The new and rising popularity of IoT (Internet of Things) devices are rapidly growing and are becoming more potent in our day-to-day life. The Internet of Things means any network of devices connected to the internet. While this definition is very broad, a simpler example of an IoT device are smart home devices. If you can open and app on your phone and check the temperature of your home, the temperature and timer on your oven, or be able to turn the lights on and off from your smartphone, that is an example of an IoT device. Many appliance manufacturers, such as LG, Samsung, Whirlpool and other manufacturers of home essentials, such as Phillips, are some of the largest producers of IoT devices. To make new products more marketable, adding in the feature that the device can be controlled from anywhere around the world with an Internet connection sells. These devices can now connect to your home network, and this is the way the user is able to control them, whether from home or away.

This new technology is not only very convenient, but is a new safety feature. I know too many people who forgot they were cooking food in the oven, and left their house. When they came back, their house had caught fire. Thanks to fire alarms, which are being implemented with IoT, most time the damage doesn’t spread to the entire house. However, the home owner is left with thousands of dollars of damage and months left of repairs.

While this new technology is a convenience as well as a home safety feature, there are some downfalls to it. One being that if your home router is down, you cannot access your IoT home devices. This can be catastrophic, if you planned on leaving the house for a few hours, and wanted to turn the oven off while you were not home, you then have to go home and turn off the oven. If you are too far away, it could mean that whatever is in the oven can catch on fire.

Another risk to IoT devices is human threats. These devices, like any computer, can be hacked. One type of attack these devices are vulnerable to is called botnets, which is a network of “infected” (or hacked) devices. Each device is called a zombie, and the code deployed onto these devices is used to hack other devices. This is known as a DDoS attack (distributed denial of service).

Threats such as a DDoS attack can be catastrophic and cause lots of damage. In 2016, one of the largest botnets was created using the Mirari malware. The Mirari malware was complex but ran on a very simple principle. It used a list of 62 common username and password combinations to get access to home routers, security cameras, and other IoT devices.

To me, it sounds like the Mirari malware used a brute-force style attack. It would just keep trying the list of usernames and passwords until it a.) used the list and nothing matched or b.) was locked out after a certain number of attempts. This malware is very clever because you can just go online and look at the default username and password for any router. My guess is that the developers behind the malware did that for the most popular IoT devices. By default, routers also broadcast their SSID (or router name) so anyone in the vicinity can see it. If it’s just the default name (which is most likely the router name, and it’s not configured), then the hacker can just research the username and password for that specific router and break into the system.

I used to read a thread on Reddit about how someone would go around to different neighborhoods and see which router’s still had their default configurations. Some wouldn’t even have any password to authenticate to the network, and most times the router login was just default. While this person never did anything malicious to harm or change their network, it just went to show how easy it can be to hack into someone else’s home network.