- War in Context - http://warincontext.org -

Iran targeted in cyber attack

Posted By Paul Woodward On August 5, 2010 @ 9:00 am In Defense Department, Editorials, Iran, Israel | Comments Disabled

Last September, *Reuters* reported [1]: "Israel has been developing "cyber-war" capabilities that could disrupt Iranian industrial and military control systems. Few doubt that covert action, by Mossad agents on the ground, also features in tactics against Iran. An advantage of sabotage over an air strike may be deniability."

Now it seems, such an attack may have occurred in recent months.

"Looks like this malware was made for espionage," was the assessment of industry analyst Frank Boldewin [2] when describing the recently discovered computer worm, known has Stuxnet. It targets Siemens SCADA (supervisory control and data acquisition) management systems that control energy utilities, transportation, and other vital systems. Elias Levy, senior technical director with Symantec Security Response, said: "The most we can say is whoever developed these particular threats was targeting companies in those geographic areas," when explaining why this particular trojan has had its greatest impact in Iran [3].

It is just two months since the newly-created United States Cyber Command [4] based at Fort Meade, Maryland, became operational. The creation of CYBERCOM is ostensibly a response to the United States' vulnerability to cyber attacks. "Given our increasing dependency on cyberspace, this new command will bring together the resources of the department to address vulnerabilities and meet the ever-growing array of cyberthreats to our military systems," Defense Secretary Robert Gates said in a statement.

But as Robert Fry [5], a former Deputy Commanding General of coalition forces in Iraq, notes, "the speed of cyber operations places a premium on first strike and so inverts the Clausewitzian principle of the inherent advantage of defense." Thus, as *Federal Computer Week* [6] points out: "CYBERCOM also oversees offensive cyber capabilities, and that involves developing weapons and the doctrine that governs when and how those weapons can be used."

Did we just witness one of the opening shots in a cyber war against Iran? Stuxnet is, according to Andy Greenberg [7], "the first publicly-known threat, aside from occasional unattributed reports, to target the long-vulnerable infrastructure systems." As such, the most likely instigator of such an attack would be a hostile government.

The question is: which government? Israel and/or the United States have to be the prime suspects.

Share [8]

URLs in this post:
[1] *Reuters* reported: **http://www.reuters.com/assets/print?aid=USLQ156361**
[2] Frank Boldewin: **http://krebsonsecurity.com/2010/07/experts-warn-of-new-windows-shortcut-flaw/**
[3] greatest impact in Iran: **http://www.businessweek.com/idg/2010-07-23/iran-was-prime-target-of-scada-worm.html**
[4] United States Cyber Command: **http://en.wikipedia.org/wiki/United_States_Cyber_Command**

[5] Robert Fry: **http://online.wsj.com/article/SB 10001424052748703724104575379343636553602.html**
[6] *Federal Computer Week*: **http://fcw.com/Articles/2010/07/26/FEAT-Cyber-Command-tackles-cyber-war.aspx?p=1**
[7] Andy Greenberg: **http://blogs.forbes.com/firewall/2010/07/23/stuxnet-spyware-still-mostly-infecting-middle-east/**
[8] Share: **http://www.facebook.com/sharer.php**