Fri, 24 Sep 2010

San Francisco, California and London, England (FT.com) –

Stuxnet Computer Worm

A piece of highly sophisticated malicious software that has infected an unknown number of power plants, pipelines and factories over the past year is the first program designed to cause serious damage in the physical world, security experts are warning.

The Stuxnet computer worm spreads through previously unknown holes in Microsoft's Windows operating system and then looks for a type of software made by Siemens and used to control industrial components, including valves and brakes.

Stuxnet can hide itself, wait for certain conditions and give new orders to the components that reverse what they would normally do, the experts said. The commands are so specific that they appear aimed at an industrial sector, but officials do not know which one or what the affected equipment would do.

While cyber attacks on computer networks have slowed or stopped communication in countries such as Estonia and Georgia, Stuxnet is the first aimed at physical destruction and it heralds a new era in cyberwar.

At a closed-door conference this week in Maryland, Ralph Langner, a German industrial controls safety expert, said Stuxnet might be targeting not a sector but perhaps only one plant, and he speculated that it could be a controversial nuclear facility in Iran.

According to Symantec, which has been investigating the virus and plans to publish details of the rogue commands on Wednesday, Iran has had far more infections than any other country. "It is not speculation that this is the first directed cyber weapon", or one aimed at a specific real-world process, said Joe Weiss, a US expert who has testified to Congress on technological security threats to the electric grid and other physical operations. "The only speculation is what it is being used against, and by whom."

Experts say Stuxnet's knowledge of Microsoft's Windows operating system, the Siemens program and the associated hardware of the target industry make it the work of a well-financed, highly organised team.

They suggest that it is most likely associated with a national government and that terrorism, ideological motivation or even extortion cannot be ruled out.

Stuxnet began spreading more than a year ago but research has been slow because of the complexity of the software and the difficulty in getting the right industry officials talking to the right security experts.

Microsoft has patched the vulnerabilities in Windows but experts remain concerned because of the worm's ability to hide once it is in a system.

Experts have only begun publishing more of their analyses in the last few weeks, hoping that such steps will get more answers from private companies and government leaders.
Siemens said that since July 15, when it first learnt about Stuxnet, 15 of its customers had reported being infected by the worm. The company would not name the customers but said that five were in Germany and the rest were spread around the world. Siemens said critical infrastructure had not been affected by the virus and in each case the worm had been removed.

The German conglomerate said it had offered its customers a fix for the virus and that since the Stuxnet virus was detected, there had been 12,000 downloads of its anti-virus software.

FT.com