CSRIC III

Communications Security, Reliability and Interoperability Council

2012年3月

最终报告

美国互联网服务提供商反机器人行为守则（ABC）

（自愿代码）

“本行为准则将是向前迈出的重要一步，是政府对僵尸网络进行更广泛努力的重要补充。”

FCC主席Julius Genachowski
2012年2月22日

目录

1 结果简介

1.1 执行摘要

恶意“机器人”指的是系统上安装的程序，通常使该程序自动在恶意远程管理员的命令和控制下执行一项或一组任务。受机器人感染的终端用户设备的增长对互联网的活力和弹性以及对在线经济构成了重大威胁。[1] 僵尸网络是指感染了僵尸恶意软件的互联网连接终端用户计算设备网络，由第三方出于恶意目的进行远程控制。僵尸网络和僵尸网络可能导致个人信息盗窃，对公共和私人网络的攻击以及最终用户计算能力和互联网访问的利用。

CSRIC III责成僵尸网络补救工作第7组工作组提出了一系列商定的自愿做法，这些做法将构成供互联网服务提供商选择采用的实施模式，以减轻僵尸网络威胁。对此，美国制定了《互联网服务提供商反机器人行为守则》，旨在通过自愿参与解决僵尸网络和僵尸网络在住宅宽带网络中的威胁。在制定该《守则》时，确定整个互联网生态系统的组成部分在应对僵尸网络威胁方面可发挥重要作用，而互联网服务提供商则依赖于生态系统其他部分的支持。

《行为准则》鼓励互联网服务提供商参与支持最终用户教育的活动，以防止僵尸感染，侦测机器人，通知潜在的机器人感染，补救机器人以及协作和信息共享。准则包含在附录中。

工作组提出了一套商定的自愿做法，将构成供互联网服务提供商选择加入实施模式的框架，以帮助应对僵尸网络威胁。工作组建议提供住宅宽带互联网接入的互联网服务提供商（ISP）如果选择采用该准则，可以采取的措施。工作组进一步建议互联网服务提供商（ISPs）和其他服务提供商通过联系最终管理守则的行业组织，表明他们同意加入自愿守则。最初建议参与的ISP和其他服务提供商将有关代码参与的选择通知实体，或者在自己的网站上声明。确定的未来工作包括确定守则参与的长期管理，守则的定期更新，确定守则参与的障碍，定义指标，以及识别守则参与者和支持生态系统贡献者的最佳实践和经验教训。

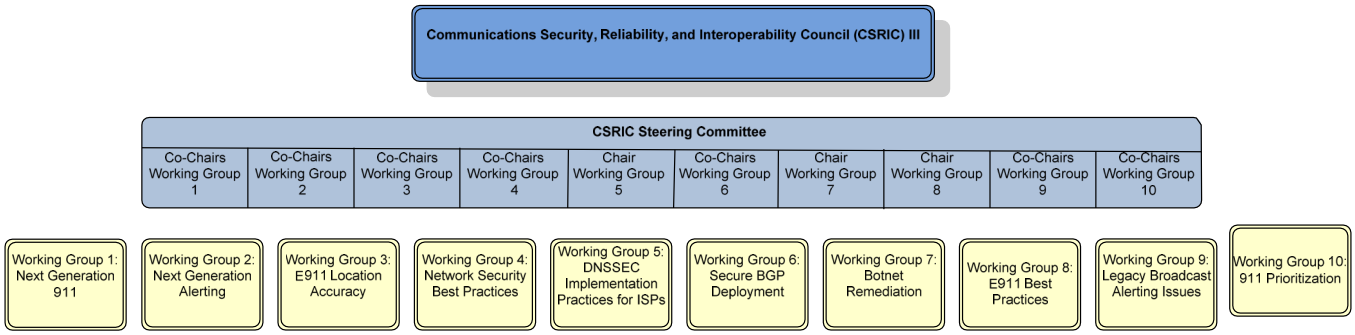
1本文档中术语“机器人”和“机器人感染”可互换使用。

2 引言

CSRIC III建立了第7工作组（WG7），致力于解决宽带网络中的僵尸网络修复问题。第7工作组调查了IETF，日本，澳大利亚，芬兰，德国和其他地区正在开展的机器人补救工作，以确定应对美国宽带网络中机器人威胁的最佳方法。

这项工作的结果是附录中的美国互联网服务提供商自愿反机器人行为守则。

2.1 CSRIC结构



2.2 CSRIC WG7结构

WG7工作组由邮件反滥用工作组（MAAWG）主席Michael O'Reirdan主持，由国土安全部网络安全和通信办公室首席技术官Peter Fonash博士担任副主席。
WG7的成员包括互联网服务提供商，软件和网络设备供应商，学术界以及互联网生态系统一部分其他组织的代表。

