Before the:
National Telecommunications and Information Administration
United States Department of Commerce

Public Comments on Promoting Stakeholder
Action Against Botnets and Other
Automated Threats

Docket No. 170602536-
7536-01.

COMMENTS OF THE INTERNET INFRASTRUCTURE COALITION

Submitted by:

Christian Dawson,
Executive Director

i2Coalition
718 7th Street, NW
2nd Floor
Washington, DC 20001
(202) 780-7237

July 28, 2017

I. INTRODUCTION

Thank you for the opportunity to present our comments regarding the National Telecommunications and Information Administration's (NTIA) "Request for Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats."

The Internet Infrastructure Coalition (i2Coalition) was founded in 2012 by a diverse group of Internet infrastructure companies to be an effective advocate for those entities that provide the services necessary for the Internet to function and help keep the Internet open, free, and secure. Since our founding, we have made great strides on initiatives that affect our industry and the Internet as a whole—including on issues regarding online threats—and have grown to become the leading voice for the Internet infrastructure community and relevant stakeholders.

Our 90-plus members include web hosting companies, data centers, domain registrars, security companies, software vendors, and other infrastructure-related businesses. Our members range in size from household names such as Google and GoDaddy to small businesses such as HandyNetworks, based in Colorado, and Open Spectrum Inc., based in North Carolina.

II. EXECUTIVE OVERVIEW

Botnets present an understandable concern for the federal government, as they represent a threat to the Internet's infrastructure. However, it is important to understand clearly that there will never be a threat-free Internet. In an environment where both the Internet infrastructure and threat ecosystems are constantly evolving, abuse is a problem that will never actually be "solved," only mitigated. When faced with security breaches, our community—and the relatively mature infrastructure ecosystem we've created and maintain—builds in more resiliency and increases redundancy. Security is an evolutionary practice that requires an adaptive, market-driven process for governance. Each new market must evolve before it achieves effective security and stability by design. The ecosystem has natural incentives to continually improve security. Companies are incentivized to do good work and fight threats, because companies that fail face market consequences, and those that succeed reap market success. Fostering this process by trusting the natural evolution of the market, and engaging in its continued natural technical progression, is the most effective way to help minimize the threat landscape at the governmental level.

III. IDENTIFICATION OF CORE CONCERN

The Internet infrastructure community's most significant concern is that NTIA will focus its attention on two concentrated groups—Internet carriers and the DNS community of registries and registrars. Our ecosystems have cybersecurity mitigation paths that have been developed by our technical communities. They are already working—and working well. We strongly encourage NTIA to focus on solutions that address the source of the problem, and that identify the natural, self-healing ecosystem that has led to a mostly stable and secure Internet.

IV. OVERVIEW OF CURRENT THREAT LANDSCAPE

The Internet infrastructure ecosystem has been on the front lines of battling Internet abuse for decades—we are continually finding and patching vulnerabilities. As a result, a mature ecosystem has developed to identify and mitigate attacks, one that systemically evolves to meet and match threats, including botnets.

However, we must acknowledge that while the last two years have seen some significant service disruptions, given the constantly evolving threat vectors, the relatively small number of successful, large-scale attacks can and should be seen as a market success. But, largely due to issues of scale from the rapid growth of Internet-connected devices, the cybersecurity battle is increasingly challenging, with vast numbers of potential threat vectors.

Over the course of the Internet's history, there have been other market sectors that have caused the kinds of cybersecurity issues we are seeing from the Internet of Things marketplace. With time, the ecosystem always self-corrects, and those threat centers minimize. We have seen this over the past decade, with vast improvements in the handling of Distributed Denial of Service (DDoS) attacks. Internet-connected, Operating System (OS)-level system exploits were driving massive DDoS attacks, but in each case the ecosystem evolved quickly to curtail the damage done by these devices. To address these attacks, we have also seen greatly improved patching and redundancy practices.

