wiley

NEWSLETTER

Botnet Report Will Impact Private Sector; Comments Sought

January 2018

Privacy in Focus®

On January 5, 2018, the U.S. Department of Commerce and the U.S. Department of Homeland Security released a draft of their *Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*. The Report responds to the President's May 11, 2017 Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" which directed federal agencies "to identify and promote action" with the goal of "dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)." Comments on the Draft Report are due February 12.

The Report calls for several efforts, and 23 "Actions" that will involve the private sector. It addresses public-private partnerships, certifications, standards, procurement demands, regulation and international coordination. The Report tasks industry with enhancing security in software and product development, improving enterprise security, accounting for activity on ISP networks, collaborating more with agencies and regulators, and assisting with the creation of a new *Cybersecurity Framework Profile for Enterprise DDoS Prevention and Mitigation*, among others. In a special section, the Report notes private sector concern about legal risks and uncertainties, but it makes no recommendations, pointing to existing—and limited—protections.

The Report Paints a Serious Picture of the Complex Threat Landscape

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

The Report is structured to offer several "visions" for future states in each of several key areas. But first, it highlights major recent DDoS and other attacks, and analyzes the global situation. It identifies six core themes.

- Automated, distributed attacks are a global problem.
- Effective tools exist, but are not widely used.
- Products should be secured during all stages of the lifecycle.
- Education and awareness are needed.
- Market incentives are misaligned.
- Automated, distributed attacks are an ecosystem-wide challenge.

The Draft analyzes the ecosystem: infrastructure, enterprise networks, edge devices, and home and small business networks. It discussed the need for collaboration (both on a small scale and globally), best practices, and shared defense. Notably, it raised concerns about enterprise networks, finding that "[m]any at-risk enterprises are unaware of the potential impacts of DDoS attacks on their operations" and that many may not understand their Internet service contracts or use available DDoS mitigations. It called for more widespread enterprise use of the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*, as well as for consumer education, and for "edge devices" to be designed more securely.

The Report also looks at governance, policy, and coordination. Although coordination does take place across sectors, countries, and between industry and law enforcement, the Report suggests much more can be done. Looking ahead, the Report presents "Visions" in which purchasers are aware of basic security properties of connected devices, information is better shared and analyzed, and cooperation occurs across sectors, agencies and countries. The Report states that the U.S. government and international partners should conduct their technology and device procurements to create incentives for more secure products, and promote open, voluntary, industry-driven standards. It further emphasizes the need for the U.S. to engage with other countries, particularly through the National Telecommunications and Information Administration (NTIA) within the Department of Commerce. Finally, the Report calls for more coordination between industry and law enforcement to detect and prevent threat activity.

The Report Sets Out 5 Goals and 23 "Actions" Impacting the Government and the Private Sector

In its *Goals and Actions*, the Draft offers five goals to reduce the threat of automated, distributed attacks and improve the resilience of the ecosystem. For each goal, the Report suggests four to five Activities for the government and private sector. The Commerce Department's NIST and the NTIA receive many assignments. Regulators and the Federal Trade Commission (FTC) receive praise for their work on Internet of Things (IoT) security, as "[c]areful enforcement actions can benefit consumers and honest participants in the market."

While the Report emphasizes the voluntary nature of many Actions directed at the private sector, companies can expect additional scrutiny and expectations. The Report calls for work on topics ranging from device labeling to increased engagement with "operational technology" companies. There are suggested mandates related to procurement, and calls for standards that will impact the IoT and connected-device ecosystem, from software and product developers to Internet Service Providers (ISPs) and network carriers.

Goal 1: *Identify a clear pathway toward an adaptable, sustainable, and secure technology marketplace*. The report proposes "market incentives [to] encourage manufacturers to feature security innovations as a balanced complement to functionality and performance, adoption of tools and processes that result in highly secure products is easier to justify." Among several suggested Actions, it wants NIST to create additional guidance and profiles that can help government and industry.

Goal 2: *Promote innovation in infrastructure for dynamic adaptation to evolving threats*. This section seeks establish "a more resilient Internet and communications ecosystem, standards and practices that deter, prevent, and/or mitigate botnets and distributed threats should be continuously implemented and upgraded in all domains…" Its Actions include a more muscular role for ISPs and others in managing traffic.

Goal 3: *Promote innovation at the edge of the network to prevent, detect, and mitigate bad behavior*. This section identifies actions stakeholders can take to manage the impact of compromised IoT devices. Its Actions include driving standards for devices.

Goal 4: *Build coalitions between the security, infrastructure, and operation technology communities domestically and around the world*. The Report notes that no stakeholder can address this issue alone and calls for actions that "cross geopolitical, public-private, industrial sector, and technical boundaries." This section calls for collaboration between law enforcement and industry, with little discussion of barriers and risks.

Goal 5: *Increase awareness and education across the ecosystem*. This section identifies several Actions to "close gaps between current skills and responsibilities" and focuses on disclosures, labels and certifications.

The Report Overlooks Barriers and Obstacles to Achieving Many Goals

One major topic seems missing. The Report does not address obstacles to implementing the many Actions called for. To be sure, the Report acknowledges challenges posed by complexity and global activity. But other than a short section noting some commenters' concerns about liability and risk, the Report offers little recognition of the serious challenges in getting representative stakeholders engaged on things like labels, standards, and other initiatives. Throughout, the Report hints at the potential role of regulators, perhaps to signal to the private sector that failure to act voluntarily may require more assertive government action. But it does not offer a Roadmap or call for incentives that might motivate the various necessary actors to contribute.

Next Steps and Timeline

Comments on the Draft Report are due on **February 12, 2018**. This is a good opportunity for groups identified in the Report (software providers, enterprises, IoT innovators, DDoS prevention and security service providers, the Internet community, and operational technology developers) to identify their views on the path described, and what they need in order to take action.

After this, NTIA will host a workshop from February 28 – March 1, 2018 to discuss comments. The Final Report is due to the President on May 11, 2018.

For years, Wiley Rein LLP has actively engaged on cybersecurity law and policy. We actively participate in drafting and implementing key NIST documents, federal agency standards, and best practices across the economy. We have advised clients on products and services, responded to government investigations, and advocated before numerous agencies and policymakers on issues related to cybersecurity, connected devices and the Internet of Things (IoT).

Please let us know if you have questions or would like to discuss.