CSDE

Council to Secure the Digital Economy

国际僵尸网络和物联网安全指南 2020年

USTELECOM
THE BROADBAND ASSOCIATION

Consumer Technology Association™

注意

《国际僵尸网络和IoT安全指南》旨在通过全球互联网和通信生态系统不同利益相关方之间的自愿参与和协作，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攸关方提供信息和鼓励，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，没有多种措施能够保证消除所有威胁和风险，但他们相信，基准和高级实践为ICT利益相关者提供了一个宝贵的框架，可用于确定和选择自己的实践以减轻自动化分布式攻击威胁。《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，考虑因素和优先级。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：

高级功能（如IP流量的DPI）在某些情况下很有用，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

自CSDE去年发布《2018年国际反僵尸网络指南》以来，业界一直在加紧努力遏制分布式攻击。但是，恶意行为者也加大了努力。今年的《指南》版本一直在更新和更新，但《2020年指南》有两个重要补充，需要特别强调。首先，第3节包含有关僵尸网络威胁在过去一年中如何演变的全新且重要的“年度回顾”讨论。我们的分析的一些关键要点包括：

- 僵尸网络越来越多地采用策略，使其更有效地造成破坏，同时避免被发现。
- 僵尸网络更频繁地针对企业物联网和具有更复杂处理器和架构的其他物联网设备。
- 加密货币僵尸网络正在崛起，这些僵尸网络的运营商经常相互竞争。
- 僵尸网络越来越多地用于商业和零售欺诈。
- 社交媒体机器人伪造社交证据，传播受版权保护或非法分发的内容。
- 我们开始看到IPv6分布式拒绝服务攻击，至少有一个经过验证的示例。

其次，第5节中涉及设备和设备系统的部分，以及家庭和小型企业系统安装部分，得益于CSDE在全球领先的IoT安全行业共识中的发展。 CSDE利用来自数千家不同公司的数百名安全专家提供的技术投入，召集了20个主要的网络安全和技术组织，行业协会，财团和标准机构，为快速增长的IoT市场确定基线安全要求。这项工作被称为“召集召集人”或“ C2”，旨在应对四个挑战：

1. 促进全球统一，防止安全规格和要求分散化。
2. 与新兴的全球市场力量合作，自然而然地倾向于安全设备和系统。
3. 在这些问题上开发一致的通用语言，吸引各种政策和技术受众。
4. 协助国际和美国，包括州一级的政策制定。

这项具有里程碑意义的努力的结果是，2019年9月17日发布了IoT设备安全基线能力C2共识或“ C2共识基线”。C2共识基线是一组通用的设备安全功能，可应用于新的连接到互联网的IoT设备-最佳实践功能，在市场上纵向和横向广泛应用。它适用于各种新型IoT设备，可适应广泛的设备复杂性，无论部署环境如何。
基线旨在灵活而非规定性的。取决于多种因素，包括设备

复杂性，设备可管理性，风险概况，用例和环境–基线中概述的安全能力可以通过多种方式实现，关键是通过适用于特定设备的方式实现最终基线能力。

此外，今年NIST的广泛多方利益相关方流程（有关基础IoT设备安全）也将作为本年度指南的依据。 NISTIR 82591草案和C2在基线设备功能方面达成了实质性协议，双方还针对组织功能，客户信息和生命周期活动提出了其他建议。

最后，必须强调的是，在2016年基于Mirai IoT的僵尸网络事件（美国和欧洲的互联网大部分被毁）的情况下，CSDE的成员公司还制定了应对大规模僵尸网络行业协调的蓝图。该蓝图包含在我们的报告《网络危机：多方利益相关者协调基础》或“网络危机基础”中。报告考虑了总共12项重大网络安全事件的策略。

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，网络钓鱼攻击以及放大虚假社交媒体的虚假信息传播运动和其他恶意行为。2不幸的是，随着人数的增长，企业，和设备的增长，这些恶意攻击的可能性也在增加。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。全球网络成本犯罪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，并且是持续不断的威胁，并将在未来几年内寻求发展和适应。

> IBM安全情报报告说，Mirai变体的活动几乎翻了一番在2018年至2019年之间。

本指南旨在扭转这些趋势。尽管本指南的开发者大力支持政府在召集多元化生态系统中发挥的重要作用，但强加规定性，以合规性为重点的监管要求将抑制安全创新，而创新正是应对当今复杂威胁的关键。此外，较早的政策努力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，并由利益相关者在全球数字经济中实施的动态，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。

《国际僵尸网络和IoT安全指南：实践和功能摘要》。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）IoT设备，（4）家用和小型企业系统安装，以及（5）企业。对于上述每一个组成部分，《指南》都列出了所有这些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，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，而且软件定义网络和其他系统，也反映了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。3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. *物联网设备。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"，我们建议基准实践和高级功能包括：*

   - 安全开发
   - 安全功能
   - 产品生命周期管理

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的指数增长，各类企业（政府，私营部门，学术界，非营利组织）在保护数字安全方面发挥着至关重要的作用。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
   - 缓解过期和盗版产品问题

展望未来。正如《 2018年指南》的发布只是第一步一样，本指南也是CSDE持续战略的一部分，该战略旨在吸引广泛的利益相关方（包括志趣相投国家的政府）促进基准实践和先进能力，我们将继续展望不断变化的威胁需求。如《 2018年指南》所述，我们将每年更新，发布和推广新版本的《指南》。从今年开始，《指南》的标题将反映来年，因此，这是2020年版。

虽然今年与僵尸网络作斗争的标志是物联网设备安全，但由于迫切需要有一个被广泛接受的基准，但并非所有重要僵尸网络都以连接设备为目标，实际上，世界上最具破坏性的僵尸网络并不以僵尸网络为目标。连接的设备。因此，很明显，僵尸网络的未来与物联网安全的未来息息相关，而CSDE将继续在这一方面保持领先地位，我们还将探索其他方式通过会员的领导层可以大大减少僵尸网络和其他分布式威胁。认识到僵尸网络威胁的复杂性和层次性后，CSDE中的公司将在多个方面应对这些威胁。

The digital economy has been an engine for commercial growth and quality-of-life improvements across the world and may already represent 20% of global economic value.

02 /简介

数字经济安全理事会（CSDE）的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。

自产生《2018年国际反僵尸网络指南》以来，CSDE成员（Akamai，AT&T，CenturyLink，思科，爱立信，IBM，英特尔，NTT，甲骨文，三星，SAP，西班牙电信和Verizon）由美国电信和消费者技术协会（CTA）支持），一直在推动基础设施，软件，设备和数字经济其他领域在全球市场上采用更高安全性，以统一全球行业，对抗恶意僵尸网络。

世界已经注意到。 2019年，联合国互联网治理论坛表彰CSDE采取了有意义的行动，以协作，全生态系统的方式应对僵尸网络和其他自动化，分布式威胁，安全是共同的重点。在美国政府的僵尸网络路线图中，我们也被认为是这场斗争的主要贡献者。我们的全球项目正在影响CSDE成员开展业务的世界许多地区，包括欧洲，亚洲和拉丁美洲。

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%。7虽然仅靠国内生产总值不能捕捉数字经济对全球经济价值的全部贡献-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。8年可能增至23万亿美元，占全球GDP的近四分之一。数字经济的增长持续受到商业和消费者对新技术的采用。9
如此惊人的增长是信息和通信技术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。它们能够传播恶意软件，10进行拒绝服务攻击，11并在社交媒体上人工传播腐蚀性信息。12一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。 13由于数字经济本身的巨大增长以及令人鼓舞的增长，当今的系统比以往任何时候都更易受到攻击，尤其是在数十亿个物联网设备的快速部署方面，预计到2020年将达到200亿个互联设备。14互联经济带来的好处正在彻底改变商业和消费者活动，而制定本指南的公司在部署设备时也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。15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进行大规模的邪恶活动。16

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，恶意软件遍及欧洲，亚洲和美洲，造成的损失超过100亿美元.17据估计，在未来五年内，仅网络犯罪就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）。18

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，不仅规定性的监管要求很少有效，而且实际上通常与安全目标相反。19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。

出版《2018年指南》只是第一步。目前，我们正在与志趣相投国家的政府等广泛的利益攸关方合作，推广《指南》的基准实践和先进能力。此外，我们将继续每年更新，发布和推广新版本的《指南》。

2020年指南中的新材料。今年的《指南》版本一直在更新和更新，但《2020年指南》有两个重要补充，需要特别强调。首先，第3节包含有关僵尸网络威胁在过去一年中如何演变的全新且重要的“年度回顾”讨论。我们的分析的一些关键要点包括：

- 僵尸网络越来越多地采用策略，使其更有效地造成破坏，同时避免被发现。
- 僵尸网络更频繁地针对企业物联网和具有更复杂处理器和架构的其他物联网设备。
- 加密货币僵尸网络正在崛起，这些僵尸网络的运营商经常相互竞争。
- 僵尸网络越来越多地用于商业和零售欺诈。

‣社交媒体机器人伪造社交证据，传播受版权保护或非法分发的内容。

‣我们开始看到IPv6分布式拒绝服务攻击，至少有一个经过验证的示例。

其次，第5节中涉及设备和设备系统的部分，以及家庭和小型企业系统安装部分，得益于CSDE在全球领先的IoT安全行业共识中的发展。 CSDE利用来自成千上万不同公司的数百名安全专家的技术投入，召集了20个主要的网络安全和技术组织，行业协会，财团和标准机构，为快速增长的IoT市场确定基线安全要求。这项工作被称为“召集召集人”或“ C2”，旨在应对四个挑战：

1. 促进全球统一，防止安全规格和要求分散化。
2. 与新兴的全球市场力量合作，自然而然地倾向于安全设备和系统。
3. 在这些问题上开发一致的通用语言，吸引各种政策和技术受众。
4. 协助国际和美国，包括州一级的政策制定。

这项具有里程碑意义的努力的结果是，2019年9月17日发布了IoT设备安全基线能力C2共识或“ C2共识基线”。连接到互联网的IoT设备-最佳实践能力，在市场上纵向和横向广泛应用。它适用于各种新型IoT设备，可容纳设备复杂度，与部署环境无关。基线旨在灵活而不是规定性的。取决于多种因素，包括设备复杂性，设备可管理性，风险概况，用例
和上下文—安全功能
基线概述中的概述可以通过多种方式实现，关键是通过适用于特定设备的方式实现最终基线能力。

Based on a study of 180 countries and territories, Verizon reported that 84% of botnets involved in data breaches targeted the finance and insurance industries.

