PHYS.ORG

No apparent Stuxnet impact in US: cyber official

December 7 2010

Iranian President Mahmoud Ahmadinejad visiting the Natanz uranium enrichment facilities some 300 kms south of the capital Tehran. Most Stuxnet infections have been discovered in Iran, giving rise to speculation it was intended to sabotage nuclear facilities there.

Computer software targeted by Stuxnet is used in US infrastructure but the virus does not appear to have affected any systems in the United States, a US cybersecurity official said Tuesday.

Greg Schaffer, assistant secretary for cybersecurity and communications in the Department of Homeland Security (DHS), told reporters here that Stuxnet demonstrates the increasingly sophisticated nature of cyber threats today.

"It was a very tiered, very complex, very sophisticated virus," Schaffer told the Defense Writers Group.

"It was looking for specific kinds of software and very special implementations within that software," he said.

Stuxnet targets computer control systems made by German industrial giant Siemens and commonly used to manage water supplies, oil rigs, power plants and other critical infrastructure.

Most Stuxnet infections have been discovered in Iran, giving rise to speculation it was intended to sabotage nuclear facilities there.

Computer security firm Symantec said last month that Stuxnet may have been specifically designed to disrupt the motors that power gas centrifuges used to enrich uranium.

Schaffer said Stuxnet "focused on specific software implementations and those software implementations did exist in some US infrastructure so there was the potential for some US infrastructure to be impacted at some level."

"There was some risk because those software packages exist within the US ecosystem, but it's not clear that there's any particular process that is in the United States that would have triggered the software," he said.

Schaffer said US cybersecurity experts "made a lot of information available to the community of interest with respect to what the code was really designed to do, which systems it was designed to attack and how it actually worked."

He added cyber threats today are becoming "more sophisticated, more targeted, more capable, harder to detect, harder to mitigate."

"This is no longer a world in which malicious defacements of Web pages are what we are focused on," he said. "We are worried about the migration towards things of value, intrusions that are very targeted and very specific."

"I cannot rule out the potential vulnerability of any system that is connnected to the network today," he said.

"It is widely recognized that the cyber ecosystem that we have today favors the offense and not the defense," he said.

Schaffer declined to discuss the release of secret US diplomatic cables by WikiLeaks. "I really have no comment on the WikiLeaks problem," he said. "DHS has as its focus the protection of our networks."

Citation: No apparent Stuxnet impact in US: cyber official (2010, December 7) retrieved 6 May 2024 from https://phys.org/news/2010-12-apparent-stuxnet-impact-cyber.html