Report: Stuxnet cyberweapon older than believed (Update)

February 27 2013, by Raphael Satter

The sophisticated cyberweapon which targeted an Iranian nuclear plant is older than previously believed, an anti-virus company said Tuesday, peeling back another layer of mystery on a series of attacks attributed by many to U.S. and Israeli intelligence.

The Stuxnet worm, aimed at the centrifuges in Iran's Natanz plant, transformed the cybersecurity field because it was the first known computer attack specifically designed to cause physical damage. The precise origins of the worm remain unclear, but until now the earliest samples of Stuxnet had been dated to 2009, and The New York Times—in the fullest account of the attack published so far—traced the origins of the top-secret program back to 2006.

In a new report issued late Tuesday, Symantec Corp. pushed that timeline further back, saying it had found a primitive version of Stuxnet circulating online in 2007 and that elements of the program had been in place as far back as 2005.

Independent security experts who examined the report said it showed that the worm's creators were well ahead of their time.

"To me, it's amazing," said Mikko Hypponen, whose Finland-based F-Secure has studied Stuxnet. "We had no idea the U.S.-Israel cyberoperations were so advanced already almost a decade ago."

Hypponen is one of a host of experts who've concluded that Stuxnet was

an attempt to sabotage the uranium enrichment centrifuges at Iran's Natanz nuclear plant, a key element in the Islamic republic's disputed atomic energy program. Because the United States and Israel are two of Iran's biggest foes, the shadow of suspicion immediately settled on their tech-savvy intelligence services.

That theory got a boost when the Times reported that President George W. Bush had ordered the deployment of Stuxnet against Iran, laying out in unprecedented detail how the worm had been crafted so as to surreptitiously send Natanz's centrifuge machines spinning out of control.

U.S. and Israeli officials have long declined to comment publicly on Stuxnet or their alleged involvement in creating and deploying the computer worm.

Symantec's report suggests that an intermediate version of the worm—Stuxnet 0.5—was completed in November 2007. That worm lacked some of the sophistication of its descendant, Symantec said, and was designed to interfere with the centrifuges by opening and closing the valves which control the flow of uranium gas, causing a potentially damaging buildup in pressure.

That approach was dropped in later improved versions of the Stuxnet code.

Symantec said the servers used to control the primitive worm were set up in November 2005, suggesting that Stuxnet's trailblazing authors were plotting their attack at a time when many parts of the Internet now taken for granted were not yet in place. Twitter did not exist, Facebook was still largely limited to U.S. college campuses, and YouTube was in its infancy.

Alan Woodward, a professor of computer science at the University of Surrey, said that had troubling implications.

"Clearly these were very forward-thinking, clever people that were doing this," he said. "There's no reason to think that they're less forward-thinking now. What are they up to?"

More information: The Symantec report: bit.ly/128ux2s