此外，今年NIST的广泛多方利益相关方流程（有关基础IoT设备安全）也将作为本年度指南的依据。 NISTIR 825920草案和C2工作在基线设备功能方面达成了实质性协议，双方还针对组织功能，客户信息和生命周期活动提出了其他建议。

最后，必须强调的是，在2016年基于Mirai IoT的僵尸网络事件（美国和欧洲的互联网大部分被毁）的情况下，CSDE的成员公司还制定了应对大规模僵尸网络行业协调的蓝图。该蓝图包含在我们的报告《网络危机：多方利益相关者协调基础》或“网络危机基础”中。报告考虑了总共12项重大网络安全事件的策略。

03 /僵尸网络的演变：年度回顾

与《2018年国际反僵尸网络指南》发布时一样，僵尸网络是对全球互联网和通信生态系统的自动化分布式威胁，最主要的类别是僵尸网络，大型互联网与计算机连接的计算机和设备与具有命令和控制功能。

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21。

僵尸网络：一个持续存在的全球性问题。随着CSDE中的公司与全球社区不断合作，向僵尸网络运营商施加越来越大的压力，这些恶意行为者也并非闲着。他们不想看到业务被拆除，看到我们公司的行为直接威胁到利润和其他关键目标。在2019年期间，我们观察到各种趋势，这些结论使我们得出结论，尽管与僵尸网络的斗争取得了进展，但挑战在不断升级。

我们的对手一直在关注我们的一举一动，并聪明地制定应对策略。僵尸网络运营商不断发明新工具，采用新技术并研究如何与破坏性机器人进行斗争，以反击我们的努力。我们正在与资金充沛的积极主动，日益老练的敌人作斗争，其中包括民族国家和大规模犯罪组织。这些组织有效地保护自己免受归属之害，同时有能力通过犯罪手段获得巨大的不义之财。

在本节中，我们将回顾僵尸网络威胁在过去一年中如何演变。我们的分析的一些关键要点包括：

- 僵尸网络越来越多地采用策略，使其更有效地造成破坏，同时避免被发现。
- 僵尸网络更频繁地针对企业物联网和具有更复杂处理器和架构的其他物联网设备。
- 加密货币僵尸网络正在崛起，这些僵尸网络的运营商经常相互竞争。
- 僵尸网络越来越多地用于商业和零售欺诈。
- 社交媒体机器人伪造社交证据，传播受版权保护或非法分发的内容。
- 我们开始看到IPv6分布式拒绝服务攻击，至少有一个经过验证的示例。

Mirai不会死亡：超过60种变体，活动量几乎翻倍。自三年前Mirai僵尸网络源代码在线泄漏以来，恶意行为者一直在进行实验并创建自己的升级版本。截至2019年7月，Mirai僵尸网络至少有63个已确认变体22，很可能仍有其他变体未被发现。

IBM安全情报报道，2018年至2019年期间，Mirai变种的活动几乎翻了一番。23。在2019年3月发布的一次关于新物联网利用的采访中，AT&T网络安全研究人员表示："每当研究新的IoT恶意软件时，几乎不可避免地会出现一个新的Mirai变体。每天，我们都会看到有不同有效载荷的新型Mirai变体……" 24 2016年，美国和欧洲历史性网络攻击关闭了互联网的相当大一部分之后，与Mirai相关的活动有所减少，但这种复苏标志着恶意软件仍然是一种严重的恶意软件。威胁。

不同的Mirai变体由运营商控制，运营商相互竞争争夺易受攻击的IoT设备的统治地位。可以预期，鉴于僵尸网络运营商在多方面开展技术军备竞赛（反对执法和相互对抗），新型僵尸网络通常比Mirai更为灵活。25Echobot是例如Mirai变体，于2019年发现，使用至少有26种漏洞感染设备。26

在某些情况下，僵尸网络创建者会将Mirai代码与其他来源的代码结合使用以实现目标。例如，根据IBM X-Force数据，Gafgyt占Mirai的27%，而这是针对Mirai的，尽管共享了部分泄漏的源代码，但它仍然独立于Mirai研究。

CenturyLink 2019年威胁报告28并排排列了Gafgyt，Mirai和其他IoT僵尸网络恶意软件，基于CenturyLink的Black Lotus Labs数据。29该数据显示，Gafgyt和Mirai的平均正常运行时间正在减少。可以解释为，更多的研究人员和威胁团队正在追踪恶意软件的移动；威胁研究人员越来越善于识别旨在逃避检测的IoT恶意软件变体；而且提供商在主动跟踪其网络上的威胁方面也越来越好。30

企业和高复杂度设备风险增高。尽管企业一直是减少僵尸网络的整个生态系统方法的重要组成部分，但越来越多地遭受破坏和损失。我们看到的僵尸网络威胁格局正在迅速扩大，最近的IBM X-Force数据显示，Mirai变体感染企业系统的频率更高。31Telefónica的数据表明，企业在此期间最有可能被僵尸网络感染部署新服务后的最初两个月。32

僵尸网络经常助长数据泄露，以至于Verizon的《2019年数据泄露调查报告》分别分析了僵尸网络攻击，"以掩盖"其他类型的事件。可以针对任何行业。但是，某些行业显然很容易受到僵尸网络攻击。根据对180个国家和地区的研究，Verizon报告称，涉及数据泄露的僵尸网络有84%以金融和保险行业为目标。 10%的目标是信息产业； 33%的目标是专业，科学和技术服务产业。这项研究没有区分物联网僵尸网络和其他僵尸网络。

过去，基于IoT的僵尸网络主要感染家庭中发现的连接设备和系统，如照相机，录像机，照明设备和恒温器。但是，从罪犯的角度来看，任何新类别的IoT设备（无论在家中，企业级别还是在生态系统中的其他地方）都是僵尸网络军队的新营，这是有道理的。许多拥有连接设备的利益相关者（不仅仅是企业）面临的风险正在增加。

例如，在2019年期间，CenturyLink的黑莲花实验室一直在分析TheMoon，这是一个针对宽带网络中路由器漏洞的物联网僵尸网络。34尽管这一特殊威胁已得到缓解，但它表明了物联网安全如何影响基础设施和生态系统。作为一个整体。

2019年2月，安全研究人员发现了Mirai示例，影响了以前无法作为目标的一系列处理器和架构.35我们现在可以预期会感染更多类型的路由器，网络传感器，无线电和数字信号微处理器36。为更大的僵尸网络打开大门。

专家认为，未来的攻击媒介可能会越来越多地包括工业物联网系统和互联可穿戴设备37，因此，对于行业和政府而言，协调确定识别与复杂性不同级别相关的独特考虑因素的安全功能至关重要。

智能自动化僵尸网络：Swarmbots和Hivenets。想象成千上万只蜂拥而至的单个目标。从本质上讲，这是一个群机器人。 Swarmbot通常仅凭纯粹的数量就能压垮传统防御手段。38更糟糕的是，这些bot是由被称为hivenet的人工智能控制的。

Hivenet是“自发思考的僵尸网络”，具有在攻击过程中学习的能力。39实时学习能力是造成危险的重要原因。传统僵尸网络需要等待操作员发出命令40，而蜂巢网络会根据群体机器人的学习情况自动协调策略。

Swarmbots共享有关发现的漏洞的信息以及其他战略信息，以提高配置单元的集体情报。机器人还自动协调和共享资源。各个机器人可能配备有不同的工具；当蜂巢网络发现漏洞时，将动员具有正确工作工具的蜂群机器人41。

通过部署基于群体的技术，僵尸网络运营商可以通过减少渗透设备或设备系统所需的时间来显着提高攻击效率。罪犯需要更高效率的主要原因之一就是跑赢网络安全工具，网络安全工具在全球市场上的部署频率越来越高。42我们处于长期技术军备竞赛中，基于群聚的技术是罪犯为升级是因为旧工具失效了。

Emotet回来了超过200,000被盗的电子邮件和密码。思科公司Talos报告称，僵尸僵尸网络Emotet经过数月的中断后于2019年9月复仇。43

TrickBot特洛伊木马和Ryuk勒索软件，两者都深入挖掘受害者的网络，增加了造成破坏的可能性。44 NTT目前正在使用网络流量数据捕获，并利用对40%的全球互联网流量的洞察力，分析TrickBot背后的基础设施和威胁行为者，到去年年底，TrickBot被视为对企业的最大威胁。45由于TrickBot通常如果下载了Emotet感染后下载，缓解TrickBot可以帮助限制Emotet的破坏潜力。

通常，Emotet发送的电子邮件似乎来自合法联系人。电子邮件中可能包含来自收件人真实对话的详细信息。众所周知，Emotet会引用以前的电子邮件线索，甚至像人类一样发送后续电子邮件。此类策略使僵尸网络越来越难以被垃圾邮件过滤器和人类检测到。46

Emotet进入电子邮件帐户并从受害者计算机窃取联系人列表和电子邮件，从而获得欺骗电子邮件收件人的必要信息 。思科Talos在对Emotet的研究中发现了202,675种独特的用户名和密码组合。47思科Talos还报告说，在名为Threat Grid的恶意软件沙箱中分析Emotet 10个月时，恶意僵尸网络试图发送垃圾邮件近19,000次。48

虽然科技新闻出版物称Emotet为“世界上最具破坏性的僵尸网络”49和“当今最危险的僵尸网络”50，但它并不是目前活跃的唯一高容量垃圾邮件机器人。例如，Gamut and Necurs这类垃圾邮件（几年前仅占互联网垃圾邮件流量的97%）继续造成麻烦。51

思科报告称，截至2019年，Gamut僵尸网络一直在发送约会和亲密垃圾邮件，以及制药和就业机会广告52。并发起分布式拒绝服务攻击。 CenturyLink的分析显示，Necurs病毒主要发生在发展中国家。53但是，由于僵尸网络无视管辖范围，因此这些感染在世界各地可能产生重大溢出效应。

