**Threat Landscapes**

**Stuxnet**

**Stuxnet Dossier**

Sophisticated malware attack targeting Iranian industrial control systems.

Included zero-day exploits, a windows rootkit, the first PLC rootkit, antivirus evasion techniques, complex process injection, and hooking code.

Self-replicates via removable drives exploiting LNK/PIF automatic file execution vulnerability.

**WannaCry**

**Enisa WannaCry Ransomware Outburst**

Malware that encrypts infected system and prompts for a payment in Bitcoin to decrypt files, after payment there is no guarantee that files will be decrypted.

Acts as a worm once in a system, self-propagating through the network in order to spread.

Affected 150 countries and over 230,000 systems.

Ransomware usually spreads via phishing emails. Method often uses social engineering to mislead recipient.

WannaCry exploits a Server Message Block vulnerability to propagate, this is often known as “EternalBlue”