2.3 第7工作组成员

第7工作组由以下成员组成。

名字	公司
Michael O'Reirdan – Chair	MAAWG
Peter Fonash – Vice-Chair	Department of Homeland Security
Neil Schwartzman - Secretary	CAUCE
Robert Thornberry - Editor	Bell Labs, Alcatel-Lucent
Paul Diamond - Editor	CenturyLink
Vernon Mosley – Liaison	FCC
Alex Bobotek	AT&T
Adam O'Donnell	Sourcefire
Alfred Huger	Sourcefire
Barry Greene	ISC
Bill McInnis	IID
Bill Smith	PayPal
Brian Done	Department of Homeland Security
Chris Roosenraad	Time Warner Cable
Chris Sills	IID
Craig Spiezle	Online Trust Alliance (OTA)
Daniel Bright	EMC
Eric Osterweil	Verisign
Gabe Iovino	REN-ISAC
Greg Holzapfel	Sprint
Gunter Ollmann	Damballa
James Holgerson	Sprint
Jay Opperman	Comcast
Joe St Sauver	University of Oregon and Internet2
Johannes Ullrich	SANS Institute
John Denning	Bank of America
John Griffin	Telecommunication Systems Inc.
John St. Clair	Verizon
Jon Boyens	National Institute of Standards and Technology
Kevin Sullivan	Microsoft
Kurian Jacob	FCC
Matt Carothers	Cox
Maxim Weinstein	StopBadware
Merike Kaeo	ISC
Michael Fiumano	Sprint
Michael Glenn	CenturyLink
Robert Mayer	USTelecom
Tice Morgan	T-Mobile
Tim Rohrbaugh	Intersections
Timothy Vogel	Verizon

表1-第7工作组成员列表

3 目的，范围和方法

3.1 目的

CSRIC责成第7工作组僵尸网络补救工作，提出一系列商定的自愿做法，这些做法将构成供互联网服务提供商选择采用的实施模式的框架，以减轻僵尸网络威胁。对此，美国制定了《互联网服务提供商反机器人行为守则》，旨在通过自愿参与解决僵尸网络和僵尸网络在住宅宽带网络中的威胁。

3.2 范围

本节确定了CSRIC III第7工作组章程中概述的问题陈述，工作组描述和交付成果。

问题陈述：被机器人感染的终端用户设备的增长对互联网和在线经济的生命力和弹性构成了重大威胁。僵尸网络是指感染了僵尸恶意软件的互联网连接终端用户计算设备网络，由第三方出于恶意目的进行远程控制。僵尸网络和僵尸网络可能导致个人信息盗窃，对公共和私人网络的攻击以及最终用户计算能力和互联网访问的利用。[2]

为减少僵尸机器人在住宅最终用户设备中的感染并减轻对僵尸机器人的潜在利用，第7工作组制定了自愿的《互联网服务提供商反机器人行为守则》。

第7工作组的描述：该工作组将审查在国际社会内部开展的工作，如澳大利亚互联网行业行为守则，以及在国内利益相关方组织（如IETF和消息反滥用工作组）中对美国的适用性。互联网服务提供商。僵尸网络补救工作组应在CSRIC II第8工作组ISP网络保护实践工作的基础上，提出一套商定的自愿实践，将构成ISP选择加入实施模式的框架。工作组将为互联网服务提供商提出一种加入工作组提议的框架的意图。工作组还将为新起草的《行为准则》确定潜在的ISP实施障碍，并确定FCC可以采取的有助于克服这些障碍的措施。最后，工作组应确定绩效指标，以评估《守则》在抑制机器人感染传播方面的有效性。

2本文档中术语“机器人”和“机器人感染”可互换使用。

报告可交付成果：

1. **美国互**联网服务提供商反机器人行为准则：2012年3月22日
2. 代码参与的障碍：2012年9月12日
3. Bot补救效果指标：2012年12月5日

该报告是《美国互联网服务提供商反机器人行为守则》，是第7工作组的三份报告交付成果中的第一份。

3.3 方法论

第7工作组由来自行业，政府和学术界的代表不同利益相关者的专家组组成的团队，开始研究为互联网服务提供商制定的美国反机器人行为守则。第7工作组审查了包括澳大利亚互联网行业行为准则和日本网络清洁中心在内的国际社会以及互联网工程任务组（IETF）和消息传递反滥用工作等国内利益相关方组织的努力。组，适用于美国互联网服务提供商。在CSRIC II第8工作组ISP网络保护实践的工作基础上，CSRIC III 7工作组每两周召开一次电话会议，讨论建立美国反机器人相关努力的发展，内容和相关性互联网服务提供商行为准则。第七工作组定期召开电话会议，讨论僵尸网络相互补救的共同领域，与商务部和白宫国家安全人员协调制定法规。第七工作组与成员举行了两次面对面会议，一次会议于2011年11月举行，以制定守则草案各部分的结构并讨论其内容，最后一次面对面会议于2012年2月举行，审议了守则草案的各节内容。最终法规草案。由此产生的《美国互联网服务提供商反机器人行为守则》基于第7工作组成员的共同投入，并与这些成员及其公司与其他利益相关方进行了讨论，以减少机器人感染的发生率。

4 背景资料[3]

恶意或潜在恶意“机器人”指的是安装在系统上的程序，目的是使该系统能够自动（或半自动）执行一项任务或一组任务，通常在邪恶的远程管理员的命令和控制下，或“机器人大师”。僵尸机器人也被称为“僵尸”。此类机器人可能是秘密安装的，用户无法完全理解该机器人一旦安装将执行的操作，在不知不觉中作为另一软件安装的一部分，以虚假借口或以各种其他可能的方式。

