February 12, 2018

VIA EMAIL: counter_botnet@list.commerce.gov

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

Re: Comment of NETSCOUT Arbor

NETSCOUT Arbor submits this comment in response to the Request for Comments ("RFC") issued by the National Telecommunications and Information Administration ("NTIA") on January 11, 2018.[1] The RFC seeks input and feedback on the draft Report on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats ("Report") published by the Departments of Commerce and Homeland Security.[2] The Report identifies a number of actions organizations can take to better defend against and respond to botnet attacks, including implementing more effective mitigation strategies and improving visibility within their networks. It also highlights the role the federal government can play in realigning market incentives, and it calls for greater cooperation by all stakeholders, underscoring the need for such cooperation to occur on a global scale.

NETSCOUT Arbor supports the themes and goals set out in the draft Report. NETSCOUT Arbor agrees that the threat posed by Distributed Denial of Service ("DDOS") botnet attacks is significant and growing. It further agrees that addressing the botnet threat will require leadership from the federal government, cooperation amongst all stakeholders, and improved organizational planning, management and response to DDoS risk and mitigation efforts. Through this comment, NETSCOUT Arbor seeks to highlight the following key points:

- DDoS attacks are becoming more frequent and complex and have increasingly been focused on attacking the application-layer;
- Service providers, enterprise and government organizations need to implement more effective mitigation strategies.
- Organizations should consult the DDoS Profile developed by the Coalition for Cybersecurity Policy & Law ("Coalition") to assess their preparedness for a DDoS attack and identify areas for improvement;
- Organizations should engage in broader information sharing regarding DDoS and Botnet threats, network architectural and operational best practices, and effective use of mitigation tools;

[1] 83 Fed. Reg. 1342 (January 11, 2018) (Docket No. 180103005-8005-01).
[2] Depts. of Commerce and Homeland Security, *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* (January 5, 2018) ("*Report*")

- The federal government can play a key role in setting best practices for DDoS prevention and mitigation and realigning market incentives.

NETSCOUT Arbor appreciates the opportunity to participate in this critically important discussion. NETSCOUT Arbor submitted comments in response to the NTIA's June 13, 2017 RFC on botnets, participated in the Botnet Workshop hosted by the National Institute of Standards and Technology ("NIST"), and seeks to continue engaging with the NTIA on this important topic. As one of the top providers of network visibility and DDoS protection products, NETSCOUT Arbor has substantial experience with the growing threat presented by botnets. NETSCOUT Arbor provides network visibility, DDoS, and advanced threat protection solutions to more than 1,200 enterprise, cloud, and service provider customers in 107 countries.[3] NETSCOUT Arbor serves 90% of tier 1 service providers, 8 of the 10 largest cloud service providers, and 3 of the 5 largest social media networks.[4] This experience informs NETSCOUT Arbor's suggestions and recommendations set out in more detail below.

I. Current Threat Landscape

NETSCOUT Arbor's role as a provider of network visibility and DDoS protection products enables it to collect information about global DDoS activity. Last year, NETSCOUT Arbor observed an increasing number of DDoS attacks in 8 of the 10 most attacked countries.[5] In the United States, NETSCOUT Arbor observed the number of DDoS attacks increase by 23.3%.[6] These attacks were more sophisticated than in years past with an increasing proportion of such attacks involving multiple attack vectors.[7] In 2017, 48% of organizations that experienced a DDoS attack reported that the attack involved multiple vectors, which is up from 40% the year before. NETSCOUT Arbor also observed a shift from volumetric attacks to application-layer attacks. In 2017, 52% of DDoS attacks against organizations were volumetric, which was down from 60% of such attacks in 2016.[8] NETSCOUT Arbor saw a corresponding increase in the percentage of application-layer attacks from 25% to 32%.[9] These attacks primarily targeted the HTTP, DNS, and HTTPS application services with 73% of such attacks targeting HTTP, 69% targeting DNS, and 68% targeting HTTPS.[10]

II. NETSCOUT Arbor Supports Broader Adoption of Best Practices To Protect against Application Layer and Other Complex Attack Types

NETSCOUT Arbor agrees with the Report's conclusion that effective tools for mitigating DDoS attacks exist in the marketplace but broader implementation of best practices in terms of planning and response strategies is needed. The Report focuses on the need for more wide-

[3] Information about the types of customers to whom Arbor provides products and services is available on its website at https://www.arbornetworks.com.
[4] *Id.*
[5] *See* Netscout Arbor Atlas Attack Intelligence Findings: Top DDoS Attacked Countries of 2017, available at http://resources.arbornetworks.com/wp-content/uploads/ARBOR_ATLAS_2017Overview_Infographic.pdf.
[6] *Id.*
[7] Arbor Networks, *Insight into the Global Threat Landscape*, 87 (2017) ("*Global Threat Landscape*").
[8] *Id.* at 61.
[9] *Id.*
[10] *Id.* at 62.

spread implementation of ingress and egress filtering, broader adoption of IPv6, and improved network security.[11] NETSCOUT Arbor notes that many service providers and organizations have already implemented these tools but agrees that there is still significant room for improvement. In particular, NETSCOUT Arbor encourages the NTIA to support broader use of the Coalition's DDoS Profile. The Coalition's DDoS Profile provides a framework in which service providers and organizations can assess their current security measures and preparedness for a DDoS attack, identify their risks, and measure their progress towards their target security profile.

