路线图

增强抵御僵尸网络的能力

十一月29，2018

目录

I. 背景资料

2017年5月11日，总统发布了第13800号行政命令，“加强联邦网络和关键基础设施的网络安全”，呼吁“抵御僵尸网络和其他自动化，分布式威胁。”总统指示商业和国土安全部部长“领导一个公开透明的过程，识别和促进适当的利益相关者采取行动”，目标是“大幅减少自动化和分布式攻击（僵尸网络）造成的威胁”。[1][2]

商务部和国土安全部共同努力，于2018年5月发布了《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抵御力的报告》，即僵尸网络报告。工业和政府，报告呼吁联邦政府明确划定行动重点。这份初始路线图列出了可大幅减少僵尸网络威胁和类似攻击的行动，符合国家网络战略规定的管理优先级。路线图确定了五项工作，每项工作都有一组任务和完成时间表。在此初始版本中，列出了85个任务，但随着一些任务的完成和新任务的产生，该数字会随着时间变化。[3][4]

正如僵尸网络报告所述，该报告的许多行动在设计上相互支持，甚至跨目标。一些行动已经在进行中，其他行动取决于外部因素，最后的决定有待领导和/或资金支持。由于资源限制或相关利益相关方社区的复杂程度不同，我们预计并非所有行动都会同时发生。值得注意的是，尽管这些行动在僵尸网络报告中已经确定，但实施这些行动将使整个互联网生态系统更加安全，其影响将远远超出报告本身的范围。

接下来的路线图列出了与五项努力相关的每项行动的任务：

1. 物联网；
2. 企业；
3. 互联网基础设施；
4. 技术开发和过渡；和
5. 意识和教育。

有些任务将由联邦政府直接负责，而另一些则专门针对私营部门。有些任务并不直接涉及联邦政府，但支持或支持依赖联邦参与或领导的行动。通过表明自己的优先事项，联邦政府可以增强利益相关者的信心，即投入资金用于由联邦政府主导的行业主导行动将产生丰硕成果。

---

1 执行订单号13800，美联储82。注册22,391，截至22,394（2017年5月11日），可用 https://www.federalregister.gov/d/2017-10004.

2 ID。

3 美国商务部和美国国土安全部，致总统的报告，《增强互联网和通信生态系统对僵尸网络和其他自动分布式威胁的抵御能力》（2018年5月），网址：https://www.commerce.gov/page/report-president-enhancing-resilience-against-botnets.

4 Nat’l Sec。理事会，《美国国家网络战略》（2018年9月），网址：https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

商务部和国土安全部继续欢迎希望为僵尸网络报告采取行动的私营部门成员的关注。许多路线图行动应由行业，学术界或民间社会牵头。在适用的情况下，本路线图确定了相关任务的现有私营部门领导人或治理结构。如果现有机构已经在采取相关行动，或者已经代表关键社区，则鼓励他们领导。政府有权召集和这样做，但要实现僵尸网络报告规定的结果，需要整个生态系统中的行业和公民社会参与。所识别的任务和相关信息应被视为非约束性和灵活的，以适应数字生态系统随时间的变化。

如果尚未确定由私营部门共同商定的一个或多个政党领导，则联邦政府将提供协调和沟通机制。联邦政府还将定期与有关各方举行会议，促进合作并分享调查结果。在下面的任务突破中被确定为“贡献者”的那些组织不完整地列出为解决方案做出贡献的当前努力。鼓励组织寻找在可行范围内合作的机会。美国政府重视创新，并期望市场为已确定的问题确定最快捷的解决方案。

除了联邦依赖性外，某些行动还具有自然的时间顺序。例如，行动5.1和5.2中的评估计划取决于行动1.1中适当的安全能力基准的建立，因此不能立即开始。其他优先事项的优先工作已经成熟，因为这项工作已经在进行中，例如行动2.2中描述的美国国家标准技术研究院（NIST）网络安全框架（CSF）概况。最后，由于准备周期长（例如，行动1.3、5.3和5.4）或事态发展正在缩小美国影响方向的窗口，因此某些行动具有特别紧迫性（行动1.2）。