互联网用户使用的设备可能感染了恶意软件，其中可能包含或安装了一个或多个机器人。由于多种原因，它们可能会带来重大问题。首先，这些机器人可以用来发送垃圾邮件，在某些情况下还可以发送大量垃圾邮件。这种垃圾邮件可能导致ISP浪费网络，服务器或人力资源，造成额外成本。

3见《ISP网络中僵尸机器人补救建议》，http://tools.ietf.org/rfc/rfc6561.txt

许多其他潜在成本和副作用。此类垃圾邮件还会对ISP，其客户的声誉以及ISP使用的IP地址空间的电子邮件信誉（通常简称为“ IP信誉”）产生负面影响。

此外，这些机器人还可以充当指挥，参与或以其他方式对关键互联网基础设施进行攻击的平台。僵尸机器人通常出于犯罪，政治或其他动机，被用作协调分布式拒绝服务攻击的一部分。

互联网服务提供商（ISP）在向互联网用户提供服务中扮演着角色，使互联网服务提供商（ISP）能够尝试检测和观察网络中运行的僵尸网络。此外，互联网服务提供商可能也能够将僵尸程序感染机器人的实际，潜在或可能的情况通知其客户。

从最终用户的角度来看，被通知可能在网络上感染了设备可以提供重要的信息。一旦知道了这一点，就可以采取措施删除僵尸机器人，解决可能由僵尸机器人感染引起的所有问题，并保护自己免受未来威胁的侵害。

第七工作组为互联网服务提供商制定了自愿的美国反机器人行为守则，以解决住宅宽带网络中如上所述的僵尸网络和僵尸网络威胁。互联网服务提供商自愿采用本准则。这不是强制性的。

5 建议

5.1 建议

工作组提出了一套商定的自愿措施，将构成互联网服务提供商选择加入实施模式的框架，以帮助应对僵尸网络威胁。工作组建议提供住宅宽带互联网接入的互联网服务提供商（ISP）如果选择采用该准则，可以采取的措施。工作组进一步建议互联网服务提供商（ISPs）和其他服务提供商通过联系最终管理该守则的行业组织，表明他们同意加入自愿守则。作为行业（以及行业）自愿制定的行为守则，目标是建立一个中立的行业论坛，接收和整理与参与守则有关的报告。
最初是为了表明参与，建议参与的ISP和其他服务提供商或者将有关其代码参与的选择通知实体，也可以在自己的网站上声明。

5.1.1 未来的工作

本报告是《美国互联网服务提供商自愿反机器人行为守则》，是第7工作组的三份报告交付物中的第一份。为解决《守则》的长期管理和定期更新，仍有工作要做。接下来，工作组将确定守则参与的潜在障碍。最后，工作组将确定潜在的机器人补救性能指标。

建议进一步开展工作，解决来自受感染和邪恶网站和托管服务的机器人感染传递机制，从而使WG7的工作无处不在并有效。

5.1.2 致谢

WG7 WG感谢日本CERT的Yurie Ito所作的介绍性丰富的演讲，并讨论了从日本反僵尸网络计划日本网络清洁中心汲取的教训。我们还要感谢美国国家标准研究院（NIST）的Ari Schwartz关于僵尸网络威胁和缓解策略的演讲。另外，WG7还感谢微软，MAAWG和FC C主持了面对面的WG7会议。

第7工作组特别感谢以下小组成员的不懈努力，为守则制定流程做出了巨大贡献：

Alcatel-Lucent（编辑）和Bell Labs的 Robert ThornberryPaul
Diamond，CenturyLink（编辑）
俄勒冈大学和互联网大学乔·乔·索弗（Joe St Sauver）（词汇表）
CAUCE的Neil Schwartzman（秘书）

6 结论

为响应CSRIC III向工作组7提出的任务，制定了自愿性的ISP美国反机器人行为守则，旨在通过自愿参与解决僵尸网络和僵尸网络在住宅宽带网络中的威胁。在制定该《守则》时，确定整个互联网生态系统的组成部分在应对僵尸网络威胁方面可发挥重要作用，而互联网服务提供商则依赖于生态系统其他部分的支持。

2012年3月22日的这份报告，即针对互联网服务提供商的美国反机器人行为守则，是工作组7的三份报告交付物中的第一份。接下来，工作组将确定守则参与的潜在障碍，并将于9月发布报告。 2012年，最后一步，工作组将确定僵尸网络补救措施绩效指标并于2012年12月提交有关此主题的报告。

7 附录

美国互联网服务提供商反宽带行为守则（ABCs），应对宽带网络中的僵尸行为
决赛
2012年3月22日

1. 引言

最终受感染的最终用户设备数量的增长对互联网和在线经济的生命力和弹性构成了重大威胁。请注意，本文档中机器人感染和机器人同义使用，指感染机器人恶意软件的最终用户设备。* * 僵尸网络是指感染了僵尸恶意软件的互联网连接终端用户计算设备网络，由第三方出于恶意目的进行远程控制。*

僵尸网络和僵尸网络可能导致个人信息窃取，对公共和私人网络的攻击以及最终用户计算能力和互联网访问的利用。公众对于机器人程序及其影响以及由此产生的安全和隐私问题的意识很低。本自愿行为守则（“守则”）提供了一系列原则和建议的活动，互联网服务提供商可能会采用这些原则和建议的活动来应对僵尸网络和僵尸网络在住宅宽带网络中所带来的威胁。*

