提供。验证使用数字签名以密码方式完成。由于第一个元素与受信任的授权机构联系在一起，因此也可以信任由链加密验证的每个元素。

当系统收到签名的软件更新时，可以检查数字签名。由于系统本身植根于原始权威实体的信任中，因此在验证软件更新后，就可以信任该软件。

a) 硬件基础安全

基准实践：考虑如何将基于硬件的安全性融入当前和未来产品的安全开发生命周期。

高级功能：在技术上可行的情况下，利用基于硬件的安全性。

3. 产品生命周期管理，包括生命周期终止

产品生命周期管理是指从构思到设计，制造，支持和寿命终止，积极管理产品。寿命终止管理是指对产品达到生命周期中的定义端点（包括定义的支持期限或功能终止或日历周期结束）应采取的措施制定明确的政策等

基准实践：设备制造商可能会向消费者发出有关安全支持策略的通知，以及在支持期间如何为设备提供更新支持，以及支持期后的期望值。在可能的情况下，设备应通过启用逻辑和物理方法识别并审核设备并具有适当的访问控制，从而支持网络资产管理。

在支持期过后，消费者应该有能力并被告知如何"停用"设备。退役应允许消费者将产品恢复为出厂默认值，并删除所有个人身份信息（PII）。此功能涵盖各种场景，例如产品的销售，废弃或回收，包括出售安装了IoT设备的物业。

供应商应创建安全漏洞策略和流程，识别，缓解并适当披露其产品中的已知安全漏洞。

高级功能：在技术上可行的情况下，在定义的安全支持期内通过防滚回保护和适当的访问控制进行安全更新的计划69。

4. 安全专注的工具链使用

以安全为中心的工具链是软件或硬件的集合，不仅可以支持产品的开发，生产和管理，还可以增强终端产品的安全性。

基准实践：应使用能够检查实施是否遵循安全编码准则并能够在开源软件中搜索已知常见漏洞和暴露（CVE）子集的工具。

高级功能：使用模糊测试，符号执行，沙箱，静态和动态分析以及内存安全语言等工具查找和缓解漏洞。

D. 家用和小型企业系统安装

家庭和小型企业可以从几种类别的连接设备中受益。连接供暖，通风和空调（HVAC）系统，以实现智能功能和乘员远程访问。安全系统包括摄像头，锁和警报系统，所有这些都可以通过互联网进行管理。娱乐系统受益于中央控制，因此可以轻松管理复杂的音频和视频配置。在这些类别中，制造商和系统千差万别。这些系统可以由自己动手的家庭和企业主安装，也可以由专业人员安装，例如集成商，警报承包商等。

理想情况下，进入家庭，办公室，零售，医疗或工业环境的每台设备和系统都应在设备整个生命周期中采用最佳实践进行保护。此生命周期包括设备的安装和配置。良好的安装将达到制造产品的“最佳可用安全性”。本节介绍了从最常见的设备类型实现最佳可用安全性的基准实践和高级功能。

下面的内容主要来自互联家庭安全系统。70

家用和小型企业系统安装的基准实践和高级功能

1. 认证和凭证管理

安装可以受益于密码管理系统，该系统是密码的加密存储。这些系统减轻了用户记住和管理密码并将密码放在安全位置的负担。

基准实践：如果设备密码不是唯一的，安装程序应更改为强密码。 （请参阅[1]，“密码”）。所有设备和系统必须使用不同的密码。安装应使用受信任的密码管理系统。

高级功能：使用多因素身份验证用户访问控制。

2. 网络配置

网络配置是指网络组件的物理和逻辑布局以及连接和设置。

a) 一般

基准实践：系统（台式机，笔记本电脑等）应安装并运行最新的反病毒和反恶意软件工具。除非明确要求，否则任何具有管理特权的系统都不应运行。

b) 防火墙，接入点和路由器配置

基准实践：除非出于合法目的（例如，对等游戏）要求，否则应在广域网一侧（面向互联网的一侧）禁用UPnP。应为预期使用量分配足够的DHCP空间，但不得超过预期使用量。应启用防火墙，并且仅解锁必需的端口。应禁用端口转发，除非需要特定的应用程序。

高级功能：应监控网络，在应用程序上使用非标准端口值，并为特定应用程序选择性地启用端口转发（结合防火墙保护）。尽管高级攻击者可以克服，但仍应使用MAC地址过滤。

c) 物理和逻辑结构

基线实践：就无线功率和物理布线而言，应限制客户端站点物理结构之外的网络访问。网段应根据目的分开，并使用单独的物理或逻辑网络，使用选项，例如单独的无线电信道，电缆，单独的接入点或网关。

高级功能：应另外使用VLAN或VPN分隔网段以用于不同目的。端口扫描工具可用于监控专用网络。

3. 网络硬件管理

网络硬件管理是指保持网络设备正确识别和配置的持续过程。

a) 调制解调器和路由器，网络管理设备

基准实践：网络设备应具有定期更新固件的过程或手段。

先进的功能：对于ISP提供的调制解调器/路由器/ AP系统，可以添加单独的售后路由器/ AP处理局域网流量，实现对软件更新的本地控制。

b) 网络协议

网络协议是用于在网络上进行通信的多层次语言设备，如TCP，UDP，IP，RTP等。

基准实践：不应使用不建议使用的协议。特别是，请勿使用或不允许协商SSL（任何版本）或TLS 1.0或1.1。

高级功能：在适当的情况下配置最新协议。

c) 无线链接

无线链接是设备之间基于无线电的网络连接。这些链接可以是双向的，也可以使用多个设备之间的网络拓扑。

(1) 蓝牙功能

基准实践：应启用可用的安全功能。如果可用，应使用“不可发现”选项。蓝牙低功耗（BLE）信标信号中不得暴露任何敏感信息。

(2) NFC

基准实践：不得放置或安装NFC读取器，以方便“嗅探”或轻易篡改。

(3) 无线网络

基准实践：除了其他部分所述的基准网络配置实践之外，还应使用最新的Wi-Fi加密选项，例如使用AES的WPA2-Personal（首选）或使用TKIP的WPA2-Personal。应禁用WPS。不应使用默认SSID或广播SSID。

许多接入点都提供“访客网络”选项。应启用此功能，并将其提供给较高风险的用户，例如访客或临时居民/工人。如果可用，应启用802.11aw管理帧保护。确保按照本文档其他部分所述的最佳实践，使用强密码保护接入点配置访问。在适当的地方启用端口过滤。选择一个具有可更新固件的接入点/路由器。

