ACM US Public Policy Council

Association for Computing Machinery
US Public Policy Council (USACM)

usacm.acm.org
facebook.com/usacm
twitter.com/usacm

February 12, 2018

By Electronic Mail

Evelyn L. Remaley, Deputy Associate Administrator
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

Re: Promoting Stakeholder Action Against
Botnets and Other Automated Threats
Docket No. 180103005-8005-01

Dear Ms. Remaley:

Thank you for the opportunity to comment on the draft *Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* (Report), 83 Fed. Reg. 1342 (January 11, 2018), in the above-referenced docket. We provide responses to specific questions below.

With more than 100,000 members, ACM (the Association for Computing Machinery) is the world's largest educational and scientific computing society, uniting computing educators, researchers, and professionals to inspire dialogue, share resources, and address the field's challenges. These comments were developed by the ACM U.S. Public Policy Council (USACM), which serves as the focal point for ACM's interaction with the U.S. government in all matters of U.S. public policy related to information technology. The membership of the ACM U.S. Public Policy Council is comprised of computer scientists, educators, researchers, and other technology professionals. The following comments represent the views solely of USACM.

Responses to Specific Questions

1. *The Ecosystem:* Is the Report's characterization of risks and the state of the current internet and communications ecosystem accurate and/or complete? Are there technical details, innovations, policy approaches, or implementation barriers that warrant new or further consideration?

The Report rightly notes (p. 16) that use of pirated software exacerbates the problem of distributed threats by enabling attackers to exploit systems with relative ease. However, the Report leaves the impression that this constitutes an insoluble problem, also asserting that it is unreasonable to expect vendors to support unlicensed software.

Yet, if the percentages of pirated software cited in the Report are accepted (noting such statistics are open to dispute), the attack surface represented by these systems is so broad that it is simply impossible to address the threat effectively without addressing this specific vector. It is instructive that although for many years Microsoft was the largest victim of illegal copying, it has long had a policy of making security-critical updates available for *all* copies of Microsoft software whether or not legally obtained.

The legitimate interests of software vendors and those of society must somehow be reconciled so that those running pirated software are not rewarded, while the dangers to society are nonetheless mitigated. Further, this must be accomplished without introducing significant new risks for legitimate users, including ones related to privacy.

Squaring this circle will not be easy. We thus recommend that the Report make clear that it is essential that proven approaches be replicated while innovative approaches are researched and developed. Doing nothing, in our view, is not an option.

2. *Goals:* Are the Report's stated goals appropriate for achieving a more resilient ecosystem? Do the actions support the relevant goals? In aggregate, are the actions sufficient to significantly advance the goals?

While tools have an undeniably important role to play in reducing software vulnerabilities, we are concerned that the Report presents them as an isolated and independent means of addressing vulnerabilities. Rather, they must be viewed as simply one component of software engineering and as inherently integral to, and interdependent upon, system development life cycles (SDLCs). Consistent development of secure software across different areas of application is broadly a function of a discipline of software engineering that leverages different SDLCs as appropriate.

While the Report does indirectly reflect the importance of SDLC activities (p. 25), it seems to assume that these invariably are purely sequential. There are, however, a wide variety of SDLCs and that fact has important implications for tool selection and use. Tools effective in the context of one SDLC may be less effective in others, and any tool is less effective when its application is not integrated into a software engineering discipline. We urge that the Report explicitly endorse a more holistic approach, one in which tools are mixed and matched to support integrated approaches to engineering secure software.

We are also concerned about the role described in the Report for the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The objective of developing a CSF profile for Enterprise Distributed Denial of Service (DDoS) Prevention and Mitigation (p. 29), while understandable, appears inconsistent with the nature of such profiles. In practice, CSF profiles tend to be driven by specific missions and domains, not by specific types of threats as the Report suggests. We recommend, therefore, that the Report detail the basis for conceptualizing a CSF profile in this way. Alternatively, we suggest that the use of CSF profiles be repurposed in the Report to support the sector-specific security requirements commendably called for in Action 4.3 (p. 34).

Finally, however inadvertently, minimizing the importance of key issues may result in a concomitant de-emphasis on their solutions. Accordingly, we urge a more explicit focus in the Report on three additional issues. Specifically, we recommend:

- In-depth treatment of the potential privacy impacts of measures, such as observation of device-specific behavior via IPv6 (Action 3.4, p. 32) and streamlined information sharing (Action 4.1, p. 33). While we appreciate the broad caveat that Internet user privacy must be protected, the potential for these and other measures to seriously compromise privacy, we believe, deserves greater emphasis in the Report.
- Enhanced focus on the difficulty of re-architecting networks (Action 3.3, p. 32). One possible response to the difficulty of re-architecting networks worth exploring would be to move toward more flexible software-defined networking (SDN). We note, however, that the resulting change in the economics of networking necessarily would mean a change in the economics of security, as well.[1]
- Increased recognition of the challenge of developing an Internet of Things (IoT) product assessment and awareness mechanism (Action 5.1, p. 36) that is "lighter weight" than those, such as Energy Star, applied to products in less complex contexts.

Thank you again for the opportunity to comment on the Report. ACM's U.S. Public Policy Council would be pleased to provide additional information or answer any questions concerning these comments that you may have. Please contact Adam Eisgrau, ACM's Director of Global Policy and Public Affairs, at eisgrau@acm.org or 202-580-6555 if USACM may be of further assistance.

Sincerely,

Stuart Shapiro

Stuart Shapiro, Chair

[1] Use of SDN could provide improvements in filtering at the endpoints and in network flows thus enabling more effective defenses against DDoS or better botnet identification and isolation. However, an SDN controller, for example, can also present new security risks as a consequence of its flexibility. SDN also creates challenges for the operation of basic tools, as exfiltrated data and subverted control messages could be in one flow while traditional investigation and verification protocols are sent elsewhere. In other words, SDN alters the characteristics of the attack surface in both positive and negative ways, enabling botnet isolation by defenders, but also botnet obfuscation by attackers.