In early 2008 the German company Siemens cooperated with one of the United States' premier national laboratories, in Idaho, to identify the vulnerabilities of computer controllers that the company sells to operate industrial machinery around the world — and that American intelligence agencies have identified as key equipment in Iran's enrichment facilities.

Seimens says that program was part of routine efforts to secure its products against cyberattacks. Nonetheless, it gave the Idaho National Laboratory — which is part of the Energy Department, responsible for America's nuclear arms — the chance to identify well-hidden holes in the Siemens systems that were exploited the next year by Stuxnet.

The worm itself now appears to have included two major components. One was designed to send Iran's nuclear centrifuges spinning wildly out of control. Another seems right out of the movies: The computer program also secretly recorded what normal operations at the nuclear plant looked like, then played those readings back to plant operators, like a pre-recorded security tape in a bank heist, so that it would appear that everything was operating normally while the centrifuges were actually tearing themselves apart.

" a former psychologist who runs a small computer security company in a suburb of Hamburg. Eager to design protective software for his clients, he had his five employees focus on picking apart the code and running it on the series of Siemens controllers neatly stacked in racks, their lights blinking.

He quickly discovered that the worm only kicked into gear when it detected the presence of a specific configuration of controllers, running a set of processes that appear to exist only in a centrifuge plant. "The attackers took great care to make sure that only their designated targets were hit," he said. "It was a marksman's job."

"

For example, one small section of the code appears designed to send commands to 984 machines linked together.

Curiously, when international inspectors visited Natanz in late 2009, they found that the Iranians had taken out of service a total of exactly 984 machines that had been running the previous summer.

But as Mr. Langner kept peeling back the layers, he found more — what he calls the “dual warhead.” One part of the program is designed to lie dormant for long periods, then speed up the machines so that the spinning rotors in the centrifuges wobble and then destroy themselves. Another part, called a “man in the middle” in the computer world, sends out those false sensor signals to make the system believe everything is running smoothly. That prevents a safety system from kicking in, which would shut down the plant before it could self-destruct.

“Code analysis makes it clear that Stuxnet is not about sending a message or proving a concept,” Mr. Langner later wrote. “It is about destroying its targets with utmost determination in military style.”

This was not the work of hackers, he quickly concluded. It had to be the work of someone who knew his way around the specific quirks of the Siemens controllers and had an intimate understanding of exactly how the Iranians had designed their enrichment operations.

In fact, the Americans and the Israelis had a pretty good idea. "

Full Text here

https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=3