僵尸网络租金：黑暗网络和社交媒体上现在都可用。在整个黑暗网络中（使用特定软件访问互联网的区域），存在犯罪市场，网络罪犯可以低价租用僵尸网络。这种安排称为恶意软件即服务（MaaS），将破坏性工具投入到更广泛的恶意行为者手中。54一些租用僵尸网络的罪犯缺乏制作自己的僵尸网络的技术能力。但是，也有人认为租用僵尸网络纯粹是务实的商业决策。像合法企业一样，犯罪企业也对投资回报感兴趣，并愿意优先考虑可产生最高回报的投资。55有时，技术娴熟的犯罪分子会租用僵尸网络来补充其现有的军队-在这种情况下，人们会想到租用的僵尸网络作为雇佣军。

在2019年网络危机基金会的报告中，CSDE记录了一家利比里亚电信公司的案例，该公司雇用一名犯罪黑客对竞争对手发动分布式拒绝服务攻击以获取不公平的竞争优势后成为诉讼对象.56黑客使用了一种习俗基于Mirai的僵尸网络，并从其他黑客那里租用了受感染的安全摄像头和路由器。57在高峰时，攻击使该国大多数互联网用户无法访问，进一步加剧了全球对物联网安全的担忧。58

为避免所有恶意活动在黑暗网络的秘密中扩散，越来越多的僵尸网络创建者正在主流平台上宣传其作品。有时，创作者甚至会租借僵尸网络

仍在开发中，热切的犯罪分子排队寻找位置。例如，Cayosin的创建者（一个被称为“ Frankenstein”的僵尸网络，因为它是由不同的开源恶意软件（包括Mirai）制成），已经在YouTube和Instagram上宣传了自己的项目，公开嘲笑法律并收取低廉的租赁费。激励罪犯成为他们的客户59。

僵尸网络创造者可以使用社交媒体进行市场研究，以提高利润为目标-有时他们会公开要求客户提供所提供服务的反馈意见，以便改善服务并与犯罪客户建立联系。60僵尸网络罪犯的文化发展发生了显着变化。

隐形机器人使用技巧避免被发现。僵尸网络开发人员正在不断发展战略，保持僵尸机器人的隐藏和活动时间更长。 Akamai最近的一份报告解释说：“机器人最多可以代表整体网络流量的60％，但实际上不到一半被宣布为机器人，这使得跟踪和阻止变得非常困难。” 61进一步复杂的因素是，并非所有这些机器人都是恶意攻击，因此在检测到自动化时根除犯罪行为具有挑战性。

例如，为了避免在访问网站时被检测到，恶意机器人冒充了流行的浏览器和移动应用程序，或者在某些情况下假装是很好的机器人。62一些机器人篡改浏览器属性，欺骗“指纹特征”，这些特征通常被列入白名单或丢弃饼干，甚至收获优质饼干，使饼干看上去合法，从而篡改饼干。63

我们还看到了“低速缓慢攻击”的持续增长，僵尸机器人试图躲在雷达下，
随着时间的流逝，我们会毫不留情地窃取大量信息。64使用这种方法时，机器人会更改其IP地址或使用多个IP地址。这样机器人就可以绕过速率限制，而不会被注意到。多个IP地址每小时发送少量请求。65

僵尸机器人还使用其他技术来保持“低速运行”时避开速率限制。僵尸网络运营商以更高的频率通过住宅宽带和无线连接对恶意流量进行匿名处理。66僵尸网络还通过隐藏在VPN和Tor67等匿名网络（包括最近发现的Mirai变体）中，通过代理更改其IP地址。68当敌人可以躲在人群中而不暴露自己时，侦察和防御敌人的工作就更加困难。

僵尸网络一直在利用另一把戏-本质上是在玩死。 CenturyLink的黑莲花实验室分析的Necurs僵尸网络会在不同的间隔进入持续宕机时间。在一个观察到的实例中，Necurs活跃了三周，安静了两周，然后又被激活.69 2019年，Necurs出现了几个月基本上没有活动的状态，仅在短时间内每周大约行动一次70。事实证明，Necurs具有域生成算法（DGA），可以抵抗各种破坏企图（由执法机构或安全研究人员部署僵尸网络陷阱）。但是，分析僵尸网络的DGA 向研究人员展示未来会生成哪些域名，因此他们能够检查相关的域名系统和网络流量并部署缓解策略。71

僵尸机器人冒充人类，欺诈在线零售商和广告商。 Akamai最近发布的互联网安全状况报告72显示，恶意机器人现在占据了针对在线零售商的互联网带宽的近一半。73鉴于这一令人震惊的事实，报告称机器人为“大规模（零售）破坏工具”。 。

多年来，犯罪分子一直使用僵尸网络来发动广告欺诈，将机器人而非真正的人眼发送到在线目的地。这会给广告客户造成数百万美元的损失，并为用户提供更差的网络浏览体验。74僵尸机器人也被用于其他以利润为导向的活动中，如购买流行商品或热门活动门票并放大规模。75

今年早些时候，甲骨文公司的安全专家发现了一项涉及DrainerBot的重大欺诈操作，该欺诈行为通过在数百种手机应用程序和游戏中使用的软件开发套件（SDK）传播。一旦被感染的应用程序安装在毫无戒心的用户手机上，每月将使用超过10 GB的数据（即使手机处于睡眠模式），并欺骗广告客户以为他们正在吸引人流量。76

在2019年，很难判断在线活动是否是人类活动。在过去，如果引起怀疑，识别非人类行为（如打开和关闭数百万个窗口）相对容易。77但是，恶意机器人行为越来越类似于真实的人类网络浏览，即使专家也无法分辨出差异。

社交僵尸网络传播虚假信息和非法链接。僵尸网络流量类似于普通的人类流量，其影响范围不仅包括欺骗零售商和广告客户。僵尸网络以各种不同的方式滥用社交媒体，从冒充数百万用户到促进访问受版权保护或非法分发的内容。

在去年的指南中，我们观察到僵尸网络可以在腐蚀性信息虚假信息传播中发挥作用，这可能会使公众失去做出明智决定的机会。模仿人类行为的机器人可能会通过伪造社会证据来影响人类在几乎任何主题上的观点，从音乐潮流到政治。78

对于僵尸网络传播版权内容的常见示例，我们可以考虑体育。 2018年12月，西班牙电信发布了一份趋势报告，内容涉及“ Twitter在体育赛事中的僵尸网络检测”。79这些僵尸机器人大规模散布与非法流媒体内容的链接，干扰权利持有者的利益。

减少利用社交媒体的僵尸网络绝非易事。在2019年9月，Twitter的透明度报告显示，该平台删除了数千个与国家支持的社交媒体活动明显联系的账户.80总共，该平台清除了数百万个虚假账户.81然而，僵尸网络正在不断学习，适应和发展僵尸网络。升级以逃避禁令，并继续侦察其运作。

僵尸机器人涌向矿山匿名加密货币。加密货币的崛起已成为僵尸网络活动的助推器。 2018年，网络威胁联盟发现加密矿恶意软件增长了459％82，有可能在2019年底之前面临同样令人震惊的数字。

僵尸网络采矿业务由利润驱动。因此，当门罗币在2019年夏季的加密货币价值翻了三倍时，僵尸网络活动显着增加.83一般来说，罪犯更喜欢匿名的门罗币和ZCash等加密货币，而不是比特币，后者更容易追踪.84

尽管受害者的受感染系统通常可以继续运行，但犯罪并非并非没有受害者。 85受害者可能会注意到性能下降和延迟时间增加，因为资源被转移到了为罪犯牟利的任务上。 商业运营可能会受到负面影响，受害者可能会注意到更高的能源费用。86

僵尸网络草坪大战迁移到云端。罪犯在争夺尽可能多的设备和系统的竞争中频频发生僵尸网络“草皮战争”。僵尸网络感染已经被其他僵尸网络感染的设备，并删除其竞争对手，以提高自身的力量和利润。

在2019年，洛克和帕斯查之间的竞争升级，加密采矿黑客团体在Linux云计算环境上争夺主导地位87.这两个团体都使用了不正确的云资源来推进加密采矿业务。同时，另一个加密采矿僵尸网络Smominru一直在从Windows 7计算机中删除竞争对手。88另外两个加密采矿僵尸机器人Fbot和Trinity则继续去年开始控制成千上万的非安全Android设备。89

随着删除其他机器人的机器人越来越普遍，而且利润stake可危，僵尸网络运营商面临巨大压力，要求其使用最新工具与竞争对手竞争，或者至少采取措施自卫。对于
例如，某些僵尸网络闯入设备后会主动修补安全漏洞，以防止竞争对手入侵。

对可以关闭其竞争对手的强大僵尸网络的需求已反映在黑暗网络上的犯罪市场上，导致强大的恶意软件（如Mylobot）泛滥成灾，可利用的工具数量空前。90

由于犯罪骇客担心竞争对手会过时，因此，他们还需要考虑“网络治安警察”对他们的运营造成的威胁。僵尸网络（如BrickerBot91和Hajime92）旨在清除恶意僵尸网络，
表面上提高安全性。
被感染的系统。尽管这些僵尸网络的意图并不是
恶意的，但还是要保持警惕。
但是，僵尸网络违反了许多国家/地区的法律。

Sometimes, criminals with advanced technical proficiency will rent botnets to supplement their already-existing armies — in these cases, one can think of the rented botnets as mercenaries.

