wiley

ALERT

Summary of the May 2018 Botnet Report issued by the Departments of Commerce and Homeland Security

May 31, 2018

On May 30, 2018, the Departments of Commerce and Homeland Security 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 or Report). This builds on a draft report released on January 5, 2018, and responds to the President's May 11, 2017 Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." Comments were taken on the draft report from 49 filers, and the National Telecommunications and Information Administration (NTIA) held workshops on the topic.

In general, the Report aims to combat botnets by focusing on six principle themes and five goals. Each goal includes several action items, with a heavy emphasis on private sector activity and accountability. The Report includes a section on next steps for stakeholder action, which calls for the development of a road map with government, industry, civil society, and international partner coordination, and a "status update that will evaluate the level of progress made by stakeholders in countering automated, distributed threats."

The final Report expands on its discussion of liability as a potential barrier to productive action and information sharing, and calls for more work on that issue. And it emphasizes the global nature of the botnet challenge, calling for more international engagement by industry and the government.

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
Telecom, Media & Technology

This Report will set in motion additional work across government and the private sector if its recommendations and goals are taken seriously. There remains much work to be done on automated, distributed threats because the problem cannot be solved by domestic regulation or one technological solution.

The Report Describes the Complex Threat Landscape, Noting Ongoing Activity by ISPs and Others, but Indicates More Needs to Be Done

Highlighting recent DDoS and other major attacks, the Report analyzes the global landscape. 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.
- Awareness and education are needed.
- Market incentives should be more effectively aligned.
- Automated, distributed attacks are an ecosystem-wide challenge.

The Report analyzes the ecosystem: infrastructure, enterprise networks, edge devices, and home and small business networks. Notably, it raises 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. The Report calls for more widespread enterprise use of the National Institute of Standards and Technology (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 is more inclusive, occurring across sectors, agencies, and countries.

Specifically, the Report emphasizes the need for industry-led approaches and consensus-based standards. Yet in its "Vision for the Future of Edge Devices" section the Report states: "Devices must be able to resist attacks throughout their deployment lifecycles—at the time of shipment, during use, and through to end-of-life. For this to occur, security must become a primary design requirement." "Requirement" was changed from "goal" in the draft. It also states that the U.S. government and international partners should conduct their technology and device procurement actions to create market 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. Finally, the Report calls for more coordination between industry and law enforcement.

The Report Calls for 24 "Actions" That Promote Ongoing Discussions in Congress, DHS, NIST and NTIA

In its *Goals and Actions* section, the Report enumerates five goals. For each goal, the Report suggests activities for the government and private sector. NIST receives many assignments. Regulators and the Federal Trade Commission (FTC) receive praise for their work on Internet of Things (IoT) security, as the Report says "[c]areful enforcement actions can benefit consumers and honest participants in the market."

While there is emphasis on the voluntary nature of many actions directed at the private sector, companies can expect additional scrutiny and demands. The Report's emphasis on several topics dovetails with efforts underway, including the IoT Cybersecurity legislation championed by Senators Mark Warner and Cory Gardner and an expected NTIA effort on software assurance (*see* Action 1.3).

The Report calls for work on topics ranging from device labeling to increased engagement with "operational technology" companies. It also suggests mandates related to government procurement and calls for standards that will impact industry broadly across 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 calls for "market incentives [to] encourage manufacturers to feature security innovations as a balanced complement to functionality and performance." It notes that "Publishing documents is not enough," the "IoT community must work collaboratively to identify and adopt existing best practices, frameworks, and guidelines [.]" This section calls for:

- Establishing accepted baseline security profiles for IoT devices in home and industrial applications, to be promoted by device labeling, bilateral arrangements, and the use of international standards (Action 1.1). The Report calls for collaborative development of "Performance-based security profiles appropriate capability baselines—which identify suites of voluntary standards, specifications, and security mechanisms that represent the combination of best practices for home and industrial applications of IoT lifecycle security for a particular threat environment[.]"
- The government should then "leverage industry-developed capability baselines, where appropriate, in establishing capability baselines for IoT devices in U.S. government environments to meet federal security requirements, promote adoption of industry-led baselines, and accelerate international standardization." (Action 1.2);
- Reducing security vulnerabilities in commercial-off-the-shelf software. "NTIA should engage diverse stakeholders in examining the strategies and policies necessary to foster a marketplace for greater software component transparency, including identifying and exploring market and other barriers that may inhibit progress in this space." (Action 1.3);
- Expediting the development and deployment of technologies to prevent and mitigate distributed threats, including through "targeted [federal] funding and collaborative technology transition activities." (Action 1.4);

- Government, industry, and civil society collaboration to ensure adoption of best practices in the IoT ecosystem (Action 1.5), with a focus on NTIA. The Report cites NTIA's multistakeholder process on IoT Security Upgradability and Patching, but notes that broader adoption and promotion of best practices, frameworks, and guidelines is essential.

