U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

November 14, 2016

TO: Members, Subcommittee on Commerce, Manufacturing, and Trade, Subcommittee on Communications and Technology

FROM: Committee Majority Staff

RE: Hearing entitled "Understanding the Role of Connected Devices in Recent Cyber Attacks."

I. INTRODUCTION

On November 16, 2016, at 10:00 a.m. in 2175 Rayburn House Office Building, the Subcommittee on Commerce, Manufacturing, and Trade and the Subcommittee on Communications and Technology will hold a hearing entitled "Understanding the Role of Connected Devices in Recent Cyber Attacks." The hearing is intended to review the recent series of connected device-based DDoS attacks, understand current countermeasures, and consider future efforts to combat malicious actors that could target vulnerabilities in modern digital infrastructure.

II. WITNESSES

- Dale Drew, Senior Vice President, Chief Security Officer, Level 3 Communications;
- Kevin Fu, CEO, Virta Labs, and Associate Professor, Department of Electrical Engineering and Computer Science, University of Michigan; and,
- Bruce Schneier, Adjunct Lecturer, Kennedy School of Government, Harvard University, and Fellow, Berkman Klein Center, Harvard University.

III. BACKGROUND

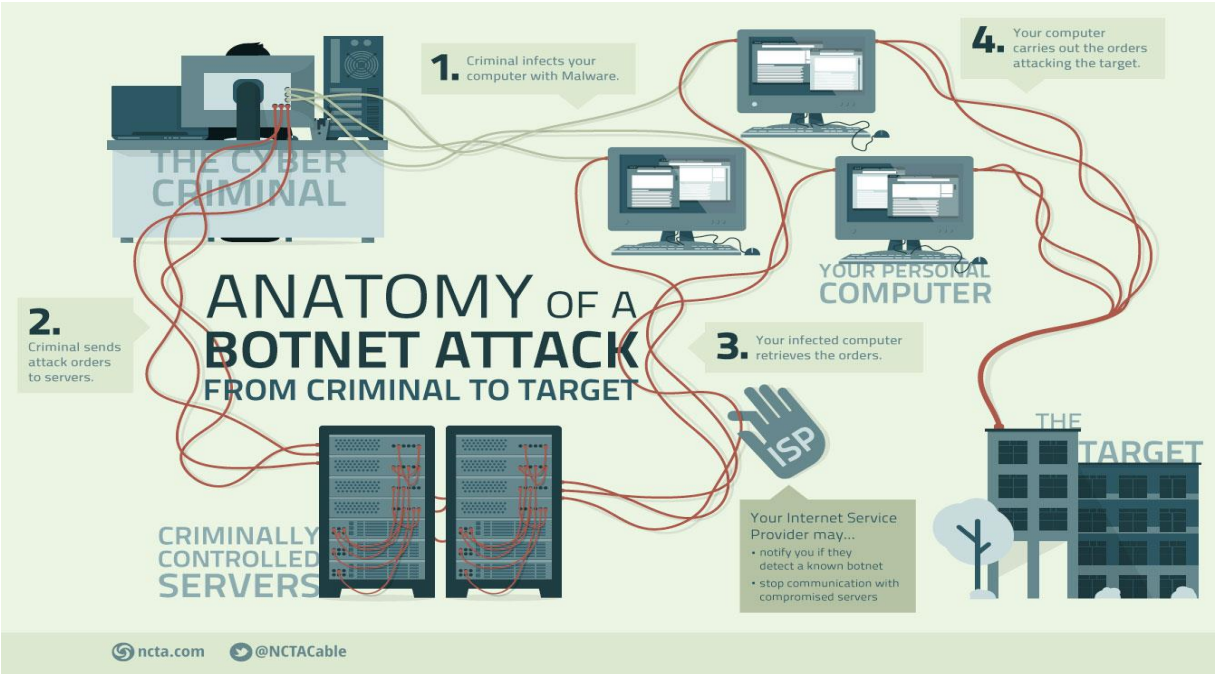
On October 21, 2016, consumers were unable to reach Netflix, Twitter, CNN, and a number of other well-known websites. This was because Dyn, a company that provides core Internet services for these websites, was experiencing a global distributed denial of service (DDoS) attack. A DDoS attack occurs when a malicious actor hacks into devices (referred to as "bots" and collectively as a "botnet") and uses them to flood the targeted site with so much junk traffic that the victim can no longer serve legitimate visitors. This attack was the largest DDoS yet seen – over one terabyte per second, approximately double the size of a similar attack two weeks prior. This DDoS attack leveraged hundreds of thousands of connected devices across the globe, internet-connected security cameras in particular, to mount this attack on Dyn.

