Word Count: 474

One of the risks and attacks the book mentions is hacking. Real life hacking does not usually take place like they are portraited in the movies and the risks of being hacked are relatively low. One of the famous examples of hacking in real life is The Mirai Botnet, also known as Dyn Attack. Back in October of 2016, the largest DDoS attack ever was launched on service provider Dyn using an IoT botnet. This lead to huge portions of the internet going down, including Twitter, the Guardian, Netflix, Reddit, and CNN. [1] This IoT botnet was made possible by malware called Mirai. The risk of this event of hacking is enormous. Once infected with Mirai, computers continually search the internet for vulnerable IoT devices and then use known default usernames and passwords to log in, infecting them with malware. These devices were things like digital cameras and DVR players. As an online user, we could take precautions to prevent this attacks by doing the following: We should be regularly changing our passwords and should never use default username and password combination, however tempting that might be; passwords for the IoT device should be unique per device, especially when they are connected to the internet; and always patch IoT device with the latest software and firmware updates to mitigate vulnerabilities.

Another kind of risks and attacks the book mentions is malware. Compared to hacking, malware usually does the “labor” work and the risk of getting a malware on the computer or digital devices is pretty high. One of the most famous malware that is discovered is named Stuxnet. Stuxnet is a malicious computer worm that was responsible for causing substantial damage to Iran’s nuclear program. [2] It hid invisible inside USB drives and replicate itself when inserted into a computer. However, Stuxnet does not do anything except waiting for a chance to get on to a new USB drive if the inserted computer was not operating the targeted operating system. This way Stuxnet managed to hide for 5 years without being noticed by anyone and able to deal damage to the target but no one else. It is precise, undetectable and deadly. As normal users that have nothing to do with national secrets, we also need to take precautions towards USB driven malicious worm. First, we should never trust free USBs lying around because this is how Stuxnet is transmitted in the first place. Next, we need to install malware detectors from the USB on our laptop. Finally, we need to run antivirus software regularly and install updates to the operating system. Through these ways, we could do our best to protect ourselves from malicious software.

[1] “DDoS Attack that Disrupted Internet was Largest of Its Kind”, Bryn Bill, online, accessible, https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[2] “An Unprecedented Look at Stuxnet”, Kim Zetter, online, accessible, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/