wiley

NEWSLETTER

Agencies Release Update on Cybersecurity Efforts Against Botnets

August 2020

Privacy in Focus®

Overview

On July 30, The Departments of Commerce and Homeland Security (DHS) released a progress report (Status Update) on the status of government and private sector efforts to implement recommendations from the 2018 Botnet Report and related Road Map. The Status Report documents more than 50 activities led by industry and government that demonstrate progress in the drive to counter the threats from botnets and introduces next steps as these efforts continue.

Background

In May 2018, Commerce and DHS released the final *Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* (Botnet Report) which responded to the President's May 11, 2017 Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." In producing the final Report, comments were taken from 49 stakeholders, and the National Telecommunications and Information Administration (NTIA) held workshops on the topic. In general, the Report aimed to combat botnets by focusing on six principle themes and five goals. Each goal included several action items, with a heavy emphasis on private sector activity and accountability.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

In late 2018, the Departments released a Road Map which built upon and was aimed at implementing actions and recommendations from the Report (and other overlapping efforts from across federal agencies). The Road Map "chart[ed] a path forward, setting out steps to stop the cyber threat to our internet infrastructure. It outline[d] a plan for coordination among government, civil society, technologists, academics, and industry sectors to develop a comprehensive strategy for fighting these threats." The five "Lines of Effort" laid out in the Road Map included numerous tasks for all stakeholders – including private sector players in the communications, internet, and information technology industries.

Wiley previously summarized both the Botnet Report and Road Map.

Key Highlights from the Status Update

NTIA, which announced the Status Update, underscored that "[s]topping botnet threats is an ecosystem-wide challenge that will take significant cooperation over time to accomplish. The Botnet Report and Road Map emphasized that the U.S. government cannot and should not attack the botnet problem alone." The document details efforts across the ecosystem to enhance the resilience of the Internet against distributed, automated attacks.

Section II offers a reassessment of the threat of automated, distributed attacks based on two 2019 DHS-commissioned research reports on botnets. These reports were reviewed to determine whether significant course changes in the overall effort were warranted. "Collectively, the two reports suggest that botnets will continue to be a threat for the foreseeable future" and will evolve in power and sophistication. The Status Update concludes "that the urgency of mitigating botnet attacks expressed in Executive Order 13800 is still warranted."

- The report *Technical Options and Approaches for Implementing Botnet Recommendations* found, among other things, that "[b]otnets will continue to grow in sophistication in order to counter efforts to disrupt them. This will likely include developing new techniques to evade detection, secure command and control, and increase overall resiliency of the botnet [and they] will expand to utilize new types of connected devices."
- The report *Targeting Trends for Botnet Growth* highlighted that "[there are] three important implications for global botnet behavior that arise from trends in botnet targeting practices: botnet sizes, global distribution patterns, and drivers of target expansion[.]"

Section III reviews progress the community as a whole is making in the areas highlighted by the Road Map and the impacts of those activities. The Status Update notes more than 50 activities under the Road Map's five Lines of Effort, including, among others:

- Under the Internet of Things (IoT) Line of Effort, the "significant progress [has been made]. In particular, the public and private sectors have contributed initial capability baselines, and consensus baselines are emerging." The Report goes on to mention numerous government activities and reports, for example NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy

Risks; NISTIR 8259: Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline; and NIST NCCoE's Cybersecurity Practice Guide Special Publication 1800-15 on mitigating IoT-based DDoS. From the private sector, the Status Update notes the Council to Secure the Digital Economy (CSDE) released the C2 Consensus on IoT Device Security Baseline Capabilities (C2 Consensus Baseline) and several others.