(4) Z波

基线实践：基本安全涉及唯一的家庭ID，受密码保护的管理功能以及在可用的情况下使用启用AES-128的设备。

先进的功能：为了提高安全性，射频功率可以满足距离要求，可以单独使用支持AES-128的设备。

(5) Zigbee

基线实践：唯一连接互联网的设备应该是ZigBee网关，并应使用防火墙保护它。

高级功能：进入和离开ZigBee网络时，可以按地址（源和目的地）和端口号过滤互联网流量。可以在802.15.4级别和网络加应用程序级别（如果可用）上启用可选的802.15.4安全功能。

(6) 远程设备访问控制

此类涉及普通设备功能的各种远程访问控制，如安全摄像机视频，HVAC温度控制，车辆子系统（如远程启动或门解锁）等。

基线实践：设备故障或篡改警报应启用（如果可用）。所有远程访问都应位于受IP限制的防火墙之后，无论端口如何，仅允许白名单IP地址和子网访问设备。如果需要从防火墙外部进行远程访问，则应使用VPN和非标准互联网端口进行远程访问。

4. 安全维护

基准实践：应尽可能跟踪和审查网络违规尝试或其他安装尝试。违反尝试应为
相关联以识别网络内常见的被攻击个人或目标。应记录网络配置，枚举连接的设备，并明确定义安全维护计划。

E. 企业

随着网络设备和系统的主要所有者和用户（包括数量不断增长的IoT设备系统），各类企业（政府，私营部门，学术界和非营利组织）在保护数字生态系统中发挥关键作用。71虽然企业通常是自动化，分布式攻击和数据泄露企图的受害者，但也可以劫持其庞大系统，增加分布式拒绝服务和其他分布式攻击对他人的影响。因此，企业共同属于重要的利益相关者，共同承担充分保护其网络和系统的责任，以帮助保护更广泛的数字生态系统。

全球数以百万计的私营部门和政府企业在技术知识和技能，获得资源和采用基准安全实践的动机方面存在很大差异。例如，大型企业通常设有首席信息官和首席信息安全官，各自负责确保组织网络的安全。
系统和设备，包括任何物联网系统。较小的企业可能没有资源专用于IT和信息安全专业人员，而是依靠现成的解决方案。

组织越来越多地开发和提供工具来帮助大小规模的企业保护网络和系统。也许与《反僵尸网络指南》最相关的是网络安全联盟努力开发和推进分布式拒绝服务和僵尸网络配置文件
网络安全框架下的预防和缓解概况，72旨在帮助企业和其他组织应对和缓解分布式拒绝服务和其他自动化，分布式攻击。

各种规模的企业还可以采取主动措施降低生态系统风险，例如，实施适当的身份和访问管理技术，并停止使用不接收更新的遗留和盗版产品和软件等。此类步骤可以帮助企业保护网络上的敏感数据和知识产权，并通过减少分布式拒绝服务和其他分布式攻击的攻击面来保护整个生态系统。

当然，制定本指南的供应商和提供商本身就是大型全球企业。此外，我们提供高端解决方案来保护企业网络安全并缓解分布式拒绝服务攻击和其他自动化，分布式威胁。该市场的"供应"面强劲且不断增长。从各种规模的企业请求和谈判这些服务的需求这一市场的进一步发展，将为这些服务带来进一步的创新，完善和成本效益。

企业基准实践和高级能力

1. 安全更新

产品制造商负责创建安全更新，但未经用户许可或采取其他措施，通常不会自行安装这些更新。组织可能需要通过更新控制的级别取决于客户类型。例如，拥有合格人员的大型企业或政府机构可以合理地确定哪种安全更新适当，以及何时实施。另一方面，普通家庭用户可能会从自动更新中受益最大。73

基准实践：企业应在更新发布后立即安装。通常，自动更新是更可取的。

高级功能：拥有合格技术人员的企业可以就安全更新的实施做出明智的决定。

> 企业共同属于重要的利益相关者，共同承担充分保护其网络和系统的责任，以帮助保护更广泛的数字生态系统。

2. 实时信息共享

具有大型网络或高度敏感网络的企业（例如大型企业和政府机构）可以与其他相关利益相关方和生态系统参与者共享关键威胁信息。近年来，这些努力取得了显着改善，在抵御僵尸网络和其他自动化分布式威胁方面迈出了一大步。74

基准实践：即使尚未承诺主动共享信息，企业也应准备接收和应对信息共享活动提供的网络威胁信息，并采取负责任的行动。例如，来自政府和执法部门信息共享活动的信息，各种CERT，行业组织，网络提供商，RFC2142地址以及供应商和其他来源的更新和警报。

企业应订阅多个威胁情报源或服务，以与安全信息和事件管理（SIEM）相关/结合使用自动化工作。企业应建立适当的流程，与内部股东及时有效地共享在内部或外部获得的威胁信息。企业应与共享社区保持联系，并了解适当报告/共享其所在地区和行业网络安全事件的流程和保障措施。企业应持续进行内部威胁情报共享。应定期共享危害指标（IOCs）和显着威胁。

高级功能：高级企业应致力于通过与各种适当的共享社区（政府，行业等）负责任地及时共享脱敏网络威胁信息，增强网络威胁信息共享社区。先进企业应确保具有足够的能力，以有利于共享活动的格式检测，分析和捕获网络威胁信息。先进企业应积极参与适用于其所在地区和行业的网络威胁信息共享社区的治理和增强。先进企业应寻求不断提高其检测，分析，响应和共享能力。

3. 安全管理流量的网络体系结构

企业可以控制网络架构的设计，以限制在使用僵尸网络或其他手段进行的分布式拒绝服务攻击期间的恶意流量。75以安全为明确目标的网络架构可以补充其他预防措施，例如-基础设施提供商和其他生态系统参与者提供的分布式拒绝服务。应用程序编程接口（API）管理应用程序，设备和后端数据系统之间的连接。从广义上讲，API使企业可以打开后端数据和功能，以便在新的应用程序服务中重复使用。通过API网关在外围部署安全措施，可以帮助企业在威胁进入企业之前阻止威胁，从而为应用程序开发人员提供对企业数据的访问权限，同时保持强大的安全性。

基准实践：企业应通过使用网络服务提供商提供的功能和服务来获得针对分布式拒绝服务的内部网防御。企业应标准化互联网到企业内部网互连架构，运营策略和流程，访问和数据包流控制配置设置。企业应实施确保该架构正确部署和运行的机制。此外，企业应检查所有入站和出站数据流以及电子邮件和
阻止带有恶意软件的数据包或电子邮件；阻止未经授权的网络流量进入内联网；并利用行业标准DMZ体系结构和运营实践。

