July 28, 2017

Ms. Evelyn L. Remaley
Deputy Associate Administrator
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave NW, Rm 4725
Washington, District of Columbia 20230

RE: *Promoting Stakeholder Action Against Botnets and Other Automated Threats* [Docket No. 170602536–7536–01]

Dear Ms. Remaley,

ACT | The App Association (the App Association) appreciates the opportunity to submit comments to the National Telecommunications and Information Administration (NTIA) on efforts to address the ongoing threat of harmful botnets and other automated threats.[1] This issue is of great concern to our members who rely on a resilient and trustworthy internet ecosystem, especially alongside development of 5G infrastructure that will drive next generation internet of the things (IoT) innovations and efficiencies across the economy. The App Association applauds NTIA's efforts on this important and timely issue.

The App Association[2] is a non-profit trade association representing thousands of software application development companies and information technology firms across the digital economy. We advocate for an environment that inspires and rewards innovation, while providing resources to help our members leverage their intellectual assets to raise capital, create jobs, and continue innovating.

As NTIA is aware, a botnet is a network of internet-connected end-user computing devices controlled by third parties that are infected with bot malware for a variety of purposes. However, it is important to distinguish between a bot and a botnet, because not all bots are malignant. A bot is merely a program installed on a system that is controlled by a remote administrator to perform a single, or set of, functions.[3] Bots are common throughout the tech industry, for example, the gaming industry and Internet Relay Chat software utilize bots to provide their respective services.

[1] *Promoting Stakeholder Action Against Botnets and Other Automated Threats*, 82 Fed. Reg. 27042 (Jun 13, 2017).

[2] *See* http://actonline.org.

[3] Communications Sector Coordinating Council, Industry Technical White Paper (Jan., 17 2017) https://docs.wixstatic.com/ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf (CSCC Report).

Conversely, bad acting botnets often use bots to perform nefarious and illegal tasks, such as distributed denial of service (DDoS) attacks.[4] The frequency of these malicious attacks is increasing, with the number of U.S. data breaches growing 29 percent in the first half of 2017 to a record high of 791 breaches.[5] Illegal botnet attacks are responsible for approximately 90 percent of all security incidents in today's digital economy today,[6] with the United States leading the charge as the most attacked country in the world.[7] Aside from the security consequences of these attacks, their financial impact is expected to top $2 trillion by 2019.[8] Malicious botnets typically employ some, or all of the following tactics:

- Impersonating legitimate web users to spy on or steal information or money from businesses;
- Infecting additional systems with malware;
- Stealing and/or reverse-engineering protected content for illegal re-posting on websites; and/or
- Luring site visitors away from a legitimate site to trick an end-user into sharing sensitive data.

In addition, botnets have established their own economy in the online illegal hacking community. Web users can easily find online classified ads offering bots for hire at discounted rates. For example, Mirai, a botnet infamously known for successfully exploiting IoT endpoints, has been widely reported to be available for rent. In some cases, this particular botnet enabled the buyer to leverage more than 400,000 infected bots to carry out DDoS attacks at anyone's behest.[9]

In addition to the direct damage they cause, botnets indirectly, but effectively, reduce trust in the digital economy, driving customers away or destroying some businesses completely. As our members grow their businesses and create new jobs, we are cognizant that the more successful their businesses and websites, the greater the incentive and likelihood to be subject to a criminal botnet attack. App developers represent the segment of the digital economy most vulnerable to botnet attacks, often because small businesses do not have the resources to dedicate to cybersecurity risk management.[10]

---

[4] A DDoS attack is a cyberattack attempts to prevent legitimate users from accessing information or services by targeting your computer and its network connection. See U.S. Department of Homeland Security, Website (last revised Feb. 6, 2013) https://www.us-cert.gov/ncas/tips/ST04-015.

[5] Identity Theft Resource Center and CyberScout Breach Report (July 2017), *available at* http://www.idtheftcenter.org/Press-Releases/2017-mid-year-data-breach-report-press-release.

[6] https://www.incapsula.com/blog/how-bots-impact-global-economy.html.