Goal 2: *Promote innovation in infrastructure for dynamic adaptation to evolving threats*. This section seeks to establish "a more resilient Internet and communications ecosystem, standards and practices that deter, prevent, and/or mitigate botnets and distributed threats should be continually implemented and upgraded in all domains…" The Report notes that "[w]hile network providers cannot be expected to serve as traffic cops and identify all bad packets, both common and newer tools and practices can help filter out some types of bad traffic." Potential solutions cited include "inter-autonomous system, internetwork peering, and transit agreements [which] might improve traffic management accountability." Action items call for:

- ISPs to expand information sharing (Action 2.1) by "work[ing] collaboratively with civil society and government to improve coordinated responses to actionable information and lead the development, refinement, and standardization of information sharing protocols to increase speed and permit automated response. Special attention should be given to engagement and inclusion of smaller ISPs and protocol developments that enhance their participation." The Report identifies the Comm-ISAC as a key venue and expanding information sharing agreements with international peers as an additional enhancement;
- The development of a *Cybersecurity Framework Profile for Enterprise DDoS Prevention and Mitigation* (Action 2.2). "An industry-led effort, in consultation with NIST, academia, and other subject matter experts, should develop a CSF Profile for Enterprise DDoS Prevention and Mitigation, focusing on the desired state of organizational cybersecurity to mitigate DDoS attacks," citing Comments from the Coalition for Cybersecurity Policy and Law;
- The federal government to create greater market incentives (Action 2.3), by looking at "effective ways to incentivize the use of software development tools and processes that significantly reduce the incidence of security vulnerabilities in all federal software procurements, such as through attestation or certification requirements;"
- Industry, government, and civil society organizations to collaborate with stakeholders to enhance and standardize information-sharing protocols (Action 2.4). The Report recognizes that small businesses "do not contribute to or benefit from most current information-sharing arrangements;"
- U.S. and global infrastructure providers to work together to expand best practices on network traffic management across the ecosystem (Action 2.5). The Report calls for a "broad coalition of domestic and international experts—industry, academia, civil society, and government—[to] examine the extent to which inter-autonomous system, internetwork peering, and transit agreements might improve traffic management accountability—for instance, as applied to anti-spoofing and filtering."

Goal 3: *Promote innovation at the edge of the network to prevent, detect, and mitigate automated, distributed attacks*. This section identifies actions stakeholders can take to manage the impact of compromised IoT devices. Actions call on:

- Industry to expand current product development and standardization efforts for effective and secure traffic management in home and enterprise environments (Action 3.1);
- Industry to design user interfaces on home IT and IoT to be used securely and privately (Action 3.2);
- Industry to migrate to network architectures with better defenses and consider how their own networks put others at risk (Action 3.3);
- Government to investigate how wider IPv6 deployment can alter the ecosystem (Action 3.4). The Report expects that "As we transition to IPv6, consumer ISPs may be better positioned to observe device-specific misbehavior when IPv6 addresses are not subjected to NAT. This information can, in turn, map to other edge-focused solutions."

Goal 4: *Promote and support 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." It hits several topics that may give the communications sector pause. Seemingly sensitive to challenges posed by shifting international requirements, it calls for governments to "work with private-sector entities responsible for compliance with data privacy protection regulations, as well as with those entities involved in botnet investigatory work, to ensure that both equities are preserved (compliance and botnet investigations)." It does not state that global privacy and security regimes may impede botnet mitigations or offer solutions.

The Report also paints a rosy picture of the government's approach to victim companies. It states that "law enforcement treats companies that have suffered an intrusion or distributed attack as victims of a crime, and conducts their investigations of such reported crimes with discretion to avoid the unwarranted release of information concerning the incident, whenever possible." It does not call for more protections for victimized companies, nor does it address the potential backlash against companies cooperating with the government. The Report calls for several actions that would impact the private sector:

- ISPs and enterprises should increase information sharing with law enforcement (Action 4.1). The Report calls for "[l]aw enforcement [to] proactively identify what kinds of data will help them investigate and prosecute bad actors, and work with infrastructure providers to make it cheaper and easier to share this information with government while protecting Internet user privacy;"
- Federal government should promote international adoption of best practices, including through NTIA leadership on global DNS security work (Action 4.2);
- Sector-specific regulatory agencies should engage industry to ensure nondeceptive marketing and "foster appropriate sector-specific considerations" (Action 4.3). This section touts FTC activity and its unfairness authority under Section 5. These efforts, with sector-specific enforcement, "can contribute to, and benefit from, the broader ecosystem security discussion." It is not clear what this means but the

Report may be suggesting a reexamination of some agency efforts;

- Community should identify leverage points and disrupt attacker tools and incentives (Action 4.4). The Report states that "Many threats stem from asymmetries that favor attackers by distributing the exploitation across diffuse actors in the ecosystem [and i]n some cases, relatively light coordination efforts should be able to disrupt broader attack classes;"
- Engagement with the operational technology community to accelerate cybersecurity (Action 4.5).

