MARK R. WARNER
VIRGINIA

886

United States Senate

WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

October 25, 2016

The Honorable Tom Wheeler
Chairman
Federal Communications Commission
445 12th Street S.W.
Washington, D.C. 20554

Dear Chairman Wheeler,

I have watched with growing concern over the past two months as an ever-larger network of infected devices has been leveraged to conduct the largest series of Distributed Denial of Service (DDoS) attacks ever recorded. According to global telecommunications provider Level 3 Communications, the 'Mirai botnet' has more than doubled since the source code was first made public on October 1st.[1] The Mirai botnet functions by taking control of highly insecure devices, such as 'Internet of Things' (IoT) products, and using them to send debilitating levels of network traffic from these compromised devices to particular sites, web-hosting servers, and internet infrastructure providers.[2] By infecting consumer devices with this malware, attackers can hijack the communications capabilities of users' devices, using large numbers of them to flood sites and servers with overwhelming traffic. As the co-Chair of the Senate Cybersecurity Caucus, I invite your prompt response to a number of important questions raised by these incidents.

While the precise form of Mirai's attacks is not new, the scale of these volumetric attacks is unprecedented. The weak security of many IoT devices provides an attractive target for DDoS attackers, leveraging the bandwidth and processing resources of millions of connected devices. Botnets are frequently referred to as "zombie computers" and the metaphor is fitting: bad actors infect unsuspecting computers and network devices with malware, sending remote commands to hordes of compromised computers. Analysts have also noted the dynamic nature of Mirai Command and Control (C&C) servers (platforms used by attackers to send these remote commands to the botnets), with the malicious operator or operators switching C&C servers far more rapidly than in past botnet attacks. The United States Computer Emergency Readiness Team (US-CERT) notes in its alert that the release of the Mirai source code has increased the risk of similar botnets being created, acknowledging at least one new separate malware family leveraging IoT vulnerabilities in a manner similar to Mirai.[3]

Mirai's efficacy depends, in large part, on the unacceptably low level of security inherent in a vast array of network devices. Attackers perform wide-ranging scans of IP addresses, searching

---

[1] Level 3 Threat Research Labs, *How the Grinch Stole IoT* (October 18, 2016), http://blog.level3.com/security/grinch-stole-iot/.
[2] *See* Brian Krebs, *DDoS on Dyn Impacts Twitter, Spotify, Reddit,* KrebsOnSecurity (October 16, 2016), https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/.
[3] US-CERT, *Alert (TA16-288A): Heightened DDoS Threat Posed by Mirai and Other Botnets* (October 14, 2016), https://www.us-cert.gov/ncas/alerts/TA16-288A.

for devices with poor security features such as factory default or hard-coded (*i.e.,* unchangeable) passwords, publicly accessible remote administration ports (akin to open doors), and susceptibility to brute force attacks.[4] In my June 6th letter to the Federal Trade Commission (FTC), I raised serious concerns with the proliferation of these insecure connected consumer products, noting that the "ever-declining cost of digital storage and internet connectivity have made it possible to connect an unimaginable range of products and services to the Internet," potentially without adequate market incentives to adopt appropriate privacy and security measures. Juniper Research has projected that by the end of 2020, the number of IoT devices will grow from 13.4 to 38.5 billion – yet there is no requirement that devices incorporate even minimal levels of security. The internet's open architecture has been a catalyst for its growth, allowing an enormous range of devices and services to connect to a global, interoperable network. The lack of gating functions, however, has potentially created a systemic risk to the resiliency of the internet.

Additionally, the global nature of the supply chain for such devices requires attention not just to the final product integrator's practices, but also to that of suppliers throughout the manufacturing process. In the recent Mirai botnet, researchers have identified a single software supplier as responsible for vulnerabilities in a wide range of manufacturers' products, with Flashpoint concluding that over 500,000 connected devices were vulnerable to Mirai because of an exploitable component from a single vendor's management software.[5] Manufacturers today are flooding the market with cheap, insecure devices, with few market incentives to design the products with security in mind, or to provide ongoing support. And buyers seem unable to make informed decisions between products based on their competing security features, in part because there are no clear metrics. Because the producers of these insecure IoT devices currently are insulated from any standards requirements, market feedback, or liability concerns, I am deeply concerned that we are witnessing a 'tragedy of the commons' threat to the continued functioning of the internet, as the security so vital to all internet users remains the responsibility of none.[6] Further, buyers have little recourse when, despite their best efforts, security failures occur.

Under the Federal Communications Commission's (FCC's) Open Internet rules, ISPs cannot prohibit the attachment of "non-harmful devices" to their networks. It seems entirely reasonable to conclude under the present circumstances, however, that devices with certain insecure attributes could be deemed harmful to the "network" – whether the ISP's own network or the networks to which it is connected. While remaining vigilant to ensure that such prohibitions do not serve as a pretext for anticompetitive or exclusionary behavior, I would encourage regulators to provide greater clarity to internet service providers in this area.

---

[4] *See* Liron Segal, *Mirai: The IoT Bot That Took Down Krebs and Launched a Tbps DDoS Attack on OVH*, F5 Features (October 7, 2016), https://f5.com/about-us/news/articles/mirai-the-iot-bot-that-took-down-krebs-and-launched-a-tbps-ddos-attack-on-ovh-21937.

[5] *See* Jai Vijayan, *7 Imminent IoT Threats*, Dark Reading (October 21, 2016), http://www.darkreading.com/endpoint/7-imminent-iot-threat-/d/d-id/1327233?image_number=3.

[6] *See* Jeffrey Vagle, *Cybersecurity, Unscrupulous Diners, and Internet Stewardship,* Stanford Center for Internet and Society (October 22, 2016), https://cyberlaw.stanford.edu/blog/2016/10/cybersecurity-unscrupulous-diners-and-internet-stewardship.

DDoS attacks can be powerful tools for censorship, criminal extortion, or nation-state aggression. Tools such as Mirai source code, amplified by an embedded base of insecure devices worldwide, accomplish more than isolated nuisance; these are capabilities – weapons even – that can debilitate entire ranges of economic activity.[7] While the internet was not designed with security in mind, its *resiliency* –which serves as its animating principle – is now being undermined.

I respectfully request that you respond to the following questions:

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.[8] 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] See Bruce Schneier, *Someone Is Learning How To Take Down The Internet*, Schneier on Security (October 6, 2016), https://www.schneier.com/blog/archives/2016/09/someone_is_lear.html.

[8] See Jennifer Valentino-Devries, *Rarely Patched Software Bugs in Home Routers Cripple Security*, Wall Street Journal (January 18, 2016), http://www.wsj.com/articles/rarely-patched-software-bugs-in-home-routers-cripple-security-1453136285.

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?

I look forward to your response. If you should have any questions or concerns, please contact Rafi Martina in my office at 202-224-2023.

Sincerely,

Mark R. Warner
United States Senator