Amongst service providers, NETSCOUT Arbor has observed increasing implementation of NetFlow-based analysis tools, SNMP-based tools, and inline DDoS detection/mitigation tools.[12] These tools are viewed some of the most effective DDoS mitigation tools available; however, not all service providers have implemented them.[13] While 81% of service providers have adopted NetFlow-based analysis tools, only 64% of service providers have implemented SNMP-based tools and even fewer service providers, 51%, have implemented inline DDoS detection/mitigation systems.[14] However, outbound and cross-bound attacks are not monitored by 46% of service providers.[15] Although greater adoption of these tools by service providers is important, there is reason to be optimistic, as the percentage of service providers using SNMP-based tools and inline DDoS detection/mitigation systems increased substantially last year from 53% to 64% and from 42% to 51% respectively.[16]

Organizations, however, have been slow to adopt more effective DDoS prevention and mitigation tools. This has resulted in more outages and losses, with 57% of enterprise, government and education (EGE) organizations seeing their internet bandwidth saturated due to DDoS attacks, up from 42% in the previous year.[17] Over half of organizations rely on firewalls, access control lists, and IPS/WAF even though these devices are susceptible to state-exhaustion attacks.[18] Only 43% of organizations have implemented intelligent DDoS mitigation systems (IDMS) and only 33% of organizations have implemented cloud-based DDoS mitigation services or layered/hybrid DDoS protection systems despite these tools being more effective.[19] Broader adoption of these tools would improve organizations' ability to identify and mitigate DDoS attacks more rapidly.

NETSCOUT Arbor further agrees with the Report's conclusion that broader adoption of IPv6 monitoring, which enables device-specific recognition across a network, would improve resiliency against DDoS attacks. In 2017, just over a third of organizations were operating IPv6 in their environments or planning to do so while 60% of organizations provided internet-facing

[11] *Report* at 10.
[12] *Global Threat Landscape* at 8.
[13] *Id.* at 15.
[14] *Id.*
[15] *Id.* at 8.
[16] *Id.*
[17] *Id.* at 10.
[18] *Id.* at 61.
[19] *Id.* at 64.

services with IPv6 support and 65% deployed IPv6 on their private networks.[20] Unfortunately, these numbers are the same or less as what NETSCOUT Arbor observed in 2016.[21] Increased adoption of IPv6 monitoring will enable organizations to more quickly identify devices on their networks that may be infected with botnet malware and take them offline. In doing so, organizations can increase the cost of mounting botnet attacks, which will have a deterrent effect.

III. NETSCOUT Arbor Supports Improved Security Training by Academic Institutions and Organizations

NETSCOUT Arbor agrees with the Report that better security training is needed; however, such training should not be limited to secure coding practices. Better training is needed in all aspects of cybersecurity at both educational institutions and in the industry. More than half of organizations surveyed by NETSCOUT Arbor indicated that hiring and retaining skilled personnel is their most significant obstacle to building out an operational security team.[22] Better training is also needed at organizations to ensure that the responsible personnel at each organization are aware of the DDoS mitigation strategies and tools available to them and the procedures they should follow to prepare for and protect against DDoS attacks. NETSCOUT Arbor further agrees that more should be done to ensure that organizations understand which DDoS mitigation tools are most effective. Last year, firewalls and IDS/IPS were the most commonly used DDoS mitigation tools with 83% and 72% of organizations using them, respectively.[23] However, over half of organizations using these tools experienced a failure during a DDoS attack.[24] Because state-based security devices, like firewalls and IPS devices are vulnerable to state-exhaustion attacks, they should be used primarily to supplement other DDoS mitigation technologies.[25] Promoting greater awareness of which tools are most effective is likely to increase resiliency across the industry.

NETSCOUT Arbor also supports efforts to educate organizations on the benefits of performing regular DDoS training and preparedness exercises. In 2017, NETSCOUT Arbor observed a decrease in the percentage of organizations performing DDoS defense simulations from 55% to 50%.[26] Additionally, only 32% of organizations perform quarterly incident response exercises.[27] Conducting regular exercises is an important component of ensuring organizational awareness and training on appropriate response procedures. It also provides organizations with an opportunity to assess their progress towards their target profile using the Coalition's DDoS profile.