高级功能：高级企业可能会发现可观察到的行为，这些行为表明僵尸网络流量，如僵尸网络C&C流量，fastflux域名系统和访问可疑URL。高级企业可以自动阻止僵尸网络流量并进行补救。从入站电子邮件中删除可访问互联网的URL链接；共享和接收用于识别僵尸网络参与者的信息；并防止域名系统（DNS）请求者和域名系统（DNS）服务器进行不正确的域名系统（DNS）操作。

为了提高抵御分布式攻击的弹性，高级企业可以使用应用程序编程接口网关。应用程序编程接口（API）管理应用程序，设备和后端数据系统之间的连接。通过API网关在集中式架构中部署安全性可以帮助组织为应用程序开发人员提供对企业数据的访问，同时保持强大的安全性。

4. 增强的DDOS弹性

即使在非常成功的客户意识和教育宣传努力下，许多客户仍将缺乏保护自己的网络所需的技术专业知识。而不是忽略
为应对僵尸网络和其他分布式攻击可能造成的威胁，企业应购买适合其风险状况的商业分布式拒绝服务保护。76商业服务可能包括场外保护或结合更强大地保护企业安全的内部和内部保护结合使用。抵抗分布式攻击。客户购买商业产品和服务时，可以大大减少僵尸网络和其他分布式攻击的威胁。

CSDE的成员提供一些市场上最高端的商业分布式拒绝服务解决方案。示例包括具有集成安全性的家庭网关，任播服务和各种托管安全服务。任播服务通过提供内容传输的多个路由并平衡可能分布在世界各地的多个网络元素的工作负载，提高抵御分布式拒绝服务攻击的弹性。如果分布式拒绝服务攻击危及网络的某些部分，流量会自动重新路由到另一部分。托管安全服务包括商业清理服务。77其他商业服务包括基于网络的防火墙，移动设备管理系统，威胁分析和事件检测，与云的安全VPN连接，网络和应用程序安全以及电子邮件安全。

供应商可能会提供针对客户独特需求和风险状况而量身定制的过滤解决方案。理想情况下，这些解决方案将集成内部防御和内部防御。商业服务可能允许将恶意流量阻止到更靠近攻击源的位置，从而为客户创建额外的安全层。

基准实践：企业应拥有足够的保留/应急支持以有效应对网络安全事件并保持合理水平
安全性。企业应选择产品和服务包括适当安全功能的商业提供商（即具有分布式拒绝服务保护功能的互联网服务提供商和云/托管提供商，具有自动更新功能的软件等）。企业应该已经制定了文件化的，经过测试的事件响应计划，包括分布式拒绝服务和僵尸网络响应。企业应选择可以提供自动或默认-
根据响应。企业应定期重新评估商业提供商的有效性。

高级功能：高级企业应该对分布式拒绝服务和僵尸网络保护采取多层方法，包括得到良好支持的内部和外部部署功能。
先进企业应积极增加员工的技术专长，确定这些专业知识的不足之处，并通过适当的培训，保留/应急支持和额外人员来弥补这些不足。先进企业应考虑提供先进功能的商业服务和软件，如机器学习和模式分析，以实现更高质量的结果。先进企业应设法通过定期重新评估市场上可用的能力来不断提高自身的能力。

5. 身份和访问管理

身份构成跨应用程序，设备，数据和用户的统一控制点。身份和访问管理工具对个人和服务进行身份验证，并管理允许其采取的操作。 IT风险最重要的领域之一涉及特权用户，例如IT管理员，CISO和其他具有增强的系统访问权限的个人。无论是无意还是恶意，特权用户的不当行为都会对IT运营以及组织资产和信息的整体安全性和隐私性造成灾难性影响。应该为管理员建立系统，使其仅执行对其角色至关重要的操作，即启用“最低特权访问”以降低风险。威胁分析可以洞悉活动和工作，以预防或标记任何表明安全风险的异常事件。[78]

值得注意的最新发展是使用物理安全密钥而不是密码或一次性代码。自2017年初以来，Google开始要求其所有员工（总数超过85,000）使用物理安全密钥，但从未窃取一个员工与工作相关的帐户。[79]

当客户购买商业产品和服务时，僵尸网络和其他分布式攻击的威胁。

基准实践：组织的身份和访问管理实践至少应包括以下内容：

- 身份验证（包括多因素和基于风险的身份验证）–一种访问操作时间，可确保主体实际上是真实主体，而不是冒名顶替者；
- 授权–访问操作时间，在给定当前状态下，确定是否应授予访问权限；
- 访问控制—帮助业务领导者定义和完善策略以确定适当访问的过程；
- 记账—记录访问系统资源的个人用户的活动数据的数据，以分析趋势和识别可疑行为；
- 供应/编排–在更改时发生的一组操作，用于促进连接/移动/离开过程以及不同连接资源之间的更改事件的协调；和
- 身份存储库—永久存储主题配置文件的当前状态和属性值。

企业还应采用离岸做法，即在24小时内为特权访问和云资源访问及时从企业目录中删除身份，并撤销身份和相关访问。

为了提高身份验证，企业应该使用更强大和更容易记住的密码短语，而不是基于语法规则的密码。检查密码字典；并使用密码强度计。此外，企业应使用第二或多重身份验证（2FA / MFA）进行特权访问，例如系统管理员。企业应针对单次登录的网络和SaaS应用程序使用集中式身份验证服务，对于以前未经审查和信任的设备，需要2FA（逐步身份验证）。此外，企业应使用FIDO U2F令牌阻止网络钓鱼攻击或采取其他合理的预防措施，减少网络钓鱼攻击造成的风险。

企业应遵循最低特权访问原则-基于角色的访问请求（基于角色的访问控制）和/或流程外，异常，休眠和职责分离的批准，检测和补救（SoD）违规访问，并通过定期重新验证访问权限（持续业务需求或CBN）来访问治理。