最后，为跟踪进展，商务部和国土安全部将为总统制定365天的状态更新，路线图发布后一年。此更新将审查：1）整个社区根据路线图取得的进展；2）这些路线图活动的影响；3）重新评估自动分布式攻击的威胁，包括威胁是在增加还是在减少，以及任何已知的此类改变原因；4）来年应优先开展哪些活动。

II. 路线图

以下小节介绍了从僵尸网络报告中列出的24项行动中采取的五项努力中得出的任务：

1. 物联网；
2. 企业；
3. 互联网基础设施；
4. 技术开发和过渡；和
5. 意识和教育。

这五项工作本身可以细分为由任务组成的工作流。如果任务具有依赖性，则将任务进一步组织为一系列。每个任务描述都包含一个

简短摘要和对僵尸网络报告动作编号的引用，确定任务负责人（如果确定）和支持人员，确定必须开始或完成的任务，并按日历年季度提议开始和完成日期。商务部和国土安全部欢迎利益攸关方就路线图任务的所有方面提供反馈，特别是确定牵头行列和为确定的行动做出贡献的合作伙伴，以及时间表。

物联网工作流：提高物联网安全性标准

僵尸网络报告认识到互联设备对扩展针对生态系统目标的自动分布式攻击范围和规模的影响。物联网（IoT）的工作重点是通过建立适用于连接设备整个生命周期的基准安全标准，降低整个IoT生态系统的安全风险。

物联网工作流1：为可信赖的物联网设备开发稳健的市场

该工作流程侧重于为三个领域提供适当安全功能的设备的强劲市场开发：消费者/家庭用户，工业用户和联邦政府。基本初始任务描述了一组核心安全能力，广泛适用（理想情况下，适用于所有三个部门），并可由广泛的评估方案支持。定义核心后，将为三个部门中的每个部门启动并发系列任务。每一系列任务都定义了适用于该领域的核心基准的超集，其后是一系列旨在开发稳健产品一致性市场的支持活动。

定义核心安全能力基准

此任务将建立安全部署IoT设备所需的核心安全功能集，而不管预期的环境如何。通用开发平台应提供或促进核心安全功能，以限制对上市时间的影响并实现创新。这些基准能力还必须适用于基于证明和第三方评估的合格评定方案。

任务名称：定义核心安全能力基线
行动编号：1.1
任务摘要：比较/分析不同的基线文档，确定可以被全方位评估方案支持的广泛接受的和广泛适用的“核心安全能力”。至少，能力基准可以解决设备和数据安全问题。 NIST将以NIST白皮书或机构间报告（NISTIR）形式发布共识基准，以供将来任务参考和使用。
贡献者：NIST（负责人），基准所有者，开发人员套件供应商，消费者财团，数字经济安全理事会（CSDE）/消费者技术协会（CTA）前提任务：无[5]
预计开始时间：19年第一季
度预期完成时间：19年第三季度[6]

[5]参见安全挖掘委员会。经济，见https://securingdigitaleconomy.org/

[6]所有开始日期均为日历年估计，并取决于资源确定。

为可信赖的消费者/家庭IoT设备建立稳健的市场

以下任务旨在为具有高产品可用性和强大客户识别度的消费者/家庭IoT产品建立广泛采用的安全能力基准。这些任务首先通过针对消费者/家庭物联网市场的特定要求增强核心安全能力基线。为鼓励开发和部署兼容设备，将创建认证或评估方案以及教育和意识工具，帮助客户做出明智的物联网购买选择。

任务名称：开发消费者/家庭物联网安全基线
行动编号：1.1
任务摘要：以核心能力为基础，确定适用于消费者/家庭物联网的安全基准。
贡献者：物联网行业，公民社会，NIST，CSDE / CTA前提任务：
发布核心安全能力基线预期开始时间：2016年第二季度
预期竣工时间：2020年第一季度