应当认识到，僵尸机器人会影响整个互联网生态系统，而成功缩减僵尸机器人或减轻其影响将需要该生态系统的各个部分共同采取行动，包括最终用户，软件开发人员，搜索提供商，网站，电子商务网站等。最终用户设备不在ISPshence的控制范围之内，互联网生态系统中的所有参与者都需要共同努力解决这一问题。该准则旨在通过定义一系列针对互联网服务提供商（ISP）在解决这一重要问题方面可发挥的有限作用的行动，为今后各利益相关方之间的协调奠定基础。* * 该准则认识到美国互联网服务提供商的规模，资源，业务模型和环境，专业知识和能力存在很大差异。互联网服务提供商活动的成功取决于其他互联网利益相关方的类似努力。

参与本《守则》的核心要求在第5节中阐明。本文档的其他部分包含背景信息或其他说明材料。

---

*在词汇表中找到定义

2. 关键术语的定义

读者注意：

关于机器人的任何讨论都不可避免地涉及到独特的技术词汇。意识到许多读者可能不熟悉其中一些专业术语，本守则在附录2中包含了一个词汇表。词汇表中出现的任何术语首次在守则文本正文中均标有星号“ *”。出现是为了提醒读者术语表中提供了定义。

3. 目标和原则

a. 本守则的目标是：

1. 为互联网服务提供商提供一个初始框架，以更好地理解和帮助解决机器人问题；和

2. 鼓励互联网服务提供商

• 向最终用户宣传机器人造成的威胁以及最终用户可以采取的预防机器人感染措施；

• 检测机器人活动或从可信第三方那里获取最终用户群中有关机器人感染的信息；

• 通知终端用户怀疑机器人感染，或帮助终端用户确定他们是否可能被机器人感染；和

• 向最终用户直接或参考其他来源提供信息和资源，帮助他们补救机器人感染。

b. 守则的实施将遵循以下原则：

1. 自愿-参与是自愿的，并鼓励互联网服务提供商采取各种行动，但本《守则》不需要任何特定的活动。

2. 技术中立性—本准则未规定任何特定手段或方法。

3. 方式中立—本准则未规定实施本准则任何部分的任何特定方式。

4. 尊重隐私-互联网服务提供商必须按照适用的法律以适当的方式解决隐私问题。

5. 遵守法律-活动必须遵守适用法律。

6. 分担责任—互联网服务提供商（ISP）单独行动，不能完全解决僵尸机器人带来的威胁。其他互联网生态系统参与者也必须尽自己的一份力量。

7. 可持续发展—互联网服务提供商应在其业务模型范围内寻求具有成本效益和可持续发展的活动。

8. 信息共享-互联网服务提供商应说明他们如何参与《守则》，并与其他适当的利益相关方分享从其活动中学到的经验教训。互联网服务提供商（ISP）与其他相关方之间的所有信息共享必须根据适用法律执行，包括但不限于反托拉斯法和隐私法。

9. 有效性—应鼓励互联网服务提供商参与被证明是适当和有效的活动。

10. 有效的沟通-与客户的沟通应考虑到语言等各种问题，并确保以合理预期接收者能够理解和访问的方式提供信息。*

* 在词汇表中找到定义

4. 范围和作用

该准则是专门为向住宅最终用户提供宽带互联网接入服务的互联网服务提供商（ISP）和其他服务提供商起草的。本守则中的活动可能适用于其他互联网提供商和参与者。

本准则并非旨在全面涵盖在线安全方法，而应与其他当前和未来的努力共存。预计它将对其他互联网生态系统参与者发挥重要作用，包括但不限于：

- 安全软件供应商
- 操作系统开发人员
- 面向最终用户的组织
- 互联网内容，应用程序和服务提供商

在线安全应采用多方面灵活的方法，运用各种知名来源的建议和工具。

a. 成功的定义

本《准则》的初步成功将由ISP社区参与评估。但是，整个互联网生态系统的支持被视为与僵尸机器人斗争最终取得成功的关键。

b. 参与守则的好处

互联网服务提供商（ISP）有意义地参与本守则可能会带来以下高级好处：

- 增强最终用户信息和设备以及美国基础设施的安全性；
- 在最终用户，互联网服务提供商和其他与互联网相关的行业参与者中增强对机器人威胁及其应对方法的认识；

*在词汇表中找到定义

- 机器人感染的最终用户设备上机器人活动的通知和补救；* *
- 在美国住宅宽带网络中创建对机器人的部署和利用更具敌意的环境；和
- 跨最终用户和ISP开发和广泛使用有效的通知和补救架构和工具。

一些参与代码开发流程的互联网服务提供商（ISP）先前已经实施了《守则》的某些方面，因此在以下领域取得了有益的成果：降低呼叫量，帮助受感染机器的客户服务台；通过拒绝服务攻击和垃圾邮件减少上行带宽消耗，提高客户信誉，降低客户流失率，并减少其他互联网服务提供商的垃圾邮件相关投诉。尽管个别结果可能有所不同，但鼓励互联网服务提供商寻求参与守则增强整体宽带业务的特定方式，并与其他互联网服务提供商分享这些经验。此外，互联网服务提供商（ISP）参与本《准则》可能使互联网服务提供商（ISP）生成具体活动对互联网服务提供商（ISP）整体宽带业务运营的影响的具体指标，进而可以支持进一步的反机器人活动的开发或部署。*