IPv6安全和物联网的未来。 IPv6是由互联网工程任务组（IETF）93定义的互联网协议，其目的是随着时间的推移替换旧的IPv4协议。94随着全球互联网用户和连接设备数量的增长，网络越来越多地提供IPv6连接， 95，在许多情况下，IPv6和IPv4一起部署。

Akamai的互联网安全状况报告指出，“ [b]因为IPv6仍然被视为流量的一小部分，并不是许多安全工具的主要卖点。并非所有组织都认为值得监控IPv6空间，即使具备该功能也是如此。” 96

像Mirai这样的僵尸网络通过自动扫描IPv4地址空间获得新机器人，而易受攻击的设备通常会在连接互联网后的几分钟内被感染。97相比之下，由于规模庞大，扫描IPv6地址空间被认为异常困难.98尽管如此，多年来，专家一直警告说，IPv6协议中未发现的漏洞，再加上物联网的增长，可能会造成大规模僵尸网络攻击。99

目前至少有一个记录在案的IPv6分布式拒绝服务攻击案例，使用的是域名系统（DNS）放大技术代替僵尸网络。100虽然这不构成重大事件，但必须提出一个问题：IPv6是否会导致更多和更多次攻击？随着时间的推移，更大的分布式拒绝服务攻击？ IPv6僵尸网络攻击的兴起将带来独特的挑战，难以轻松解决。例如，数量惊人的IPv6地址（是IPv4的8,000倍）可能使攻击者无法应付旨在处理基于IPv4的威胁的安全系统的内存。101

结论。尽管行业在与僵尸网络的斗争中取得了切实进展，但威胁仍在继续发展和增长。在不久的将来，云可能会加剧对僵尸网络的全球安全担忧迁移和物联网增长-两者的发展都从根本上增加了恶意行为者可以针对的攻击面。为了应对这一迅速发展的威胁，我们需要在全球范围内开展基于市场的运动，以期在数字经济的所有细分领域提高安全性。同时，我们需要鼓励创新的政策，并允许行业像对手一样灵活，动态地发展。

04 /解决多样化互联网生态系统中的自动化分布式威胁

在高度多样化，复杂和相互依存的全球互联网生态系统中应对僵尸网络的基本挑战仍然是：互联网的基本性质是非分层且高度连接的。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经典的"公地悲剧"挑战：如果每个人都拥有互联网公有权益，但没有人控制，那么谁负责清理威胁每个人依赖的基本功能的恶意僵尸网络？

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。

缓解僵尸网络需要一种深思熟虑的整体方法。为了个人和集体的利益，这个复杂的生态系统的各个部分必须加深和加深对自身责任及其补充方式的理解。其他。并且，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解决方案的谬误。

Sometimes, criminals with advanced technical proficiency will rent botnets to supplement their already-existing armies — in these cases, one can think of the rented botnets as mercenaries.

莫名其妙-例如，互联网服务提供商（ISP）应仅关闭所有僵尸网络，或者使数十亿个设备具有普遍安全性，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《国际僵尸网络和IoT安全指南》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。我们根据分析结果制定了本指南

考虑到以下共识指导原则，迅速发展的全球威胁，生态系统范围的脆弱性以及日益强大和坚定的对手

- 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。

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。各种著名的政府和私人部门报告均使用类似但不同的分类法定义和描述了互联网和通信生态系统，这些分类法是根据每个论坛的目的和目标量身定制的。[102]相互补充和加强。

本指南也不例外。我们将生态系统的组成部分进行分组，以促进在其相关的利益相关方群体中识别和实施反僵尸网络实践。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. 物联网设备
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，并将ISP之间相互连接，使ISP可以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

并将相应的IP地址发送回用户浏览器，然后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供应商也可以跨入其他行业，如具有分布式拒绝服务保护的网络安全和网络应用防火墙（WAF）。 CDN旨在解决称为延迟的问题，延迟是指用户请求网页之间的延迟时间
直到其内容显示在屏幕上为止。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将附近的最终用户连接到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，云服务使用在线托管的远程服务器代替本地服务器或个人设备，为客户提供了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。由于云网络是分散式的，因此通常可以承受众多网络组件的破坏。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。由于云相对于攻击目标而言是ISP的上游，因此可以缓解距攻击源更近的问题。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，103，这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，已经证明某些基线实践可以减少僵尸网络驱动的攻击（如分布式拒绝服务）的影响。
攻击，应在整个生态系统中实施。104下面，我们确定基准实践以及行业领导者用来保护生态系统免受分布式威胁的更高级功能。

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。105

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。 106签名分析更明显的局限性在于，它需要恶意软件的先知，这意味着恶意软件可以像恶意软件一样在主机之间移动并适应。

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结合使用，例如下面讨论的启发式或行为分析，以克服这种技术的固有局限性107。

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，科学家存储了
他们认为是虚拟机内部称为“沙盒”的可疑代码，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。[108]

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，有已知的迹象表明某个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时，就可能是恶意软件。通常，行为分析类似于医学专业：
在知道确切问题出在哪儿之前，医生通常可以分辨出某人何时生病。行为分析通过发现尚未发现的未知威胁，因此没有已知特征，补充其他类型的分析[109]。

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。

†*“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。*

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活动，因此可用于执法行动。

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。

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，使恶意流量似乎来自其实际来源地以外的其他地方。110通过过滤恶意流量进入提供商网络时（例如入口过滤，BCP38）和BCP84），111提供商可能会降低欺骗的有效性，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。112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。互联网服务提供商等提供商为客户端分配了许多IP地址，客户端又可以运行自己的过滤功能，还需要遵循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。113

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。114在某些情况下，可以配置ACL来考虑单个用户的访问权限，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保护，并使供应商与生态系统中的其他组织负责任。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115。

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目的地来清理流量。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。116宿醉攻击通常通过策略路由或其他路由方法完成，将路由僵尸网络中组成僵尸网络的恶意软件捕获在水池中，执法部门和研究人员。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。由于清理与其他解决方案相比是资源密集型，因此一些大型提供商将清理作为商业服务提供。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117。

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委托开展的一项研究发现，电话和邮政是与用户联系的最有效方法。118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。119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。导致对恶意软件造成现实后果的执法行动actors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。大规模的域名扣押也可能需要国际社会的共同努力。120例如，2016年，服务提供商与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中的800,000多个域名生态系统121

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，物联网设备，系统安装程序和企业）中重点介绍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，推动着软件创新和改进。因此，本节并不试图捕获与之相关的各种基准安全实践和高级功能。致力于生态系统各个部分的专业软件开发。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，SAFECode（代码卓越软件保障论坛），致力于致力于 促进软件保证，发布安全软件开发培训资源免费提供给公众，包括安全软件开发基本实践122。

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，无法在特定用例的情况下轻松破解。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某些类型的服务正常运行的需求。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。拥有产品和应用程序中使用了哪些组件的清单，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。123

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

上述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。124然而，政府与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。125

基准实践：向购买软件的公司提供安全态势证明。

高级功能：为那些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. 物联网设备

2020年版的《指南》受益于CSDE托管的一个相关项目，即《 C2 IoT设备安全基线能力共识》 126。 CSDE召集了二十个主要的标准机构，技术联盟和公民社会团体，以利用这些组织广泛的网络安全专业知识。推荐功能的C2共识白皮书于2019年9月发布。

在2020年更新的指南中，CSDE重申了2018年指南的做法，但对材料进行了重组，并重新制定了指南，以符合C2共识和其他行业工作。根据C2共识的结果（事件记录和设备意图文档），在2018年指南中添加了另外两种做法。

IoT设备的基线实践和高级功能

1. 安全发展

安全必须从需求规划开始一直贯穿到开发流程中，一直持续到认证和发布。127本节列出了一些开发实践，这些实践对物联网设备安全至关重要，但在组织外部通常无法观察到。

a. 安全开发生命周期流程

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128。

基准实践：应建立安全的开发生命周期（SDL）流程。

尽管SDL的特定元素可能有所不同，但SDL应包括以下面向安全的元素：威胁识别和处置；编码标准；第三方软件要求；软件安全控制和能力测试与验证；以及新的漏洞识别和处理。

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" 129）的一部分。 BSIMM材料是开源的，可以成为这项工作的资源。

b. 以安全为重点的工具链使用

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搜索已知的常见漏洞和暴露（CVE）的子集的工具开发，编译，构建和维护软件。还应该使用内存安全语言。

高级功能：应使用测试技术（如模糊测试，符号执行，沙箱测试，静态分析和动态分析）补充以安全为中心的工具链，在开发过程中查找漏洞。

2. 安全功能

本节列出了设备功能，这些功能通常是设备在出厂和安装后可观察的属性。在某些系统架构中，这些重要的设备属性可能不在设备本身中，而在作为整体结构一部分的网关或集线器中找到。当设备使用特定的有线或无线技术时，将需要集线器或网关连接到通用互联网。以下属性有时可能位于集线器或网关上，而不是位于设备上，并且仍然完全有效，因为除通过集线器或网关之外，无法访问设备。

a. 设备标识符

设备的身份在整个生命周期中都发挥着作用。标识符用于将设备加载到网络，注册，认证，授权，分配访问列表和策略，控制和管理设备在服务和应用程序中的性能。标识符还可以帮助您了解设备或网络受到威胁后发生的情况。

基准实践：设备应具有与之关联的唯一值，该唯一值必须与设备和所有其他设备区分开。

高级功能：应通过其他用于机密性，完整性和可用性的加密保护来增强设备标识符的安全性。

b. 安全访问

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。

基准实践：必须通过要求用户身份验证来读取或修改软件，固件和配置的设备，包括为确保用于管理访问的设备唯一凭据的手段，以及通过保护接口访问，对设备进行仔细保护。

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：应考虑多因素身份验证用户访问控制。

c. 数据受到保护

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；另请参见关于密码术的讨论以及关于硬件根安全性的讨论。

基准实践：应保护静态数据和传输数据的机密性和完整性。为此，除非风险分析另有说明，否则应加密数据通信。敏感数据应加密存储。

通常，无论使用哪种系统，都应采用可用的安全机制保护静态数据和传输数据。

高级功能：应仔细选择协议和安全机制的最新版本；请注意，规范的最新版本可能不会过时的版本。应使用负责维护相关规范（协议或安全机制）的组织确定版本适用性。

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130。

d. 行业接受的协议

好的加密技术很难。经过专家审查和测试的密码技术成功的可能性更大。业界接受的协议已经通过了这一过程，并具有嵌入式专家经验。

基线实践：使用安全的，广泛使用的协议（不推荐使用和替换的版本和协议）与设备之间进行通信。

高级功能：可以使用安全内存代替存储信息的加密。

应使用与NIST FIPS 140-2或ISO / IEC 24759相称或等效的加密密钥方法131。

e. 数据验证

可以设计外部因素可以提供的数据，包括基本字母数字字符以外的特殊字符。诸如“。”，“ \”，“%”和“ :”之类的字符可能会产生开发人员意想不到的后果。恶意数据字符串是许多攻击的一部分。

基准实践：必须管理从系统外部接收的任何输入，以使外部对手无法安排将其直接用作代码，命令或其他执行流输入。应验证输入的长度，字符类型以及可接受的值或范围。从一个子系统到另一个子系统或到另一个站点的输出也应该过滤。

