The Hour the Internet Stood Still

MAYANK METHA D

1MV14CS054

Buckminster Fuller had once quoted “Humanity is acquiring all the right technology for all the wrong reasons.” With advance in computer technology, the evil in the field has also advanced. Internet was developed for the people to learn and communicate. Ever wondered what will happen if there was an Internet blackout? Sounds like a scene from Mr.Robot or The Die Hard Series or like a task in Watchdogs. Well, partial Internet blackout did happen. 2016 witnessed a large amount of record breaking cyber attacks which were fictions a few years back.

**So, what exactly happened?**

On October 21st 2016, a quarter of the Internet was taken down. This was an action of cyber attack on DNS provider named Dyn. This was no ordinary cyber attack as the biggest online services like Amazon.com, BBC, Electronic Arts, GitHub, Netflix, PlayStation Network, PayPal, Spotify, Starbucks, Twitter, Visa, Xbox Live and many others were the victims of this attack. This cyber attack has a generic name called Distributed Denial of Service (DDoS). In simple nontechnical terms assume an intersection of some roads where one road takes the traffic away from the intersection while other gets traffic towards this intersection. Computer Networks have a similar issue. When multiple devices or network send message to a single device, the receiving device is unable to process all the messages at the same time. This leads to jamming of the network. Such a network jam makes the specific service unavailable. This is DDoS. The DDoS that took place on Dyn was caused by a Trojan called Mirai.

**Mirai**

Mirai (Japanese meaning future) is a simple Trojan. The reason for specifying this Trojan is because of the record it created. 1 Tbps of traffic on the network of the victim was a world record traffic generated by Mirai. It exploits the basic ideas to generate an attack. Let’s not get into more technical details of Mirai. The simplicity and power of Mirai was what interested me.

After reading about it on Kaspersky, Checkpoint and other tech related blogs, I was able to get hold of 6 strains of this Trojan. Going through the code, I did try to learn the working of the Trojan and analyse it. It targeted the Linux OS and IoT devices. Linux OS was converted to servers and IoT devices like webcams, CCTV, routers were made to report to the servers. Effected IoT devices also send messages to victims at same time. I too did try to use the server attack part of the code on my own system and try to find the other devices that were attack. This Trojan also showed me that however secure we think the computer is, there is still a drawback that can be exploited to create havoc.

A famous dialog from Spiderman goes, “With great power comes great responsibility”, technology is powerful but use it responsibly. Don’t use technology to disrupt others’ work or other criminal ways.