任务名称：为消费者/家庭IoT设备建立或支持评估计划
动作编号：5.1
任务摘要：为满足上述基准的消费者/家用物联网设备建立或支持敏捷评估或证明计划。
贡献者：行业，公民社会，CTIA，NIST，其他美国政府（USG）利益相关者，CSDE / CTA
前提任务：制定消费者/家庭物联网安全基线预期开始：进行中
预期竣工时间：2020年第二季度

任务名称：探索消费者/家庭物联网标签
动作编号：5.1
任务摘要：探索自愿性标签方法或其他信息选项的效用，以提高消费者/家庭IoT设备消费者的意识。
贡献者：联邦贸易委员会（FTC），NTIA，其他联邦合作伙伴，物联网行业，零售商，民间社会，学术界，CSDE / CTA
必备任务：N / A
预计开始时间：19年第三季度
预期完成时间：20年第二季度

任务名称：为可信赖的消费者/家庭物联网设备实施意识战略
动作编号：5.1
任务摘要：开发信息工具，如标签或品牌，以帮助有动机的消费者识别符合标准的消费者/家庭IoT产品。
投稿人：物联网行业，零售商，CSDE / CTA
前提任务：建立消费者/家庭IoT设备评估计划；探索消费者/家庭物联网的标签
预计开始时间：20年第二季
度预期完成时间：21年第二季度

任务名称：联邦消费者/家庭物联网安全基线和评估支持

操作编号：5.5
任务摘要：加强美国政府与目标用户社区和民间社会的互动，促进消费者/家庭IoT安全基线和支持评估计划的认识和接受；利用DHS现有的认知活动，如STOP.THINK.CONNECT。
贡献者：国土安全部，商业，FTC，民间社会
前提任务：制定消费者/家庭IoT安全基线；建立家庭物联网设备评估计划。
预计开始时间：20年第二季
度预期完成时间：23年第一季度

为可信赖的工业物联网设备建立稳健的市场

以下任务旨在为具有高产品可用性和强大客户认可度的工业物联网产品建立广泛采用的安全能力基准。这些任务首先通过针对工业物联网市场的特定要求扩展核心安全能力基线。为鼓励开发和部署兼容设备，创建了一个或多个评估方案以及教育和意识工具，以告知客户。

任务名称：开发工业物联网安全基准
行动编号：1.1
任务摘要：以核心能力为基础，确定适用于工业/ SCADA环境的安全基准。
贡献者：工业物联网行业，国家实验室，国土安全部，行业特定机构，行业协调委员会（例如，能源，健康，运输）
前提任务：发布核心安全能力基线预计开始时间：2016年第二
季度
预期完成时间：19年第四季度

任务名称：建立工业物联网设备评估计划
行动编号：5.2
任务摘要：为满足基线要求的工业物联网设备建立具有成本效益的评估计划。
贡献者：工业物联网行业，国家实验室，国土安全部，行业特定机构，行业协调委员会（例如，能源，健康，运输）
前提任务：制定工业物联网安全基线预计开始时间：19年第四
季度
预期竣工时间：20年第二季度

任务名称：探索工业物联网设备的标签或其他透明度方案
行动编号：5.2
任务摘要：努力开发一种自愿标签方法或其他信息透明模式，作为通知工业企业客户的一种选择。
贡献者：工业物联网行业，国家实验室，国土安全部，行业特定机构，行业协调委员会（例如，能源，健康，运输）
前提任务：制定工业物联网安全基线预计开始时间：19年第四
季度
预期竣工时间：20年第二季度

任务名称：工业物联网设备客户支持意识
行动编号：5.2
任务摘要：创建信息工具（如标签或品牌），帮助工业企业客户识别合格的工业物联网产品。
贡献者：工业物联网行业，零售商，国家信息共享和分析中心理事会（ISACs）的国土安全部
前提任务：制定工业物联网安全基线
预计开始时间：20年第二季度
预期竣工时间：20年第二季度

