Cyber-Weapon and the First Ever "Stuxnet"

Dilpreet Singh Bajwa

"Cyber-Weapon"

A weapon is a tool which is used to threaten or cause physical harm to any living being. In case of war various weapons are used from simple one like swords to advance weaponry like guided missiles.

Similarly, cyber-weapon is a tool or more specifically a malware can be used in case of cyber-war or in act of cyber-terrorism to deny, manipulate, degrade, disrupt or destroy targeted information systems and networks of the opponents.

"Stuxnet"

"Stuxnet" is first ever cyber weapon. It is a sophisticated malware specifically programmed to target the Iran's nuclear facility. The stuxnet malware is believed to be joint venture of America and Israel intelligence agencies under operation called "Operation Olympic Games" but neither country openly admitted it.

Capability: It was designed to make the uranium enrichment centrifuges spin faster than normal and in result causing them to get out of control to the point of damaging them. Stuxnet reportedly damage almost one fifth of Iran's nuclear centrifuges.

Stuxnet is considered as most expensive and big project not to be able to produce other than a nation-state. Kaspersky Lab's Roel Schouwenberg estimated that it took a team of at-least ten coders and two to three years time to create the worm. Stuxnet contained multiple zero-day exploits and valid security certificates, stolen from legitimate software companies. Stuxnet has

features like anti-virus evasion techniques, valid security certificates, various propagation methods, not one but multiple Zero-day exploits which are very hard to find and this combination put more weight on the theory that the stuxnet developers had extraordinary resources at their disposal.

How Stuxnet Works: As compared to other malwares, Stuxnet does nominal harm to computers and networks that do not meet specific requirement as it is specifically designed for a purpose and attackers took special care to make sure that it hit only their designated targets. The worm consists of a layered attack against three different systems:

1. The Windows operating system,
2. Siemens PCS 7, WinCC and STEP7 industrial software applications that run on Windows and
3. One or more Siemens S7 Programmable Logic Controllers(PLCs).

Stuxnet enters in to the target environment via an infected thumb drive, thereby crossing any air gap (secure network which is physically isolated from unsecured networks, such as the public Internet). The malware then spreads across the network, scanning for Siemens Step7 software on computers controlling a PLC. In the absence of either condition, Stuxnet becomes dormant inside the machine and on fulfilling of both the conditions, Stuxnet injects the infected rootkit onto the Step7 software and PLC which further modifies the codes and send unexpected commands to the PLC. The commands are controlled by two different routines used to damage centrifuge rotors. The first routine responsible for speeding centrifuges above their maximum safe speed and then briefly slowing them below their minimum safe speed. The malware would then wait weeks to avoid detection and afterwards repeats the process. The second, more complex routine is responsible for over-pressurizing centrifuges to increase rotor stress over time. As a result the Stuxnet exerted years of wear in mere months on centrifuges, causing them to fail faster than the Iranians could replace them.

Sources:

https://www.csoonline.com/article/3250248/cyberwarfare/stuxnet-the-father-of-cyber-kinetic-weapons.html.
https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html.
https://en.wikipedia.org/wiki/Stuxnet.
https://motherboard.vice.com/en_us/article/ezp58m/the-history-of-stuxnet-the-worlds-first-true-cyberweapon-5886b74d80d84e45e7bd22ee.
https://www.lexology.com/library/detail.aspx?g=65179269-c85e-4253-a9a3-5d9ba1c9c906.