企业应进行特权用户监控和审计以及安全信息事件管理（SIEM）。它们还应该具有用于服务或应用程序ID的凭证/秘密保险库-不应以纯文本格式将ID存储在配置文件中。

高级功能：高级企业可能拥有更复杂的身份和访问权限管理方法：

- 连续身份验证方法在整个用户会话中利用行为和生物识别技术监控来确定会话是否受到威胁。
- 基于风险的身份验证可让企业更好地理解身份周围的环境，例如地理位置数据或购买行为。系统可以识别身份，确定不需要传统身份验证，并允许访问。相反，如果系统检测到异常情况（例如，在密码少了几个失败后于半夜从国外登录），则此操作风险很高，如果没有其他身份验证步骤，将拒绝访问。
- 特权访问管理解决方案为拥有“王国钥匙”的用户和帐户提供所需的可见性，监控和控制。至关重要的是，只允许管理员执行对其角色至关重要的那些操作–启用“最低特权访问”以降低风险。
  这种可见性可以洞悉活动，并预防或标记任何表明安全风险的异常事件。
- 自适应身份验证使用2FA / MFA，除了设备指纹识别外，还具有更完整，更复杂的风险计算，并结合了内部网或互联网，从多个位置或地理位置同时访问，在非常奇异的时间登录等因素。
- 闭环身份治理将服务器和内部应用程序中的用户活动监控和分析与访问管理工具集成在一起，例如，如果特权用户被检测到以未经授权的方式访问服务器或应用程序内部的受保护数据，则撤消该访问。
- 借助分析和人工智能可以实现更智能的访问监管，例如，检测和撤消休眠访问–所有者长期未使用的访问会发出潜在的访问治理或离职通知信号。
- 通过集成特权访问管理与用户和实体行为分析（UEBA），可以改善检测和防御黑客行为：使用社交网络信息和电子邮件通过鱼叉式网络钓鱼将恶意软件丢弃到工作站上的行为会有所不同，并且可以表明工作站和特权用户凭据已被泄露。

在美国，几乎

1 in 5

个人计算机运行盗版软件

而

在中国，拥有盗版软件的个人计算机百分比

经常超过

70%

6. 过期和盗版产品的迁移问题

企业应停止使用已终止制造商支持的旧产品。80从技术支持的角度来看，一个密切相关的问题是盗版软件。在美国，几乎五分之一的个人计算机运行盗版软件，而在中国，拥有盗版软件的个人计算机比例通常超过70%。81当然，制造商通常不修补盗版软件，这意味着它仍然容易受到已知漏洞的利用.82企业应避免使用盗版软件，并减少全球互联网和通信生态系统中的漏洞总数。

基准实践：企业应在制造商支持终止之前更换合法的支持产品。企业应始终避免使用盗版产品。此类产品在大多数国家/地区都是非法的，也是导致整个生态系统安全漏洞的主要因素。83

高级功能：高级企业可能会提供最新的受支持产品，以及最新的安全功能。

06 后续步骤和结论

本指南1.0版的发布，是针对僵尸网络和其他自动化，分布式威胁的前所未有的行业领导战略攻势的第一步。 CSDE，USTelecom，ITI和CTA敦促利益相关者实施推荐的实践方法，应对常见挑战并扭转不利行为者的潮流。

正如《指南引言》所述，数字经济一直是全球商业增长和生活质量改善的引擎。没有一个公共或私营部门的利益相关者控制这个系统，因此，安全管理这一增长所带来的机会，是信息通信技术社区每个利益相关者的当务之急。

为此，我们列出了这些基准实践和高级功能，供所有利益相关方考虑。这些是动态，灵活的解决方案，以自愿共识标准为基础，并由强大的市场力量驱动，可由全球数字经济中的利益相关方实施。这是对付我们面临的系统网络安全挑战的最佳答案。

考虑到这一点，我们计划每年更新，发布和推广本指南的新版本，以反映最新发展和技术突破，帮助我们的公司和全球其他公司推动可观察和可衡量的安全改进。 -不仅在自己的网络和系统中，而且在整个更广泛的生态系统中。

更直接的是，我们未来几个月的下一步工作是与互联网和通信生态系统中广泛的国家和国际利益相关方一起推广本指南，这些利益攸关方既可以推广建议的实践，又可以开展建设性参与。这些不同的利益相关方承担的共同责任是确保数字经济未来的关键。

07 贡献组织

关于CSDE

安全数字经济理事会（CSDE）将信息通信技术（ICT）领域的公司召集在一起，通过协作行动应对日益复杂和新兴的网络威胁。创始合作伙伴包括Akamai，AT&T，CA Technologies，CenturyLink，思科，爱立信，IBM，英特尔，NTT，甲骨文，三星，SAP，Telefonica和Verizon。 CSDE由USTelecom和信息技术行业理事会（ITI）协调。

关于USTelecom

USTelecom是代表电信行业服务提供商和供应商的首要贸易协会。其成员广泛，从大型上市通信公司到小型公司和合作社，均为城乡市场提供先进的通信服务。

关于ITI

信息技术行业理事会（ITI）是技术行业的全球代表。作为全球领先的创新公司的首要倡导和政策组织，
ITI指导政策制定者，公司和非政府组织之间的关系，提供创新解决方案，促进全球技术的开发和使用。

关于消费者技术协会

消费者技术协会（CTA）™是代表3770亿美元的行业协会
美国消费技术行业，为超过1,500万个美国工作岗位提供支持。超过2,200家公司，其中80％为小型企业和创业公司；其他品牌属于全球最知名品牌-享受CTA会员资格，包括政策宣传，市场研究，技术教育，行业促进，标准制定以及促进业务和战略关系。 CTA还拥有并生产CES®（消费电子产品展），这是所有消费技术业务蓬勃发展的人的聚集地。来自CES的利润被重新投资到CTA的行业服务中。

08 尾注

1 恶意行为者通常也称为黑客，尽管并非所有黑客都是恶意软件。通常，本文档可互换使用术语，前提是上下文将指示被引用的个人是否为恶意行为者。还应注意的是，本文档重点关注恶意行为者，因此，一般来讲，本文档中的“黑客”是恶意行为者。

2 同时设置IoT生态系统中所有软件类型的需求不切实际。设备和设备系统，企业和基础设施有特定要求。本节适用于本指南其他地方未涵盖的领域。

3 单个连接的设备（或“端点设备”）本身可以由多个组件组成，包括硬件模块，芯片，软件，传感器或其他操作组件。成千上万的公司和数百万的开发人员为全球数十亿设备的开发做出了贡献。除了单个设备本身之外，还构成了多个附加的连接层
一个充满活力的新市场，包括安全创新。简单地说，连接的设备不再仅仅是单个设备。考虑到这种复杂性，本指南解决的是设备系统：互联端点设备（在物联网中的一个“物”）及其相关支持元素（包括应用程序和云服务）的结合。

4 连接供暖，通风和空调（HVAC）系统，以实现智能功能和乘员远程访问。安全系统包括通过互联网管理的摄像头，锁和警报系统。娱乐系统受益于中央控制，因此可以轻松管理复杂的音频和视频配置。这些类别的制造商和系统千差万别。
这些系统可以由自己动手的家庭和企业主安装，也可以由专业人员安装，例如集成商，警报承包商等。理想情况下，
每个进入家庭，办公室，零售，医疗或工业环境的设备系统，都将在设备整个生命周期内采用最佳实践进行安全保护，包括安装和配置可实现制造产品“最佳安全性”的设备。

5 消费类技术。互联网连接家庭安全系统（Assn），https：//cta.tech/Membership/Member-Groups/TechHome-Division/Device-Security- Checklist.aspx（最新访问时间：2018年10月10日）。

6 作为网络设备和系统的主要所有者和用户，包括数量不断增长的IoT设备系统，企业
各种类型的政府，私营部门，学术界和非营利组织在保护数字生态系统中都可以发挥关键作用。虽然企业通常是自动化，分布式攻击和数据泄露尝试的目标，但也可以劫持其庞大系统，增加分布式拒绝服务和其他分布式攻击对他人的影响。因此，企业属于利益相关者，共同承担充分保护其网络和系统的责任，以帮助保护更广泛的数字生态系统。全球数以百万计的私营部门和政府企业在技术知识和技能，获得资源和采用基准安全实践的动机方面存在很大差异。各种规模的企业都可以采取主动措施降低生态系统风险。这些步骤可以帮助企业保护网络上的敏感数据和知识产权，同时还有助于减少僵尸网络的攻击面，从而保护整个生态系统。制定本指南的供应商和提供商都是大型跨国企业，我们还提供高端解决方案，保护企业网络安全并缓解分布式拒绝服务攻击和其他自动化，分布式威胁。该市场的“供应”端强劲且不断增长，该市场“需求”端的进一步发展
各种规模的企业对这些服务的要求和谈判，将为这些服务带来进一步的创新，完善和成本效益

7 CSDE，ITI和USTelecom的说明如下。 41。

8 CTA说明如下。 41。

9 为简便起见，以下将“僵尸网络和其他自动分布式威胁”称为“僵尸网络”。

10 Andrew Sheehy，GDP无法解释数字经济，福布斯（2016年6月6日），https：// c无法解释数字经济/＃47c4db1218db。/www.forbes.om/sites/andrewsheehy/2016/06/06/gdp-

11 Irving Wladawsky-Berger，《数字经济中的GDP无效》，《华尔街日报》（2017年11月3日）https://blogs.wsj.com/cio/2017/11/03/gdp-doesnt-work-在数字经济中。

12 保罗·滕纳（Paul Tentena），《到2025年将数字经济翻一番，达到23万亿美元的人工智能》，东非商业周刊（2018年5月30日），busiweek.com / artificial-intelligence-to-double-digital-economy-to-23-trillion-by- 2025年。http://www.

13 *参见，例如，Catalin Cimpanu，狡猾的恶意软件作者将加密采矿僵尸网络隐藏在Ever-shifting Proxy Service背后，ZDNet（2018年9月13日），https：// hind-ever-shifting-proxy-service（“ [B] OTnets专注于加密货币挖掘运营一直是2018年最活跃的恶意软件感染形式之一。”*www.zdnet.com/article/sly-malware-author-hides-cryptomining-botnet-

14 山姆·泰尔曼和克里斯·约翰斯顿，《重大网络攻击中断了欧美的互联网服务》，《卫报》，（2016年10月21日），https：// theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service。/www

15 迈克尔·纽伯格（Michael Newberg），多达4800万个推特帐户不是人，CNBC研究（2017年3月10日），https：//。可能有近4,800万个推特帐户是bots-says-study.html。/wwwcnbc.com/2017/03/10/

16 JP Buntinx，《迄今为止最大的4个僵尸网络》，德克萨斯州空，2017年1月7日，https：//nulltx.com/top-4-largest-botnets-to-date。

17 丹尼尔·纽曼（Daniel Newman），《福布斯》（Forbes）2018年IoT趋势2018年前8大趋势（2017年12月19日），https：// ctrends-for-2018 / ＃2523096867f7（引用了《HIS Markit IoT趋势观察2018》，网址为https://ihsmarkit.com）。/industry/telecommunications.html）；另请参阅Gartner，Gartner说，2017年将使用84亿个联网“事物”，比2016年增长31％（2017年2月7日），https：// t newsroom / press-releases / 2017-02-07-gartner-说80亿连接的东西将在2017年使用中，占2016年的31％。/www.forbes.om/sites/danielnewman/2017/12/19/the-top-8-iot-/www.garner.com/en/

18 简·彼得·克莱汉斯（Jan-Peter Kleinhans），“不安全的事物互联网：安全评估能否治好市场失灵？”，新基金会速报（2017年12月），https：//insecure_things.pdf。www.stiftung-nv.de/sites/default/files/internet_of_

19 Bill Connor，“勒索软件即服务：下一次巨大的网络威胁？”，福布斯（2017年3月17日），https：// c/www.forbes.om/sites/ Forbestechcouncil / 2017/03/17 /勒索软件即服务下一个更大的网络威胁 /＃14a38e5b4123。

20 安迪·格林伯格（Andy Greenberg），白宫为NoPetya指责俄罗斯，“历史上最昂贵的网络攻击”，《连线》（2018年2月15日）https://www.wired.com/故事/ white-house-russia-notpetya-归属；俄罗斯达米恩·沙尔科夫（Damien Sharkov）被指控犯有12亿诺佩蒂网络攻击，新闻周刊（2018年2月15日）https：// c-attack-807867;哥伦比亚广播公司新闻，我们可以从历史上最具破坏性的网络攻击中学到什么？（2018年8月22日），https：//。您可以从毁灭性的notpetya网络攻击有线学习中吸取教训（讨论NotPetya恶意软件如何造成超过100亿美元的损失）/wwwwired.com//www.newsweek.om/russia-accused-massive-12-billion-cyber-/wwwcbsnews.com/news/

21 Alex Zaharov-Reutt，网络犯罪，数据泄露导致企业损失8万亿美元，到2022年，ITWire（2017年4月25日），https：// csecurity / 77782- 8万亿美元-商业成本-来自网络犯罪和数据-Breakes-thru-2022.html。/www.itwire.om/

22 可持续发展委员会第四委员会，可靠性和互操作性委员会第四届会议，网络安全风险管理和最佳实践最后报告4（2015年3月），网址：https：//transition.fcc.gov/pshs/advisory/csric4/CSRIC_ IV_WG4_Final_Report_031815.pdf（承认“非规范性方法相对于规定性和静态合规性制度的优势”）。

23 *参见上文注释1-22和下文注释24-83*。

24 丹尼尔·帕尔默（Daniel Palmer），研究人员在推特上发现巨大的加密诈骗僵尸网络，Coindesk（2018年8月7日），https：//。巨型Twitter上的僵尸网络骗局（“研究人员发现了一个巨大的僵尸网络，模仿推特上的合法账户传播加密货币“赠予”诈骗。”）。/wwwcoindesk.com/researchers-discover-