[7] https://www.incapsula.com/blog/how-bots-impact-global-economy.html.

[8] https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

[9] Bleeping Computer, "You Can Now Rent a Mirai Botnet of 400,000 Bots," *available at* https://www.bleepingcomputer.com/news/security/you-can-now-rent-a-mirai-botnet-of-400-000-bots/ (last accessed July 27, 2017).

[10] *E.g.*, Deccan Chronicle, "Magala Trojan cashes-in at the expense of small businesses" (July 19, 2017), *available at* http://www.deccanchronicle.com/technology/in-other-news/190717/magala-trojan-cashes-in-at-the-expense-of-small-businesses.html (last visited July 27, 2017).

Cumulatively, malicious botnets threaten the growth of the digital economy, the future 5G infrastructure that supports it, and the American end users who depend on it. Botnet attacks degrade the integrity of the internet and jeopardize our country's national cybersecurity.

The App Association appreciates NTIA's questions and considerations within in its request for comment. We offer the below recommendations to find effective ways to ameliorate the rise of botnets:

The U.S. Government Should Leverage the Public-Private Partnership Approach

Public-private partnerships are a useful, collaborative vehicle to confront both current and emerging cyber-based threats, and facilitate a flexible response to ever-developing risks. The App Association is committed to working with all public and private stakeholders in these fora to ensure a secure cyberspace. For example, the App Association:

- Co-chaired the Federal Communications Commission's (FCC) Commission Communications Security, Reliability, and Interoperability Council (CSRIC) Working Group 6, which developed "security-by-design" recommendations and best practices to secure the core communications network, as well as voluntary assurance mechanisms around them.[11]
- Participates regularly in key public dialogues organized by the U.S. government, such as the Federal Trade Commission's FinTech Forum on Artificial Intelligence and Blockchain in March 2017.[12]
- Supports and engages in NTIA-convened multi-stakeholder processes to identify consensus-based solutions on security vulnerability disclosure,[13] as well as IoT security patching and upgradability.[14]
- Currently co-chairs, with the Department of Homeland Security, a Working Group within the Information Technology Sector Coordinating Council (ITSCC)[15] that is working to develop a resource for small businesses providing economic data supporting the use of the Cybersecurity Framework. We strongly encourage enhanced U.S. government support for public-private partnership efforts to bring about greater use of the voluntary Cybersecurity Framework.

We strongly encourage the U.S. government to augment existing public-private partnerships, and seek ways to create new ones, to assist in developing a coordinated response to mitigate botnet attacks.

---

[11] Federal Communications Commission (FCC), Communications Security Reliability and Interoperability Council (CSRIC) V, *Secure Hardware and Software - Security by Design* (Sept. 2016), *available at* https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability#block-menu-block-4.

[12] *See* https://www.ftc.gov/news-events/events-calendar/2017/03/fintech-forum-blockchain-artificial-intelligence.

[13] NTIA, *Multistakeholder Process: Cybersecurity Vulnerabilities*, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities (last visited July 27, 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 July 27, 2017).

[15] *See* http://www.it-scc.org/.

NTIA Should Work with Fellow Government Agencies to Streamline Law Enforcement Take Downs of Botnets

The App Association believes law enforcement plays an essential role in preventing and mitigating botnet attacks. However, today's environment would require significant upfront forensic analysis and international and domestic coordination among many stakeholders before law enforcement agencies could act on botnet attacks. Notably, most U.S. botnet attacks come from outside of the country, with one in three cyberattacks originating in China.[16]

Mitigation of botnet attacks will require close coordination across the U.S. and foreign governments. Particularly with regard to the latter, maintaining the credibility of the U.S. is vital. We believe the current posture of the Department of Justice (DOJ) regarding law enforcement access to data stored abroad is unaligned with U.S. law and guaranteed rights, and undermines international rule of law by circumventing the Mutual Legal Assistance Treaty (MLAT) process.[17] The App Association continues to work with Congress, DOJ, and others to forge a path forward that balances individual rights with law enforcement needs to legitimately access data, regardless of whether it is stored domestically or abroad.