高级功能：设备内部每个处理阶段的输入端都会对输入的设备外部源数据进行内部验证，并在输出端对其进行规范化。

f. 事件记录

日志记录对于法庭分析和实时了解系统故障至关重要。当出现问题时，了解导致失败的事件链和受影响的设备非常重要。希望登录到外部系统，但并不总是可行的。

基准实践：应记录相关的网络安全事件（取决于可用内存空间），保护安全性并提供给授权用户。相关事件是特定于应用程序的，但示例包括登录尝试失败或网络安全检查（如启动时间测量或哈希验证）带来的负面结果。

g. 密码学

基线实践：在使用加密方法确保数据完整性和机密性，权限验证和请求不可否认性的情况下，应选择与评估风险相匹配的方法。实现应使用开放，公开，经过验证和同行评审的加密方法，以及适当的参数，算法和选项选择。

在可行的情况下，加密方法应可更新。应避免使用不建议使用的方法。

应考虑以硬件为基础的安全性如何适应当前和未来产品的安全开发生命周期。

设备制造商不应仅依靠混淆来保护机密（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：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。在技术上可行的情况下，利用基于硬件的安全性。

关于信任根，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。

h. 可修补性

从技术和可行性的角度来看，这种能力可能非常困难。但是，从制造到使用寿命结束，任何产品都不能视为绝对安全。在设备脱机或退役之前，可能需要更新才能应对新发现的漏洞。工业界正在提供解决方案：一些公司提供包括远程软件更新在内的IoT“平台”。

基准实践：具有防回滚保护和适当访问控制的安全更新计划
在技术上可行的整个定义的安全支持期内。132

i. 重新配置

能够将设备还原为已知的良好“空白”状态，以便在易手时从设备中删除敏感数据，例如出售智能家居设备用房屋或回收各种设备。

基准实践：制造商为授权用户提供在售后安全地重新配置和重新部署设备的能力，尤其是将产品恢复为出厂默认设置或授权的还原点，并安全删除设备收集的数据（对于其
运营），在组织确定的规定期限内。

j. 设备意图信令

出于与设备意图文档类似的原因（请参阅下文），可以通过制造商使用描述符（MUD）等协议大幅减少僵尸网络的传播。133其他工具包括OMA-DM134和TR-69135（后两种情况适用）可以直接管理设备的安全要求，包括开放连接论坛安全配置文件（黑色，蓝色和紫色），以及建议，如IoTSense.136

高级功能：设备支持对设备进行身份验证和授权的过程
凭证，并将其配置为在适当的安全域内通信。

k. 设备网络入职

如果设备可以访问网络，则应授权该访问。家庭和企业环境中未经授权的设备会造成网络安全漏洞。安全且定义明确的入职流程减少了将设备连接到网络带来的不便，并使设备可以在授权下参与。

高级功能：设备支持设备向上游路由器或防火墙提供有关预期网络使用情况的信息的协议。同样，该设备在正常运行时提供与其自身行为有关的启发式技术，以支持网络分析。

3. 产品生命周期管理

产品生命周期管理（PLM）是指从构思到设计，制造，支持和寿命终止，积极管理产品。

a. 漏洞处理

漏洞发生。组织应该有积极的流程来寻找它们，例如内部努力，威胁共享和对外公开（道德）公开。

基准实践：提供商（制造商和零售商）应创建安全漏洞策略和流程，识别，确定优先级，缓解并在适当情况下披露其产品中的已知安全漏洞。

b. EoL / EoS更新和披露

在组织内部必须仔细考虑此功能。它与漏洞处理，产品生命周期，服务条款等相关。

基线实践：设备提供商应有定义的安全支持策略，包括处理任何寿命终止（EoL）或服务终止（EoS）安全漏洞，是否提供更新，以及更新方式和内容当时与设备有关。

c. 设备意图文档

当确定设备是否受到威胁（包括进入僵尸网络）时，设备的设计和预期网络使用情况（端口，协议，访问站点，预期数据流量级别，与其他设备的通信）是重要信息。

基准实践：设备制造商以产品文档或其他方式向设备用户公开提供设备设计网络使用情况的文档。

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。娱乐类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。此生命周期包括安装和配置
设备。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。

以下材料主要来自互联家庭安全系统。137

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）应具有最新的防病毒和防
已安装并正在运行恶意软件工具。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. 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。 “不可发现”选项应
在可用的地方使用。蓝牙低功耗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
容易篡改。

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WPA2或WPA3（最新版本）。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。138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。举例来说，大型企业通常拥有首席信息官和首席信息安全官，各自负责确保组织的网络系统和设备（包括任何物联网系统）的安全。小型企业可能没有资源专门为IT和信息安全人员提供服务，而是依赖现成的解决方案。

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。也许与本指南最相关的是网络安全联盟在网络安全框架下努力开发和推进分布式拒绝服务配置文件和僵尸网络预防和缓解配置文件139，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。这样的步骤可能会有所帮助
企业通过减少分布式拒绝服务和其他分布式攻击的攻击面，帮助保护整个生态系统，并保护网络上的敏感数据和知识产权。

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多。140

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。

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，这些努力已显着改善，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。141

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，
以及来自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/自动化工作结合使用。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。142以安全为明确目标的网络架构可以补充其他预防措施，如反-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，并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提供对企业数据的访问开发人员，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。企业应该购买适合其风险状况的商业分布式拒绝服务保护，而不是忽略僵尸网络和其他分布式攻击可能构成的威胁。143商业服务可能包括场外保护或场外和场内保护的组合，功能更强大保护企业免受分布式攻击。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。144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维持合理的安全水平。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开启响应的商业提供商。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，如IT管理员，CISO和其他个人具有增强的系统访问权限。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。145

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。146

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-在变更时发生的一组操作，用于促进连接/移动/离开过程以及不同连接资源之间变更事件的协调；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因素身份验证（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（逐步认证）。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。**

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传统产品。147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，近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所占百分比通常会超过70%。148当然，制造商通常不会修补盗版软件，这意味着仍然容易受到已知攻击。149企业应避免使用盗版软件，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。150

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2020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主导战略运动的延续。 CSDE，USTelecom和CTA敦促利益相关方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。

如导言所述，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，我们计划每年继续更新，发布和推广本指南的新版本，以反映将帮助我们的公司和全球其他公司推动可观测和可衡量的安全性的最新动态和技术突破。改进-不仅在自己的网络和系统内部，而且在整个更广泛的生态系统中。

例如，尽管今年打击僵尸网络努力的标志是物联网设备安全，但基于迫切需要一个被广泛接受的基准，但并非所有重要僵尸网络都以连接设备为目标-实际上，世界上最具破坏性的僵尸网络并不以连接设备为目标连接的设备。因此，尽管很明显，僵尸网络的未来与物联网安全的未来紧密相连，而且CSDE将继续在这方面保持领先地位，但我们还将探索通过我们的方式大幅减少僵尸网络和其他分布式威胁的其他方式成员的领导。认识到僵尸网络威胁的复杂性和层次性后，CSDE中的公司将在多个方面应对这些威胁。

更直接的是，在接下来的几个月中，我们的下一步工作是与互联网和通信生态系统中的众多国内外利益攸关方进行接触，这些利益攸关方既可以推广建议的做法，又可以进行建设性参与。这些不同的利益相关者承担的共同责任是确保数字经济未来的关键。

CSDE
Council to Secure the Digital Economy

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和消费者技术协会（CTA）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。

关于消费者技术协会

消费者技术协会（CTA）™是代表3,770亿美元美国消费者技术产业的贸易协会，为1500万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会员资格的好处包括政策宣传，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 Nat'l Inst。标准和技术研究院，NISTIR 8259（草案），安全物联网设备的核心网络安全功能基线：物联网设备制造商的起点（2019年7月），https：//csrc.nist.gov/publications/detail/nistir/8259 / 草稿。

2 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。

3 同时设置IoT生态系统中所有软件类型的需求不切实际。 IoT设备，企业和基础设施有特定要求。本节适用于《指南》其他部分未涵盖的领域

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。这些系统可由家庭和企业用户自行安装，或由专业人员安装：集成商，警报承包商和
其他。理想情况下，进入家庭，办公室，零售，医疗或工业环境的每个设备系统都应通过设备整个生命周期中的最佳实践进行保护，包括实现已制造设备"最佳安全性"的设备安装和配置。产品。

5 消费者技术协会，互联家庭安全系统，https：// Division / Device-Security-Checklist.aspx（最新访问，2018年10月10日）。www.cta.tech/Membership/Member-Groups/Smart-Home-

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），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扮演着至关重要的角色。
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，但其庞大的系统也可以
劫持以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，同时还可以通过减少僵尸网络的攻击面来保护整个生态系统。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，就各种规模的企业而言，该市场"需求"端的需求不断发展。
服务将为这些服务带来进一步的创新，完善和成本效益。

7 安德鲁·谢伊（Andrew Sheehy），《 GDP无法解释数字经济》，福布斯（2016年6月6日），https：// gdp-cannot-explain-the-digital-economy / # 47c4db1218db。www.forbes.com/sites/andrewsheehy/2016/06/06/

8 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。

9 保罗·滕纳纳（Paul Tentena），《到2025年将数字经济翻倍至23万亿美元的人工智能》，东非商业周刊（2018年5月30日），https：//busiweek.com/artificial-intelligence-to-double-digital-economy-to-23-2025亿亿/www.

