systemtek.co.uk

Dutch Engineer Used Water Pump to Get Stuxnet Malware Into Iranian Nuclear Facility

Kerry Dean

3–4 minutes

A Dutch engineer, enlisted by the country's intelligence services, reportedly utilized a water pump to deploy the notorious Stuxnet malware within an Iranian nuclear facility, as unveiled by a comprehensive two-year inquiry conducted by Dutch newspaper De Volkskrant.

"Stuxnet," disclosed in 2010, is widely attributed to the collaborative efforts of the United States and Israel, with its primary objective being the disruption of Iran's nuclear program through the compromise of industrial control systems (ICS) linked to nuclear centrifuges. This malicious software, equipped with worm capabilities, is reputed to have infected numerous devices, causing substantial physical damage to hundreds of machines.

De Volkskrant's investigation, incorporating interviews with numerous individuals, reveals that Erik van Sabben, a 36-year-old Dutch national employed at a heavy transport company in Dubai, was recruited by the AIVD, the general intelligence and security service of the Netherlands — analogous to the CIA. Van Sabben was allegedly enlisted in 2005, a few years preceding the activation of the Stuxnet malware, following a request for assistance from American and Israeli intelligence agencies. Remarkably, the Dutch agency purportedly refrained from informing the national government, leaving them unaware of the operation's full scope.

Van Sabben, deemed ideal for the task due to his technical background, business engagements in Iran, and marriage to an Iranian woman, is believed to have planted the Stuxnet malware on a water pump within the infiltrated nuclear complex in Natanz. Whether Van Sabben comprehended the precise nature of his actions remains unclear, but his family indicated signs of panic around the time of the Stuxnet attack.

Contrary to earlier reports suggesting the involvement of an Iranian engineer in Stuxnet's deployment, Van Sabben, sadly, passed away in the United Arab Emirates two weeks after the Stuxnet attack, succumbing to a motorcycle accident.

Michael Hayden, then Chief of the CIA, acknowledged engagement with De Volkskrant but could not confirm the delivery of Stuxnet via water pumps, citing ongoing classification of the information. Ralph Langner, a researcher who conducted a detailed analysis of Stuxnet, challenged the notion, stating that "a water pump cannot carry a copy of Stuxnet."

A notable revelation from De Volkskrant's investigation is the claim by Hayden that the development cost of Stuxnet ranged between $1 and $2 billion, providing a glimpse into the staggering financial investment behind the covert operation.

Kerry is a Content Creator at www.systemtek.co.uk she has spent many years working in IT support, her main interests are computing, networking and AI.