Written by **C. Mitchell Shaw** on October 25, 2016

"Internet of Things" Hack Takes Down Large Chunk of the Internet

Last Friday, millions of Internet users across the U.S. found themselves unable to access a long list of websites as a distributed denial of service (DDoS) attack took those websites offline. The technique hackers used to cripple nearly half of the Internet was not particularly innovative or clever. The surprise about this attack is not that it happened, but that it did not happen sooner.

To understand the attack (and why it was an inevitability), one needs to understand the basics of how the Internet works. When a user visits a website, he types the name of the URL (Uniform Resource Locator) into his browser. For *The New American,* the URL is http://www.thenewamerican.com (or simply, www.thenewamerican.com). That tells the browser to reach out to one or more of the various DNS (Domain Name System) servers responsible for converting the IPv4 or IPv6 address of the website the user wishes to visit. For *The New American*, the IP address is 69.167.176.82. DNS servers are something like phone books for the Internet.

One of the largest DNS service providers is DYN. On Friday, hackers took control of a range of Internet-connected devices (sometimes called "the Internet of Things" or IoT) and used those devices to launch a DDoS attack on DYN. This works by telling the devices to bombard the servers with more requests than can be handled. An easy-to-understand comparison would be what happens after a major storm or other event when millions of people all use their phones to call and check on friends and family. Once the phone systems are overloaded, everyone gets the tri-tone recording which tells them the lines are unavailable and to "try your call again later." On the Internet, all the user gets is (at best) a connection so slow as to be nearly worthless or (at worst) an error page saying the page is unavailable.

DDoS attacks are not new. This type of attack has been around for a while, and is a variation of an older attack known as DoS (denial of service) in which a group of people would plan to take a particular site offline by visiting the site and refreshing their browsers as quickly as possible. Tools were developed to make the attacks more efficient (Low Orbit Ion Cannon is one of the most famous) by refreshing the page more quickly than is humanly possible. The distributed denial of service (DDoS) attack simply takes it to the next level by using hundreds, thousands, or (in this case) millions of computers to do the refreshing.

The IoT makes it relatively simple for a hacker to build a Botnet (a network of Bots — computers which have been hijacked to do the hacker's bidding) to carry out massive DDoS attacks. In fact, as more and more people buy into the IoT without much thought to the implications, and as the companies manufacturing IoT devices give little to no thought to the security nightmares their devices can unleash, the threat only grows. Users give little thought to the fact that their fancy new smart-watch, smart TV, or IP camera is, in fact, a computer which is able to connect to the Internet and can be hacked. Manufacturers simply do not make those devices secure enough, either because they take the shortest path to get their product to market or because they plan to harvest data about the users for the purpose of marketing and advertising.

In fact, in this DDoS attack, it was the lack of anything resembling reasonable security measures that made the work of the hackers so easy. *Bloomberg* reported Monday that a "Chinese security camera maker said its products were used to launch a cyber-attack that severed internet access for millions of users, highlighting the threat posed by the global proliferation of connected devices."

Hackers took over a large number of closed-circuit TV (CCTV) cameras manufactured by Hangzhou Xiongmai Technology with a malware program called Mirai and pointed their web-traffic toward DYN, overloading the servers and bringing a large portion of the Internet to its knees. How did the hackers gain control over the cameras? Simple. Most users never change the default username and password on the devices they purchase (similar to the same problem with most home Internet routers) and Xiongmai publishes those usernames and passwords on the Internet. This perfect tech storm was a disaster waiting to happen. Hackers simply looked up the list of usernames and passwords and then hacked tens of millions of devices using those lists. That was the hardest part of this attack and it was easy. And wildly successful. Gizmodo reported that readers had reported the following sites were either partially or totally unavailable as a result of the attack:

- ActBlue
- Basecamp
- Big cartel
- Box
- Business Insider
- CNN
- Cleveland.com
- Etsy
- Github
- Grubhub
- Guardian.co.uk
- HBO Now
- Iheart.com (iHeartRadio)
- Imgur
- Intercom
- Intercom.com
- Okta
- PayPal
- People.com
- Pinterest
- Playstation Network

- Recode
- Reddit
- Seamless
- Spotify
- Squarespace Customer Sites
- Starbucks rewards/gift cards
- Storify.com
- The Verge
- Twillo
- Twitter
- Urbandictionary.com (lol)
- Weebly
- Wired.com
- Wix Customer Sites
- Yammer
- Yelp
- Zendesk.com
- Zoho CRM
- Credit Karma
- Eventbrite
- Netflix
- NHL.com
- Fox News
- Disqus
- Shopify
- Soundcloud
- Atom.io
- Ancestry.com
- ConstantContact
- Indeed.com
- New York Times
- Weather.com
- WSJ.com
- time.com
- xbox.com
- dailynews.com
- Wikia
- donorschoose.org
- Wufoo.com
- Genonebiology.com
- BBC
- Elder Scrolls Online
- Eve Online
- PagerDuty
- Kayak

- youneedabudget.com
- Speed Test
- Freshbooks
- Braintree
- Blue Host
- Qualtrics
- SBNation
- Salsify.com
- Zillow.com
- nimbleschedule.com
- Vox.com
- Livestream.com
- IndieGoGo
- Fortune
- CNBC.com
- FT.com
- Survey Monkey
- Paragon Game
- Runescape

As the IoT continues to grow, the companies building it need to put better practices into place and the people using it need to learn how to secure their own devices. Otherwise, expect to see more attacks like this. And each attack will likely dwarf all others before it.