**Stuxnet:**

Stuxnet was a computer virus, more specifically a worm which was speculated to be developed in 2005. It is believed to be developed jointly by the U.S.A. and Israel and was majorly targeted towards Iranian nuclear facilities.

Stuxnet was designed to specifically attack SCADA (supervisory control and data acquisition) configured PLC (programmable logic controllers). PLC’s are typically used for industrial automation. The malware took care to attack only PLC’s spinning within a certain frequency range (807 Hz to 1210 Hz). Each infected was limited to spread the virus onto only 3 other machines.

The primary victim is said to be Iran while other major countries infected include Indonesia and India. It was aimed at Iranian nuclear facilities (Bushehr Nuclear Power Plant and Natanz nuclear Facility) to modify the frequency to 1410 Hz and then to 2 Hz and then to 1064 Hz affecting the operation of connected motors by changing the rotational speed resulting in the destruction of centrifuges.

Siemens PLC’s have released s detection and removal tool for Stuxnet and had reported removal of the virus successfully from 22 systems in the initial 4 months of the discovery.

**Sauron**

Sauron is a computer virus, kind of a targeted attack platform designed for long-term cyber-espionages. It was used to exfiltrated data from air-gapped networks (networks isolated from the public internet) through legitimate channels of software distribution.

The modules and network protocols in the malware used very strong encryption algorithms such as RC5, AES, Salsa20 etc. It was written in a modified Lua scripting engine which was used to implement its core platform as well as up to 50 different plugin types. It was able to exfiltrate data through even air-gapped networks using specially prepared USB devices which would store data in a place invisible to the OS. It was operational from 2011 to 2016. The malware was disguised as files from legitimate software such as kavupd.exe (Kaspersky) and KB2931368.exe (Microsoft).

Countries targeted included Russia, Iran and Rwanda amongst many others. Key government organizations were prime targets such as Scientific research centers, telecom and finance providers and even the military. It was able to collect high value intelligence compromising mot entities within its reach.

Kaspersky Lab’s Anti Targeted Attack Platform discovered the virus in September 2015 when it found irregular network traffic in government organization networks.