- The Enterprise Line of Effort "includes activities to help enterprises that have embraced the NIST Cyber Security Framework (CSF) to mitigate DDOS attacks and protect against botnets, promote migration to more robust and defensible network architectures, encourage federal adoption of industry best practices, and enhance the security of operational technology (OT) devices." The Status Update highlights: the Cybersecurity Coalition's DDoS Threat Mitigation Profile and Botnet Threat Mitigation Profile; and NIST's Draft SP 800-207, Zero Trust Architecture, among others.
- The Infrastructure Line of Effort "envisioned improvements to routing security, increased information sharing in practice, more efficient information sharing protocols, and focused research and development." "Since publication of the road map, new information sharing organizations have been established by the private sector as well as government-organized public-private collaborations, protocols for efficient information sharing during DDoS attacks have been published, and industry has developed playbooks for cyber crisis communication." Among several efforts noted is the Communications Security, Reliability, and Interoperability Council's (CSRIC) *Final Report on Best Practices and Recommendations to Mitigate Security Risks to Current IP-Based Protocols*.
- The Technology Development and Transition Line of Effort "focuses on establishing a robust and sustainable market for systems and applications developed through secure software development practices." The Status Update highlights NTIA's Software Component Transparency effort and BSA – The Software Alliance's Framework for Secure Software, among others.
- Under the final Line of Effort Awareness and Education, the Update highlights some recent public-private efforts to educate consumers and professionals, including: the NICE Cybersecurity Workforce Framework; efforts by the Global Cyber Alliance; and other small business resources. The Update also highlights IoT accreditation and certification programs, noting that "commercial programs for device certification against several baselines are now available" and referencing CTIA's Cybersecurity Certification Program, among others.

Section IV provides an update on the President's National Security Telecommunications Advisory Committee's (NSTAC) Report to the President on a Cybersecurity Moonshot. The report's primary recommendation was that the government establish a Cybersecurity Moonshot Initiative to strategically address America's cybersecurity issues.

- In response to these recommendations, the National Security Council included the development of Cybersecurity Grand Challenges in its implementation plan for the 2018 National Cyber Strategy of the United States of America. Since then, industry convened working groups of key stakeholders to consider current cybersecurity threats, and developed Cybersecurity Grand Challenge topics to address them.

- Further, CISA also began researching potential competition topics with a focus on improving the cyber resilience of federal networks and other critical infrastructure sectors.

Section V identifies important activities that lie ahead in the coming year. "The numerous initiatives detailed … are evidence that we are well on our way, but there is still work to be done. The IoT work, for example, represents an impressive evolution in how government and industry approach IoT security, but it must be sustained over the long term. Across all the lines of effort, the work that is already in progress must continue, and additional activities should build on that work." Ongoing and upcoming activities that are part of the various Lines of Effort include:

- NIST's development of a baseline Federal IoT Profile;
- International standards efforts, including work in Standards Committee 27 (ISO/IEC JTC1 SC27) to develop internationally accepted security baselines for IoT devices;
- "Strategies for infrastructure security will need to evolve with the network. In the relatively near future, many devices will be connected solely via 5G, and stakeholders are already working across the ecosystem – in areas like security standards and increased transparency – to improve 5G security in comparison to earlier mobile technologies;"
- "[E]merging IoT development platforms that make it easier to meet widely recognized security capability baselines should enhance IoT security with low impact on cost and time to market. As the development platforms incorporating important security capabilities such as secure update, device authentication, and device intent become commonplace, developers will find it much easier to deliver secure products."
- Software Bill of Materials practices developed by NTIA's stakeholder-led software component transparency efforts; and
- CISA's Cyber Essentials guidance, among others.

Additionally, the Update states that "[a] key step toward better consumer awareness is an assessment and certification regime that consumers can understand. Widely adopted, efficient, and effective assessment and labeling approaches for IoT devices would allow security-conscious consumers to make informed choices and create market incentives for secure-by-design product development. Some market-specific assessment schemes have been established, and products are being evaluated against these schemes. This market-based approach will determine optimal methods, including separate assessment regimes for disparate types of devices across the ecosystem."

Conclusion

The Update notes that "the U.S. government values innovation, and expects the market to determine the most expeditious solutions to the identified concerns." Further DHS and Commerce "welcome continued creativity and innovation in addressing the botnet challenge."

Industry stakeholders should continue to engage and help shape efforts led by DHS and Commerce under the broad umbrella of the Botnet Report and Lines of Effort laid out in the Road Map. These efforts will continue to evolve as market participants build greater resiliency into the Internet and IoT ecosystems and as new and evolving threats emerge.