10 *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专注于加密货币挖矿运营一直是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-

11 山姆·蒂尔曼和克里斯·约翰斯顿，《重大网络攻击破坏了整个欧美互联网服务》，《卫报》，（2016年10月21日），https：// internet-denial-service。
www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-

12 CNBC研究称，迈克尔·纽伯格（Michael Newberg）多达4800万个推特帐户不是人，2017年3月10日，https：//www.cnbc。
com / 2017/03/10 / nearly-48m twitter-accounts-co-be-bots-says-study.html。

13 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：//themerkle.com/top-4-largest-botnets-to-date/

14 丹尼尔·纽曼（Daniel Newman），《福布斯》（Forbes）公布的2018年IoT八大趋势（2017年12月19日），https：// w/ww.forbes.com/sites/danielnewman/2017/12/19/the-top-8-iot-trends-for-2018 / # 48d7f78e67f7252309686 7f7（引用了《 HIS Markit IoT Trend Watch 2018》，网址为https://ihsmarkit.com/industry/telecommunications.html）；另请参阅Gartner，Gartner说，2017年将使用84亿个互联"物联网"，比2016年增长31％（2017年2月7日），https：// 07-gartner-says-8-billion-connected-things-将在2017年使用中，比2016年增长31％。
www.gartner.com/en/newsroom/press-releases/2017-02-

15 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_

16 比尔·康纳（Bill Connor），勒索软件即服务：下一次网络威胁？，福布斯（2017年3月17日），https：// forbestechcouncil / 2017/03/17 / ransomware-as-a-service-the-next -伟大-网络威胁/ # 14a38e5b4123。www.forbes.com/sites/

17 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://wired.com/story/white-house-russia-notpetya-attribution/ ；

俄罗斯达米安·沙尔科夫（Damien Sharkov）被控12亿NoPetya网络攻击，新闻周刊（2018年2月15日）https：//billion-cyber-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：//www.cbsnews。 com / news /从毁灭性notpetya网络攻击中学到的经验教训-有线调查（讨论NotPetya恶意软件如何造成超过100亿美元的损失）www.www.newsweek.com/russia-accused-massive-12-

18 Alex Zaharov-Reutt，网络犯罪，数据泄露给企业造成了8万亿美元的损失，到2022年，ITWire（2017年4月25日），https：//c/www.itwire.om/安全/ 77782- 8万亿美元的网络犯罪和数据泄露业务成本至2022.html。

19 通信委员会第二部分，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，第四版（2015年3月），网址：https：//transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf（承认“非监管方法相对于规定性和静态合规性制度的优势”）。

20 Nat’l Inst。标准和技术研究院，NISTIR 8259（草案），安全物联网设备的核心网络安全功能基线：物联网设备制造商的起点（2019年7月），https：//csrc.nist.gov/publications/detail/nistir/8259 /草稿。

21 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：//。发现者在Twitter上发布僵尸网络僵尸网络（“研究人员发现了一个巨大的僵尸网络，模仿Twitter上的合法账户，传播加密货币“赠予”诈骗。）。/wwwcoindesk.com/researchers-

22 查尔斯·德贝克（Charles DeBeck），约书亚·钟（Joshua Chung）和戴夫·麦克米伦（Dave McMillen），《我不能相信Mirais：跟踪臭名昭著的IoT恶意软件》，SecurityIntelligence（2019年7月18日），https：//securityintelligence.com/posts/i-cant-believe-mirais-tracking-臭名昭著的iot-malware-2 /。

23 查尔斯·德贝克（Charles DeBeck），约书亚·钟（Joshua Chung）和戴夫·麦克米伦（Dave McMillen），《我不能相信Mirais：跟踪臭名昭著的IoT恶意软件》，SecurityIntelligence（2019年7月18日），https：//securityintelligence.com/posts/i-cant-believe-mirais-tracking-臭名昭著的iot-malware-2 /。

24 马克·梅恩（Mark Mayne），《新Mirai变种》以11种新漏洞利用的目标企业，SC Media（2019年3月19日），https：// ctargets-enterprises-11-new-exploits / article / 1579535 。 /www.smagazineuk.com/new-mirai-variant-

25 *参见SentinelOne，Mirai僵尸网络后裔将导致更大的互联网中断，CSO（2016年12月22日），https：//。 article / 3153031 / mirai-botnet-descendants-will-lead-even-bigger-internet-outages.html。*/wwwcsoonline.com/

26 拉里·卡斯多拉尔（Larry Cashdollar），《最新回声机器人》：26种感染媒介，Akamai（2019年6月13日，上午11:17），https：//blogs.akamai.com/sitr/2019/06/latest-echobot-26-infection-vectors.html 。

27 查尔斯·德贝克（Charles DeBeck），约书亚·钟（Joshua Chung）和戴夫·麦克米伦（Dave McMillen），《我不能相信Mirais：跟踪臭名昭著的IoT恶意软件》，SecurityIntelligence（2019年7月18日），https：//securityintelligence.com/posts/i-cant-believe-mirais-tracking-臭名昭著的iot-malware-2 /。

28 *《2019年威胁报告》，CenturyLink 5-7，https：//。资产/ 业务/ 企业/ 报告/2019-threat-research-report.pdf（最新访问2019年10月8日）。*/wwwcenturylink.com/

29 *《2019年威胁报告》，CenturyLink 5-7，https：//。资产/ 业务/ 企业/ 报告/2019-threat-research-report.pdf（最新访问2019年10月8日）。*/wwwcenturylink.com/

30 *《2019年威胁报告》，CenturyLink 16，https：/。资产/ 业务/ 企业/ 报告/2019-threat-research-report.pdf（最新访问2019年10月8日）。*/wwwcenturylink.com/

31 查尔斯·德贝克（Charles DeBeck），约书亚·钟（Joshua Chung）和戴夫·麦克米伦（Dave McMillen），《我不能相信Mirais：跟踪臭名昭著的IoT恶意软件》，SecurityIntelligence（2019年7月18日），https：//securityintelligence.com/posts/i-cant-believe-mirais-tracking-臭名昭著的iot-malware-2 /。

32 Warick Ashford，网络钓鱼对企业的最大安全威胁，《计算机周刊》（Computerweekly.com，2019年8月12日下午4:00），https：//www.computerweekly。 com / news / 252468231 /网络钓鱼最安全威胁到企业。

33 *事故分类模式和子集，Verizon，https：// enterprise。verizon.com/resources/reports/dbir/2019/incident-classification-patterns-subsets/（最新访问时间为2019年10月8日）。*

34 *TheMoon的新阶段，CenturyLink（2019年1月31日），https：// blog。 Centurylink.com/a-new-phase-of-themoon/。*

35 Sergiu Gatlan，面向新处理器和架构的Mirai僵尸网络变体，BleepingComputer，（2019年4月9日，上午8:40），https：//。 bleepingcomputer.com/news/security/mirai-botnet-variants-targeting-new-processors-and-architectures/。 /www

36 肖恩·加拉格尔（Sean Gallagher），检测到Mirai僵尸网络的新变种，目标是更多的物联网设备，Ars Technica（2019年4月9日，下午1:49），https：//arstechnica.com/information-technology/2019/04/new-variants- mirai僵尸网络检测到的目标是更多iot设备/。

37 查尔斯·德贝克（Charles DeBeck），约书亚·钟（Joshua Chung）和戴夫·麦克米伦（Dave McMillen），《我不能相信Mirais：跟踪臭名昭著的IoT恶意软件》，SecurityIntelligence（2019年7月18日），https：//securityintelligence.com/posts/i-cant-believe-mirais-tracking-臭名昭著的iot-malware-2 /。

38 Derek Manky，不断演变的威胁格局- Swarmbots，Hivenets，恶意软件自动化，CSO（2018年8月29日，上午9:00），https：// csoonline.com/article/3301148/the-evolving-threat-landscape-swarmbots-hivenets-automation-in-malware.html。/www

39 Derek Manky，“蜂巢网络”的兴起：为自己思考的僵尸网络，DarkReading（2018年2月16日，上午10:30），https：//。漏洞-认为自己的威胁/蜂巢式僵尸网络崛起/ a / d-id / 1331062。/wwwdarkreading.com/

40 Derek Manky，“蜂巢网络”的兴起：为自己思考的僵尸网络，DarkReading（2018年2月16日，上午10:30），https：//。漏洞-认为自己的威胁/蜂巢式僵尸网络崛起/ a / d-id / 1331062。/wwwdarkreading.com/

41 Derek Manky，不断演变的威胁格局- Swarmbots，Hivenets，恶意软件自动化，CSO（2018年8月29日，上午9:00），https：// csoonline.com/article/3301148/the-evolving-threat-landscape-swarmbots-hivenets-automation-in-malware.html。/www

42 Derek Manky，不断演变的威胁格局- Swarmbots，Hivenets，恶意软件自动化，CSO（2018年8月29日，上午9:00），https：// csoonline.com/article/3301148/the-evolving-threat-landscape-swarmbots-hivenets-automation-in-malware.html。/www

43 Emotet的Colin Grady，William Largent和Jaeson Schultz，Emotet在暑假结束后又回来了，思科塔洛斯情报集团（Cisco Talos Intelligence Group，2019年9月17日），https：// blogs。cisco.com/security/talos/emotet-在夏季休息后返回。

44 丹·古丁（Dan Goodin），全球最具破坏力的僵尸网络返回，带有密码被盗和拖曳电子邮件，Ars Technica（2019年9月19日，下午2:45），https：//arstechnica.com/information-technology/2019/09/worlds-most破坏性僵尸网络返回包含被盗密码和电子邮件拖曳/。

45 *分析NTT TrickBot背后的僵尸网络基础设施和威胁行为者（2019年3月28日），https：//technical.nttsecurity.com/post/102fhgo/analytics-the-botnet-infrastructure-and-threat-actors-behind-trickbot* 。

46 丹·古丁（Dan Goodin），全球最具破坏力的僵尸网络返回，带有密码被盗和拖曳电子邮件，Ars Technica（2019年9月19日，下午2:45），https：//arstechnica.com/information-technology/2019/09/worlds-most破坏性僵尸网络返回包含被盗密码和电子邮件拖曳/。

47 Emotet的Colin Grady，William Largent和Jaeson Schultz，Emotet在暑假结束后又回来了，思科塔洛斯情报集团（Cisco Talos Intelligence Group，2019年9月17日），https：// blog。

48 Emotet的Colin Grady，William Largent和Jaeson Schultz，Emotet在暑假结束后又回来了，思科塔洛斯情报集团（Cisco Talos Intelligence Group，2019年9月17日），https：// blog。talosintelligence.com/2019/09/emotet-is-back-after-summer-break.html。

49 丹·古丁（Dan Goodin），全球最具破坏力的僵尸网络返回，带有密码被盗和拖曳电子邮件，Ars Technica（2019年9月19日，下午2:45），https：//arstechnica.com/information-technology/2019/09/worlds-most -破坏性僵尸网络返回包含被盗密码和电子邮件拖曳/。

50 Emotet，当今最危险的僵尸网络Catalin Cimpanu，复活，ZDNet（2019年9月16日），https：// todays-most-dangerous-botnet-comes-back-to-life /。www.zdnet.com/article/emotet-

51 Catalin Cimpanu，Necurs和Gamut僵尸网络占互联网垃圾邮件的97%，BleepingComputer（2018年3月12日，上午5:20），https：// botnets-account-for-97-percent-of-internets -spam-emails /。www.bleepingcomputer.com/news/security/necurs-and-gamut-

