World's first 'cyber superweapon' attacks China

September 30 2010

The Stuxnet computer worm has wreaked havoc in China, infecting millions of computers around the country, state media have reported.

A computer virus dubbed the world's "first cyber superweapon" by experts and which may have been designed to attack Iran's nuclear facilities has found a new target -- China.

The Stuxnet computer worm has wreaked havoc in China, infecting millions of computers around the country, state media reported this week.

Stuxnet is feared by experts around the globe as it can break into computers that control machinery at the heart of industry, allowing an attacker to assume control of critical systems like pumps, motors, alarms

and valves.

It could, technically, make factory boilers explode, destroy gas pipelines or even cause a nuclear plant to malfunction.

The virus targets control systems made by German industrial giant Siemens commonly used to manage water supplies, oil rigs, power plants and other industrial facilities.

"This malware is specially designed to sabotage plants and damage industrial systems, instead of stealing personal data," an engineer surnamed Wang at antivirus service provider Rising International Software told the Global Times.

"Once Stuxnet successfully penetrates factory computers in China, those industries may collapse, which would damage China's national security," he added.

Another unnamed expert at Rising International said the attacks had so far infected more than six million individual accounts and nearly 1,000 corporate accounts around the country, the official Xinhua news agency reported.

The Stuxnet computer worm -- a piece of malicious software (malware) which copies itself and sends itself on to other computers in a network -- was first publicly identified in June.

It was found lurking on Siemens systems in India, Indonesia, Pakistan and elsewhere, but the heaviest infiltration appears to be in Iran, according to software security researchers.

A Beijing-based spokesman for Siemens declined to comment when contacted by AFP on Thursday.

Yu Xiaoqiu, an analyst with the China Information Technology Security Evaluation Centre, downplayed the malware threat.

"So far we don't see any severe damage done by the virus," Yu was quoted by the Global Times as saying.

"New viruses are common nowadays. Both personal Internet surfers and Chinese pillar companies don't need to worry about it at all. They should be alert but not too afraid of it."

A top US cybersecurity official said last week that the country was analysing the computer worm but did not know who was behind it or its purpose.

"One of our hardest jobs is attribution and intent," Sean McGurk, director of the National Cybersecurity and Communications Integration Center (NCCIC), told reporters in Washington.

"It's very difficult to say 'This is what it was targeted to do,'" he said of Stuxnet, which some computer security experts have said may be intended to sabotage a nuclear facility in Iran.

A cyber superweapon is a term used by experts to describe a piece of malware designed specifically to hit computer networks that run industrial plants.

"The Stuxnet worm is a wake-up call to governments around the world," Derek Reveron, a cyber expert at the US Naval War School, was quoted as saying Thursday by the South China Morning Post.

"It is the first known worm to target industrial control systems."