September 18, 2017

Report on Responses to NTIA's Request for Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats

This document reports on the themes found in the responses to NTIA's "Request for Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats." It is not a comprehensive discussion of all comments, nor does it reflect a government decision. The full text of all comments is available at https://www.ntia.doc.gov/federal-register-notice/2017/comments-promoting-stakeholder-action-against-botnets-and-other.

Background

On May 11, 2017, the President issued Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," calling for "resilience against botnets and other automated, distributed threats."[1] The Department of Commerce, along with the Department of Homeland Security (DHS), was directed to "lead an open and transparent process to identify and promote action by appropriate stakeholders" with the goal of "dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)."

As part of that process, on June 13, 2017, the National Telecommunications and Information Administration (NTIA) issued a Request for Comments (RFC) on "Promoting Stakeholder Action Against Botnets and Other Automated Threats." The RFC asked for feedback on "current, emerging, and potential approaches for dealing with botnets and other distributed, automated attacks." NTIA expressed a particular interest in two broad approaches where substantial progress can be made: (1) mitigating ongoing attacks; and (2) securing vulnerable Internet of Things (IoT) devices that can be used in attacks.

The RFC is one part of an interagency effort to capture expert and stakeholder input. In parallel with the RFC, the National Institute of Standards and Technology (NIST) hosted a workshop on "Enhancing Resilience of the Internet and Communications Ecosystem" on July 11, 2017, to explore current and emerging solutions, which resulted in a workshop proceedings document. DHS' participation in this effort has been focused through the President's National Security Telecommunications Advisory Committee's (NSTAC) Internet and Communications Resilience (ICR) subcommittee, which is developing a report based on expert testimony. In the meantime, NTIA and NIST continue to welcome additional comments related to the process. These activities will contribute to the draft of a report to the President, which is due to be released for public comment on January 5, 2018. A final report is due on May 11, 2018.

Overview

In response to the RFC, NTIA received 47 comments. The commenters ranged from large trade associations to individual technical experts associated with a diverse range of industries and sectors, including Internet service providers, security firms, infrastructure providers, software manufacturers,

[1] *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Exec. Order 13800, 82 FR 22391 (May 11, 2017).

civil society, and academia. Comments ranged from attempts to help NTIA better understand the ecosystem and threat landscape, to sharing how recent innovations can help address these issues. Many offered specific policy suggestions and proposals.

Several broad themes emerged across the comments. While the risks from distributed, automated attacks take many forms, there was a general appreciation that addressing these risks is a shared responsibility, calling for ecosystem-wide solutions. No solution can address the overall threat. Moreover, while attacks have evolved to threaten key aspects of the digital ecosystem, the distributed, automated threat is closely linked to other cybersecurity threats across the ecosystem. These attacks are global, by their nature, and require international cooperation to work toward solutions. International standards and best practices will be necessary to achieve an effective global approach, rather than country-specific standards and regulations that could impose unnecessary costs and slow innovation.

Stakeholders resoundingly endorsed voluntary, consensus-based industry- and community-led processes, including NIST's Cybersecurity Framework and NTIA's multistakeholder processes. There were many strong voices against government playing too large a regulatory role. However, a notable number of commenters viewed the lack of existing security and market incentives as requiring more active policy interventions.

Notable Issues Identified in the Comments

Commenters raised several technology policy issues. A topic repeatedly cited was the importance of securing devices across the Internet of Things. Some asked: How can we overcome the challenges of the complexity and diversity of the ecosystem, as well as the lack of incentives and an uncertain role for consumers, to increase the security of devices we connect to the network? Many commenters noted that work has been done on this issue in the past and it should not be overlooked; existing approaches and known best practices can play a key role, if we can identify and overcome barriers to enhance their impact. Other stakeholders emphasized the importance of certifications and standards making it easier to build, deploy, and acquire more secure technology.

More generally, stakeholders recognized that the IoT marketplace is not yet fully mature, especially with respect to security. More tools and better, more widely adopted practices are needed. Numerous companies and consortia are innovating and collaborating to develop new technologies and foster their deployment across the ecosystem, but some are less knowledgeable regarding cybersecurity best practices, and others struggle with slim profit margins that may not easily accommodate security features. While some called for more active government intervention, one popular theme was the role of transparent security practices through independent testing and evaluation. Having a trusted third party to certify goods as being secure or compliant to standards could drive the marketplace by helping consumers make good decisions. Other commenters noted, however, that these types of programs are often difficult to implement successfully due to the constant evolution of the threat environment. Following a "secure development life cycle" can lead to more secure and higher quality systems, but this practice must also be something that can be communicated to the broader ecosystem. Finally, a software "bill of materials" process, similar to an inventory list of ingredients for third-party software components, if implemented from the ground up in a voluntary fashion, could help developers better understand the software code that goes into their products, and help purchasers understand exactly what is in the products they are buying.

Networks and information and communication infrastructure can play a key role in promoting a positive outcome. Existing solutions, ranging from network management tools to consumer notification practices, have been deployed in various forms, but these can be studied for effectiveness as new ones are developed. Some stakeholders urged an expansion of these existing practices, reminding NTIA that infrastructure covers a wide range of interested parties including, for example, the anti-abuse community, a community that has worked together against botnets, malware, spam, viruses, denial-of-service attacks and other online exploitation. Indeed, many industry players already work together to understand the threat and identify new solutions in industry organizations and consortia. A few examples include the Internet Engineering Task Force (IETF), North American Network Operators Group (NANOG), and Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), in addition to many other ongoing efforts. Stakeholders cited existing programs around botnets, including consumer notice, but very few were overly optimistic about the existing model scaling for the IoT threat.

Stakeholders emphasized the importance of information sharing and collaboration between infrastructure providers, defensive security services that protect against DDoS attacks, and the victims of these attacks. Information sharing can play a key role, stakeholders commented, as long as we are careful not to "punish" victims of attacks, and focus on how to align resources for defense and mitigation. Government can make it easier to share information, although there was no clear consensus on whether the government should act as a centralized hub to collect and share information.

Stakeholders were also optimistic about the opportunities to address botnets at the layer between an Internet service provider's (ISP's) network and a device, at the gateway or local area network. At this level, a network management service has a clear view of what is on the local network, and can help detect and prevent anomalous or malicious behavior. This solution can offer greater flexibility and granularity. Stakeholders discussed existing and emerging solutions, including the draft Manufacturer Usage Description (MUD) standard created at the IETF,[2] and other products on the market.

One clear area where stakeholders called for an active government role was the disruption of the networks that helped drive many of these distributed automated attacks. Law enforcement plays a critical role in the "take downs" of these networks, using its powers to disrupt, through legal and other means, the key resources on which these networks depend. Some emphasized more recent successes and effective collaboration with the private sector, while others expressed a need for the process to be faster and more efficient. Such attacks typically are global in nature, adding legal complexity and requiring cooperation across jurisdictions to identify and prosecute malicious actors.

Next Steps

As discussed above, the RFC comments, the NIST workshop proceedings, and the NSTAC report will contribute to the development of the report to the President required by Executive Order 13800. A draft of the report is scheduled to be released for public comment on January 5, 2018. After the conclusion of a 30-day comment period, a workshop will be held to discuss the plan of action and the final report. The comments and workshop will inform the final report, which is due to the White House on May 11, 2018.

[2] The Manufacturer Usage Description Specification draft dated August 9, 2017, is available on the IETF's website at https://tools.ietf.org/html/draft-ietf-opsawg-mud-08.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu