Billing Code 3510-60-P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

170602536-7536-01

RIN 0660-XC035

Promoting Stakeholder Action Against Botnets and Other Automated Threats

AGENCY: National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Notice; Extension of Comment Period.

SUMMARY: In response to requests for additional time, the Department of Commerce is extending the closing deadline for submitting comments to a request for public comments entitled ''Promoting Stakeholder Action Against Botnets and Other Automated Threats.'' In the request for comment, the NTIA seeks broad input from all interested stakeholders — including private industry, academia, civil society, and other security experts — on ways to improve industry's ability to reduce threats perpetuated by automated distributed attacks, such as botnets, and what role, if any, the U.S. Government should play in this area. Through this notice, the Department extends the comment period to July 28, 2017.

DATES: Comments are due on July 28, 2017, at 5:00 p.m. Eastern Daylight Time (EDT).

ADDRESSES: Written comments may be submitted by email to counter_botnet_RFC@ntia.doc.gov. Written comments also may be submitted by mail to the National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, N.W., Room 4725, Attn: Evelyn L. Remaley, Deputy Associate Administrator, Washington, DC 20230. For more detailed instructions about submitting

comments, see the "Instructions for Commenters" section of SUPPLEMENTARY INFORMATION.

FOR FURTHER INFORMATION CONTACT: Megan Doscher, tel.: (202) 482-2503, email: mdoscher@ntia.doc.gov, or Allan Friedman, tel.: (202) 482-4281, email: afriedman@ntia.doc.gov, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, NW, Room 4725, Washington, DC 20230. Please direct media inquiries to NTIA's Office of Public Affairs, (202) 482-7002, or at press@ntia.doc.gov.

SUPPLEMENTARY INFORMATION:

Background: The open and distributed nature of the digital ecosystem has led to unprecedented growth and innovation in the digital economy. However, it has been accompanied by risks that threaten to undermine that very ecosystem. These risks take many forms online, with different combinations of threats, vulnerabilities, and affected parties from those in the physical world. The President has directed the Departments of Commerce and Homeland Security to jointly lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the Internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks.[1] This RFC focuses on automated, distributed attacks that affect large sets of victims, and that put the broader network and its users at risk. These types of attacks have been a concern since the early days of the Internet,[2] and were a

[1] *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Exec. Order 13800, 82 FR 22391 (May 11, 2017).

[2] *See generally United States v. Morris*, 928 F.2d 504 (2d Cir. 1991) (discussing one of the first known computer worms to spread across the Internet).

regular occurrence by the early 2000s.[3] Automated and distributed attacks, particularly botnets due to their ability to facilitate high-impact disruption, form a threat that is bigger than any one company or sector. Botnets are used for a variety of malicious activities, but distributed denial of service (DDoS) attacks, which can overwhelm other networked resources, are a critical threat and developing collaborative solutions to prevent and mitigate these attacks is a priority. As new scenarios emerge, including those exploiting a new generation of connected devices (so called "Internet of Things" (IoT) devices), there is an urgent need for coordination and collaboration across a diverse set of ecosystem stakeholders. Please see the original notice (82 FR 27042 (June 13, 2017)) for more detailed questions to which NTIA is inviting feedback on this subject. The notice is available on NTIA's website at https://www.ntia.doc.gov/federal-register-notice/2017/rfc-promoting-stakeholder-action-against-botnets-and-other-automated-threats.

The original deadline for submission of comments was July 13, 2017. With this notice, NTIA announces that the closing deadline for submission of comments has been extended until July 28, 2017, at 5:00 p.m. EDT.

Instructions for Commenters: NTIA invites comment on the full range of issues that may be presented by this inquiry, including issues that are not specifically raised in the above questions. Commenters are encouraged to address any or all of the above questions. Comments that contain references to studies, research, and other empirical data that are not widely published should include copies of the referenced materials with the submitted comments.

Comments submitted by email should be machine-readable and should not be copy-protected. Comments submitted by mail may be in hard copy (paper) or electronic (on CD-ROM

[3] *See* Nicholas C. Weaver, *Warhol Worms: The Potential for Very Fast Internet Plagues, Int'l Computer Science Inst.* (Aug. 15, 2001), http://www1.icsi.berkeley.edu/~nweaver/papers/warhol/warhol.html.

or disk). Responders should include the name of the person or organization filing the comment, as well as a page number on each page of their submissions. All comments received are a part of the public record and will generally be posted on the NTIA website, https://www.ntia.doc.gov, without change. All personal identifying information (for example, name, address) voluntarily submitted by the commenter may be publicly accessible. Do not submit confidential business information or otherwise sensitive or protected information. NTIA will accept anonymous comments.

Dated: June 19, 2017.

_____

Kathy Smith,
Chief Counsel, National Telecommunications and Information Administration.

[FR Doc. 2017-13034 Filed: 6/21/2017 8:45 am; Publication Date: 6/22/2017]