[20] *Id.* at 69.
[21] *Id.*
[22] *Id.* at 72.
[23] *Id.* at 59.
[24] *Id.* at 61.
[25] *Id.*
[26] *Id.* at 73.
[27] *Id.*

IV. The Federal Government Can Incentivize Organizations to Adopt Best Practices

The Report concludes that market forces are misaligned with the aim of improving Internet of Things ("IoT") security, as product developers, manufacturers, and vendors are motivated more by being first to market and minimizing cost than incorporating better security features into their products.[28] It suggests that government and industry should work together to establish market transparency tools that will allow individuals purchasing IoT products to assess their comparative security.[29] The Report further suggests that the federal government should establish procurement guidelines that encourage product developers to incorporate stronger security features.[30] NETSCOUT Arbor agrees that the federal government should play an important role in realigning market incentives to focus on better security features; however, this should be done by setting appropriate standards for government agencies and through federal procurement guidelines rather than by singling out specific products as more or less secure through a market transparency solution.

As a larger participant in the marketplace, the federal government has substantial power to influence data security standards in both the public and private sectors. It can do so by setting specific data security requirements that organizations must meet to be able to sell their products or services to the federal government. It can also influence the market by setting strong security standards for government agencies. Over time, organizations are likely to voluntarily conform to these standards as best practices, as was the case with the broad adoption of the NIST Framework. NETSCOUT Arbor favors this approach over establishing a market transparency tool because it establishes clear standards for organizations to target, and it avoids identifying particular DDoS mitigation tools or products as stronger or weaker, which could result in bad actors targeting organizations that use these tools.

The Report also encourages stakeholders to work with NIST to develop a Framework profile for enterprise DDoS prevention and mitigation.[31] NETSCOUT Arbor supports this recommendation and encourages NTIA and NIST to use the DDoS Profile developed by the Coalition as a starting point for this effort.[32] NETSCOUT Arbor further encourages NTIA to promote broad adoption of the resulting profile by federal agencies and incorporating it into federal procurement guidelines. This will encourage private companies to use the profile to improve their own security measures, which will make the ecosystem more resilient against botnet attacks.

V. NETSCOUT Arbor Supports Greater Information Sharing and Global Engagement

The Report highlights the need for greater sharing of information relating to DDoS and botnet threats and attacks and greater coordination across the ecosystem.[33] The Report

---

[28] *Report* at 16.
[29] *Id.* at 27.
[30] *Id.* at 29.
[31] *Id.*
[32] Coalition for Cybersecurity Policy & Law, *Cybersecurity Framework DDoS Profile*, available at https://www.cybersecuritycoalition.org/threat-profile-ddos-nist-framework.
[33] *Id.* at 30.

encourages service providers and organizations to share threat information globally,[34] and it advocates for consensus-based, industry-driven standards that are flexible, appropriately timed, open, voluntary, and global in nature.[35] The Report further states that the federal government should play a role in fostering the development of such standards by engaging in bilateral and multilateral international engagement.[36]

NETSCOUT Arbor agrees that broader sharing of threat information and the development of global standards to protect against and mitigate DDoS attacks are important steps to a more resilient ecosystem. Broader information sharing includes relevant threat intelligence, vulnerabilities and network architectural and operational best practices. Multiple communities exist to share and analyze vulnerability and threat information for connected devices, including industry consortiums, international CERT organizations, law enforcement, threat intelligence vendors, and operational security communities. Participation within these entities can provide significant benefits in understanding the DDoS attack and Botnet environment, how an organization's connected devices may be introducing risk, and how best to mitigate this risk. Unfortunately, over the last two years, service providers have been engaged in less information sharing. In 2017, less than a quarter of service providers participated in a global operational security community or shared cyber-security threat information.[37] This is down from 41% of service providers in 2015.[38]

NETSCOUT Arbor also agrees that the federal government should promote the development of global standards for protecting against and mitigating DDoS attacks. Like the NIST Framework, these standards should be voluntary, flexible, and developed in coordination with the industry. The federal government can facilitate the development of such a standard by bringing together the relevant stakeholders in multilateral meetings with government and industry leaders from other countries. Facilitating this type of collaboration is also likely to foster broader sharing of cyber threat information, as stronger relationships develop between the relevant stakeholders in participating countries.

[34] *Id.*
[35] *Id.* at 16.
[36] *Id.* at 33.
[37] *Global Threat Landscape* at 33.
[38] *Id.*

VI. Conclusion

NETSCOUT Arbor thanks the NTIA for the opportunity to provide this comment. We look forward to engaging with the NTIA and with NIST to further advance efforts to promote the adoption of best practices for DDoS attack prevention, detection, and mitigation.

Sincerely,

Arabella Hallawell
NETSCOUT Arbor