**Vicko Bhayyu / 09011181520036**

**STUXNET**

Stuxnet adalah worm yang dirancang untuk menyerang beberapa sistem Siemens SCADA yang terjadi pada Juni 2010 yang menyerang paling sedikit 14 industri di Iran. Worm ini pertama menyerang mesin dan network Microsoft Windows, kemudian menyerang software Siemens Step7, yang berbasis windows dan digunakan untuk program sistem kontrol industry yang mengoperasikan peralatan.

**Cara Stuxnet bekerja**

**Penyebaran Stuxnet**

**Auto-updating**

Stuxnet dapat melakukan update dengan sendirinya melalui Step7 Project yang terinfeksi. Jika project tersebut dibuka, dan terdapat versi terbaru dari Stuxnet, maka computer tersebut akan melakukan update.

Selain itu Stuxnet menggunakan P2P network untuk mengupdate versi nya yang ada pada local network. Setiap copy akan memulai RPC (Remote Procedure Call) server.

**Command and Control**

Stuxnet mengirim IP Address target, sejumlah data, dan payload yang berisi host OS, host name, domain name, dan flag yang mengindikasikan apakah Siemens Step7 atau WinCC target terpasang ke 2 server via HTTP :

* [www.mypremierfutbol.com](http://www.mypremierfutbol.com)
* [www.todaysfutbol.com](http://www.todaysfutbol.com)

Data yang dikirimkan dari dan ke server terenkripsi, dengan berbeda key yang di XOR kan dengan data