Open, market-driven standards help. DMARC is used to mitigate spam. Though it is not a botnet tool, it is one example of the many ways the market can, will, and does come together to effectively manage threat mitigation. Open Threat Exchange (OTX) and the OASIS Organization are excellent examples of the community coming together to share intelligence to mitigate botnet abuse. Ecosystems such as these are where market-driven standards are birthed, nurtured, and eventually deployed.

The industry is facing these issues aggressively and collaboratively, through such actions as publishing best practices on botnet mitigation, including those developed by nearly a dozen organizations: the Internet Engineering Task Force (IETF), North American Network Operators Group (NANOG), Anti-Phishing Working Group (APWG), Communications Security, Reliability and Interoperability Council (CSRIC), European Network and Information Security Agency (ENISA), IT Association for Telecommunications (ETIS), Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), Cloud Security Alliance (CSA), and Online Trust Alliance (OTA).

The Internet infrastructure community's input in these forums attempts to carefully balance solutions in ways that allow them to respond to threats while still navigating the openness needed for robust innovation. Constraints are required for stability and security. Rather than attempting to predetermine the outcome, the federal government needs to aid this process, and let the ecosystem's evolutionary and maturation processes work to develop solutions to current and emerging threats. In short, the most effective way for the federal government to assist the marketplace is to allow the competitive market to continue to operate without new regulation.

In summary, the Internet infrastructure ecosystem is already fighting effectively within its technical communities on automated online threats, including botnets. We will continue to do so because it is in our interest and those of our customers and users.

V. SPECIFIC RECOMMENDATIONS

We believe there are specific measures NTIA can and should take to help foster market-driven evolution of the Internet ecosystem—and most especially nascent markets like the Internet of Things—to fight automated online threats, including botnets. Our recommendations are as follows:

- Examine market-driven ways to expedite the evolution of Internet of Things security.

    - The unified Android toolkit is an example of an apparatus that greatly aided in the security of mobile devices, as people were developing for the great mobile market expansion. As the Internet ecosystem hones and develops similar centralized development resources for the Internet of Things, the federal government could find ways to encourage the inclusion of security by design.

    - Mass deployment of IETF BCP38 and BCP84 would significantly aid in Internet infrastructure readiness to endure botnet attacks. Once a critical mass of networks has deployed BCP38 and BCP84, it will significantly increase the resiliency of the Internet as a whole. Market incentives for adoption could be explored.

- Investigate common principles for the Internet of Things in regards to “security by design.” Two obvious considerations would be “no default passwords” and “built-in automated patching,” but this is by no means an exhaustive list. The investigation should focus attention in part on the use of existing, proven security protocols and networks, e.g., the DNS and DNSSEC. There is a shared responsibility throughout the Internet infrastructure ecosystem to deal with botnets that flow from poor IoT security, but since it places a particular burden on the Internet infrastructure’s device and OS portions of the ecosystem, attention needs to be paid to solidifying and pushing common principles rather than assume users, and indeed IoT designers, can figure out the right paths on their own.

- Refrain from imposing new federal requirements at the Internet infrastructure level.

- Expand the register RFC to include a critical issue: virtual network mapping on the substrate network. This is often what enables a threat. In most of the DDoS cases, it is address spoofing that is the cause. Assisting industry in finding ways to deal with the critical issue of problem substrate deserves attention.

- The federal government could be far more aligned with the efforts of the technical communities. Ideally, representatives of government tasked with keeping Americans safe should engage with the Internet technical community in order to see, understand, and appreciate the functioning ecosystem at work. The technical elements of the government are already present at places like NANOG, IETF, and M3AAWG. The policy-focused elements of the government should be involved as well, so they can also be aware of how this evolution is proceeding. It would be helpful for not just NIST at NANOG to engage, but also for NTIA to do so, in order for all relevant stakeholders to see the ecosystem working.

- The federal government should also continue its role of fostering innovation by holding workshops, seminars/webinars, and creating industry-led working groups to keep communication open and steady.

Thank you again for this opportunity to present our thoughts. If you have comments, concerns, or questions about this particular response, i2Coalition looks forward to hearing from you.

Moreover, the i2Coalition stands ready to continue to be active in engaging on this critical issue, beyond our comments herein.