The App Association recommends that the U.S. government provide law enforcement new and sustained resources to combat botnet attacks, and work to streamline international processes for botnet takedown. NTIA is well-positioned to lead, coordinate, and facilitate U.S. government agencies in accomplishing these goals.

[16] *See* https://www.incapsula.com/blog/how-bots-impact-global-economy.html.

[17] *United States v. Microsoft*, 829 F.3d 197 (2nd Cir. 2016); *United States v. Microsoft*, 855 F.3d 53 (2nd Cir. 2017) (en banc).

The U.S. Government Should Ensure Shared Cyber Threat Information is Accessible and Actionable for American Small Businesses

The App Association believes that all organizations engaged in the sharing of information related to cybersecurity risks are invaluable to U.S. collective cybersecurity. Information sharing is a key component of the U.S. government's mission increase the private and public sectors' situational awareness of malicious cyber activity that threatens critical infrastructure and resources. A few sectors are subject to federal notification requirements, but most information sharing is voluntary, often done through the Department of Homeland Security (DHS), sector-specific agencies, or sector-specific Information Sharing and Analysis Centers (ISACs). Further, the National Cybersecurity and Communications Integration Center (NCCIC) should be used to improve information sharing and incident response, especially with respect to critical infrastructure. Some ISACs have already established relationships with the NCCIC's National Communications Center for information sharing. In addition, the Cybersecurity Information Sharing Act of 2015 (CISA) provided some liability relief to organizations sharing timely cybersecurity threat information with each other or the federal government. CISA authorizes the sharing of information among private entities for defensive measures, as long as certain personal information is "scrubbed."[18]

Despite the creation of the above-described solutions and assurances, the existing information sharing environment remains vulnerable. Private sector entities may be reluctant to share this information amongst each other due to concerns about legal liability, antitrust violations, and potential misuse. Further, small- and medium-sized entities often lack the resources, whether time or money, to be part of ISACs, and may not be sure which ISAC(s) to engage in due to the cross-sector nature of their business and supply chains.

To improve this crucial area of botnet attack mitigation, we recommend that NTIA work with government agencies, Congress, and other non-government stakeholders to provide programmatic support for small businesses to engage in effective information sharing. These incentives should include grant programs and public materials to explain information sharing and related issues to small businesses. The App Association recognizes that Information Sharing and Analysis Organizations (ISAOs),[19] if their potential is realized, may serve to alleviate some of these issues. We remain committed to improving our members' ability to share and receive timely cybersecurity threat information to help mitigate botnet attacks.

[18] https://www.dhs.gov/ciscp

[19] http://www.isao.org/

NTIA Should Encourage Continued Migration to IPv6

Currently, most residential wired broadband operates under IPv4 networks, which provides the user only one public IP address for all its devices in its local area network (LAN). Most common IP routers maintain a network address translation (NAT) function, which masks the identity of a device's specific IP address by only sharing the user's public IP address with other the devices in a LAN. By only providing one IP address, it is more difficult for law enforcement or the internet service provider to discern from which device the botnet attack derived. However, IPv6 eliminates the need to use NAT to discern an IP address because every internet-connected device can have a publicly routable IPv6, making it easier to track the host of the malicious bots. We support the efforts of the U.S. government to facilitate migration to IPv6, and urge for dedicated resources to help with this transition. The App Association is committed to assisting in the migration to IPv6.

The U.S. Government Should Encourage the Development, Adoption and Use of Machine Learning Techniques to Detect Botnets

A large number of malware use the domain generation algorithm (DGA) technique to intermittently produce a high volume of domain names to connect to their command and control servers, effectively obscuring the botnet's true source and location in the domain name system (DNS). The App Association supports industry efforts to apply machine learning techniques that automate and update processes in real-time as malware registers domain names with an internet registry. These efforts should be encouraged by NTIA and other U.S. agencies through research and development, grants to public and private institutions, public-private partnerships, among other efforts.

