Software smart bomb fired at Iranian nuclear plant: experts

September 24 2010, by Glenn Chapman

Computer security experts are studying a scary new cyber weapon: a software smart bomb that may have been crafted to find and sabotage a nuclear facility in Iran.

Malicious software, or malware, dubbed "Stuxnet" is able to recognize a specific facility's control network and then destroy it, according to German computer security researcher Ralph Langner.

"Welcome to cyber war," Langner said in a post at his website. "This is sabotage."

Langner has been analyzing Stuxnet since it was discovered in June and said the code had a technology fingerprint of the control system it was seeking and would go into action automatically when it found its target.

"It's pretty amazing," James Lewis, a senior fellow at the Center for Strategic and International Studies, told AFP on Thursday. "It looks like more than simple cyber espionage."

Stuxnet was tailored for Siemens supervisory control and data acquisition (SCADA) systems commonly used to manage water supplies, oil rigs, power plants and other industrial facilities.

It traveled by sneaking onto USB memory sticks and was able to thereby hop from system to system without needing the Internet, according to Roel Schouwenberg, senior anti-virus researcher at Kaspersky Lab

Americas.

Stuxnet is considered a malware "worm" because it burrows from machine to machine, replicating itself on the way.

Once in a computer system running on Windows software, Stuxnet checked for any of three Siemens SCADA programmable logic controllers (PLCs) that manage functions such as cooling or turbine speed, Schouwenberg told AFP.

If there was a match, Stuxnet automatically took over control of the PLC and hid any changes from workers operating or managing a system, according to Schouwenberg.

"When the operator looks at the plant, everything will look just fine," Schouwenberg said. "Meanwhile, the machine will be overloading. Its ultimate goal is cyber sabotage."

"Stuxnet manipulates a fast running process," Langner explained at his website. "We can expect that something will blow up soon. Something big."

The software saboteur has been found lurking on systems in India, Indonesia, Pakistan and elsewhere, but the heaviest infiltration appeared to be in Iran, according to software security researchers.

"This was assembled by a highly qualified team of experts, involving some with specific control system expertise," Langner said.

"This is not some hacker sitting in the basement of his parents' house. The resources needed to stage this attack point to a nation state."

The pattern of spread correlated somewhat with jobs handled by a firm

commissioned to work at nuclear facilities, according to researchers.

Langner suspected Stuxnet's mark was the Bushehr nuclear facility in Iran. Unspecified problems have been blamed for a delay in getting the facility fully operational.

On August 31, Iranian atomic chief Ali Akbar Salehi blamed "severe hot weather" for a delay in moving fuel rods into its Russian-built first nuclear power plant.

"Look at the Iranian nuclear program," Langner said. "Strange -- they are presently having some technical difficulties down there in Bushehr."

There have been Stuxnet infections all over the world and it was impossible to be certain the target was Iran, Schouwenberg cautioned.

Stuxnet creators left plenty of clues in the malware, giving the impression they didn't fear being caught, according to Langner.

"The whole attack only makes sense within a very limited timeframe," Langner said. "After Stuxnet is analyzed, the attack won't work any more. It's a one-shot weapon."

Microsoft has already patched two of four Windows operating system vulnerabilities exploited by Stuxnet, according to Schouwenberg.

"For the most part, Stuxnet has been mitigated," the researcher said. "The question now is whether this is going to be a one-off thing or is it setting a precedent?"

Citation: Software smart bomb fired at Iranian nuclear plant: experts (2010, September 24)