25 Tobias Knecht，《僵尸机器人简史及其如何塑造当今的互联网》，Abusix（2017年8月23日），https：/ u。/www.absix.com/blog/a-brief-

26 达斯汀·沃尔兹（Dustin Volz）和吉姆·芬克尔（Jim Finkle），《美国起诉伊朗人黑客入侵数十家银行》，路透社纽约大坝（2016年3月），https：// c-usa-iran-cyber / us-indicts-iranians-for-hacking-几十s-纽约大坝银行idUSKCN0WQ1JF。/www.reuters.om/article/

27 Lee Matthews，全球最大的Mirai僵尸网络正被出租进行分布式拒绝服务攻击，福布斯（2016年11月29日），https：// c leemathews / 2016/11/29 / worlds-biggest-mirai-botnet-is-being-rented- out-for-ddos攻击/＃6bdec4cb58ad。/www.forbes.om/sites/

28 *比较Elie Bursztein，《臭名昭著的Mirai IoT僵尸网络内部：回顾分析》，Cloudflare（2017年12月14日），https：//blog.cloudflare。com / inside-mirai-in-famous-iot-botnet-a追溯分析（“ Mirai攻击最大，最高达到623 Gbps”），联邦大陪审团Sean Gallagher起诉7名伊朗人“竞选（2016年3月24日）（“分布式拒绝服务攻击在峰值时达到了每秒140吉比特”）。*

29 请注意，2018年3月，针对GitHub的攻击者打破了Mirai僵尸网络的流量记录，分布式拒绝服务攻击达到了1.35 Terrabytes / s。参见Lily Hay Newman，GitHub，有线网络（2018年3月1日），生存了有史以来最大的分布式拒绝服务攻击.https：//www.wired。com / story / github-ddos-memcached。值得注意的是，攻击并未使用

僵尸网络。取而代之的是，攻击者欺骗了对易受攻击的“内存缓存”服务器（用于加速网站）的请求，导致被攻击者被洪水淹没的流量约为正常互联网流量的50倍。 （“ Memcached”是指分布式内存缓存系统，通常用于通过在随机存取存储器中“缓存”数据而不是依靠外部数据源来提高网站速度。）因为Memcached服务器会响应任何人，包括恶意行为者-不应将其暴露于公共互联网。但是，其中大约有100,000台服务器处于暴露状态和脆弱状态。许多属于安全资源有限的小型企业和组织。参见Liam Tung，《Landmark GitHub断电后新世界记录分布式拒绝服务攻击数天达1.7Tbps》，ZDNet，2018年3月6日，https：// after-landmark-github-outage。这种利用服务器漏洞的泛洪攻击在不良行为者中越来越流行。在GitHub幸存下来“有史以来最大规模的分布式拒绝服务攻击”仅几天之后，记录再次被打破：一个Arbor Networks客户的目标是遭受类似的攻击，达到1.7 Tbps。www.zdnet.com/article/new-world-record-ddos-attack-hits-1-7tbps-days-

30 赛伦（Cyren），《赛伦网络威胁报告8》（2017年1月），http：//www.vcwsecurity。 com / wp-content / uploads / 2017/01 / Cyren_2017Q1_Botnet_Threat_Report.pdf。

31 Denis Makrushin，发动分布式拒绝服务攻击的代价，卡巴斯基（2017年3月23日），https：//securelist.com/the-cost-of-launching-a-ddos-attack/77784 。

32 WannaCry Ransomware的Alfred Ng失去了杀戮开关，所以当心，CNET（2017年5月15日），https：//。补丁更新病毒杀死开关。/wwwcnet.com/news/wannacry-ransomware-

33 艾伦·中岛艾伦（Ellen Nakashima），俄罗斯军事力量在乌克兰“ NotPetya”网络攻击背后，中央情报局结论，《华盛顿邮报》（2018年1月12日），https：//。 washingtonpost.com/world/national-security/russian-military-was-behind-/www notpetya-cyberattack-uk-cia-concludes / 2018/01/12 / 048d8506-f7ca-11e7-b34a-b85626af34ef_story.html？utm_term = .bc4ce7d72018。

34 安迪·格林伯格（Andy Greenberg），《黑客正试图通过不间断僵尸网络攻击重新唤醒WannaCry》，《连线》（2017年5月19日），https：//www.wireless.com/en/us/。想要勒索软件ddos攻击。/wwwwired.com/2017/05/

35 哥伦比亚广播公司新闻，我们可以从历史上最具破坏性的网络攻击中学到什么？（2018年8月22日），https：//。来自毁灭性的notpetya网络攻击有线调查。/wwwcbsnews.com/news/lessons-to-learn-

36 美国商务部和美国国土安全部，致总统的报告关于增强互联网和通信生态系统抵御僵尸网络和其他自动分布式威胁的能力（2018年5月22日），网址为https： /。 files / media / files / 2018 / eo_13800_botnet_report _-_ finalv2.pdf；第二次委员会，可靠性和互操作性委员会第四工作组，网络安全风险管理和最佳实践的最终报告（2015年3月），请访问：https：//transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_ Report_031815 .pdf; ENISA，僵尸网络测量，检测，消毒和防御（2011年3月7日），https：//。测量，检测，消毒和防御；国际电信联盟，/wwwcommerce.gov/sites/commerce.gov//wwwenisa.europa.eu/publications/botnets-
国际电联僵尸网络缓解工具包（2008年1月），https：//cybersecurity/docs/itu-botnet-mitigation-toolkit-background.pdf。/www.itu.int/ITU-D/cyb/

37 美国商务部和美国国土安全部，致总统的报告关于增强互联网和通信生态系统抵御僵尸网络和其他自动分布式威胁的能力10（2018年5月22日），网址为https ：/。 gov / files / media / files / 2018 / eo_13800_botnet_report _-_ finalv2.pdf。/wwwcommerce.gov/sites/commerce.

38 蒂姆·波尔克（Tim Polk），《增强互联网和通信生态系统的弹性》，纳塔尔研究所。标准和技术。 7月9日至9日（2017年9月）（讨论分布式拒绝服务保护工具和技术，包括入口/出口过滤；内部和外部内部分布式拒绝服务保护），网址为https：// doi。

org / 10.6028 / NIST.IR.8192。另请参见点击率。对于民主和技术，对NTIA促进利益相关者采取行动抵御僵尸网络和其他自动威胁的评论2（2018年2月12日）（同意NTIA的报告草案，“僵尸网络缓解常见技术包括入口和出口过滤，重新路由”，并塑造互联网流量，隔离设备或其他实体。”，网址：https：//cdt.org/files/2018/02/CDT-NTIA-Botnet-Comments-Feb-2018.pdf；第二次会议，可靠性和互操作性委员会第四工作组，网络安全风险管理和最佳实践的最终报告（2015年3月），网址：https：//transition.fcc.gov/pshs/advices/csric4/CSRIC_IV_WG4_Final_Report_031815。 pdf。

