RICHARD BLUMENTHAL
CONNECTICUT

COMMITTEES:

AGING

ARMED SERVICES

COMMERCE, SCIENCE, AND TRANSPORTATION

JUDICIARY

VETERANS' AFFAIRS, RANKING MEMBER

United States Senate

WASHINGTON, DC 20510

706 HART SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-2823
FAX: (202) 224-9673

90 STATE HOUSE SQUARE, TENTH FLOOR
HARTFORD, CT 06103
(860) 258-6940
FAX: (860) 258-6958

915 LAFAYETTE BOULEVARD, ROOM 230
BRIDGEPORT, CT 06604
(203) 330-0598
FAX: (203) 330-0608

http://blumenthal.senate.gov

November 3, 2016

The Honorable Edith Ramirez
Chairwoman, Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20530

Dear Chairwoman Ramirez:

Investigators now believe that the recent hack against the internet routing company Dyn was powered by multiple massive "botnets" comprised of vulnerable Internet of Things (IoT) devices. This attack, which shut down an array of popular websites and services, including Amazon, PayPal, The New York Times, and Twitter, severely disrupted the economy, consumer access to news and entertainment, and could have endangered public safety. While unprecedented, this episode was hardly unpredictable and could just be a preview of what's to come if aggressive action is not taken to secure Internet connected devices. Too many IoT devices today remain shockingly deficient in basic security standards, making it far too easy for this kind of distributed denial-of-service attack to occur. As Ranking Member of the Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, I write to ask you to hold accountable any IoT manufacturers that fail to implement reasonable security standards, and could therefore be complicit in the next attack.

Malicious botnets operate by commandeering tens of thousands of vulnerable internet-connected devices and directing them to conduct criminal activity unbeknownst to the consumer. Such activity can include theft of sensitive personal and financial information, intrusions into online bank accounts, identity theft, or, as happened in this most recent attack, the take down of websites. Botnets, which thrive off of poorly protected IoT devices, cause more than $9 billion in harm to victims according to data gathered by the Department of Justice.[1]

One common strategy for hackers seeking to spread malicious malware and create botnets is to exploit common username and password pairs to gain access to a device. For example, devices that have "password" as their default password are easy to unlock. In an article uncovering who makes the IoT devices being used by botnets, security reporter Brian Krebs was able to link many of the devices to brand name companies that sell products in the United States (see Appendix).[2] He did this by matching to the respective IoT device maker, the 68 factory default username and password pairs contained in the source code of the "Mirai" botnet likely used in the recent attack. According to security researchers, the passwords on some of these IoT devices were hard-coded into the firmware and cannot even be remedied through a software

[1] https://www.fbi.gov/news/testimony/taking-down-botnets
[2] https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/

patch or firmware update.[3] Even if the password can be changed, many devices do not automatically prompt users to change the default password. Companies that don't prompt users to immediately change passwords, use obvious default passwords, or keep open risky communication ports as the default, may not be taking reasonable steps to provide security. Companies that neglect to implement such basic security standards, leaving their customers and the internet so openly vulnerable to attacks, deserve FTC scrutiny.

Thus, it is incumbent upon the FTC to examine and identify whether any IoT manufacturers with username password pairs that can be exploited by botnets also sell products in the United States that are so deficient in basic security standards that it warrants an aggressive and thorough investigation by the Commission. I encourage you to use the guidance you published in January 2015 to assess whether manufacturers implemented reasonable security standards.[4] Even though many of the IoT devices conscripted into the recent attack may have originated from overseas, strong FTC action can help improve the security standards of IoT products around the world since the United States is such a significant market.

In addition, I respectfully ask for feedback on any creative remedies to rapidly remove from shelves and homes insecure products that cannot be updated without changing the hardware. As you know, the Food and Drug Administration coordinates recalls unsafe food and drugs; the Consumer Product Safety Commission, recalls of consumer products that pose a threat to health and safety. However, there is no entity that currently coordinates or incentivizes the timely recall of products that do not necessarily pose a threat to health or safety, but may threaten personal privacy or national security. Furthermore, more publicized recalls of such insecure products could heighten consumer awareness regarding security risks associated with IoT devices and will encourage and educate consumers to look for adequate security in the products they purchase.

Thank you for your prompt attention to this critical and undoubtedly growing problem as more of our everyday products become connected to the Internet. I look forward to hearing your response.

Sincerely,

Richard Blumenthal
United States Senate

---

[3] https://krebsonsecurity.com/2016/10/iot-device-maker-vows-product-recall-legal-action-against-western-accusers/
[4] https://www.bulkorder.ftc.gov/system/files/publications/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf

Appendix

Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

Source: KrebsOnSecurity, available at https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/