This incident is one example of the risks associated with the increasing number of devices connecting to the global internet.[1] The proliferation of connected devices, or the Internet of Things (IoT), has been a topic of interest for the Committee. In March 2015, the Subcommittee on Commerce, Manufacturing, and Trade held a hearing entitled "The Internet of Things: Exploring the Next Technology Frontier."[2] It is estimated that 50 billion devices will be connected to the Internet by 2020.[3] While this growing technology presents a host of benefits for consumers and businesses across a variety of applications in health care, energy, education, transportation, agriculture, and others, unsecured devices can present an increasing number of entry points for malicious actors to enter the network and disrupt vital communications.

DDoS Attack Explained

Traditionally, DDoS attacks are carried out by large groups of malware-infected laptops and desktops known as "botnets." The attack traffic generated by these botnets is exacerbated through spoofing and amplification. In a typical DDoS attack, a malicious actor floods a website with illegitimate traffic, by infecting computers with malware, which then forces the infected devices to inundate a website with illegitimate traffic. Eventually, the website is disabled because it is unable to respond to all of the traffic requests.

The following graphic illustrates how cyber criminals create a botnet and, once created, how it can be leveraged to create a flood of data traffic to one target.[4]



[1] https://www.flashpoint-intel.com/attack-of-things/
[2] https://energycommerce.house.gov/hearings-and-votes/hearings/internet-things-exploring-next-technology-frontier
[3] Cisco's Internet Business Solutions Group. The Internet of Things Graphic. Available at http://blogs.cisco.com/diversity/the-internet-of-things-infographic.
[4] https://www.ncta.com/platform/technology-devices/anatomy-of-a-botnet/

The DDoS attacks seen in September and October were novel, however, in that the botnet leveraged in the attacks was not made up of laptops and desktop bots, but malware-infected IoT devices, *e.g.*, digital video recorders, remote home monitors, and webcams.[5] Termed the "Mirai" botnet after the strain of malware used to infect the bots, it successfully infected several hundred thousand devices. While the difference between computers and IoT devices may seem negligible, this fact created a DDoS attack that was unique in several ways.

First, the widespread infection and leveraging of IoT devices was novel. Second, the number of devices used meant that spoofing and amplification were not necessary; the infected devices created enough traffic to carry out a successful DDoS on their own. As most DDoS mitigation strategies rely on the detection and nullification of spoofing and amplification, stakeholders throughout the Internet struggled to respond to the attack. These factors resulted in a highly effective DDoS attack.