*在词汇表中找到定义

5. 参与参数

参与本守则是自愿的。

自愿行为守则参与要求

为参与本守则，互联网服务提供商将在以下各个常规领域中至少开展一项活动（即采取有意义的行动）：

- 教育：旨在帮助提高最终用户对僵尸网络问题以及如何防止僵尸病毒感染的认识和认识的活动；
- 检测-检测活动，旨在识别ISP网络中的僵尸网络活动，获取有关ISP网络中僵尸网络活动的信息，或使最终用户自行确定最终用户设备上潜在的机器人感染；
- 通知-旨在向客户通知怀疑的机器人感染或使客户确定是否可能被机器人感染的活动；
- 补救-旨在向最终用户提供有关他们如何补救机器人感染的信息，或协助最终用户补救机器人感染的活动。
- 协作-与其他互联网服务提供商分享从参与互联网服务提供商代码活动中获得的反馈和经验的活动。

在上述总体领域中的每个领域开展“至少一项活动”的概念旨在鼓励在上述五个领域中的每个领域开展一定水平的活动，作为在美国住宅宽带网络中营造环境的总体全国流程的一部分，对机器人的部署和利用更具敌意。旨在支持和鼓励广泛的灵活努力，采用各种教育，检测，通知和补救方法进行实验和创新。同样，与其他互联网服务提供商共享反馈的要求并不旨在规定共享此类反馈的任何具体手段或方法。*

6. 最终用户教育

a. 概述

最终用户最终有责任保护自己的设备并补救被感染的设备。互联网服务提供商（ISP）与许多其他互联网参与者和政府行为体一样，可以协助帮助教育最终用户有关僵尸机器人的威胁以及最终用户可以采取的保护设备和补救感染的措施。

b. 建议的操作：

1. 关于机器人防护的教育：*

互联网服务提供商应提供预防机器人感染和相关问题的信息。此类信息至少应包括：

- 最终用户如何以及为什么必须使用随时可用的软件更新来为计算机和设备更新软件。
- 使用信誉良好的卖方的有效最新安全软件的重要性。
- 备份用户数据和软件的重要性以及如何有效进行备份。
- 最终用户的基本操作，以最小化使用互联网时受到机器人感染的风险。

可以预期，许多互联网服务提供商（ISP）可以通过直接向订户提供此类信息或链接到此类信息的现有公共可用来源来实现这一目标。

2. 支持最终用户机器人补救措施：

除了预防信息外，互联网服务提供商还应（例如通过互联网服务提供商出版物，第三方出版物或网络链接）提供有关最终用户通常如何补救机器人感染的信息。在这一领域，预计互联网服务提供商（ISP）将通过与此类信息的现有可公开获得的来源链接或通过单独或结合其他方式创建此类信息的新来源来实现这一目标。

与互联网服务提供商的最终用户通知活动相关，互联网服务提供商应在此类通知或其他通知中包含有关收件人可能转向何处寻求更多信息和帮助的信息。此类信息可能包括指向公众可用在线信息的链接，安全工具或寻求计算机专业人员帮助的建议。 ISP可能希望包括的其他主题和参考：

- 使用认为被感染的设备会对最终用户和互联网社区造成风险，
- 如何识别和清除常见形式的机器人感染，
- 公开检测工具或服务（免费或付费），帮助检测和清除机器人感染；以及
- 关于在何处找到更多（免费或付费）帮助的指南。

3. 指导原则：

在满足上述要求时，互联网服务提供商应考虑以下准则：

- 直接或通过推荐第三方服务提供教育信息和资源。
- 保持教育内容简洁，专注于用户需要了解的最重要内容。
- 确保非技术用户的受众可以遵循说明。
- 使用多种媒体，例如图像，视频，文本，字幕等，并在有用的情况下使用多种语言，最大限度地提高客户的了解和可访问性。
- 提供信息或指向描述被机器人感染的设备异常行为以及机器人检测软件工具或服务的可用性和使用的信息，帮助最终用户确定是否感染了机器人。

7. 僵尸机器人检测

a. 概述

随着机器人的发展，用于检测机器人的工具和技术也必须不断发展。检测面临的挑战在于，机器人流量必须具备多功能性，才能避免许多用于检测机制的奇异技术（如简单模式匹配）。某些互联网应用程序（如基于主机托管的分布式内容分发网络，在线游戏应用程序和其他此类服务）可能表现出与恶意机器人类似的行为，并且可能利用类似的技术，因此可能会使检测复杂化。互联网服务提供商应谨慎识别受影响的各方，以进行通知和补救。

b. 建议的操作：

互联网服务提供商可以通过多种方式查找恶意活动和被僵尸机器人感染的终端用户设备：

1. 接收来自外部实体的通知，尤其是那些旨在帮助整体了解和实时传播与机器人相关的数据的通知。附录2列出了资源列表。
2. 在其网络内部署有助于识别潜在机器人感染的功能。
3. 将客户引导到工具，网络门户或其他使客户能够自我识别潜在机器人感染的资源。

