February 12, 2018

Comment from the Internet Society on the National Telecommunications and Information Administration's

Request for Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats

Docket No. 180103005-8005-01

The Internet Society (ISOC) and the Online Trust Alliance (OTA), an initiative of ISOC, are pleased to submit these comments in response to NTIA's Request for Comments on Promoting Stakeholder Action against Botnets and Other Automated Threats.

In these comments, we address botnets and automated threats from two angles: the devices that could become bots (Internet of Things) and the way they could propagate over the Internet (through the global routing system). Securing both aspects - IoT and routing - is important in mitigating these threats, and requires collaborative action from multiple actors.

Addressing botnets and automated threats is a shared responsibility across all parts of the Internet ecosystem. The Internet Society and OTA are happy to see that shared responsibility reflected in the draft *Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem against Botnets* (the "Draft"), through its focus on strengthening incentives for better security practices, improving coordination and collaboration among stakeholders, and developing policy and technical solutions through open, multistakeholder processes. The goals and actions outlined in the Draft offer a

internetsociety.org
@internetsociety

Galerie Jean-Malbuisson 15,
Geneva, CH-1204 Switzerland

Tel: +41 22 807 1444
Fax: +41 22 807 1445

1775 Wiehle Ave, Suite 201,
Reston, VA 20190 USA

Tel: +1 703 439 2120
Fax: +1 703 326 9881

strong set of recommendations to promote stakeholder action against botnets and other automated threats.

To provide further incentives for implementing strong routing security and IoT security we propose that the Draft incorporate the following actions:

1. **Government should expand its use of procurement as a tool to improve security practices among network operators.**

   The Internet Society is pleased to see government procurement recommended in the Draft as a policy lever for strengthening IoT security. The federal government has significant market influence that should be leveraged to build market demand for good IoT security.

   However, the role government procurement can play in strengthening market incentives for better security should not be limited to IoT and edge devices. Procurement can also be a tool for promoting stronger routing security practices among network operators. Governments, when procuring network services, should prioritize network operators who use routing security best practices. Ingress and egress filtering (as noted in the Draft as being effective at mitigating the class of DDoS attacks that leverage IP-source address spoofing) should be the norm for network operators.

2. **Government, in collaboration with other stakeholders, should strengthen awareness and improve signaling for the level of routing security.**

   Enterprise-level demand for secure connectivity is a valuable way to improve market incentives for better routing security. Enterprises value strong routing security: In a 2017 study commissioned by the Internet Society, researchers found that network operators generally vastly underestimate the value their customers place on their broad security

positioning.[1] Some enterprise respondents indicated that they would be willing to pay more, a median of 15% more, for network services from a vendor that implemented the MANRS actions (described below), than one that was not.

However, enterprises must also be able to recognize good routing security from bad routing security to impact the market for routing security. To develop routing security as a competitive differentiator among network operators, the government in collaboration with other stakeholders should strengthen awareness and improve signaling for the level of routing security.

3. **Government, in collaboration with other stakeholders, should clarify how existing liability and consumer protection regulations apply to IoT.**

   Liability and consumer protection laws can be a strong incentive for investing in security. Responsibility for harm caused by inadequate IoT security may be hard to pinpoint. This can lead to uncertainty and difficulties in assigning responsibility post-incident and compensating those affected. Without clear up-front liability, users are often the ones who pay the price for poor IoT security. Government should provide clarity as to how existing liability and consumer protection laws apply to IoT.

At the Internet Society, we use two sets of principles that guide our approach to routing and IoT security: the OTA IoT Trust Framework and the Mutually Agreed Norms for Routing Security (MANRS).

The **OTA Internet of Things Trust Framework**[2] ("the Framework") is a set of core of security, privacy and sustainability principles. The Framework offers a

[1] MANRS Project Study Report https://www.routingmanifesto.org/wp-content/uploads/sites/14/2017/10/MANRS-451-Study-Report.pdf

[2] ISOC IoT Trust Framework: https://otalliance.org/initiatives/internet-things

holistic approach to IoT trust, addressing the interconnected areas of IoT security, privacy and product lifecycle, at each part of the IoT ecosystem. By limiting the ease with which botnets can grow, IoT security plays an important role in addressing botnets. The Framework can serve as both a strong foundation and model for similar or complementary efforts to address the spread of botnets and other automated threats.

We invite NIST to consider the principles in the Framework in connection with Action 1.1 ("… establish broadly accepted baseline security profiles for IoT devices in home and industrial applications, and promote international adoption through bilateral arrangements and the use of international standards…"). The Framework may also be helpful for Action 1.4 ("… collaborate to ensure existing best practices, frameworks, and guidelines relevant to IoT, as well as procedures to ensure transparency, are more widely adopted across the digital ecosystem … ").

The **Mutually Agreed Norms for Routing Security (MANRS)**, a set of voluntary principles, guides our approach to routing security. MANRS comprises four concrete actions (filtering, anti-spoofing, coordination, and global validation) for network operators to take to help eliminate common routing issues and attacks, increase global adoption of best practices, and decrease the likelihood of future routing incidents on their networks. We invite NTIA to consider the MANRS principles in connection with Action 2.5 ("… work with U.S. and global infrastructure providers to expand best practices on network traffic management across the ecosystem …").

About the Internet Society and Online Trust Alliance

The Internet Society is a global not-for profit organization committed to the open development, evolution and use of the Internet for the benefit of all people throughout the world. Working in partnership with our global community, comprised of nearly 110,000 members, 130 chapters and special interest groups, as well as 149 organizational members. The Internet Society

is also the organizational home of the Internet Engineering Task Force (IETF) and the Online Trust Alliance (OTA).

OTA is an initiative within the Internet Society with a mission to enhance online trust, empower users' innovation through convening multi-stakeholder initiatives, and to develop and promote best practices, ethical privacy practices and data stewardship.