PHYS ORG

Stuxnet-like virus points to new round of cyber war

October 20 2011, by Glenn Chapman

The McAfee logo, pictured on August 19, 2010, is displayed outside the company's headquarters in Santa Clara, California. Internet security specialists have warned of a new round of cyber warfare in the form of a computer virus similar to the malicious Stuxnet worm believed to have targeted Iran's nuclear program.

Internet security specialists have warned of a new round of cyber warfare in the form of a computer virus similar to the malicious Stuxnet worm believed to have targeted Iran's nuclear program.

Analysts at US firms McAfee and Symantec agreed that a sophisticated virus dubbed "Duqu" has been unleashed on an apparent mission to gather intelligence for future attacks on industrial control systems.

"This seems to be the reconnaissance phase of something much larger," McAfee senior research analyst Adam Wosotowsky told AFP about the virus, named for the "DQ" prefix on files it creates.

McAfee and Symantec said that, based on snippets of the virus they were given to study, portions of the encrypted Duqu code matched identically scrambled portions of Stuxnet.

"The threat was written by the same authors (or those that have access to the Stuxnet source code) and appears to have been created since the last Stuxnet file was recovered," Symantec said on its website.

"Duqu's purpose is to gather intelligence data and assets from entities, such as industrial control system manufacturers, in order to more easily conduct a future attack against another third party.

"The attackers are looking for information such as design documents that could help them mount a future attack on an industrial control facility."

Symantec said the virus had been aimed at "a limited number of organizations for their specific assets," without providing further information.

McAfee was working to trace a timeline of Duqu's spread and the areas it has reached.

"It seems to be primarily centered on the Middle East, then India, Africa and Eastern Europe," Wosotowsky said. "I haven't seen any reports in North or South America."

Duqu was crafted to steal information by logging computer key strokes or mining machines for valuable data such as passwords or credentials that could be used to slip into networks undetected, according to

McAfee.

Duqu is able to pass information to its creators through "command and control" computers that could then be used to issue new orders, such as seizing control of factory machinery.

File photo shows a security officer standing next to journalists outside the Russian-built Bushehr nuclear power plant in southern Iran on August 21, 2010. Most Stuxnet infections have been discovered in Iran, giving rise to speculation it was intended to sabotage nuclear facilities there.

"Our guess is that it is going after infiltrating certificate authorities to then use those to sign programs and install itself much more cleanly on more protected, locked-down networks," Wosotowsky said.

Symantec said it was alerted to the threat on October 14 by a "research lab with strong international connections."

McAfee, like Symantec, declined to identify the research facility that tipped it off.

Wosotowsky saw Duqu as evidence that nation states are taking their conflicts into the cyber world.

"Normal people shouldn't be highly concerned with getting an infection in their personal, independent systems," Wosotowsky said.

"But they should be concerned that we are going to see the militarization of cyber space going forward... This is a new face of international conflict."

Stuxnet was designed to attack 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. The worm was crafted to recognize the system it was to attack.

The New York Times reported in January that US and Israeli intelligence services collaborated to develop the computer worm to sabotage Iran's efforts to make a nuclear bomb.

Tehran has always denied it is seeking nuclear weapons.

Citation: Stuxnet-like virus points to new round of cyber war (2011, October 20) retrieved 20 March 2024 from https://phys.org/news/2011-10-stuxnet-like-virus-cyber-war.html