BILLING CODE: 3510-60-P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

[Docket No. 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, request for public comment.

SUMMARY: The National Telecommunications and Information Administration (NTIA), on behalf of the Department of Commerce (Department), is requesting comment on actions that can be taken to address automated and distributed threats to the digital ecosystem as part of the activity directed by the President in Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." Through this Request for Comments (RFC), 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.

DATES: Comments are due on or before 5 p.m. Eastern Time on [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

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 NW, 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.

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

These types of attacks have been a concern since the early days of the Internet,[2] and were a 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.

As part of this effort, the Department will also host a public workshop at the National Institute of Standards and Technology's National Cybersecurity Center of Excellence on July 11-12, 2017, entitled, "Enhancing Resilience of the Communications Ecosystem." Outputs from this workshop will also help to guide implementation activities related to the President's Executive Order. More information about the workshop will be available on the NIST website at: www.nist.gov.

The Federal government has worked with stakeholders in the past to address new threats as they arise. Previous efforts include the White House-led Industry Botnet Group[4] (which led to

---

[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).

[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.

[4] U.S. Dep't of Commerce, *White House Announces Public-Private Partnership Initiatives to Combat Botnets* (May 30, 2012), http://2010-2014.commerce.gov/news/press-releases/2012/05/30/white-house-announces-public-private-partnership-initiatives-combat-b.html.

an Anti-Botnet Code of Conduct[5]), the Communications Security, Reliability and Interoperability Council's (CSRIC) reports on ISP Network Protection Practices[6] and Remediation of Server-Based DDoS Attacks,[7] as well as the active and ongoing work by the Department of Justice and its many partners on attacking and "sink-holing" the infrastructure supporting these threats.[8] These initiatives, and others like them, underscore the need for active collaboration between the public and private sectors.

The Department has played an important role in facilitating engagement around cybersecurity between public policy interests and the innovative force of the private sector. The Department was tasked to work with industry to develop a framework for use by U.S. critical infrastructure to improve cybersecurity practices,[9] leading to NIST's Cybersecurity

---

[5] Working Group 7 – Botnet Remediation, Communications Security, Reliability and Interoperability Council III, *Final Report, U.S. Anti-Bot Code of Conduct (ABC) for Internet Services Providers (ISPs)*, Barrier and Metric Considerations (Mar. 2013), https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf.

[6] Working Group 8, Communications Security, Reliability and Interoperability Council I , *Final Report, Internet Service Provider (ISP) Network Protection Practices* (Dec. 2010), http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf.

[7] Working Group 5, Communications Security, Reliability and Interoperability Council IV Working Group 5, *Final Report, Remediation of Server-Based DDoS Attacks* (Sept. 2014), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG5_Remediation_of_Server-Based_DDoS_Attacks_Report_Final_(pdf)_V11.pdf.

[8] *See, e.g.*, U.S. Dep't of Justice, *Avalanche Network Dismantled in International Cyber Operation* (Dec. 5, 2016), https://www.justice.gov/opa/pr/avalanche-network-dismantled-international-cyber-operation.

[9] *Improving Critical Infrastructure Cybersecurity*, Exec. Order 13636, 78 FR 11737 (Feb. 12, 2013).

Framework.[10] Other initiatives include Green Papers developed by the Department built on industry input on cybersecurity[11] and IoT.[12] NTIA has also convened multistakeholder processes to identify consensus-based voluntary solutions on security vulnerability disclosure[13] and IoT security patching and upgradability.[14]

The private sector is also playing a key role in tackling botnets. Internet service providers in the United States and around the world have been experimenting with how to notify customers that their devices may be involved in an attack. Standards bodies have offered guidance on how to mitigate some styles of attacks.[15] Technology providers are innovating around tools to protect resources from DDoS attacks. Application and software manufacturers

---

[10] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[11] Internet Policy Task Force, U.S. Dep't of Commerce, *Cybersecurity, Innovation and the Internet Economy* (June 2011), https://www.nist.gov/sites/default/files/documents/itl/Cybersecurity_Green-Paper_FinalVersion.pdf.

[12] Internet Policy Task Force & Digital Economy Leadership Team, U.S. Dep't of Commerce, *Fostering the Advancement of the Internet of Things* (Jan. 2017), https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

[13] NTIA, *Multistakeholder Process: Cybersecurity Vulnerabilities*, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities (last visited May 17, 2017).

[14] NTIA, *Multistakeholder Process: Internet of Things (IoT) Security Upgradability and Patching*, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security (last visited May 17, 2017).

[15] *See, e.g.*, P. Ferguson & D. Senie, *Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing*, Internet Engineering Task Force (May 2010), https://www.ietf.org/rfc/rfc2827.txt.

are working to eliminate exploitable vulnerabilities. This community has worked hard to address the threats over the last decade.