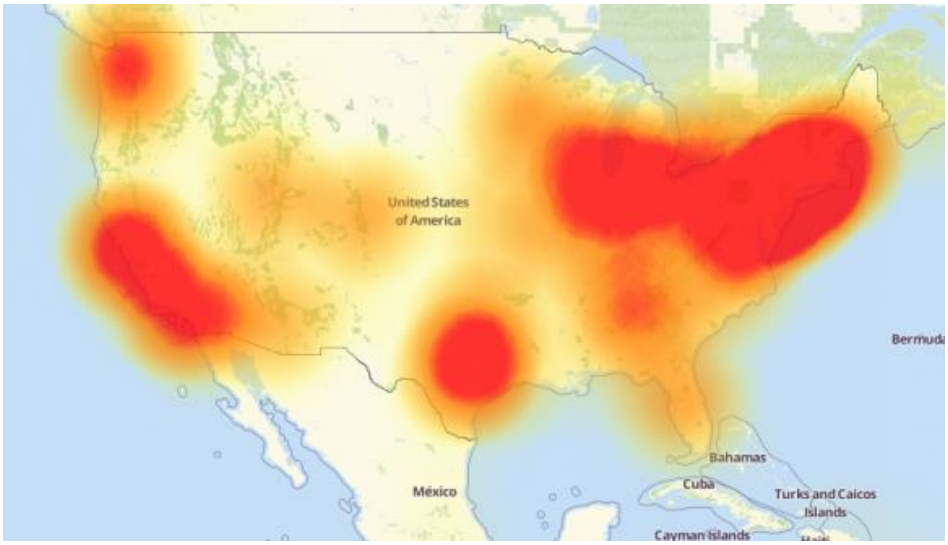
Mirai Botnet Attack Timeline

On September 21, 2016, a DDoS attack leveraging the Mirai botnet was launched against KrebsOnSecurity.com designed to knock the website offline.[6] The attack was the largest recorded to date with over 600 gigabits of traffic per second—"orders of magnitude more traffic than is typically needed to knock most sites offline."[7] Mirai was able to infect hundreds of thousands of connected devices through automatic scanning of the internet. It would search for connected devices with known username and password combinations, then use these weak credentials to take control of the devices. Researchers studying the affected devices also discovered that, for some devices, the manufacturers had not provided a method for consumers to change the usernames or passwords, and many consumers were unaware that their devices were vulnerable.

In early October, the source code for the malware strain Mirai was released publicly. On October 21, 2016, a DDoS attack was launched against Dyn, a "cloud-based Internet Performance Management (IPM) company, that offers, among others, DNS services."[8] Dyn has confirmed that the malicious traffic originated from Mirai-based botnets.[9] As a result, for two extended periods of time throughout the day, traffic was disrupted to a number of consumer-facing websites.[10] Dyn utilized a number of mitigation techniques to restore normal traffic flows including "traffic-reshaping incoming traffic, rebalancing of that traffic by manipulation of anycast policies, application of internal filtering, and deployment of scrubbing services."[11] Reports indicate that malicious traffic was generated from 100,000 connected devices, mostly

[5] https://www.flashpoint-intel.com/attempted-ddos-trump-and-clinton-websites/
[6] https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
[7] *Id.*
[8] http://dyn.com/about/
[9] http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
[10] Brian Krebs, "DDoS on Dyn Impacts Twitter, Spotify, and Reddit" October 16, 2016, available at https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/
[11] http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

physically located overseas, directed at Dyn's servers.[12] The following image is a heat map of outages caused by the attack. [13]



Select Federal Activity

The Federal Trade Commission (FTC) has initiated enforcement actions against IoT device marketers. TRENDnet settled claims alleged by the FTC for failure to use reasonable security to protect consumers' privacy in conflict with product claims that the device was secure.[14] In January 2015, the FTC produced a staff report on IoT devices after holding a workshop in November 2013.[15] The report acknowledged the many benefits of IoT as well as making recommendations about industry self-regulation on privacy and security sensitive practices.[16]

The Commerce Department has also convened and Internet Policy Task Force, comprised of the National Telecommunications and Information Administration, the Patent and Trademark Office, the National Institute of Standards and Technology, and the International Trade Administration. The Task Force has recently initiated a multi-stakeholder effort to promote transparency in IoT security, with a specific eye to how patches or upgrades to consumer IoT devices and applications are deployed.[17]

---

[12] http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
[13] Downdetector.com, October 21, 2016 reported by KrebsOnSecurity.com available at https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/.
[14] See http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles.
[15] https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
[16] While finding that IoT specific legislation is premature, the staff did call for Federal data security and privacy legislation. *Id*. at 48-50.
[17] *See* https://www.ntia.doc.gov/internet-things-security-multistakeholder-process-learn-more.

IV. ISSUES

The following issues may be examined at the hearing:

- What are the key risks associated with DDoS attacks? How is industry addressing these risks when developing new products?

- What role does the proliferation of connected devices play in the execution of a DDoS attack? How should device manufacturers assume responsibility for cybersecurity risks?

- What supply chain issues and challenges exist for hardware and software developers in the Internet of Things ecosystem? What industry consensus mechanisms exist on how to address these challenges?

V. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Paul Nagle, David Redl, Grace Koh, or Melissa Froelich of the Committee staff at (202) 225-2927.