任务名称：促进关键基础设施采用评估制度
行动编号：5.2
任务摘要：通过物联网和信息技术产品（ISAT）理事会，国土安全部和工业界将评估物联网和信息技术产品在关键基础设施上的适用性时的商业认证制度。
贡献者：国土安全部（领导层），工业物联网行业，国家实验室，国土安全部，行业特定机构，部门协调委员会（例如，能源，健康，运输）
前提任务：建立工业物联网设备评估计划
预计开始时间：20年第三季度
预期竣工时间：23年第一季度

为可信赖的联邦物联网设备建立稳健的市场

下列任务旨在为具有高产品可用性和强大客户认可度的联邦物联网产品建立广泛采用的安全能力基准。这些任务首先通过针对联邦物联网市场的特定要求增强核心安全能力基线。为鼓励采购和部署合格设备，建立了以联邦基准为基础的联邦采购法规。

任务名称：识别联邦物联网安全要求
操作编号：2.3
任务摘要：在一系列会议中召集关键利益相关者，确定联邦环境通用/特定的非核心安全功能。
贡献者：管理和预算办公室（OMB），总务管理局（GSA），国防部（DOD），国土安全部，国家标准与技术研究院（NIST），联邦首席信息官（CIO）理事会，联邦首席信息安全官（CISO）
前提任务：发布核心安全能力基线
预期开始：待定
预期竣工时间：待定

任务名称：指定联邦物联网安全能力基准
操作编号：2.3
任务摘要：与行业和机构合作，制定和发布联邦物联网安全能力基线。
贡献者：NIST（负责人），国土安全部，联邦CIO理事会，联邦CISO，行业，CSDE / CTA前提任务：确定联邦IoT安全要求
预计开始时间：19年第三季
度预期完成时间：20年第一季度

任务名称：建立联邦物联网采购法规
操作编号：2.3
任务摘要：建立联邦采购法规，支持符合联邦物联网安全能力基准的物联网设备采购。
投稿人：GSA（领导），OMB，联邦CIO委员会，联邦CISO和采购人员前提任务：指定联邦IoT安全能力基准
预计开始时间：待定预计完
成时间：待定

物联网工作流2：物联网安全的采用和可持续性

此工作流程总体上侧重于IoT设备全球生态系统的开发。也就是说，此工作流程中指定的一系列操作可增强物联网产品的安全性，并增强对物联网市场的信心，而无需考虑三个特定于部门的安全基准。任务重点是网络安全和运营技术社区之间的协作，以及国际政策倡导，统一和标准。除了制定全球相关的物联网标准外，这些活动几乎没有依赖性。一个关键挑战将是确定活动的优先级以反映资源可用性。

扩展物联网风险管理

许多企业网络安全计划已转向基于风险的方法，例如NIST的网络安全框架。这些组织利用框架和相关方法来管理与网络安全相关的风险的标准，准则和最佳实践，历来集中于信息技术和传统信息网络。在这一系列任务中，扩展了风险管理方法，以帮助组织更好地理解和管理与IoT设备整个生命周期相关的网络安全和隐私风险。

任务名称：为物联网安全启用风险管理方法
动作编号：1.5
任务摘要：发布NISTIR 8228，“管理物联网（IoT）网络安全和隐私风险的考虑因素”，以支持物联网安全的风险管理方法。贡献者：NIST（行业），行业
前提任务：N / A
预计开始时间：正在进行中
预期完成时间：19年第一季度

任务名称：为物联网设备制造商发布最佳实践
动作编号：1.5
任务摘要：使用核心安全功能，识别有助于新兴NISTIR 8228“管理物联网（IoT）网络安全和隐私风险的考虑因素”中确定的客户成果的最佳实践。
投稿人：NIST（负责人），待定
前提任务：为物联网安全启用风险管理方法；发布核心安全能力基准
预计开始时间：19年第二季
度预期完成时间：20年第二季度

任务名称：商品化安全更新技术

N / A

2.5

强 9

N / A

1.4

9

N / A

意识和教育努力

意识和教育努力范围有两个互补的工作流程：

- 提升消费者信心
- 教育劳动力

意识和教育工作流1：提升消费者信心

消费者对物联网设备安全性缺乏信心可能会阻碍物联网的采用。这一系列任务的重点是建立消费者信心，使消费者能够识别满足需求的产品，遵守供应商的安全声明，并通过应用商业可用的网络安全技术提供真正的保护。