8. 最终用户可能感染机器人的通知

a. 概述：

许多最终用户并未意识到自己的设备已被感染并以机器人程序运行。结果，这些用户及其数据仍然处于风险之中，机器人可以无限期保持活动状态。互联网服务提供商应利用第7节中所述的检测工作，使客户意识到主动感染。

通知的设计应有助于减轻机器人及其造成的伤害。通知可能包括有关机器人是什么，感染方式，机器人可能没有明显症状以及通知含义的信息。通知还可能包含或标识其他有助于感染预防，验证和缓解的资源，如工具，指南和服务。他们还可能提供有关检测到的任何特定机器人的信息。*

最终用户通知可以采用许多不同的形式。它可以直接由ISP执行，也可以由第三方代表ISP执行。互联网服务提供商可能会直接向最终用户发出警报，或提供允许最终用户请求和接收有关感染状况信息的机制。同样，互联网服务提供商可能会做出安排，使最终用户与其有关系的其他生态系统参与者（如互联网应用程序或服务提供商）向终端用户发送通知。

互联网服务提供商应考虑采用以下机制，确保客户能够轻松地将通知认证为真实，并且很难欺骗此类通知。

在可行的情况下，互联网服务提供商可能希望跟踪通知的接收。这可以帮助ISP更好地了解各种通知机制的有效性。

每个互联网服务提供商（ISP）都需要评估不同的通知方法，以便找到最适合特定互联网服务提供商（ISP）和特定机器人僵尸威胁的方法。选择的通知方法可能需要与现有业务流程和现有网络集成

---

*在词汇表中找到定义

基础设施。可能需要进行研究和分析，以开发和维护适当的通知系统和政策。

b. 建议的操作：

向客户提供疑似机器人感染的通信，或帮助客户确定是否可能被机器人感染。附录2的参考文献中概述了许多通知方法。但是，可以使用其他方法。

9. 僵尸机器人补救

a. 概述

机器人防护和补救是任何机器人感染通知程序的最终目标，也是最终用户的责任。对于技术用户而言，仅通知就足够了，但大多数用户通常需要某种形式的帮助才能从受感染的设备中删除机器人恶意软件。然而，补救可能很困难，可能涉及其他复杂功能，例如在许多共享互联网连接的设备中隔离感染源；提前备份所有数据和系统软件，以保留最终用户恢复的能力（但也不备份受感染的文件或程序）；并确保最终用户具有源磁盘和其他材料，以便在补救过程中根据需要重建设备映像。

可以理解，一些互联网服务提供商可能没有资源提供这种级别的服务，也无法免费甚至收费支持此类活动。在许多情况下，可能需要推荐终端用户专业计算机支持服务的提供商，以对他们的机器进行全面补救。 ISP通知可能会预料到这一事实，并建议客户寻求第三方帮助，以避免因有限服务台或支持热线不具备或无法完全解决补救问题的支持用户而感到沮丧。

b. 建议的操作：

1. 僵尸机器人被设计为隐形且难以移除。作为通知的一部分，互联网服务提供商应如上所述提供指导。其中可能包括指向各种可公开获得的在线和第三方信息，软件和工具来源的链接。它还可能包括指向专业服务的链接。这些不必由ISP本身提供，而可以由第三方提供。

2. ISP可以在通知过程中或通知过程之后向最终用户提供补救工具。但是，ISP不应强制最终用户运行补救工具。如果ISP向最终用户提供工具，则应允许最终用户退出流程而无需运行任何建议的工具或过程。

3. 作为通知流程的一部分，互联网服务提供商可能希望包括一些指南（取决于所讨论机器人的性质），以指导客户拥有的网络设备（如家庭网关和路由器）设置

进行了更改，应恢复到安全状态，具体取决于机器人感染的性质。

c. 指导原则：

1. 僵尸清除工具和服务必须尊重用户隐私。

2. 附录2中引用了CSRIC II WG 8最佳实践和自动修复IETF RFC中概述了可能的感染补救方法。

10. ISP协作

a. 概述：

僵尸机器人缓解和管理是由ISP，搜索提供商，最终用户，IT部门，托管公司，博客提供商，安全提供商，研究人员，政府，金融服务公司，云服务提供商和其他各方共同发挥作用的活动。有了多方利益相关者的投入和协作，结果将超过单独采取独立行动可能取得的结果。可以预料，互联网服务提供商（ISPs）将参与僵尸网络僵尸网络威胁防护，以及互联网生态系统其他领域采取的补充和协作方法。

b. 建议的操作：

参与代码需要在ISP，行业或更广泛的论坛之间通过协作活动进行协作，以下为示例：

1. 共享计划或部署在ISP网络中的检测，通知或缓解方法，以及在可行时评估其有效性。

2. 共享可能对机器人防护，防御或补救有用的情报或操作攻击数据。

3. 识别ISP网络以外的系统或参与者所需的关键数据或技术资源。

4. 参与超出ISP网络边界的综合防御策略或系统的定义，开发或操作。

5. 其他协作活动包括与ISP外部的各方共享信息或与ISP网络外部的系统共享数据。

互联网服务提供商与其他相关方之间的所有信息共享将根据适用法律执行，包括但不限于反托拉斯法和隐私法。

11. 本准则的进一步发展

由于僵尸程序威胁的动态性质以及对互联网服务提供商的经验和评估，该守则将随着时间的推移而发展。

12. 附加信息和资源

附录1 –术语表附录2 –参考

附录1 –术语表：

1. 僵尸机器人

以下定义主要来自“ ISP网络中僵尸程序补救建议”（附录2中引用）：

恶意（或潜在恶意）“机器人”（源自“机器人”一词，以下简称为“机器人”）指的是安装在系统上以使系统能够自动（或半-自动）通常在远程管理员（通常称为“僵尸机器人”或“僵尸机器人”）的命令和控制下执行一项或一组任务。

