KAISER PERMANENTE®

Kaiser Foundation Health Plan
Program Offices

February 12, 2018

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

Submitted to *counter_botnet@list.commerce.gov*

RE: *Request for Comment on Promoting Stakeholder Action Against Botnets and Other Automated Threats*

Kaiser Permanente commends the Administration on its *Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* (Report*)*. We offer the following comments including our observations on its six principal themes, four technical domains, five goals, and associated action items.

Principal Themes

We agree with the six principal themes overall, and we suggest adding a seventh theme: consumer (and other stakeholders) perceptions around security and their role in mitigating risk.

The potential for consumer devices to be vulnerable to botnets appears to be much higher than for most enterprise/business devices where there is likely to be installed technology focused on prevention, detection, and remediation, particularly within larger or hosted environments. Adding a consumer/stakeholder principal theme would relate to and reinforce the discussion in the Technology Domains (e.g., under *Home and Small Business Networks*).

Technical Domains

The technical domains appropriately describe a broad range of attack vectors. We recommend emphasizing the role of social media in spreading botnets, possibly by expanding the brief discussion currently in the *Background* section.

We also recommend removing infrastructure, because it is too generic to adequately describe a connection to other domains, nor does it represent a threat vector in the same way that enterprise networks, edge devices, and home and small business networks do.

One Kaiser Plaza
Oakland, CA 94612

The definition of edge devices should be expanded to include devices "that operate outside of a corporate location or Data Center, and close to where data sources exist."

Policy Domains

We appreciate the existing policy domains and recommend adding a policy domain for configuration management. This would include secure configurations for hardware and software, and patch management. Explicitly identifying these activities would impose corresponding responsibilities to perform these activities as part of system/device security hygiene.

Current Status of the Ecosystem and Vision for the Future

Embedded in the narrative are several ways to protect against botnets (e.g., web-filtering services; changing browsers and/or operating systems; disabling scripts; using intrusion detection systems/intrusion prevention systems (IDS/IPS); protecting against user-generated context; deploying remediation tools as well as disabling noncritical software features; implementing hardware roots of trust; trusted execution technologies). Though unlikely to be included in the current version of the Report, we recommend that future guidance on botnet resilience should include an anthology of appropriate controls by theme and/or domain.

Kaiser Permanente strongly supports integration of the NIST Cybersecurity Framework (CSF) into federally-generated guidance; for example, in the *Vision for Enterprise Networks*. We recommend, however, providing the Report footnotes in a reference section regardless of technical domain. As an extension to that compendium of references, it would be beneficial to add technical guidance on some of the technology components and/or solutions (e.g., Regional Internet Register (RIR), Border Gateway Protocol (BGP), IPv4 vs. IPv6, and DNS resolvers), and to explain why these would be appropriate remediation actions.

Goals and Actions

Goal #1: Identify a clear pathway toward an adaptable, sustainable, and secure technology marketplace

We support establishing baseline security profiles, not limited to Internet of Things (IoT) devices and industrial applications. The developers of applications such as content sharing platforms, Enterprise File Synchronization and Sharing (EFSS) platforms, and common applications (e.g., email, social media, mobile applications), should also be responsible for developing secure hardware and software profiles that mitigate attacks. Thus, we recommend establishing more comprehensive baseline security profiles that apply to developers of applications as well as underlying hardware platforms.

We support the adoption and use of international standards. Given the lifecycle of most Standards Development Organizations (SDOs), Kaiser Permanente encourages partnerships with SDOs that use agile development methodologies instead of the linear, waterfall-style multi-year development cycle employed by the many SDOs. We also recommend greater involvement by

NIST in U.S. standards development to help ensure that the standards developed are open standards that are readily available.

Kaiser Permanente recommends adding a goal to minimize or eliminate commercial vulnerabilities that enable nation-state backed hackers to launch botnet attacks. Eliminating these vulnerabilities will help create and maintain a more secure technology marketplace. We also support expedited development processes and deployment of innovative technologies for prevention and mitigation of distributed threats.

Goal #2: Promote innovation in the infrastructure for dynamic adoption to evolving threats

NIST is highly effective and well-recognized as an excellent convener of public-private partnerships. Establishing and mentoring communities of interest to encourage and facilitate information sharing is discussed in the *Legal Landscape* section. Leveraging the *Cybersecurity Information Sharing Act of 2015* (CISA) as well as the Communications Information Sharing and Analysis Center (ISAC) can provide mechanisms to help identify, protect, detect, and mitigate these types of attacks. We encourage including other ISACs outside the communication sector to help ensure a broader distribution of information.

We support the recommendation to develop a CSF profile for *Enterprise DDoS* (Distributed Denial of Service) *Prevention and Mitigation* under the auspices of NIST; we also support an aggressive timeline for providing such a profile; we agree with the action item for the federal government to create market incentives for early adopters to help ensure the success of this effort. Kaiser Permanente also encourages consideration of market incentives for both adopters and developers of these technologies.

Goal #3: Promote innovation at the edge of the network to prevent, detect, and mitigate bad behavior

Expanding current product development and standardization efforts is an important goal for the networking industry. However, product and standards development can be costly to an organization. Clearly articulated and well-documented mechanisms to encourage these efforts will help to promote further innovation.

Goal #4: Build coalitions between the security, infrastructure, and operational technology communities domestically and around the world

The concept of DevSecOps[1] has been maturing in the technology communities for the last several years as the concept that security is everyone's responsibility becomes common wisdom. The Report extends law enforcement's access to information but does not clarify or delineate boundaries for how that information will be used. Sharing information that might place blame versus responsibility can continue to inhibit information sharing because of the reputational risks and potential legal liability.

[1] http://www.zdnet.com/article/devsecops-what-it-is-and-how-it-can-help-you-innovate-in-cybersecurity/

It is our understanding that "fast flux hosting" is a technique used by botnets to hide phishing and malware delivery sites behind a changing network environment of compromised hosts acting as proxies. Including "fast flux hosting" in this goal suggests that the Report promotes voluntary adoption and broader implementation without providing a roadmap for achieving this outcome.

Kaiser Permanente supports promoting collaboration among stakeholders and recommends providing guidance about both the collaborative process and specific measures to detect and defend against "fast flux hosting."

Goal #5: Increase awareness and education across the ecosystem

In addition to educating the end user, continued emphasis on secure software development practices in computer science, information technology, and engineering programs is important.

There are many standards and guidelines available that promote sound engineering practices. Kaiser Permanente supports these practices and encourages ongoing dialogue with institutions of higher education to encourage integration into their curriculum. We support adopting a home IoT device security profile believing that the manufacturers, developers, and distributors of these devices are more likely to support voluntary participation.

Conclusion

Kaiser Permanente appreciates your willingness to consider our comments on strategies, standards, and technologies to improve the critical infrastructure's botnet resiliency. Please contact me at (510)-271-5639 (email: jamie.ferguson@kp.org) or Beth Pumo at (303) 246-8258 (email: beth.pumo@kp.org) with any questions or concerns.

Sincerely,

Jamie Ferguson
Vice President
Health IT Strategy and Policy