任务名称：促进适当的产品部署
操作编号：4.3
任务摘要：对消费者进行不同的基线和评估计划教育，以表明所部署的产品正在使用适当的安全性。
贡献者：特定领域的机构，民间社会，消费者团体，FTC，DHS，NTIA，CTA。建立工业物联网设备评估计划；指定物联网安全能力基准
预计开始时间：20年1季度预
计完成时间：23季度

任务名称：制止非法营销行为
操作编号：4.3

任务摘要：通过执法行动制止和阻止物联网和信息技术供应商的非法营销行为。
贡献者：FTC（领导）
前提任务：N / A
预期开始：进行中
预期完成：正在进行

任务名称：缓解基于物联网的分布式拒绝服务
动作编号：1.5
任务摘要：演示结合制造商使用说明（MUD），威胁信号，安全更新和基本网络卫生的影响和实用性，以保护物联网设备并减轻受损的物联网设备的影响。
贡献者：NIST（领导），公民社会，互联网工程师
前提任务：N / A
预期开始：进行中
预期完成：持续

意识和教育工作流2：教育劳动力

随着各种各样的产品和服务上线，新型产品中会出现网络安全威胁。产品设计师沉迷于与产品相关的传统风险，但通常不知道当产品连接到网络时可能引入的新风险。这一系列任务的重点是对现有和新兴劳动力（无论工程学科如何）进行基本网络安全教育。

任务名称：准备编程人员
操作编号：1.3
任务摘要：在整个学习过程中的编程课程中纳入设计安全原则和支持工具。 贡献者：学术界，安全软件开发社区，培训和认证提供商，认证机构，政府
前提任务：N / A
预计开始时间：正在进行中
预期完成时间：20年第二季度

任务名称：准备工程人员
行动编号：5.4
任务摘要：在所有工程学科的学习过程中纳入网络安全原则。
投稿人：学术界，联邦和州政府
前提任务：N / A
预期开始：进行中
预期完成时间：20年第二季度
任务名称：根据员工需求调整课程
行动编号：5.3

任务摘要：继续促进国家网络安全教育倡议（NICE）框架，作为开发课程内容（尤其是软件开发方面）的参考工具。
贡献者：NIST（领导），学术界，认证机构，专业协会，认证提供者
前提任务：N / A
预计开始时间：正在进行中
预期完成时间：2018年第四季度

任务名称：建立工程师网络安全教育计划
行动编号：5.4
任务摘要：将网络安全作为所有工程学科的基本要求，并为工程师创建或利用现有的在线网络安全培训。
投稿人：NIST，网络安全教育界，认证计划
前提任务：N / A
预期开始：进行中预期完成
时间：21年第一季度

III. 后续步骤

商务部和国土安全部将与其他美国政府机构和私营部门合作，协调和跟踪路线图活动。国土安全部将跨部门特定机构与关键基础设施组织进行协调。商务部将通过NIST协调标准和技术活动，并将通过NTIA跨政府和数字经济进行协调。

我们还将定期提供更新，包括：

- 定期与私营部门利益相关者举行会议和沟通，私营利益相关者领导着共享信息和进步的关键举措。
- 在中期（路线图发布后大约六个月）召集利益相关者，通过研讨会或其他会议讨论路线图实施进展。
- 根据僵尸网络报告的详细情况，在最终路线图发布后一年，向总统提供365天状态执行情况报告。此更新将审查整个社区的进度，在切实可行的范围内重新评估威胁，并将讨论来年的关键活动。

正如僵尸网络报告和本文件第二节所讨论的那样，自动化分布式攻击问题无法由一个实体解决，而是需要政府，私营部门（包括行业，学术界和公民社会）。新闻部期待在未来一年及以后与私营部门和其他政府实体合作，改善互联网生态系统的安全性。