ConsumersUnion®

POLICY & ACTION FROM CONSUMER REPORTS

July 28, 2017

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Attn: Evelyn L. Remaley, Deputy Associate Administrator
Washington, DC 20230

Re: Docket No. 17062536-7536-01
Request for Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats

Dear Deputy Associate Administrator:

Consumers Union, the policy and mobilization arm of Consumer Reports,[1] appreciates this opportunity to comment on the National Telecommunications and Information Administration's (NTIA) request for comments on ways to improve industry's ability to reduce threats perpetrated by automated distributed attacks, such as botnets, and what role, if any, the government should play in this area. We are pleased that the NTIA is considering the implications of repeated automated distributed attacks on our economy and our society, and we look forward to working with you to help ensure that NTIA's efforts serve the interests of consumers.

Botnets have threatened our digital ecosystem since the early 2000s, but the proliferation of connected devices has made it easier for botnets to launch automated distributed denial of service attacks. The presence and proliferation of connected devices for consumers, industrial operations, and public infrastructure without sufficient digital security measures endangers the internet that these devices depend on. These concerns require the sustained attention of a variety of experts in and out of the government. Until and unless all connected devices are made more secure, botnet attacks will continue to be a threat. As shown by the October 2016 distributed denial of service (DDoS) attack, botnets have the capability to make large sections of the internet

[1] Consumers Union is the policy and mobilization arm of Consumer Reports. Consumers Union is an expert, independent, nonprofit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. It conducts this work in the areas of telecommunications reform, as well as financial services reform, food and product safety, health care reform, and other areas. Consumer Reports is the world's largest independent product-testing organization. Using its more than 50 labs, auto test center, and survey research center, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 8 million subscribers to its magazine, website, and other publications.

unavailable to users, such as popular sites like Twitter, Reddit, and Paypal. The Mirai virus, the perpetrator of the October 2016 DDoS attack, took down a major infrastructure provider for the internet, Dyn, through an overwhelming amount of fake clicks,[2] also known as click fraud. Click fraud can be used for financial gain since sites like Google pay site owners according to how many clicks they receive on any one advertisement. The continued existence of click fraud through botnets also has the ability to undermine the current economic model of the internet since it is challenging for sites to determine which clicks are legitimate and which are from a botnet and not an individual user. Additionally, botnets can be used to evade spam filters, speed up guessing passwords in order to break into online accounts, and mine bitcoins. The ability to evade spam filters and break passwords more quickly puts consumer data, including highly personal data, at risk. The use of botnets to mine bitcoins also increases the financial incentive for malicious actors to make use of insecure devices.

Due to the continued and increased proliferation of internet connected devices, as well as the poor security provided on many of these devices, DDoS attacks perpetrated by botnets is expected to increase and continue. In 2015, there were 4.9 billion connected devices in use, and this number is expected to balloon to 20-50 billion devices by 2020.[3] Consumers use the majority of IoT services for connected devices. In 2017, 63 percent of the overall number of IoT applications were consumer applications. Not only are most of these services used by consumers, but the danger presented by botnet attacks is only growing as we connect more and more devices that affect our physical security, including medical devices, smart home systems, drones, cars, and other essential devices, to the internet without sufficient security.

Although consumers desire connected devices that can make their lives easier, more efficient, and more productive, consumers are generally unaware or unable to protect against the security concerns posed by vulnerable or outdated IoT devices and accompanying software. Currently, the safety of connected devices is often obscured or unknown to the common consumer. Although earlier forms of attacks on computers, like viruses and worms, affected the functionality of the infected device, newer cybersecurity threats, like the Mirai virus, are difficult or even impossible to detect by a user because they frequently do not affect how users experience the device. Because of this, many owners are unaware that their connected routers, cameras, or DVRs are compromised and part of a botnet attack.

Because the poor security of connected devices tends to affect people *other* than the users or creators of the devices, manufacturers and owners of insecure devices tend to have little incentive to make the devices more secure. Manufacturers are incentivized by the function and features of the device rather than security of the connect product. Many connected products are shipped with default passwords that are rarely changed by the end user and many connected

[2] There are various ways to commit click fraud. One easy way is to embed a Google ad in a web page that the individual owns. The attacker then instructs all the connected devices on his botnet to repeatedly visit the site and click on the advertisement. Bruce Schneier, *Botnets*, SCHNEIER ON SECURITY (Mar. 1, 2017), https://www.schneier.com/blog/archives/2017/03/botnets.html.
[3] *Gartner Says 8.4 Billion Connected "Things" Will be in Use in 2017, Up 31 Percent from 2016*, GARTNER (Feb. 7, 2017), http://www.gartner.com/newsroom/id/3598917.

products are not designed to be patched, rendering the product vulnerable to attack.[4] As a result, government action to increase the security of connected devices—in the form of law enforcement, education, and fostering strong self-regulatory measures—is warranted. Among other things, manufacturers of connected devices should be encouraged to run secure software. This means that IoT devices should be designed with the security of the devices in mind. In addition, products should be regularly patched and updated in order to respond to attacks and prevent vulnerable devices from being hijacked by botnets. Even inexpensive connected devices should be patched regularly and designed with security in mind. Nongovernmental standards—like the Digital Testing Standard[5] that Consumer Reports recently developed and announced with its partners—can play a significant role in strengthening and complementing government efforts to promote stronger security.

We urge the NTIA to facilitate stakeholder conversations and recommendations that will lead to safer and more secure connected devices in order to protect our digital infrastructure and the security of consumers and their data.

Respectfully submitted,

Katie McInnis
Staff Attorney
Consumers Union

[4] Bruce Schneier, *Security and the Internet of Things*, SCHNEIER ON SECURITY (Feb. 1, 2017), https://www.schneier.com/blog/archives/2017/02/security_and_th.html.

[5] The Digital Testing Standard (theDigitalStandard.org) was launched on March 6th, 2017 and is the result of a collaboration with our cybersecurity partners, Disconnect, Ranking Digital Rights, and the Cyber Independent Testing Lab. The Standard is designed to hold companies accountable and equip Consumer Reports and other organizations to test and rate products for how responsibly they handle our private data. This is a collaborative and open source effort. The Standard is designed to empower consumers to make informed choices about the connected products, apps, and services consumers use everyday.