Goal 5: *Increase awareness and education across the ecosystem*. This section identifies actions to "close gaps between current skills and responsibilities." Many of these actions veer toward certifications, disclosures, and labeling. This section calls for several Actions:

- The private sector should "establish and administer voluntary information tools for home IoT devices" (Action 5.1) because the Report finds that "[i]n an ideal world, consumers would prefer IoT products that also protect their security and privacy, but security-conscious consumers cannot easily identify which IoT products were designed to be secure." This Action would include "consumer-oriented testing organizations;"
- The private sector should "establish voluntary labeling schemes for industrial IoT applications" (Action 5.2). "The private sector should establish an efficient but robust evaluation process to ensure that IoT devices for these sectors offer enhanced resilience at an appropriate level of assurance;"
- Government should encourage the academic and training sectors to integrate secure coding practices into computer science and related programs (Action 5.3);
- The academic sector, in collaboration with NIST's National Initiative for Cybersecurity Education, should establish cybersecurity as a requirement across all engineering disciplines (Acton 5.4);
- Government should lead a public awareness campaign to "support recognition and adoption of the home IoT device security baseline and branding" (Action 5.5).

The Report calls for many efforts that will impact the private sector.

As is highlighted in the suggested actions for private sector stakeholders, the Report has implications for industry. It calls for public-private partnerships, greater engagement with and from a variety of stakeholders, certifications, standards, procurement mandates, a multistakeholder process "to explore requirements for a viable labeling approach," the possibility of regulation, and international coordination. It tasks industry with enhancing security in several areas, increasing accountability, and network activity. Topics include software and product development, accounting for activity on networks, working more closely with agencies, regulators, and other stakeholders, and assisting with the creation of a new *Cybersecurity Framework Profile for Enterprise DDoS Prevention and Mitigation*, among others. The Report notes private sector concerns about legal risks and uncertainties, as raised by CTIA in its comments. The final report expands upon this commentary in the draft, noting that a balanced approach must be taken:

"Some stakeholders noted that any new legal or regulatory regimes may have unintended negative impacts on the IT industry if clear guidance is not included regarding what a vendor can do to limit its exposure. However, advocates caution against blanket liability protections without clear social gains from improved security processes. Some stakeholders, including civil society organizations, called for additional clarity regarding how existing laws in various jurisdictions apply in this area, how these laws can or should affect different stakeholders along the supply and distribution chains, and how to properly address harms. As this area continues to evolve, it is vital that the federal government better understand the interaction between liability and market incentives, as well as how any proposed changes might alter that dynamic. Care must be taken to ensure that our liability laws benefit consumers, protect stakeholders when appropriate, and avoid chilling innovation in today's digital environment. As public-private sector collaboration in this area continues, the federal government should continue to monitor whether protection from liability related to information sharing is sufficient in today's environment to effectively address ongoing and new threats."

Next Steps

While the Report is in its final form, the government plans to continue collaborative work on this effort. Within 120 days, the Departments of Commerce and Homeland Security, in coordination with industry, civil society, and in consultation with international partners, will develop an initial road map for prioritized actions. "Government and the private sector will work together to ensure that the road map is updated and maintained as stakeholders accomplish the identified actions." Further, in one year, a status report will be provided to the President, tracking progress made by the "community as a whole" against the road map on the implementation of the recommendations found in the Report.

The Report and Plan for Continued Action Come Amidst Several Ongoing Efforts on the Internet of Things and Overall Internet Resiliency.

The Report addresses risks from botnets and automated, distributed attacks, which can be launched using IoT devices that are vulnerable, either due to lack of basic security configurations at the time of manufacture, or from failures to update or patch devices. Several efforts are underway to address security in the increasing array of connected devices that will up the IoT.

- NIST has numerous workstreams on IoT, with dozens listed, including efforts to map international standards in NISTIR 8200, the Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT), and to develop a draft document identifying security and privacy considerations for IoT
- The Department of Homeland Security addressed Security Principles for Security the Internet of Things (IoT) and is expected soon to release a cybersecurity strategy that will include connected devices. As Secretary Nielsen told the RSA Cybersecurity Conference in March 2018, "the proliferation of internet-connected devices—which make our lives easier, and in some cases more fun—have also made it easier to attack us."
- The Food and Drug Administration has issued guidelines and developed a Medical Device Safety Action Plan to enhance connected device security.

- The Department of Justice has issued IoT guidelines with the Consumer Technology Association, and it may address cybersecurity and botnets in the report to be developed by its Cyber Digital Task Force
- NHTSA is actively engaged in automotive security, related to connected vehicles.
- The U.S. Consumer Product Safety Commission is looking at possible hazards from connected devices.