

StuxNet

Summary

- **StuxNet** was labeled as the most significant cyberweapon ever created. It is a computer virus designed to infiltrate the target's control system, especially Iran in those times because Iran is responsible for creating and enriching its Nuclear Program. According to a journalist named Kim Zetter, the US and Israel are responsible for creating "**StuxNet**". The objective of this virus is to sabotage the system through the USB drives; once the USB is injected into the computer, it manipulates the system and creates a physical damage on the entire infrastructure. Because of the sabotage and damage, it stopped Iran from moving forward in the process of nuclear enrichment program.

The spreading of the modified virus was too aggressive and affected all the computers that were connected to the same shared drives, as well as the computers that were taken to other networks are also infecting other systems. The virus didn't affect Iran's entire system only but also the rest of the world. The discovery of Stuxnet and its impact on Iran's nuclear program raised numerous concerns such as the impact on creating this kind of cyberweapon that potentially causes physical damage to critical infrastructure and demonstrated the evolving nature of warfare in the technology world.

Reaction/Conclusions

- The creation of "**StuxNet**" only tells us that through network, it can be use as a weapon in a warfare that potentially cause damage to infrastructure. It is also served as a lesson to all individuals, organizations, or even nations that we need to focus on enhancing our cybersecurity defense to prevent those kinds of cyber-attacks.