Stuxnet worm targets Iran's nuclear reactor

Security firm Symantec said it found evidence that the Stuxnet worm was intended to target uranium enrichment complexes at the Bushehr reactor, Iran. With the help of experts from Dutch Profibus, Symantec decoded the entire code system that made up Stuxnet.

Security firm Symantec said it found evidence that the Stuxnet worm was intended to target uranium enrichment complexes at the Bushehr reactor, Iran. With the help of experts from Dutch Profibus, Symantec decoded the entire code system that made up Stuxnet.

Bushehr nuclear power plant of Iran
(Artwork: News.com.au)

Accordingly, **Stuxnet has clearly been created for a single purpose: hijacking control of the frequency converter** , which is the main device that determines the rotation speed of engines used in enrichment complexes. uranium and used to make nuclear bomb materials.

This discovery by Symantec also points out that the Stuxnet worm targets national industrial targets in the presence of the following elements: the target computer must use a S7-300 CPU, and this CPU must be Profibus' ability to control up to six CP-342-5 signal transmission modules, each of which is capable of connecting up to 31 frequency converters. Symantec said the Stuxnet worm only attacks transducers manufactured by two companies: Finnish Vacon and Fararo Paya in Iran's capital, Tehran.

Considered to be the most sophisticated malicious code ever, Stuxnet targeted Windows operating systems to run industrial complexes in large companies and enterprises. Special systems of this type are called SCADA, controlling everything from power plants to fuel pipelines, even military bases.

Stuxnet was first discovered in June, and security circles believe that Stuxnet is actually the result of a project funded by . governments of countries that want to undermine Iran's nuclear program. Later in September, the Tehran government announced that it had detected more than 30,000 Stuxnet-infected computers, but said the SCADA system at the Bushehr Nuclear Plant remained unharmed.

After successful penetration, the Stuxnet worm only requires the transducer to operate at a level between 807 Hz and 1210 Hz. By changing the output frequency (which is also the speed of the entire system) of the transducer engine for short periods of several months, Stuxnet succeeded in reducing progress of the factory.

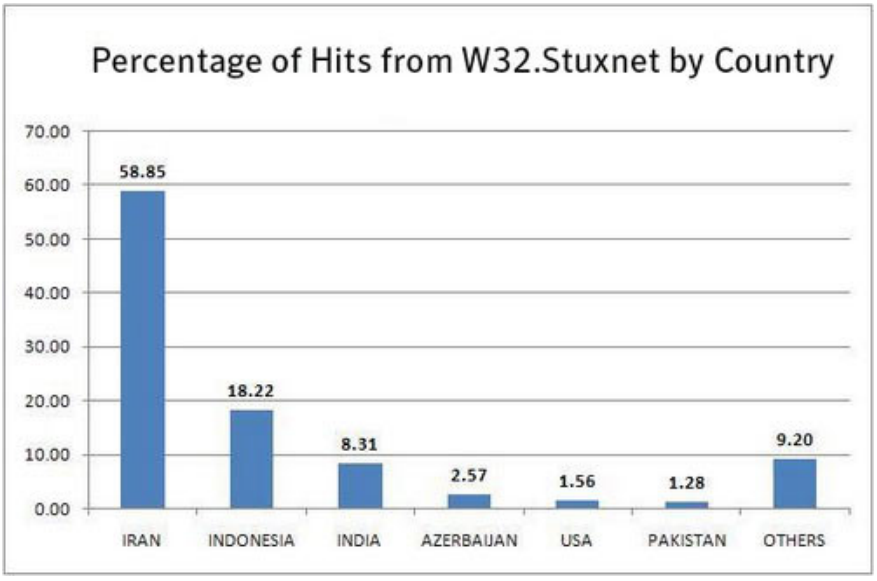
Symantec said the results from this assessment also reduced the number of potential Stuxnet malware targets to just a few. According to this security firm, Stuxnet only targets the converters of two separate manufacturers and the fact that ' *it* ' increases the output frequency also further clarifies the meaning of this ' *worm* ' activity.

In addition, Symantec said in the United States, the export of products with an output capacity of more than 600Hz is strictly sanctioned by the US Nuclear Supervision Commission, as these are devices that can be used used for uranium enrichment process, an important step in the production of nuclear bombs.

According to Eric Chen, one of the three Symantec experts successfully deciphered Stuxnet, the malicious code designed to target industrial systems using ultra-high-speed electric motors used in centrifuges, which are used to manufacture nuclear energy.

But the latest discovery from Symantec shows that the Bushehr Plant was never the true goal of Stuxnet, but **that the new uranium enrichment system was the " *bait* " that the worm targeted** .

The specific device here is the ' *frequency converter* ', which is directly connected to SCADA, these are special devices that use normal power, then increase the output frequency to a high level. more, usually 600 Hz or more. This high frequency is then used to power high-speed centrifugal motors. According to the American Science Association, the power to run centrifuges must continuously operate at high efficiency, while maintaining a stable and accurate output level of the frequency.



Stuxnet's national chart is attacked, Iran tops the list
(Artwork: PCMag)

And **Stuxnet was built to disrupt this process** , when it found the converters operating at 807 Hz-1210 Hz, the worm would increase the frequency to 1410 Hz, then every 27 days. reduced to . 2 Hz, then " *inflated* " to . 1064 Hz. Just like that, the process continues steadily and continuously.

Iran began experimenting with the operation of 164 centrifuges in 2006, soon after it announced it had synthesized an insignificant amount of poor uranium. Just one year later, Iranian President Mahmoud Ahmadinejad announced that they started the uranium enrichment process with 3,000 centrifuges.

Now some sources say Iran has 4,000 centrifuges or maybe more .