

Cyberattack forecast after spy virus found

By Emily Chung, [CBC News](#)

Posted: Oct 19, 2011 11:45 AM ET

Last Updated: Oct 19, 2011 4:55 PM ET



I think that Stuxnet is coming from the U.S. government, most likely in cooperation with the Israelis, said computer virus researcher Mikko Hypponen. Like other security experts, he thinks the new virus, Duqu, was written by the same authors as Stuxnet. Emily Chung/CBC
The discovery of an espionage computer virus in Europe similar to the virus that attacked Iran's nuclear plants last year suggests that a new, similar cyberattack is about to launch, a computer virus researcher says.

The new virus, Duqu, was first reported by security company Symantec on its blog Tuesday. Its code is very similar to that of Stuxnet, the virus detected last year that was designed to sabotage equipment at Iranian nuclear plants. However, Duqu is designed for spying and information gathering rather than for sabotaging industrial control systems.

Mikko Hypponen, chief research officer for F-Secure, a Helsinki-based IT security company, said Wednesday that Stuxnet likely also went through a spying phase, likely in late 2008 or early 2009, that helped its creators plan their subsequent attack, which began in the summer of 2009.

"If that theory is correct, this information gathering phase [by Duqu] will next lead to a future attack," Hypponen told the SecTor computer security conference in Toronto during a keynote talk.

He said it's not clear who the target is.

Hypponen agrees with other IT security experts that Duqu was almost certainly written by Stuxnet's authors, since a lot of their source code is identical.

"No one else has the Stuxnet source code," he said.

"I think that Stuxnet is coming from the U.S. government, most likely in cooperation with the Israelis," added Hypponen, who has been conducting research on computer viruses for 20 years. "Can't prove that, but that's pretty clear when you look at the amount of know-how that went into building Stuxnet, the amount of money it must have taken, the amount of skilled persons behind it."

Symantec said it first obtained samples of Duqu from European computer systems on Oct. 14 via a research lab with "strong international connections."



Duqu's purpose appears to be to "gather intelligence and assets from entities, such as industrial control system manufacturers, in order to more easily conduct a future attack against another third party," Symantec reported. Associated Press Symantec said Duqu, a type of malicious code known as a remote access Trojan, has parts that are "nearly identical" to the Stuxnet. It targeted companies such as industrial control system manufacturers to gather information that could be useful for a future cyberattack. For example, Duqu was used to install another program that could record keystrokes.

According to a blog post from McAfee Labs, another security company that has received the code for Duqu, the virus communicates with a command server in India.

Symantec estimates attacks using Duqu may have been first conducted as early as December 2010. Duqu does not self-replicate to spread and it deletes itself from the system after 36 days. It sends its data in the form of files that look like JPG image files, including some data that is encrypted. It was named for the fact that it creates files with the prefix "~DQ."

U.S. issues public alert

Following the reports from Symantec and McAfee, the U.S. Department of Homeland Security issued a public alert through its Industrial Control Systems Cyber Emergency Response Team.

"The full extent of the threat posed by W32.Duqu is currently being evaluated," the alert said. "At this time, no specific mitigations are available; however, organizations should consider taking defensive measures against this threat."

It recommended taking measures such as minimizing network exposure for control system devices, putting control system networks behind firewalls, and using secure methods such as Virtual Private Networks for remotely accessing control devices.

The alert added that while security experts don't yet know how Duqu spreads, "the targeted nature of the thread would make social engineering a likely method of attack."

Social engineering refers to a method used to trick a user into installing malware by delivering it through what looks like a person or website that they trust.