Stuxnet

Stuxnet er navnet på en data orm som ble oppdaget i 2010 og senere ble betraktet som en av de mest sofistikerte skadevarene gjennom tidene. Stuxnet var laget spesifikt for å påvirke SCADA systemet til produsenten Siemens. Dette var et kontrollpanel som kontrollerer og overvåker industrielle prosesser, i dette tilfellet, i Iran sitt atomkraftverk.

Ettersom nettverket til Iran ikke var koblet til internett er det antatt at Stuxnet infiserte første gang gjennom en flyttbar enhet, som f.eks. bærbar PC, USB pinne eller annet media for å deretter spre seg gjennom det interne nettverket. Deretter lå skadevaren i dvale frem til den oppdaget programvaren til Siemens på en datamaskin. Ormen var deretter i stand til å gjøre fysisk skade på materiell gjennom kontrollene på SCADA systemet. Slik den oppnådde dette var å endre hastigheten på sentrifugene som, enten opp eller ned, samtidig som den manipulerte kontrollpanelene til å vise tilsynelatende normale verdier, slik at det ikke skulle bli oppdaget. Alt i alt resulterte dette i skade på tusenvis av sentrifuger og et stort tilbakeslag mot Iran.

Til dags dato er det ingen som har tatt på seg ansvaret for Stuxnet, men den mest trodde teorien er at det var USA og Israel som sto bak ormen. En så sofistikert skadevare som også benyttet seg av fire zero-day exploits utelukker alt annet enn statlige aktører, blant dem har både USA og Israel stor interesse for hindre fremgangen til andre land innen atomteknologi. Målet her var å sinke eller ødelegge Iran sin fremgang mot å utvikle atomvåpen. Ifølge rapporter var angrepet en del av den større operasjonen Operation Olympic Games, som startet allerede i 2007, og kan ifølge Symantec ha startet allerede så tidlig som 2005..

Skapelsen av Stuxnet var begynnelsen på en ny type krigføring. Her kan regjeringer og aktører som er sponset av staten bruke mer sofistikert skadevare for å angripe kritisk infrastruktur som kan ramme hele land. Tilsvarende angrep har stort potensiale for å ikke bare gjøre stor fysisk skade, men kan også resultere i at liv går tapt. Flere land har som en respons lagt større ressurser i cyber-forsvar for å både beskytte seg mot slike angrep, men også ha muligheten til å utføre lignende selv.

Oppdagelsen av Stuxnet har skapt oppmerksomhet og bekymringer rundt de potensielle skadene som lignende angrep kan ha på kritisk infrastruktur som nasjonale strømnettverk, helsesektor og transport. Et angrep på slike systemer kan sørge for store økonomiske tap, tap av menneskeliv og starte internasjonal krig.

Til slutt så representerer Stuxnet en ny æra innen krigføring og skinner et lys på behovet for samarbeid mellom nasjoner og skaper et behov for regler innen digital krigføring. Dette var bare starten på hvilke farer som er mulig og det kan godt hende at det er utallige lignende ormer eller skadevare som er i bruk, men ikke oppdaget enda.

Skrekkscenario

Et scenario som er reelt og det har vært eksempler på, som kan påvirke «vanlige mennesker», er hacking av biler. Det er allerede vært oppdager flere sårbarheter ved moderne biler som benytter seg av mer og mer digital teknologi i sine funksjoner. Så langt har nøkler, gps og lignende blitt angrepet, men nå finnes det allerede selvkjørende biler, selv om de ikke er i produksjon kommersielt. Kan disse på sikt bli utsatt for angrep og kan da menneskeliv stå i fare?

Kilder:

https://en.wikipedia.org/wiki/Stuxnet

https://en.wikipedia.org/wiki/Operation_Olympic_Games#:~:text=Operation%20Olympic%20Games%20was%20a,uses%20of%20offensive%20cyber%20weapons.

https://docs.broadcom.com/doc/stuxnet-missing-link-13-en

https://www.imdb.com/title/tt5446858/