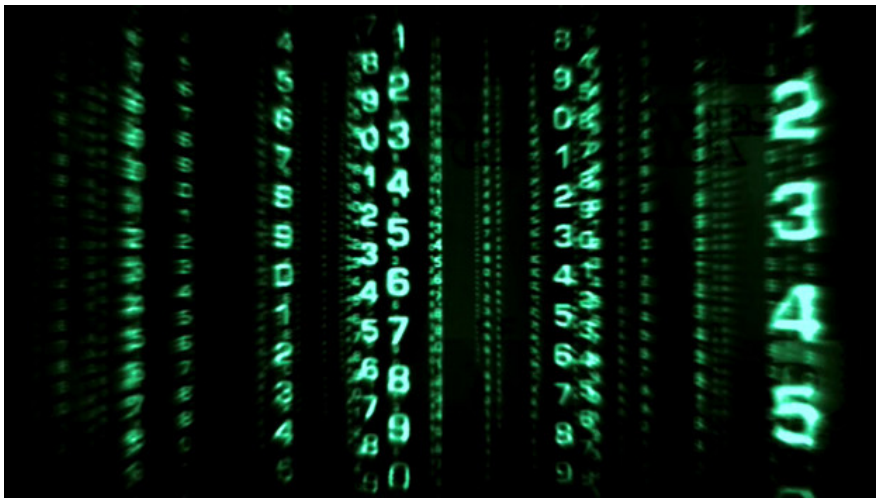
New discovery of the first version of Stuxnet malicious code

On the afternoon of February 27, 2013, Symantec announced in Vietnam the new version of the Stuxnet malware version, and said that the Stuxnet project could be launched in 2005 instead of 2009 as announced. before.

On the afternoon of February 27, 2013, Symantec announced in Vietnam the new version of the Stuxnet malware version, and said that the Stuxnet project could be launched in 2005 instead of 2009 as announced. before.

Stuxnet is the largest and most complex malware software in history, considered the first virtual weapon in the world to prove that malicious programs implemented in the successful online world can affect Important national infrastructure.



Stuxnet is the first virtual weapon in the world to demonstrate that malicious programs implemented in the successful cyber world can affect important national infrastructure. *(Artwork. Source: Internet).*

This complex and dangerous computer worm was written with the aim of sneaking into computers in Iran to undermine the nation's nuclear enrichment program and prevent President Mahmoud Ahmadinejad from building a dance program. nuclear gas.

According to previous reports, the earliest version of Stuxnet was the 1,001 version created in 2009.

However, Symantec's security department recently analyzed a sample of Stuxnet before the 1,001 version. The analysis of this code shows that version 0.5 was put into operation between 2007 and 2009, and the signs that the Stuxnet project began to start in early 2005.

With the support of the International Institute of Science and Security (ISIS) in understanding uranium enrichment centrifuges, Symantec's security experts have discovered new information about the operating mechanism of the version. the first stage of Stuxnet. That instead of affecting the speed of the uranium enrichment centrifuge, this Stuxnet 0.5 version was designed to close important valves that supply uranium hexafluoride gas to centrifuges, causing serious damage. for centrifuges as well as the whole uranium enrichment system.

So far, version 0.5 is the oldest variant of Stuxnet ever found, capable of infecting USB, and has stopped spreading since July 4, 2009.

A source from the US intelligence agency said a double Iranian national spy was the culprit behind the Stuxnet infection inside the Natanz reactor of the Islamic Republic of Iran. The tool this person uses is simple: A traditional USB hard drive, and click on the Stuxnet program icon to activate malicious code in the Windows operating system environment.

Stuxnet had ' *completed the task* ' after interrupting uranium enrichment at Natanz nuclear plant in 2011.

Experts have described Stuxnet as a collection of a *'matrix of complex code snippets* ', which has infected hundreds of thousands of computer systems by exploiting 20 *'zero-day'* classified vulnerabilities , which was present in every version of Windows operating system at the time.