Published on *The National Law Review* https://natlawreview.com

Battling Botnets – Evolving U.S. Government Policies and Frameworks to Address Security and Resiliency Challenges

Article By:

Laura H. Phillips

The Secretaries of the Department of Commerce and the Department of Homeland Security, through the National Telecommunications and Information Administration (NTIA), in early January 2018 issued a draft report to further public discussion about enhancing the resilience of the Internet and communications ecosystem against botnets and other automated distributed threats. This report continues work initiated under Presidential Executive Order 13800, "Strengthening the Cyber Security of Federal Networks and Critical Infrastructure." The report seeks additional public comment on known and evolving risks within and to the ecosystem and aims to forge consensus on what approaches warrant consideration for the government either to adopt or to encourage. Commenters are asked to evaluate a range of proposed goals and actions to achieve a more resilient ecosystem as well as to address the roles various stakeholders play in achieving and maintaining resiliency of the ecosystem nationally and globally. Comments are due on the draft report by February 12, 2018 and the final report is due the president by May 11, 2018.

Six principal themes emerged from the government's analysis of prior comments on identifying and mitigating botnet and other cyber threats, namely that:

- Automated distributed attacks are a global problem;
- While effective tools exist, they are not widely used
- Products should be secured during all stages of their life cycle.;
- Improved education and awareness are necessary;
- Current market incentives are misaligned; and
- Automated distributed attacks are an ecosystem-wide challenge.

Drawing from these themes, the draft report identifies for further comment a range of mutually supportive goals and proposed actions designed to reduce the threat of botnet attacks and improve the resilience of the ecosystem. They are:

Identify a clear pathway towards an adaptable, sustainable and secure technology marketplace. Proposed actions to realize this goal include establishment of broadly accepted baseline security profiles for IT devices both for in-home and industrial applications as well as promoting international adoption of these baseline profiles through bilateral agreements and use of international standards. It is suggested that the federal government accelerate this process by

adopting baseline security profiles for IT devices present in U.S. government environments. Another proposed action is the encouragement of widespread use of software development tools and processes to reduce the incidence of security vulnerabilities in commercial off-the-shelf software. The report suggests that the federal government collaborate with industry to encourage further enhancement and application of software tools to improve both marketplace adoption and industry accountability. The report suggests that the industry do what it can to expedite the development and deployment of new technologies for prevention and mitigation of distributed threats. Where applicable, the report also proposes that the government prioritize the application of R&D funds and technology transition efforts to support advancements in the DDoS prevention and mitigation area, as well as prioritize funding addressing foundational technologies that might prevent the creation of botnets. Finally, the report proposes that government and industry collaborate to ensure existing best practices frameworks and guidelines relevant to IoT are widely adopted across the ecosystem.

Promote innovation in the infrastructure for dynamic adaptation to evolving threats call. Continuous implementation and upgrades throughout the ecosystem are necessary to ensure a more resilient set of practices and standards to combat botnets and similar threats. Four actions that stakeholders might take are highlighted for comment. First, Internet service providers (ISPs) and their peering partners should expand their current information sharing activities in order to achieve more timely and effective sharing of actionable threat information on both the global and domestic scale. Second, it is recommended that stakeholders and subject matter experts, in consultation with NIST, should lead the development of a Cybersecurity Framework (CSF) profile for enterprise DDoS prevention and mitigation. Once IoT device profiles are developed as the draft report recommends, the federal government should lead by example and demonstrate the practicality of technologies, which is expected to create market incentives for early adopters. Industry and government should collaborate with all stakeholders to continue to enhance and standardize information sharing protocols so that they are effective. It is also suggested that the federal government work with U.S. and global infrastructure providers on ways to continuously identify and expand best practices on network traffic management to identify “bad” traffic across the ecosystem.

Promote innovation at the edge of the network to prevent detect and mitigate bad behavior. Devices and hubs at the edges of networks also have a role to play in identifying and mitigating threats. The draft report proposes that the networking industry expand current product development and standardization efforts to enhance effective and secure traffic management for both home and enterprise environments. It is suggested that user interfaces and home IT and IoT products be designed to maximize security while reducing or eliminating the need for users to have security knowledge for appropriate device administration. Further, enterprises should migrate to network architectures that facilitate detection, disruption and mitigation of automated distributed threats. It is also recommended that the federal government investigate how wider IPv6 deployment could alter the economics of both attack and defense.

Build coalitions between the security, infrastructure, and operational technology communities both domestically and globally. The specific actions suggested to advance this goal are that ISPs and large enterprises take steps to increase information sharing with law enforcement to provide timely and actionable information regarding threats. The federal government should promote international adoption of best practices and relevant tools through bilateral and multilateral international engagement efforts. Regulatory agencies in specific sectors (such as the FDA with medical devices) should work with industry to establish appropriate sector specific guidelines, while agencies such as the FTC should continue to enforce its deceptive marketing standards on the marketers of devices that misrepresent security or privacy capabilities afforded to their users. It is suggested that all communities should take concrete steps to limit fast flux hosting, which is the rapid

modification of IP addresses designed to mask illegal or malicious activities. Finally the draft report recommends that the cybersecurity community should continue to engage with the operational technology community to promote joint awareness and accelerate cybersecurity technology transfers.

Increase awareness and education across the ecosystem. In this area the specific actions suggested include that the private sector establish and administer voluntary informational tools for home IoT devices that would be supported by a scalable and cost-effective assessment process that consumers can intuitively trust and understand. It is also suggested that the private sector establish voluntary labeling schemes for industrial IoT applications to be supported by scalable and cost-effective assessment processes that offer sufficient assurance for critical infrastructure applications of IoT. It is suggested that the government encourage academic and training sectors to integrate secure coding practices into computer science and related programs. The academic sector, in collaboration with the national initiative for cyber security education, should establish cybersecurity as a fundamental requirement across all engineering disciplines. Finally, the draft report recommends that the federal government establish a public awareness campaign to support recognition and adoption of home IoT device secured security profile and branding activities.

Certainly the proliferation of IoT devices with vastly different operating characteristics and security profiles heightens the risk that these devices can be compromised and misused to great adverse effect. We will continue to track the initiatives proposed in the draft report and summarize the final report in May.

National Law Review, Volume VIII, Number 19