39 *参见，例如美国DHS自动指标共享（AIS）系统，https：// t（最新访问时间：2018年10月17日）;英国，网络安全信息共享合作伙伴关系（CiSP），https：//www.ncsc。 gov.uk/cisp（最新访问时间：2018年10月17日）;日本，网络清洁中心，https：//（最新访问2018年10月17日）;*/www.us-cer.gov/ais www.telecom-isac.jp/ccc/en_index.html
新西兰CORTEX，https：// c保证/ cortex-faqs（最新访问2018年10月17日）。/www.gsb.govt.nz/our-work/information-

40 *请参阅David Strom，什么是多态恶意软件，为什么要关注？（2015年10月16日），https：//securityintelligence.com/what-is-polymorphic-malware-and-why-should-i-care。*

41 Verizon，2012年数据泄露调查报告71（2012年），https：//Report-2012.pdf。
www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-

42 *见斯蒂芬·斯拉达里兹，《关于启发式算法》，SANS研究所4（2002年3月23日），网址：https：// a-about-heuristics-141（比较两种不同类型的启发式分析）；另请参见John Aycock，计算机病毒和恶意软件74（2006年）（解释道，静态和动态启发式方法唯一的区别在于“数据的收集方式”，否则数据相同）。*/www.sans.org/reding-room/whitepapers/malicious/

43 *参见，例如，思科，思科认知威胁分析v1（2016年2月），https：//dcloud-cms.cisco.com/demo_news/cisco-cognitive-threat-analytics-v1。*

44 Nat’l Inst。标准和技术，高级分布式拒绝服务缓解技术（2017年10月18日）（“十多年来，行业一直在开发技术规范和IP级过滤技术的部署指南，以阻止带有欺骗性源地址的网络流量”），可在https：/ s mitigation-techniques获得/www.nit.gov/programs-projects/advanced-ddos-

45 P. Ferguson和D. Senie，网络入口过滤：击败利用IP源地址欺骗的拒绝服务攻击，互联网
工程任务组（IETF）网络工作组（2000年5月），网址：https：//tools.ietf.org/html/bcp38； F. Baker＆P. Savola，《多宿主网络入口过滤》，互联网工程任务组（IETF）网络工作组（2004年3月），网址：https：//tools.ietf.org/html/bcp84。

46 ID。

47 *一般请参见，例如克里斯·本顿（Chris Benton），SANS研究所的出口过滤常见问题解答（2006年4月19日），网址：https：//防火墙/出口过滤-faq-1059。*
/www.sans.org/redingroom/whitepapers/

48 *参见思科，访问控制列表（最新更新于2018年7月17日），https：// 。cisco.com/c/en/us/td/docs/security/asa/asa99/asdm79/firewall/asdm-79-firewall-config/access-acls.html。*/www

49 *参见思科，《警务和成形概述》（最新更新，2017年11月23日），https：//。 guide / fqos_c / qcfpolsh.html。*

/wwwcisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/

50 *一般请参见，例如，SANS研究所域名Sinkhole的Guy Bruneau（2010年8月7日），https：// w sinkhole-33523。*/ww.sans.org/reading-room/whitepapers/dns/dns-

51 *参见思科，实施BGP Flowspec（最新更新于2018年1月31日），https：//。asr9k_r5-2 / routing / configuration / guide / b_routing_cg52xasr9k / b_routing_cg52xasr9k_chapter_011.html。*
/wwwcisco.com/c/en/us/td/docs/routers/asr9000/software/

52 *见佐治亚州技术研究人员，域名系统（DNS）变更补救研究，向M3AAWG第27届股东大会演讲，加利福尼亚州旧金山（2013年2月19日），网址：https：// w*/www.m3aag.org/sites/default/files/document / GeorgiaTech_DNSChanger_Study-2013-02-19.pdf（最新访问时间：2018年10月17日）；另请参阅委员会委员会部门协调网络僵尸网络白皮书24-25（2017年7月17日）（列出了基础设施提供商通知用户的多种方式，包括电子邮件，电话，邮政信箱，
短信，网络浏览器通知，围墙花园以及其他方法（如社交媒体），请访问https://docs.wixstatic.com/ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf。

53 *参见点击率。对于民主和技术，对NIST模型进行评论，以向消费者发出有关僵尸网络和相关恶意软件非法使用计算机设备的自愿企业通知（2011年11月14日）（表达了对"切断或以其他方式干扰"的做法表示关注）客户的互联网连接"*
僵尸网络补救），请访问：https：//sdocuments/itl/CDT-Comments-on-BotNet-FRN-11-14-11.pdf；电气。前沿发现，针对僵尸网络和相关恶意软件向消费者发出自愿向消费者发出的企业组织自愿通知的NIST模型注释（5，2011年11月4日）（解释未感染方如何隔离隔离感染互联网），网址为https：//s-to-BotNet-RFI_11-4-11.pdf。
/www.nit.gov/sites/default/files//www.nit.gov/sites/default/files/documents/itl/EFF-

54 *参见委员会区域协调委员会，僵尸网络白皮书21（2017年7月17日），（"没有任何一种技术比导致逮捕肇事者的执法行动更有效。这是解决根除犯罪行为根源的唯一解决方案。问题，而不仅仅是症状……[E]执行一个*僵尸网络的瘫痪需要进行大量的前期法庭分析，并经常需要跨国际边界在许多利益相关方之间进行仔细的协调……。大多数僵尸网络本质上是国际性的，需要国家之间资源密集且耗时的合作。"，网址为https：// docs。wixstatic.com/ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf。

55 *参见罗伯特·韦恩赖特和弗兰克·Cilluffo，《应对网络犯罪：案例研究》，欧洲刑警组织和乔治华盛顿大学。点击率针对网络和国土安全部门。（2017年3月），网址为https://cchs.gwu.edu/sites/g/ files / zaxdzs2371 / f / Responding %20to %20Cybercrime %20at %20Scale %20 FINAL.pdf。*

56 *参见SAFECode，《安全软件开发基本实践》（2018），https：//safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf。*

57 Arora等人，卡耐基梅隆大学，《软件供应商修补行为的实证分析：漏洞披露的影响》（2006年1月）（分析大型供应商相对于其他供应商的激励机制），网址：https：//。/wwwheinz.cmu.edu/~rtelang/disclosure_jan_06.pdf.

