**Weekly Cyber Intelligence Assessment**

**The Real Story of Stuxnet**

**https://www.malwarebytes.com/stuxnet**

In July 2010, *Iran's*security experts found out that **Stuxnetmalware** had spread to factories after getting into the computers of factories. The attack happened in the ***middle of July 2010,*** and the **malware was introduced to the PCs via infected USB drives**. . Iran thinks Stuxnet, the attack that slowed down Iran's work on making nuclear weapons, was caused by a malicious software program to connect the computers. This shows that non-state actors can contribute just as much to the environment of cyberwar as state actors can, which could have dangerous or even catastrophic results. Iran's security experts must use powerful antivirus software like Comodo Antivirus, which filters routinely and makes it simple to dispose of spyware and the Stuxnet malware.

Legend: **Who, What, *When,*** *Where*, Why, How, So What?!, **Possible Solution**