被“破坏”的计算机系统和其他最终用户设备通常也称为“僵尸”。

恶意机器人通常在未经用户同意的情况下秘密安装，或者在用户未完全了解机器人安装后可能会做什么的情况下进行秘密安装。

僵尸机器人通常用于发送垃圾电子邮件，侦听或攻击其他系统，窃听网络流量或托管非法内容，例如盗版软件，儿童剥削材料等。

许多司法管辖区都认为，最终用户主机的非自愿感染是非法入侵计算机的一个例子。

2. 僵尸网络

僵尸网络是指感染了僵尸恶意软件的互联网连接终端用户计算设备网络，由第三方出于恶意目的进行远程控制。
僵尸网络受指定的“ botherder”或“ botmaster”控制。一个僵尸网络可能只有少数几个僵尸主机，甚至数百万个。

3. 客户（或“直接客户”）

与ISP签订服务合同的一方。区分“客户”和“授权用户”：例如，一家咖啡店可以从ISP购买互联网服务。咖啡店将是ISP的客户。咖啡店可能会选择免费向从咖啡店购买咖啡的用户免费使用其连接（如果互联网服务提供商的可接受使用政策或AUP允许）；然后，咖啡买家将成为咖啡店购买连接的授权用户，但不是ISP的直接客户。

4. 检测

检测是服务提供商或最终用户意识到特定系统或设备已感染恶意软件的过程。服务提供商可能会以多种不同方式检测到系统感染病毒，包括接收到来自第三方的有关垃圾邮件，网络扫描或源自该系统的攻击的投诉。最终用户可以通过软件工具或其他手段检测系统感染。

5. 生态系统

该术语通常用于描述各种互联网参与者之间的相互关系，硬件制造商，软件开发人员，互联网服务提供商（ISPs）和各种使互联网运转并对终端用户有用的互联网内容，应用和服务的提供商。

互联网生态系统包括操作系统供应商，面向最终用户的组织，互联网内容，应用程序和服务提供商，ISP，搜索提供商，最终用户，IT部门，托管公司，博客提供商，安全提供商，研究人员，政府，金融服务公司和其他各方。

所谓的“地下经济”也经常被描述为“生态系统”，多个参与者扮演着不同的专门角色。例如，一些参与者可能专注于编写恶意软件，而其他参与者可能会“收获”网页和邮件列表中的电子邮件地址，而另一些参与者可能专注于将恶意软件分发给那些收获的电子邮件地址。
恶意软件生态系统通常还将包括目标潜在受害者的人群，以及致力于打击网络犯罪的执法机构。

6. 最终用户

最终用户：在计算和网络环境中，最终用户是指最终授权使用产品或服务的人。

最终用户通常可能与购买产品或服务的人不同。例如，一家咖啡店所有者可以购买连接服务，供其客户使用；在这种情况下，即使他们没有直接与ISP签定使用连接的连接协议，但咖啡店的客户而不是咖啡店的所有者代表实际的“最终用户”。

在未经购买者授权的情况下使用产品或服务的一方（例如黑客/爆竹）通常被视为网络入侵者，而不是“最终用户”本身。

7. 互联网服务提供商

互联网服务提供商（ISP）是为公众，企业和其他组织提供零售到互联网访问的公司。这些连接可以通过电缆，DSL，卫星，无线，拨号或其他技术进行。互联网服务提供商有时也称为“访问提供商”。

仅为其雇员提供互联网访问权限的企业通常不视为ISP。同样，仅向其他ISP提供批发访问互联网的网络运营商通常会被视为网络服务提供商（NSP），而不是ISP。

8. 恶意软件

“恶意软件”是“恶意软件”的简称。

恶意机器人是恶意软件的一种。其他形式的恶意软件包括以下类别的软件：病毒，特洛伊木马，蠕虫，Rootkit，犯罪软件，击键记录器，拨号程序，间谍软件，广告软件等。区分这些不同类型的恶意软件的重要性并不比理解为什么恶意软件重要。可能会被视为“恶意”。

