Cooley

Internet Attacks Using IoT Devices Spur Government Calls for Improved Cybersecurity

October 31, 2016

The recent massive distributed denial of service (DDoS) attack that caused major internet outages was led by an army of security cameras, digital video recorders, and other Internet of Things ("IoT") devices that had been compromised by a malicious botnet called Mirai. The botnet controlled some 100,000 IoT devices and used them to target a company that controls much of the internet's domain name system.

In response, Senator Mark Warner (D-VA), in his role as co-chair of the recently established **Senate Cybersecurity Caucus**, contacted the Federal Communications Commission ("FCC"), Federal Trade Commission, and the Department of Homeland Security's National Cybersecurity & Communications Integration Center (NCCIC) with questions about existing and future tools needed to combat these kinds of attacks. In a **letter to FCC Chairman Tom Wheeler**, Senator Warner asked specifically whether the agency could do more to ensure that IoT devices meet a reasonable level of security. This is but one of a number of governmental inquiries in the US and the European Union to examine and address perceived security vulnerabilities of IoT devices.

Senator Warner noted the "unacceptably low level of security inherent in a vast array of network devices," and suggested several avenues for the agency to explore, including enlisting broadband internet service providers to help prevent the malicious use of IoT devices and requiring IoT equipment manufacturers to meet minimum security requirements. The specific questions posed by Senator Warner are included at the end of this alert.

Enlisting ISPs

The Senator asked whether the FCC's Open Internet rules could be used to require ISPs to prevent "insecure" IoT devices from being connected to the internet, including by refraining from assigning them IP addresses. Although the Open Internet (or Net Neutrality) rules generally ban ISPs from blocking internet traffic, the FCC's decision adopting these rules suggests ISPs could legally restrict internet traffic that harms the network. It specifically references blocking "traffic that constitutes a denial-of-service attack on specific network infrastructure." Senator Warner asked whether the domain name service company targeted by the DDoS attack should be considered a type of network infrastructure that ISPs should be empowered to protect.

The FCC's Open Internet rules also may be interpreted to give ISPs some leeway to prevent harmful or insecure devices from being connected to their networks. The rules bar ISPs from preventing customers from attaching devices that do not harm the network, but permit ISPs to bar the attachment of devices that can cause harm. These questions could lead to difficult technical determinations regarding when and how a device could be deemed harmful or "insecure."

Enlisting manufacturers

In addition to noting steps ISPs might take, the FCC letter also addressed possible requirements for IoT device manufacturers. The letter asked the FCC about mechanisms to take "harmful" devices out of circulation, or to ensure that they are updated with new security features, such as patches, after they are sold. This line of inquiry dovetails with the current efforts underway by the Commerce Department's National Telecommunications and Information Administration's ("NTIA") voluntary, multi-stakeholder

process to address upgrading the security of IoT devices once they have been sold. The NTIA held its initial multi-stakeholder meeting on October 19, 2016 and is establishing working groups to assess various aspects of this problem.

Senator Warner also asked about the development of minimum technical security standards and the feasibility (including costs to manufacturers) of requiring device security testing and certification, similar to the FCC's existing authorization process used for equipment that wirelessly connects with the internet using WiFi, Bluetooth, or other connection protocols. The FCC enforces a robust set of testing, certification, and labeling requirements to ensure that such devices do not cause harmful interference when connecting to the internet using the wireless spectrum. The letter calls on the FCC to assess whether the testing and labeling requirements could be expanded to include security concerns.

The European Union has begun a similar process. The European Commission reportedly is drafting new cybersecurity requirements for the IoT as part of its overhaul of the EU's telecommunications laws. The EU requirements could include testing and certification, as well as encouraging industry to develop labeling requirements for approved and secure IoT devices. Standards resulting from the EU's process could provide an example for the US regulators.

Pressure to act

The number of IoT connected devices is rapidly increasing – there are about 6 billion interconnected devices in use worldwide, and that number is expected to increase to over 20 billion by 2020. Last week's DDoS attack apparently utilized only about 100,000 devices, yet created one of the largest DDoS attacks ever recorded. The attack demonstrated that many of these devices lack even moderate security, making them ready targets for inclusion in large scale botnets that can cause considerable disruption to the internet. At a time of increasing government oversight of the internet more generally, regulators are likely to consider seriously requests for regulation of IoT cybersecurity. Indeed, when asked about Senator Warner's letter in a recent new conference, Chairman Wheeler stated he thought "it was a very thoughtful letter and I look forward to responding to it in kind." This is likely not the last inquiry to the FCC or IoT companies.

The Communications , Government Analytics and the Privacy & Data Protection Practice Groups at Cooley have highly complementary skills that uniquely situate the firm to help companies address IoT, FCC, and related issues. The Communications Group has a deep and sophisticated understanding of communications networks and how they are regulated, including recent FCC actions on **privacy and cybersecurity**, while the Privacy & Data Protection Group has technical expertise and substantial experience in assessing risks and responding to cybersecurity threats. We can help you understand the implications of Senator Warner's letter and related developments and how they apply to your organization, as well as assessing likely FCC responses, other regulatory actions or congressional inquiries that might follow.

Below are the specific questions posed by Senator Warner to the FCC:

1. What types of network management practices are available for internet service providers to respond to DDoS threats? In the FCC's Open Internet Order, the Commission suggested that ISPs could take such steps only when addressing "traffic that constitutes a denial-of-service attack on specific network infrastructure elements." Is it your agency's opinion that the Mirai attack has targeted "specific network infrastructure elements" to warrant a response from ISPs?
2. Would it be a reasonable network management practice for ISPs to designate insecure network devices as "insecure" and thereby deny them connections to their networks, including by refraining from assigning devices IP addresses? Would such practices require refactoring of router software, and if so, does this complicate the feasibility of such an approach?
3. What advisories to, or direct engagement with, retailers of IoT devices have you engaged in to alert them of the risks of certain devices they sell? Going forward, what attributes would help inform your determination

that a particular device poses a risk warranting notice to retailers or consumers?

4. What strategies would you pursue to take devices deemed harmful to the network out of the stream of commerce? Are there remediation procedures vendors can take, such as patching? What strategy would you pursue to deactivate or recall the embedded base of consumer devices?
5. What consumer advisories have you issued to alert consumers to the risks of particular devices?
6. Numerous reports have indicated that users often fail to install relevant updates, despite their availability. To the extent that certain device security capabilities can be improved with software or firmware updates, how will you ensure that these updates are implemented?
7. Do consumers have meaningful ability to distinguish between products based on their security features? Are formal, or third-party, metrics needed to establish a baseline for consumers to evaluate products? If so, has your agency taken steps to create or urge the creation of such a baseline?
8. Should manufacturers have to abide by minimum technical security standards? Has your agency discussed the possibility of establishing meaningful security standards with the National Institute of Standards and Technology?
9. What is the feasibility, including in terms of additional costs to manufacturers, of device security testing and certification, akin to current equipment testing and certification of technical standards conducted by the Federal Communications Commission under 47 CFR Part 2?

Key Contacts

Matthew D. Brown San Francisco	brownmd@cooley.com +1 415 693 2188
J.G. Harrington Washington, DC	jgharrington@cooley.com +1 202 776 2818
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090

Vince Sampson Washington, DC	vsampson@cooley.com +1 202 728 7140