Learn super viruses that are threatening the global industry

Highly skilled hackers can use public information about code known as the Stuxnet virus to develop attack variants in many industries.

Many security experts and government officials simultaneously warned that highly skilled hackers could fully use publicly available information about code known as the Stuxnet virus to develop variables. can attack many other industries.

Stuxnet is a worm (worm) on the Windows operating system. It was first discovered in June 2010 by a Belarusian security company called VirusBlokAda.

Stuxnet is the first computer worm discovered to be able to penetrate and restructure industrial systems, as well as the first computer worm that contains a built-in logic-controlled rootkit (PLC rootkit). Stuxnet was written to directly attack control and data acquisition (SCADA) systems used in industrial process control.

Stuxnet can automatically infiltrate a system, steal a recipe for mixing products, tamper with ingredients; fool the operating system and anti-virus software that everything is still working normally.

Picture 1 of Learn super viruses that are threatening the global industry

Stuxnet was written to directly attack control and data acquisition (SCADA) systems used in industrial process control.

The first damage Stuxnet caused so far has been reported as an attack on Iran's system of controlling nuclear programs. Iran uses Siemens control system. And, although Siemens denied any harm of the worm, Iran admitted that it was late in the nuclear deployment plan at Natanz because of Stuxnet's destruction on November 29.

In the report to the Senate Committee on Territorial Security and US Government Affairs, Sean McGurk, acting director of the Commission's national cybersecurity center, affirmed: Some industries specifically use software "involved" with Windows and may be attacked by this malicious code. Many key industrial sectors will be affected, from the car industry to chemicals or food chemistry.

Dean Turner, Symantec's Director of Global Intelligence Network, confirmed that the virus was fully capable of launching the above mentioned attack, and argued that " *Stuxnet's impact on the real world is much higher." much more than any threat we've ever encountered in the past* . "

Russian cyber security company Kaspersky Labs described Stuxnet as *a "flexible and scary smart weapon* ".

Although Stuxnet's code is extremely sophisticated and complex, it does not mean that stunned hackers cannot use it for various attack purposes. Especially when it is sold on the black market of hackers.

Except for Iran, an incomplete statistic shows that Stuxnet is threatening global information security.

In Vietnam, Bkav's September 2010 Security Newsletter said Stuxnet ranked fourth in the list of 10 most contagious viruses in September 2010. The newsletter did not specify Stuxnet's attack object.

Here are some of the countries affected by Stuxnet:

Water Number of computers infected with China6,000,000 (not verified) (November 1)Iran62,867Indonesia13.336India6,552United States2,913Australia2,436England1,038Malaysia1,013Pakistan993Finland7Germany5 (September)