

Submit Query

October 2, 2010



Marcus Baram

Marcus@huffingtonpost.com | HuffPost

Reporting

## Stuxnet Malware Mystery Deepens: Another Hint Of Israeli Origins

First Posted: 10- 1-10 01:04 PM | Updated: 10- 1-10 02:59 PM

What's Your Reaction?

It's like a 21st-century version of a John Le Carre novel, in which all the dashing spies have been replaced by computer geeks.

The mystery continues to deepen over the origin of one of the world's most damaging computer viruses -- Stuxnet -- which some experts believe is targeted at Iran's nuclear power plants, slowing that country's quest for a nuclear weapon.

On Tuesday, a German computer specialist offered a hint that Israel may be behind the sophisticated malware, by demonstrating that a file inside the code uses the word "Myrtus" -- which could be a reference to the Book of Esther, the Old Testament story about how the Jews prevented a nefarious plot by the Persians, according to the *New York Times*.

The next day, a trio of security researchers offered another clue at a conference in Vancouver, describing how Stuxnet includes references to the 1979 execution of the leader of Iran's Jewish community at the time. Specifically, the researchers from Symantec -- Nicolas Falliere, Liam O Murchu and Eric Chen -- showed that the code includes a marker with the numbers "19790509" which, if prompted, stops the code from infecting a targeted computer.

According to their report:

The value appears to be a date of May 9, 1979. While on May 9, 1979 a variety of historical events occurred, according to Wikipedia "Habib Elghanian was executed by a firing squad in Tehran sending shock waves through the closely knit Iranian Jewish community. He was the first Jew and one of the first civilians to be executed by the new Islamic government. This prompted the mass exodus of the once 100,000 member strong Jewish community of Iran which continues to this day."

Elghanian, a prominent businessman, was the first Jew to be targeted in a purge after the country's Islamic revolution, reported *Time* magazine at the time. He was sentenced to death after being charged with "corruption", "contacts with Israel and Zionism", "friendship with the enemies of God", "warring with God and his emissaries", and "economic imperialism."

The researchers warned not to draw too many conclusions -- noting that "Attackers would have the natural desire to implicate another party."

ADVERTISEMENT

Stuxnet, which has been called the world's most sophisticated malware ever targets computers that oversee SCADA systems, which monitor machinery in power plants and military installations.

According to Symantec, Iran has been the clearest target, as almost 60% of infected hosts are in the country, followed by Indonesia (17%), India (10%), Azerbaijan (3.4%) and Pakistan (1.4%). Almost 35,000 organizations have been infected in Iran (based on IP addresses).

"The concentration of infections in Iran likely indicates that this was the initial target for infections and was where infections were initially seeded," says the report.

Late in August, Iran seems to have blocked outward connections to their servers, since the country was no longer reporting new infections.

Though reports have indicated that Stuxnet may have been aimed at Iran's Bushehr atomic plant or Natanz uranium enrichment plant, the former chief of U.N. nuclear inspections is doubtful. Olli Heinonen doesn't believe that the malware was specifically targeted at Iran, since other countries were also infected.

"This is all speculation until the facts are found," he told Reuters in a telephone interview on Thursday.

Yet Israeli intelligence correspondent Yossi Melman believes that Israel or the USA were behind the cyber attack, though he's skeptical of the clues.

He tells *Politico's* Laura Rozen:

"When you plan such an operation, you check and recheck and double check each digit and each letter," he continued. "Israeli intelligence is not that sloppy to leave behind him such clumsy fingerprints. If it wanted to engage in a mind game, they would have done it in a more amusing and sophisticated manner."

Israel has not commented on whether Stuxnet "has any connection to the secretive cyberwar unit it has built inside Israel's intelligence service," reports the *Times*.

[Report Corrections](#)

### More in Technology...

Comments

193

Pending Comments

1

[View FAQ](#)

**HuffPost Social News** BETA

[View All](#)

[Favorites](#)

[Recency](#) |

[Popularity](#)

Page: [1](#) [2](#) [3](#) [4](#) [5](#) [Next](#) [Last](#) » (6 total)

Page: [1](#) [2](#) [3](#) [4](#) [5](#) [Next](#) [Last](#) » (6 total)