Stuxnet:

→ It is a malicious computer worm, first uncovered in 2010. It has been developed since 2005, it targets SCADA systems and is believed to be responsible for causing substantial damage to Iran's nuclear program.

→ It targets programmable logic controllers (PLC's), which allow the automation of electromechanical processes such as those used to control machinery on factory assembly lines, amusement rides, or centrifuges for seperating nuclear material.

→ Exploiting 4-zero day flaws, stuxnet functions by targeting machines using microsoft windows operating system and network then seeking out siemens step7 software.

→ It has three modules:

1) A worm that executes all routines related to the main payload of the attack

2) A link file that automatically executes the propagated copies of the worm

3) A root ~~link~~ kit component responsible for hiding all malicious files and process, preventing detection of the presence of stuxnet.

→ It is typically introduced to the target environment via an infected USB flash drive, thereby crossing any air gap. The worm then propagates across the network, scanning for siemens step7 software on computers controlling a PLC. In absence of either criterion, stuxnet becomes dormant inside the comp. If both the conditions are fulfilled, stuxnet introduces the infected rootkit onto the PLC and step7 software, modifying the codes and

giving unexpected commands to the PLC while returning a loop of normal operations system values feedback to users.