Stuxnet virus could target many industries

November 17 2010, By LOLITA C. BALDOR , Associated Press

(AP) -- A malicious computer attack that appears to target Iran's nuclear plants can be modified to wreak havoc on industrial control systems around the world, and represents the most dire cyberthreat known to industry, government officials and experts said Wednesday.

They warned that industries are becoming increasingly vulnerable to the so-called Stuxnet worm as they merge networks and computer systems to increase efficiency. The growing danger, said lawmakers, makes it imperative that Congress move on legislation that would expand government controls and set requirements to make systems safer.

The complex code is not only able to infiltrate and take over systems that control manufacturing and other critical operations, but it has even more sophisticated abilities to silently steal sensitive intellectual property data, experts said.

Dean Turner, director of the Global Intelligence Network at Symantec Corp., told the Senate Homeland Security and Governmental Affairs Committee that the "real-world implications of Stuxnet are beyond any threat we have seen in the past."

Analysts and government officials told the senators they remain unable to determine who launched the attack. But the design and performance of the code, and that the bulk of the attacks were in Iran, have fueled speculation that it targeted Iranian nuclear facilities.

Turner said there were 44,000 unique Stuxnet computer infections worldwide through last week, and 1,600 in the United States. Sixty percent of the infections were in Iran, including several employees' laptops at the Bushehr nuclear plant.

Iran has said it believes Stuxnet is part of a Western plot to sabotage its nuclear program, but experts see few signs of major damage at Iranian facilities.

A senior government official warned Wednesday that attackers can use information made public about the Stuxnet worm to develop variations targeting other industries, affecting the production of everything from chemicals to baby formula.

"This code can automatically enter a system, steal the formula for the product you are manufacturing, alter the ingredients being mixed in your product and indicate to the operator and your antivirus software that everything is functioning as expected," said Sean McGurk, acting director of Homeland Security's national cybersecurity operations center.

Stuxnet specifically targets businesses that use Windows operating software and a control system designed by Siemens AG. That combination, said McGurk, is used in many critical sectors, from automobile assembly to mixing products such as chemicals.

Turner added that the code's highly sophisticated structure and techniques also could mean that it is a one-in-a-decade occurrence. The virus is so complex and costly to develop "that a select few attackers would be capable of producing a similar threat," he said.

Experts said governments and industries can do much more to protect critical systems.

Michael Assante, who heads the newly created, not-for-profit National

Board of Information Security Examiners, told lawmakers that control systems need to be walled off from other networks to make it harder for hackers to access them. And he encouraged senators to beef up government authorities and consider placing performance requirements and other standards on the industry to curtail unsafe practices and make systems more secure.

"We can no longer ignore known system weaknesses and simply accept current system limitations," he said. "We must admit that our current security strategies are too disjointed and are often, in unintended ways, working against our efforts to address" cybersecurity challenges.

The panel chairman, Sen. Joe Lieberman, I-Conn., said legislation on the matter will be a top priority after lawmakers return in January.

More information: Senate Homeland Security and Governmental Affairs Committee: http://hsgac.senate.gov/public/

Citation: Stuxnet virus could target many industries (2010, November 17) retrieved 20 March 2024 from https://phys.org/news/2010-11-stuxnet-virus-industries.html