52 *电子邮件：小心谨慎地单击，思科31，https：// w cn / us / products / collateral / security / email-security / email-threat-report.pdf*/ww.cisco.com/c/dam/

53 *《 2019 年威胁报告》， CenturyLink 19， https：//asset/business/enterprise/report/2019-threat-research-report.pdf （最新访问时间：2019年10月8日）*。www.centurylink.com/

54 克里斯·宾（Chris Bing），您现在可以在黑暗网络上购买Mirai供电的僵尸网络，CyberScoop（2016年10月27日），https：// botnet-for-sale-ddos-dark-web。www.cyberscoop.com/mirai-

55 德里克·曼基（Derek Manky），《不断演变的威胁格局》 —— Swarmbots，Hivenets，恶意软件自动化，CSO（2018年8月29日，上午9:00），https：//swarmbots-hivenets-automation-in-malware.html。www.csoonline.com/article/3301148/the-evolving-threat-landscape-

56 利比里亚互联网服务提供商Catalin Cimpanu起诉竞争对手，要求其雇用黑客攻击其网络ZDNet（2019年1月14日），https：// isp-sues-rival-for-hiring-hacker-to-attack-its-network。www.zdnet.com/article/liberian-

57 利比里亚互联网服务提供商Catalin Cimpanu起诉竞争对手，要求其雇用黑客攻击其网络ZDNet（2019年1月14日），https：// isp-sues-rival-for-hiring-hacker-to-attack-its-network。www.zdnet.com/article/liberian-

58 利比里亚互联网服务提供商Catalin Cimpanu起诉竞争对手，要求其雇用黑客攻击其网络ZDNet（2019年1月14日），https：// isp-sues-rival-for-hiring-hacker-to-attack-its-network。www.zdnet.com/article/liberian-

59 小柯蒂斯·富兰克林（Curtis Franklin Jr.），《新僵尸网络表明技术与犯罪文化的演变》，《黑暗阅读》（2019年2月4日，下午6:30），https：//www.darkreading。 com / attacks-breaches / new-botnet-shows-evolution-of-tech-and-criminal-culture / d / d-id / 1333792。

60 小柯蒂斯·富兰克林（Curtis Franklin Jr.），《新僵尸网络表明技术与犯罪文化的演变》，《黑暗阅读》（2019年2月4日，下午6:30），https：//www.darkreading。 com / attacks-breaches / new-botnet-shows-evolution-of-tech-and-criminal-culture / d / d-id / 1333792。

61 Akamai，《零售攻击和API流量》，互联网安全状况5，https：//w-internet/state-of-the-net-security-retail-attacks-and-api-traffic-report-2019.pdf（最新（2019年10月8日访问）/ww.akamai.com/us/en/multimedia/documents/state-of-

62 Akamai，零售攻击和API流量，互联网安全状况5，https：// w/ww.akamai.com/us/en/multimedia/documents/state-of-互联网/互联网安全状态-零售连接攻击和api-traffic-report-2019.pdf（最新访问时间：2019年10月8日）。

63 Akamai，《零售攻击和API流量》，互联网安全状况18，https：// w-internet / state-of-the-net-security-retail-attacks-and-api-traffic- report-2019.pdf于2019年10月8日访问）。/ww.akamai.com/us/en/multimedia/documents/state-of-

64 Jay CuteJ，僵尸机器人说是打败互联网2019年的其他趋势，TechRadar（2019年2月21日），https：//。打败2019年的互联网和其他趋势。/wwwtechradar.com/news/bots-try-to-

65 Akamai，分布式拒绝服务和应用程序攻击，互联网安全状况17，https：/ c internet / state-of-the-internet-security-ddos-and-application-attacks-2019.pdf（最后访问时间为2019年10月8日）。/www.akamai.om/us/en/multimedia/documents/state-of-the-

66 *"防弹"住宅网络的兴起，KrebsonSecurity（2019年8月19日），https：//krebsonsecurity.com/2019/08/the-rise-of-bulletproof-residential-networks。*

67 Akamai，分布式拒绝服务和应用程序攻击，互联网安全状况18，https：//c/internet/state-of-the-internet-security-ddos-and-application-attacks-2019.pdf（最新访问，2019年10月8日）。/www.akamai.om/us/en/multimedia/documents/state-of-the-

68 查理·奥斯本（Charlie Osborne），新Mirai僵尸网络潜伏在Tor网络中，处于监控之下，ZDNet（2019年8月1日），https：//。僵尸网络潜伏在雷达网络中，停留在雷达下。/www.zdnetcom/article/new-mirai-

69 Tara Seals，Necurs僵尸网络演变为隐藏在阴影下，具有新的负载，Threatpost（2019年3月1日，上午10:41），https：//threatpost.com/necurs-botnet-hide-payloads/142334。

70 将光投射在神经元阴影上，CenturyLink（2019年2月28日），https：//blog.centurylink.com/casting-light-on-the-necurs-shadow。

71 *将光投射在神经元阴影上，CenturyLink（2019年2月28日），https：//blog.centurylink.com/casting-light-on-the-necurs-shadow。*

72 *参见Akamai，《零售攻击和API流量》，互联网安全状态5，https：//互联网的状态/互联网安全状态-零售-攻击-api-流量报告-2019。pdf（最后访问时间为2019年10月8日）。*/www.akamai.om/us/en/multimedia/documents/state-

73 *"防弹"住宅网络的兴起，《安全克雷布斯》（2019年8月19日），https：//krebsonsecurity.com/2019/08/the-rise-of-bulletproof-residential-networks。*

74 甲骨文公司知情人士罗宾·库泽（Robin Kurzer）发现另一项影响安卓用户和移动广告客户的重大欺诈操作，Marketing Land（2019年2月20日，上午7:00），https：//marketingland.com/oracle-discovers-another-major-fraud-operation影响Android用户和移动广告商257322。

75 Conor Reynolds，僵尸网络攻击：从分布式拒绝服务到Hivenets和Sextoration，CBR（2019年8月29日），https：//。攻击改变剧院。/wwwcbronline.com/feature/botnet-

76 甲骨文公司知情人士罗宾·库泽（Robin Kurzer）发现另一项影响安卓用户和移动广告客户的重大欺诈操作，Marketing Land（2019年2月20日，上午7:00），https：//marketingland.com/oracle-discovers-another-major-fraud-operation影响Android用户和移动广告商257322。

77 杰夫·斯通（Jeff Stone），从分布式拒绝服务攻击到广告欺诈：更智能的机器人正在复制人类行为，CyberScoop（2018年12月10日），https：//。智能僵尸网络人类行为ddos和欺诈methbot。/wwwcyberscoop.com/

78 杰夫·斯通（Jeff Stone），从分布式拒绝服务攻击到广告欺诈：更智能的机器人正在复制人类行为，CyberScoop（2018年12月10日），https：//。智能僵尸网络人类行为ddos和欺诈methbot。/wwwcyberscoop.com/

79 *参见Telefonica，Etisalat&Singtel，体育赛事中*/wwwelevenpaths/wp-content/uploads/2018/12/twitter-botnets-detection-in-sports-events.pdf（最新访问时间：2019年10月8日）。

80 克里斯蒂娜·费舍尔（Christine Fisher），推特禁止成千上万个传播错误信息的国家支持帐户，Engadget（2019年9月20日），https：//www.engadget。com/2019/09/20/twitter-bans-states-backed-misinformation。

81 本·科林斯（Ben Collins）和肖尚娜·沃丁斯基（Shoshana Wodinsky）推特推倒了僵尸机器人网络，推动了亲沙特谈论失踪记者的话题，NBCNews（2018年10月18日，下午6:39），https：// c twitter-pulls-down-bot-network-推送专业沙特谈话n921871。/www.nbcnews.om/tech/tech-news/exclusive-

82 网络威胁联盟的杰西卡·里昂斯·哈德卡斯尔（Jessica Lyons Hardcastle）报告说，SDxCentral加密货币恶意软件激增459%（2018年9月21日，1：18 PM），https：//。sdxcentral.com/articles/news/cyber-threat-alliance-459-spike-cryptomining-恶意软件/2018/09。/www

83 ZDNet（2019年9月18日），https：//www.catalincimpanu.com.cn/Monero价值翻了三倍。文章/加密采矿恶意软件看到的夏季新生命成为单核价值三倍。/www.zdnetcom/

84 Michael Nadeau，什么是加密劫持？如何预防，检测和从中恢复，CSO（2019年8月2日，凌晨3:00），https：//。article/3253572/What-is-cryptojacking如何防止从it.html进行检测和恢复。/wwwcsoonline.com/

85 *非法加密货币采矿威胁，网络威胁联盟4，https：//CryptoMining-Whitepaper.pdf（最后访问时间为2019年10月8日）。*www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-

86 *非法加密货币采矿威胁，网络威胁联盟15，https：//。CryptoMining-Whitepaper.pdf（最新访问2019年10月8日）。*/wwwcyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-

87 Catalin Cimpanu，两个加密货币采矿组织正在就不安全的Linux服务器展开一场激烈的争夺战，ZDNet（2019年5月10日），https：//。文章/两个加密货币矿业集团在不安全的Linux服务器上争夺地盘之战。/www.zdnetcom/

88 Lucian Constantin，新攻击中揭示的最新Smominru僵尸网络授权令的秘密，CSO（2019年9月18日，上午6:00），https：//。article/3439400/secrets-of-latest-smominru-botnet-variant-revealed-in-new-attack.html。/wwwcsoonline.com/

89 Catalin Cimpanu，两个僵尸网络正在为数以千计的非安全Android设备ZDNet（2018年11月2日），https：//的控制权作斗争。文章/两个僵尸网络在争夺成千上万不安全的安卓设备的控制权。/www.zdnetcom/

90 塔拉海豹（Tara Seals），Mylobot僵尸网络以罕见的复杂性兴起，Threatpost（2018年6月20日，1：12 PM），https：//threatpost.com/mylobot-botnet-emerges-with-rare-level-of-complexity/132967。

91 Catalin Cimpanu，一个神秘的灰色帽子正在修补人们过时的MikroTik路由器，ZDNet（2018年10月12日），https：//。神秘的灰色帽子正在修补人民过时的mikrotik路由器。/www.zdnetcom/article/a-