恶意软件通常会违反以下一项或多项基本原则：

(a) 同意：即使用户没有故意要求进行恶意安装，也可能安装了恶意软件。

(b) 诚实：恶意软件可能假装做一件事，而实际上却在做完全不同的事情。

(c) 尊重隐私：恶意软件可能会侵犯用户的隐私，可能会捕获用户密码或信用卡信息。

(d) 非侵入性：恶意软件可能会通过弹出广告，更改网络浏览器主页，使系统运行缓慢或不稳定并易于崩溃或干扰已经安装的安全软件来惹怒用户。

(e) 无害：恶意软件可能是会伤害用户的软件（如破坏我们系统，发送垃圾邮件或禁用安全软件的软件）。

(f) 尊重用户管理：如果用户尝试删除软件，则可能会重新安装自身或以其他方式覆盖用户首选项。

所有这些加起来就是“软件用户不想要的”。

用户可能会在不知不觉中安装恶意软件，方法是打开通过电子邮件收到的受污染的附件，或者访问包含恶意内容的网页。攻击者针对可能可以远程利用的已知漏洞，或者由用户安装受感染的CD，DVD或拇指驱动器，也可能导致远程攻击者直接感染系统。

9. 缓解

缓解是管理或控制与机器人相关的效果的过程。例如，如果系统感染了垃圾邮件机器人，并散发了不必要的商业电子邮件，缓解措施可能包括过滤从该设备发出的垃圾邮件。

请注意，缓解通常不涉及解决基础状况（即“补救”）；缓解只管理与疾病相关的症状。

10. 通知功能

通知是一个过程，互联网服务提供商与最终用户就机器人恶意软件可能感染最终用户设备或订户如何预防或识别此类感染进行沟通。通知还可能需要一个流程，将最终用户定向到能够自我发现机器人感染的工具。通知可以采用不同的形式，包括ISP向最终用户的直接通知，或通过可用的自我发现工具或第三方的间接通知。通知可以通过多种潜在渠道完成，包括（但不限于）电子邮件，邮政邮件，电话呼叫，浏览器内通知，基于网络的自我发现工具或SMS消息。

11. 预防措施

预防是强化系统或服务，使其较不容易受到破坏和利用的过程。例如，在许多系统上，预防可能涉及：

— 使用可用的安全修补程序修补操作系统和所有应用程序
— 安装或启用防火墙
— 使用防病毒软件
— 确保定期备份系统
— 使用强密码
— 禁用所有不需要的网络服务
— 鼓励用户安全使用互联网服务（例如，电子邮件，网络浏览等）

12. 补救措施

补救是最终用户清理被机器人破坏的计算机，使其不再受到感染的过程。在简单的情况下，这可能涉及安装和运行防病毒产品。在更困难的情况下，修复可能涉及更实质性的干预，直至“裸露”系统（从头开始或至少从最后一次已知的清洁备份格式化和重新安装系统）。系统清洁或重新安装后，通常会经过加固以防止再次感染。

13. 垃圾邮件

不需要和不需要的电子邮件，通常为商业性质，通常以基本上相同的形式发送给大量收件人。垃圾邮件通常由“关联公司”发送，当接收者购买垃圾邮件产品时，这些会员会由运行会员计划的人支付。

附录2 –参考

1. 关于如何管理感染了恶意机器人的计算机的建议：“ ISP网络僵尸修复建议”

http://tools.ietf.org/rfc/rfc6561.txt

2. CSRIC II工作组8-ISP网络保护最佳实践

http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf

3. icode –解决网络安全的澳大利亚互联网行业业务守则

http://iia.net.au/images/resources/pdf/icode-v1.pdf

4. 日本网络清洁中心–反僵尸网络项目

https://www.ccc.go.jp/en_index.html

5. 德国反僵尸网络咨询中心–反僵尸网络项目

https://www.botfrei.de/en/

6. 日本计算机应急响应小组（CERT）

http://www.jpcert.or.jp/english/

7. 美国CERT-了解隐藏威胁：Rootkit和僵尸网络http://www.us-cert.gov/cas/tips/ST06-001.html

8. 电信行业解决方案联盟（ATIS）http://www.atis.org/

9. 国土安全部

http://www.dhs.gov/files/programs/gc_1158611596104.shtm

10. 国土安全部-美国计算机应急准备小组（US-CERT）

http://www.us-cert.gov/

11. 国际电信联盟僵尸网络缓解工具包http://www.itu.int/ITU-

D/cyb/cybersecurity/projects/botnet.html

12. 美国商务部国家标准与技术研究院（NIST）

http://www.nist.gov/index.html

13. 商务部/国土安全部信息请求-预先向消费者发出关于僵尸网络和相关恶意软件非法使用计算机设备的自愿公司通知的模型

http://www.gpo.gov/fdsys/pkg/FR-2011-09-21/pdf/2011-24180.pdf

14. 收到的回应商务部/国土安全部信息请求的评论-提前向消费者发出关于僵尸网络和相关恶意软件非法使用计算机设备的自愿公司通知的模型

http://www.nist.gov/itl/botnetcomments.cfm

15. 邮件反滥用工作组（MAAWG.org）-行为准则

http://www.maawg.org/sites/maawg/files/news/CodeofConduct.pdf

16. M3AAWG互联网服务提供商和网络运营商最佳实践集合

http://www.maawg.org/published-documents

17. 国家漏洞数据库–国家标准技术研究院http://nvd.nist.gov/

http://isc.sans.edu/index.html

19. 影子服务器基金会

http://shadowserver.org

20. Spamhaus策略阻止列表

http://www.spamhaus.org/pbl/

21. 复合阻止列表

http://cbl.abuseat.org

22. OnGuard在线

http://www.onguardonline.gov/default.aspx

23. IETF BCP38网络入口过滤

http://tools.ietf.org/html/bcp38