'Deep' decoding attacks the Iranian nuclear reactor

Security researchers say the Stuxnet worm has sneakily attacked heavy industry targets, such as Iran's nuclear reactor ...

Security researchers say that the Stuxnet worm has been stealthily attacking heavy industry targets, such as Iran's nuclear reactor, but the creator of the Stuxnet worm has failed because of its inability. Stuxnet.

USB ruins the plan

Deeply designed penetrates into heavy industry control programs. This is a program to monitor and manage factories, oil pipelines, power plants, . This worm was only detected on researchers' radar during the summer, nearly a year after they first appeared.

However, the dispersal of them may be intentional targets, according to Roel Schouwenberg, a senior antivirus researcher at Kaspersky Lab (one of two security firms took a long time to analyze the Stuxnet worm).

Most researchers agree that Stuxnet has grown more sophisticated than before and is called "groundbreaking", that is, they are built by a group of financially capable, powerful people behind it. can be a government. Perhaps the goal of the worm is to target Iran and its nuclear power program systems.

Earlier this week, Iranian officials said tens of thousands of Windows computers were infected with the Stuxnet worm, including several locations in a nuclear power plant in southwestern Iran. However, they denied that the attack had damaged any means. However, the Stuxnet worm contributed to the delay of the reactor operation.

But if Stuxnet targets a specific target list, why do they infect thousands of PC computers outside Iran, in some countries like China, Germany, Kazakhstan and Indonesia?

Liam O Murchu, Symantec's security manager, said that even though Stuxnet manufacturers have spread limitations, there are some things that don't work as expected.

O Murchu said the method of infection is usually via USB devices, including a counter to limit the spread to three computers. This clearly shows that attackers do not want Stuxnet to spread. They want Stuxnet to maintain close to the original infection points.

O Murchu's research also shows that the window of 21-day infection limits or in other words worms will invade other machines in a network in just 3 weeks before exiting. Although there was anti-humanity, Stuxnet still spread. So where is the cause?

Kaspersky's Schouwenberg believes that it was because the USB device was infected with the Stuxnet worm and corrupted the plan that Stuxnet producers wanted.

Spread based on network hardware identification

In Schouwenberg's view, the first variant of Stuxnet did not reach their goal. He also mentioned the 2009 version of the worm (which lacks many flexible spread mechanisms that address many of the zero-day vulnerabilities in Windows). Therefore, they created a more sophisticated version to achieve the ultimate goal.

The more complex version was developed in March this year, but the previous version had been in operation for months and even longer before the first vendor of lesser known antivirus software from Belarus discovered. released in June. The first version was not spread enough and Stuxnet's author ventured to ignore the invisibility idea for this worm.

Under Schouwenberg's assumption, Stuxnet developers have actually failed to penetrate purposeful goals. Schouwenberg asserted, they spent a lot of time and money on the Stuxnet worm. They can try again and will still fail or can add more functions to 'boost' Stuxnet.

O Murchu agreed that the author was mistaken when using Stuxnet to infect computer systems. The Stuxnet worm evolved over time, adding new ways to spread on the Internet in hopes of finding specific PLCs (logic programmatic programs) to gain control. But perhaps these attacks did not manage all of their goals. The complexity of Stuxnet increased in 2010 but they did not reach the goal set.

With the rise of Stuxnet, Schouwenberg said that the country that created this worm could be affected by itself. That risk may be quite small because their critical infrastructure has not been affected by the Stuxnet worm and because the system does not use Siemens PLCs.

Stuxnet only tried to invade the PLCs built by the German giants - Siemens. The company offers a large number of hardware and control software for the Iranian industry.

O Murchu's research seems to return to Schouwenberg's point of view. Stuxnet searched for specific types of PLC hardware today. There is no clear evidence that hardware is the target of Stuxnet's attack. But the Stuxnet worm code only infects PLC using a specific network card.

Both Schouwenberg and O Murchu said, it may never know Stuxnet's author but what is worth mentioning is that, hackers want people to think that Israel is behind the attack against Iran.

Source: PCW, Cnet