58 *参见SAFECode，软件保障评估原则（2015），网址：https：//safecode.org/publication/SAFECode_Principles_for_Software_Assurance_Assessment.pdf；CA Tech。，Veracode，https：//。veracode.com/verified（最新访问时间：2018年6月18日）。*/www

59 Nat'l Inst。标准和技术局局长，NTIA软件组件透明性，https：// o（最新访问时间：2018年11月6日）。/www.ntia.doc.gv/SoftwareTransparency

60 本部分中的设备和系统借鉴了消费类技术。 Ass'n，为家庭消费者确保互联设备的安全-制造商指南（CTA-CEB33），https：//members.cta.tech/ctaPublicationDetails/？id = c12 ebabe-84cd-e811-b96f-0003ff52809d（最新访问） 2018年10月15日）。

61 早期需求规划和最终认证对该过程至关重要。例如，CTIA管理物联网设备的认证计划，建立无线网络设备安全的行业要求，并提供认证计划。有关程序的详细信息，包括要求和设备认证方式，请参见：https：//。/wwwctia.org/about-ctia/programs/certification-resources.

62 *请参阅Microsoft，什么是安全开发生命周期？，https：//。microsoft.com/en-us/sdl/default.aspx（最新访问时间：2018年10月19日）*。/www

63 *参见BSIMM，https：//bsimm.com（最新访问2018年11月6日）*。

64 有关更多国际标准，请参阅Nat'l Inst。标准和技术委员会，密码模块验证计划，https：//csrc.nist.gov/projects/cryptographic-module-validation-program/standards。此外，NIST还提供国际标准摘要草案：Nat'l Inst。标准和技术局，《物联网国际网络安全标准化现状机构间报告》，https：//csrc.nist.gov/publications/detail/nistir/8200/draft（最新访问2018年10月10日））。

65 有关当前的建议建议书，请参见IETF，制造商使用说明规范，https：//datatracker.ietf.org/doc/draft-ietf-opsawg-mud（最新访问时间：2018年10月19日）。

66 思科，制造商使用说明是什么？ （MUD），https：//developer.cisco.com/docs/mud/#！what-is-mud（最新访问时间：2018年10月19日）。

67 IEEE，802.1AR：安全设备身份，https：//1.ieee802.org/security/802-1ar/（最新访问2018年10月19日）。

68 可信计算小组，设备标识符组合引擎（DICE）架构，https：//trustedcomputinggroup.org/work-groups/dice-architectures（最新访问时间，2018年10月19日）。

69 有关更新的讨论，请参见Nat'l Inst。标准和技术，利益相关方起草IoT安全文档，https：// o IoTSecurity（最新访问，2018年10月10日）。/www.ntia.doc.gv/

70 消费类技术。互联网连接家庭安全系统（Assn），https：//cta.tech/Membership/Member-Groups/TechHome-Division/Device-Security- Checklist.aspx（最新访问时间：2018年10月10日）。

71 美国商务部和美国国土安全部，致总统的报告关于增强互联网和通信生态系统抵御僵尸网络和其他自动化分布式威胁的能力12-15（2018年5月22日）在https：/。 gov / files / media / files / 2018 / eo_13800_botnet_report _-_ finalv2.pdf。/wwwcommerce.gov/sites/commerce.

72 网络安全联盟，分布式拒绝服务威胁缓解配置文件，https：//。cybersecuritycoalition.org/ddos-framework（最后访问时间为2018年11月14日），以及网络安全联盟《僵尸网络威胁缓解配置文件》，https：//。 cybersecuritycoalition.org/botnet-framework（最新访问时间：2018年11月14日）。/www/www

73 *参见第二委员会，可靠性和互操作性委员会第二工作组，关于ISP网络保护的最终报告16（尤其建议用户应"配置计算机，将关键更新下载到两个操作系统"并自动安装应用程序。"）（11月。*

2011年），网址：https：// e
FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf。
/www.atis.org/01_lgal/docs/CSRICII/CSRIC_WG8_

74 蒂姆·波尔克（Tim Polk），《增强互联网和通信生态系统的弹性》，纳塔尔研究所。标准和技术。 13（2017年9月）（引用了2017年7月11日至12日举行的NIST增强互联网和通信生态系统抵御能力研讨会参与者的意见），网址为https://doi.org/10.6028/NIST.IR.8192。

75 斯科特·鲍文（Scott Bowen），Akamai，按设计防御：如何通过弹性网络抑制分布式拒绝服务攻击，福布斯（2017年9月14日）https：// csites / akamai / 2017/09/14 / defense-by-design-how-to -使用弹性网络进行阻尼ddos攻击/＃79144da56f8a。 /www.forbes.om/

76 *参见AT＆T的《分布式拒绝服务防御》（DDoS）防御（2014），网址为https：//。 ddos_prodbrief.pdf; Verizon，《分布式拒绝服务盾牌解决方案简介》（2016年），见brief_en_xg.pdf；CenturyLink，分布式拒绝服务缓解（2014），见http：// pdf；西班牙电信，Anti-DDoS，https：//。云/产品/安全/反ddos（最新访问时间：2018年5月14日）；NTT，分布式拒绝服务保护服务，https：//。 ddos.html（最新访问2018年5月14日）。*
/wwwbusiness.att.com/content/productbrochures/http://www.verizonenterprise.com/resources/ddos_shield_solutions_
www.centurylink.com/asset/business/enterprise/brochure/ddos-mitigation./wwwcloud.telefonica.com/en/open-
/www.nttcom/en/services/network/gin/transit/

77 *参见上文第5.A.2（e）部分的讨论（解释清理中心在缓解僵尸网络中的功能）。*

78 Nat'l Inst。标准与技术学院，数字身份指南（2017年6月），*网址为https://doi.org/10.6028/NIST.SP.800-63-3。*

79 布莱恩·克雷布斯（Brian Krebs），谷歌：安全密钥中和员工网络钓鱼，克雷布斯安全（2018年7月23日）https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing。

80 *请参阅Microsoft，Windows XP支持已终止，https：// support。microsoft.com/zh-cn/help/14223/windows-xp-end-of-support（上次访问日期为2018年5月15日）。*

81 *参见BSA软件联盟，通过许可证合规抓住机遇：BSA全球软件调查6-7（2016年），媒体/文件/研究下载/BSA_GSS_US.pdf。* http://www.bsa.org/~/

82 *ID。第4页（讨论恶意软件和未经许可的软件之间的"强相关性"）*
。

83 新加坡国立大学，非正版软件带来的网络安全风险，亚太地区盗版软件来源与网络犯罪攻击之间的联系6（2017年11月1日），https：//news.microsoft.com/uploads/2017/10/白皮书-非网络正版风险软件（英文）。（"在世界许多地方，盗版/假冒/非正版软件的使用对网络风险和造成广泛的经济损失和生产力损失，也造成网络犯罪攻击和相关损失的增加。"）

CSDE

Council to Secure the Digital Economy

securedigitaleconomy.org