The cybersecurity challenge is particularly vexing because it involves adaptive adversaries. Existing tools, institutions, and initiatives are critical, but we must acknowledge that the threat continues to evolve, and more progress is needed, at an accelerated rate, to address the current landscape. The DDoS attacks launched from the Mirai botnet in the fall of 2016, for example, reached a level of sustained traffic that overwhelmed many common DDoS mitigation tools and services, and even targeted a Domain Name System (DNS) service that was a commonly used component in many DDoS mitigation strategies.[16] This attack also highlighted the growing insecurities in – and threats from – consumer-grade IoT devices. As a new technology, IoT devices are often built and deployed without important security features and practices in place.[17] The issue is not the particular botnet, or the particular target, but the risks posed by botnets of this size and scope, and the expected innovation and increased scale and sophistication of future attacks. Meanwhile, old threats continue to evolve. The WannaCry ransomware that threatened to destroy the data of thousands of individuals and organizations, including hospitals, did not initially involve a botnet. It was spread by a worm-like mechanism

[16] U.S. Computer Emergency Readiness Team, *Alert (TA16-288A): Heightened DDoS Threat Posed by Mirai and Other Botnets*, https://www.us-cert.gov/ncas/alerts/TA16-288A (last revised Nov. 30, 2016).

[17] National Security Telecommunications Advisory Committee, *Report to the President on the Internet of Things* (Nov. 19, 2014), https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf.

similar to attacks of 15 years ago. However, criminals were later observed using the Mirai botnet to attack a key defense against the WannaCry ransomware.[18]

It is difficult to predict what the next significant attack vector will be, but that should not preclude taking steps to mitigate the potential impact of those that are known. Left unchecked, without meaningful progress, these new classes of automated and distributed attacks could be a serious risk to the entire ecosystem. Since poorly considered action would likely create significant unnecessary costs and unintended consequences, substantial, carefully considered action must be considered, and it is most likely to be effective and efficient if built on engagement from all stakeholders across the ecosystem.

Request for Comments

The goal of this RFC is to solicit informed suggestions and feedback on current, emerging, and potential approaches for dealing with botnets and other automated, distributed threats and their impact. The Department is interested in comments that address all aspects of this issue, but particularly those that address two broad approaches where substantial progress can be made:

- Attack Mitigation: Minimizing the impact of botnet behavior by rapidly identifying and disrupting malicious behaviors, including the potential of filtering or coordinated network management, empowering market actors to better protect potential targets, and reducing known and emerging risks.
- Endpoint Prevention: Securing endpoints, especially IoT devices, and reducing vulnerabilities, including fostering prompt adoption of secure development practices, developing practical plans to rapidly deal with newly discovered vulnerabilities, and

[18] *See* Andy Greenberg, *Hackers are Trying to Reignite Wannacry with Nonstop Botnet Attacks*, Wired (May 19, 2017), https://www.wired.com/2017/05/wannacry-ransomware-ddos-attack/.

supporting adoption of new technology to better control and safeguard devices at the local network level.

Respondents are invited to respond to some or all of the questions below:

1. What works: What approaches (e.g., laws, policies, standards, practices, technologies) work well for dealing with automated and distributed threats today? What mechanisms for cooperation with other organizations, either before or during an event, are already occurring?
2. Gaps: What are the gaps in the existing approaches to dealing with automated and distributed threats? What no longer works? What are the impediments to closing those gaps? What are the obstacles to collaboration across the ecosystems?
3. Addressing the problem: What laws, policies, standards, practices, technologies, and other investments will have a tangible impact on reducing risks and harms of botnets? What tangible steps to reduce risks and harms of botnets can be taken in the near term? What emerging or long term approaches may be promising with more attention, research, and investment? What are the public policy implications of the various approaches? How might these be managed, balanced, or minimized?
4. Governance and collaboration: What stakeholders should be involved in developing and executing policies, standards, practices, and technologies? What roles should they play? How can stakeholders collaborate across roles and sectors, and what should this collaboration look like, in practical terms?
5. Policy and the role of government: What specific roles should the Federal government play? What incentives or other public policies can drive change?

6. International: How does the inherently global nature of the Internet and the digital supply chain affect how we should approach this problem? How can solutions explicitly address the international aspects of this issue?
7. Users: What can be done to educate and empower users and decision-makers, including enterprises and end consumers?

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 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 8, 2017.

Leonard Bechtel, Chief Financial Officer and Director of Administration, Performing the non-exclusive duties of the Assistant Secretary for Communications and Information, National Telecommunications and Information Administration.