

STUXNET: PANDORA'S BOX OR STROKE OF GENIUS?

Lecture and talk show organized in Paris by NanoJV

Tuesday 8th March 2011, 6.30 pm – 8.00 pm French Time, at Atelier BNP PARIBAS.

Participation fees: 30 €. Online registration mandatory: [click here](#).

With the support of



And in partnership with



and



KEYNOTE SPEAKERS:

Daniel Ventre, researcher at CNRS (French National Center for Scientific Research), expert on information and cyber warfare.

Eric Filiol, military expert. Head Scientist Officer of the Operational Cryptology and Operational Computer Virology Lab. Graduated from NATO infoops.

François-Bernard Huyghe, PhD in Political Sciences, renowned author and specialist in information warfare.

And in videoconference from the USA and Israel:

Jeffrey Carr, cyber intelligence expert, columnist for Forbes Firewall blog, and cyber warfare author. His book « Inside Cyber Warfare » has been endorsed by General Chilton, Commander USSTRATCOM.

Dr. Kozlovski, international expert in cybercrime & proactive security. Consultant to various governmental bodies in Israel and around the world, namely the FBI, IDF, Israel Ministry of Foreign Affairs.

Lior Frenkel CEO and Co-Founder of Waterfall Security leading the unidirectional security gateways market and Gita Technologies Ltd, a high-end security research and development company, which provides unique solutions for defense markets.

Moderator :

Dominique Bourra, CEO of NanoJV, expert and organizer of the France Israel Cyber Security Forum.

BACKGROUND:

On June 17, 2010, a small company from Belorussia working in the anti-virus protection field in Iran discovered a new virus using unknown weaknesses in Microsoft programs. Several weeks later, a German specialist found that the destructive software was targeting a computer-human interface developed by Siemens and utilized in a good number of strategic industrial activities.

The worm was given the name Stuxnet, a word put together based on letter repetitions found in the code. The words myrtus and guava also appeared. It was determined that in order to spread, the virus used fake authentication certificates stolen from two companies in Taiwan. Two servers commanding and controlling the virus were tracked down in Malaysia and Denmark. The virus was sending and receiving information and instructions by connecting to two domains that resembled on-line sports betting sites.

Very quickly, Symantec intercepted and analyzed the traffic flow towards the two servers. But it appeared that the virus updated itself and was communicating using a peer-to-peer function linking the infected computers. The infection most likely stemmed simple USB keys. From the onset, it hit a number of countries, including the United States and Germany. Statistical analyses also showed major infection levels in Iran, India and Indonesia.

However, Siemens officially admitted to only a handful of infection in its systems throughout the world. By the end of summer, hypotheses were pointing to programmable logic controllers at nuclear sites and then at uranium enrichment centers. German specialist Ralph Langner concluded that Israel was involved, based on the word « Myrtus », which referred to Queen Esther, a biblical hero who lived in ancient Persia, today Iran.

The international press went wild, and within several days unanimously pointed to Israel as the source of the virus, linked to its delicate security situation with Iran. Several high level Israeli experts, meanwhile, stated that based on certain characteristics of the code, the worm did not appear to be designed by the Israel Defense Forces.

Then in November, more advanced studies showed the virus was capable of hitting convertor frequencies used by centrifuges. An American think-tank reported that up to 1000 centrifuges might have been damaged by the virus at the Natanz site. But even the International Atomic Energy Agency has been careful about reaching any solid conclusions. In December, Jeffrey Carr, an American specialist close to US cyberdefense operations, came up with a possible Chinese connection.

In January, a central Israeli opponent of his country's nuclear program told the New York Times that the virus had been tested at the Dimona nuclear site in the Negev desert. However, his statement was based on elements that could not be confirmed.