The U.S. Government Should Encourage Private Traffic Filtering in Transit and Peering Agreements

While there are numerous actions that the U.S. government can take to assist in botnet attack mitigation, some functions are best handled in the private sector and do not require government intervention. The App Association believes that prudent business practices require that network service operators and their end-users facilitate the best traffic filtering and scrubbing techniques available through internet transit and peering contracts. We note that we do not believe that NTIA or any other U.S. agency should intervene into the contracting between these parties, but that it should promote and encourage this behavior in private contracting.

The U.S. Government Should Encourage the Internet Corporation for Assigned Names and Numbers (ICANN), Domain Name System Registries, and Domain Name System Registrars to Adopt that Fast Flux Mitigation Techniques Recommended by the Security and Stability Advisory Committee (SSAC)

The App Association is committed to a trustworthy and competitiveDNS, and is an active participant in the work of the Internet Corporation for Assigned Names and Numbers (ICANN), where we represent the interests of small businesses in the digital economy. We continue to work in this crucial setting to ensure that any technical protection mechanism available be permitted to avoid and mitigate cyberattacks, including those utilizing botnets. Because botnets use "fast flux" techniques to hide the computers effecting the attacks (making it extremely difficult to use IP address filtering), we support botnet attack mitigation in the DNS as recommended by the ICANN Security and Stability Advisory Committee (SSAC).[20] We do not believe that NTIA or any other U.S. agency should mandate such activities (or any others within the DNS) or intervene into the functioning of ICANN or the DNS, but urge the U.S. government to support the SSAC's development of technical solutions to botnet attacks in the DNS via its engagement in the ICANN Government Advisory Committee.

NTIA Should Promote Use of the Voluntary NIST Cybersecurity Framework and "Security-by-Design," Particularly to Enhance Cyber-Resiliency in Endpoint Connections

The rise of the IoT will bring with it countless new endpoints for the internet. While the rise of IoT brings many benefits across consumer and enterprise use cases, it also introduces new attack vectors that should be protected from attacks as they are designed ("security-by design"), and not as an afterthought or retrofit. Further, end points can be made far more resilient simply though ensuring that such end points are running the most up-to-date software and/or implement timely needed software security patches. To this end, the App Association supports the use of the National Institute of Standards & Technology's (NIST) voluntary Cybersecurity Framework,[21] a voluntary risk-based tool that guides an organization in using industry standards and best practices to effectively and flexibly manage cybersecurity risks. We believe that the Cybersecurity Framework should be used across the internet ecosystem to address cyber-threats, including botnet attacks.

[20] ICANN Security and Stability Advisory Committee (SSAC), *SAC 025 SSAC Advisory on Fast Flux Hosting and DNS* (Mar. 2008), *available at* https://www.icann.org/en/system/files/files/sac-025-en.pdf (accessed June 20, 2017).

[21] National Institute of Standards and Technology, *Cybersecurity Framework* (May 25, 2017), *available at* https://www.nist.gov/cyberframework (accessed July 28, 2017).

The U.S. Government Should Launch a New Campaign to Improve America's "Cyber Hygiene"

End user education is a crucial aspect of improving cybersecurity and resiliency to botnet attacks, both in the current environment as well as in a future enhanced by IoT deployments, because many cyber-based attacks are preventable through standard cybersecurity hygiene practices (e.g., accepting ubiquitous software security patches). We therefore urge for the U.S. government to dedicate resources to a renewed public education campaign aimed at raising basic cybersecurity hygiene practices for the American public at large, tailored to populations and use cases in particular (e.g., adolescent and ageing populations, healthcare settings, etc.). The App Association welcomes the opportunity to partner with NTIA, the U.S. government, and other stakeholders in planning and executing such a campaign.

The App Association urges NTIA to consider our views as it continues to work to find ways to mitigate illegal botnet attacks in the internet ecosystem, which pose both criminal and national security threats to the U.S. and its citizens. We commit to assist NTIA and other U.S. agencies towards this end.

Respectfully submitted,

Brian Scarpelli
Senior Policy Counsel

Joel Thayer
Associate Policy Counsel

ACT | THE APP ASSOCIATION
1401 K St NW (Ste 501)
Washington, DC 20005
202-331-2130