

Stuxnet Worm a U.S. Cyber-Attack on Iran Nukes?

Written by bad_brain

Friday, 24 September 2010 19:08 - Last Updated Friday, 24 September 2010 19:22

A top expert in protecting industry and infrastructure from cyber-attacks has told the [Financial Times](#) that a computer worm which surfaced more than a year ago may well have been a deliberate attempt by the U.S. government to destroy Iran's primary nuclear facility.

The Stuxnet worm has been researched for months, but its design is so complex that security experts are still unable to say definitively who or what it was created to attack.

The worm exploits gaps in Windows operating systems (which Microsoft has since patched) to attack very specific Siemens software used to operate industrial machinery, reports the FT.

Ralph Langner, an expert in protecting industrial systems, told a closed conference in Maryland this week that the worm may be aimed, not just at the Siemens software, but specifically at a "controversial nuclear facility in Iran," according to the newspaper.

The report did not specify which of Iran's nuclear plants Langner suspected was under attack, but the reference to a controversy makes it likely the facility at Natanz -- where Iran conducts most of its uranium enrichment despite global demands to halt the activity -- is in question.

Computer security company Symantec tells the FT that Iran has been subjected to far more infections by Stuxnet than any other country. There was no indication as to where, specifically, those infections were cropping up.

Another unusual characteristic of the Stuxnet worm, according to the experts who spoke to the

Stuxnet Worm a U.S. Cyber-Attack on Iran Nukes?

Written by bad_brain

Friday, 24 September 2010 19:08 - Last Updated Friday, 24 September 2010 19:22

FT, is that it is the first virus apparently designed to cause physical harm to systems outside a computer or computing network.

"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," says the article, which appears on the FT's front page Friday.

Siemens, which has supplied a great deal of both hardware and software to Iran for its nuclear energy program, told the FT it had provided clients with a fix for the Stuxnet worm.

It was unclear from the article whether experts believe the virus still represents a threat to Iran's nuclear program, or industrial facilities using the Siemens software elsewhere in the world.

The FT says the complexity of the virus has led experts to believe a "highly organized team" is behind Stuxnet -- most likely a government.