92 马克·萨缪尔斯（Mark Samuels），维吉兰特·怀特·黑特黑客（Vigilante White-Hate Hacker）提高物联网设备安全性，SecurityIntelligence（2017年4月20日，下午1:31），https：//securityintelligence.com/news/vigilante-white-hat-hater-hacker-boosts-iot-device -安全性。

93 RFC 2460网络工作组，互联网协议，版本6（IPv6）规范，IEFT（1998年12月），https：//tools.ietf.org/html/rfc2460。

94 MarekŠimon＆Ladislav Huraj，《IPv4 / IPv6网络中的物联网分布式拒绝服务反射攻击研究》，SpringerLink，https：//link.springer。com / chapter / 10.1007 / 978-3-030-19807-7_12（最新访问时间：2019年10月10日）。

95 Erik Nygren，《世界IPv6发行六年：进入多数阶段》，Akamai（2018年6月6日，12：00 PM），https：//blogs.akamai。com / 2018/06 / six-years-since-world-ipv6-launch-entering-the-majority-phases.html。

96 Akamai，零售攻击和API流量，互联网安全状况4，https：//c/www.akamai.om/us/en/multimedia/documents/state-of-互联网/互联网安全状态-零售连接攻击和api-traffic-report-2019.pdf》（最新访问2019年10月10日）。

97 Kelly Hill，Netscout：IoT装置在开启一分钟内受到攻击，RCRWrielessNews（2019年8月6日），https：// internet-of-things / netscout-iot-devices-under-attack-within-minutes-of -出现。www.rcrwireless.com/20190806/

98 Martin Zeiser和Aleksandar Nikolich，通过UPnP进行IPv6分解，思科（2019年3月18日），https：//blog.talosintelligence.com/2019/03/ipv6-unmasking- via-upnp.html。

99 勒内·帕普（Rene Paap），IPv6和日益增长的分布式拒绝服务危险，DarkReading（2015年11月2日，上午10:30），https：//。 the-growing-ddos-danger / a / d-id / 1322942。/wwwdarkreading.com/attacks-breaches/ipv6-and-

100 Kieren McCarthy，这开始了："第一批IPv6拒绝服务攻击使IT机构注意到了，寄存器（2018年3月3日，上午9:30），https：//www.theregister。 co.uk/2018/03/03/ipv6_ddos/。

101 马克·梅恩（Mark Mayne），"第一个真实的本地IPv6分布式拒绝服务攻击在野外发现"，SCMedia（2018年2月28日），https：// c ipv6-ddos-attack-spotted-wild / article / 1473177。/www.smagazineuk.com/first-true-native-

102 美国商务部和美国国土安全部，致总统的报告，旨在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，NIST（2018年5月22日），网址为https://csrc.nist.gov/publications/detail/white/paper/2018/01/05/enhancing-resilience-against-botnets--report-to-the-President / 草稿;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/advice/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：//消毒和防御；国际电信联盟国际电联僵尸网络缓解工具套件（2008年1月），https：// u botnet.html。www.enisa.europa.eu/publications/botnets-measurement-detection-/www.itu.int/ITU-D/cyb/cybersecrity/projects/

103 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：//csrc.nist.gov/publications/detail/white-paper/2018/01/05/enhancing-resilience-against-botnets--report-to-the-the- President / draft

104 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。

105 *参见，例如美国DHS自动指标共享（AIS）系统，https：// t（上次访问时间为2018年10月17日）;英国，网络安全信息共享合作伙伴关系（CiSP），https：// s uk / section / keep-up-to-date / cisp（最新访问时间：2018年10月17日）；日本，网络清洁中心，https：//（最新访问时间：2018年10月17日）;新西兰CORTEX，https：// w information-assurance / cortex-faqs（最新访问时间：2018年10月17日）。*/www.us-cer.gov/ais /www.ncc.gov./wwwtelecom-isac.jp/ccc/en_index.html /ww.gcsb.govt.nz/our-work/

106 *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。*

107 Verizon，2012年《数据违规调查报告71》（2012年），https：//Data-Breach-Report-2012.pdf。www.wired.com/images_blogs/threatlevel/2012/03/Verizon-

108 *参见斯蒂芬·斯拉达里兹（Stephen Sladaritz），SANS研究所4关于启发式技术（2002年3月23日），网址：https：// w / advanced / 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）。*/ww.sans.org/reading-room/whitepapers/

109 *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*

110 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获取。/www.nit.gov/programs-projects/advanced-ddos-

111 Ferguson＆D. Senie，网络入口过滤：击败使用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。

112 *ID。*

113 *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：// a whitepapers / firewalls / egress-filtering-faq-1059*/www.sans.org/reding-room/

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

115 *参见思科，《警务和成形概述》（最新更新，2017年11月23日），https：//。配置/15-mt/qos-plcshp-15-mt-book/qos-plcshp-oview.html。*/wwwcisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/

116 *一般请参见，例如，盖斯·布鲁诺（Guy Bruneau），域名系统（Sinkhole），SANS研究所（2010年8月7日），https：//isc.sans.edu/forums/diary/DNS+Sinkhole+ISO+Version+20/21153/。*

117 *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/

118 *见佐治亚州技术研究人员，域名系统（DNS）变更补救研究，向M3AAWG第二十七届大会演讲，加利福尼亚州旧金山（2013年2月19日），网址：https：// w georgia-tech-study-reveals-best-way-tell -客户-"您已被装船"（最新访问时间：2018年10月17日）；另请参阅通信部门协调*/www.m3aag.org/news/independent-理事会，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，邮政邮件，文本消息，网络浏览器通知，围墙花园以及其他方法，如社交媒体），网址为https://docs.wixstatic.com/ ugd / 0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf。

119 *参见点击率。民主和技术，对NIST模型的评论，以向僵尸网络和相关恶意软件非法使用计算机的自愿通知消费者*（2011年11月14日）（对"切断或以其他方式干扰客户的互联网连接"强迫僵尸网络补救的做法表示关注），网址：https：// sdocuments / itl / CDT-Comments-on-BotNet-FRN-11-14-11.pdf;电气。前沿发现，关于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公司自愿通知的NIST模型评论，5（2011年11月14日）（解释未感染方如何隔离隔离感染互联网），网址为https：// s BotNet-FRN-11-14-11.pdf。/www.nit.gov/sites/default/files//www.nit.gov/sites/default/fil es/documents/itl/AT-Ts-Comments-to-

120 *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。

121 *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％20 at％20Scale％20 FINAL.pdf。*

122 *参见SAFECode，《安全软件开发基础实践》（2018年3月），https：//safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf。*

123 Arora等人，《软件供应商修补行为的实证分析：漏洞披露的影响》，卡内基梅隆大学（2006年1月）（分析大型供应商相对于其他供应商的诱因），可查阅https：//。/wwwheinz.cmu.edu/~rtelang/disclosure_jan_06.pdf.

124 *请参阅SAFECode，《软件保障评估原则》（2015年），网址为https://safecode.org/wp-content/uploads/2015/11/SAFECode_Principles_for_Software_Assurance_Assessment.pdf。*

125 Nat'l Inst。标准和技术研究院，NTIA软件组件透明度（2019年10月21日），https：//o/www.ntia.doc.gv/SoftwareTransparency

126 保护数字经济理事会，《C2 IoT设备安全基线功能共识》（2019年），https：//securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf。

127 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.

128 *参见微软，《安全开发生命周期是什么？》，https：//（最新访问2018年10月19日）。*www.microsoft.com/en-us/sdl/default.aspx

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

130 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（最新访问时间：2018年10月10日）。

145 Nat'l Inst。标准和技术，数字身份指南（2017年6月），网址为https://doi.org/10.6028/NIST.SP.800-63-3。

146 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。

147 *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）。*

148 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），https：//globalstudy.bsa。组织/ 2016 /。

149 *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"）。*

150 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 / Whitepaper-Cybersecurity-Risks-from-Non-Genuine-Software.pdf（"在世界许多地方，盗版/假冒/非正版软件的使用是一个严重的问题。网络风险的增长，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。"）

132 有关更新的讨论，请参见Nat'l Inst。标准与技术，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/

133 *制造商使用说明规范，IETF（2019年3月19日），https：//datatracker.ietf.org/doc/rfc8520/。*

134 *请参阅《OMA设备管理概述》（2018年4月20日），openmobilealliance.org / wp / overviews / dm_overview.html。*http://www.

135 *参见CPE WAN管理协议，宽带论坛（2018年3月），https：//。*/wwwbroadband-forum.org/download/TR-069.pdf.

136 Bruhadeshwar Bezawada等人，《IoTSense：IoT设备的行为指纹》，科罗拉多州立大学（2018年4月），https：//arxiv.org/pdf/1804.03852.pdf。

137 消费者技术协会，互联家庭安全系统，https：//cta.tech/Membership/Member-Groups/TechHome-Division/Device-Security-Checklist.aspx（最新访问2018年10月10日）。

138 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.

139 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

140 *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。"（2011年11月），请访问https://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf。*

141 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抗灾力研讨会的参与者的意见），网址为https://nvlpubs.nist.gov/nistpubs/ir/2017/ NIST.IR.8192.pdf。

142 斯科特·鲍文（Scott Bowen），Akamai，《设计防御》：如何利用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：//www.forbes。com / sites / akamai / 2017/09/14 / defense-by-design-how-to-penpen-ddos-resilient-networks / # 79144da56f8a。

143 *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：//。ddos / index.html（最后访问时间为2019年11月3日）；NTT，分布式拒绝服务保护服务，*/wwwbusiness.att.com/content/productbrochures/http://www.verizonenterprise.com/resources/ddos_shield_solutions_www.centurylink.com/asset/business/enterprise/brochure/ddos-mitigation./wwwelevenpaths.com/technology/anti-https：/。（上次访问日期为2018年5月14日）。/www.nttcom/en/services/network/gin/transit/ddos.html

144 *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）。*

有关保护数字经济理事会的更多信息，请访问：securingdigitaleconomy.org。 或有关此报告的信息，请联系：

Robert Mayer
Senior Vice President - Cybersecurity USTelecom
rmayer@ustelecom.org

Mike Bergman
Vice President - Technology & Standards Consumer Technology Association
mbergman@cta.tech

securedigitaleconomy.org