Cybersecurity firm says spying campaign targeted Iran talks (Update)

June 10 2015, byKen Dilanian

A computer worm designed to gather foreign intelligence and widely linked to Israel was used to spy on negotiations with Iran on curtailing its nuclear program, security researchers said

A cybersecurity firm with close ties to Russian intelligence said Wednesday it uncovered a cyber-espionage campaign targeting hotels that hosted Iran nuclear negotiations, the details of which are among the most closely held secrets in world diplomacy.

The firm, Kaspersky, said the malware was so sophisticated that it must have been created by a government. Citing former U.S. intelligence officials, The Wall Street Journal attributed the spying to Israel, which opposes the emerging nuclear deal being hammered out by the U.S., Russia, several other European countries and Iran. Negotiators hope to clinch an agreement by the end of the month to curb Iran's nuclear activity for a decade in exchange for billions of dollars in sanctions relief.

A former senior U.S. intelligence official who dealt with such matters told The Associated Press that the nuclear talks are a likely espionage target of several countries, including Israel and Russia. The former official said he couldn't be quoted on the record and demanded anonymity.

The Israeli government declined comment Wednesday.

The allegation coincides with deepening tensions in the U.S.-Israeli relationship, much of it linked to Iran. The Obama administration has rejected much of the hawkish advice of its close Mideast ally in favor of what U.S. officials say would be an accord that removes the threat of a nuclear-armed Iran. The Jewish state has aggressively lobbied against the package both internationally and within the United States.

Kaspersky's cyberspying discoveries are taken seriously by security experts, and the U.S. antivirus company Symantec confirmed Kaspersky's technical findings Wednesday, though not the source of the campaign.

Eugene Kaspersky, the chairman and CEO, served in the Soviet military during the 1980s and maintains close ties with Russian intelligence officials.

In a statement, the company said it began investigating an intrusion into its own systems earlier this year, a probe that led it to discover "one of the most skilled, mysterious and powerful threat actors" in the world of cyberspying. The malware is a more advanced version of an attack it previously discovered, dubbed "Duqu," the company said.

The malware used three "zero day" vulnerabilities, which are flaws in Microsoft's operating system that are previously unknown and therefore undefended. Each one can cost as much as $300,000 on the black market.

Victims of the spying were identified in Western countries, as well as the Middle East and Asia, Kaspersky said.

The State Department, which has led the U.S. delegation in the Iran talks, didn't immediately comment. It likely wouldn't have used hotel computer systems or unsecure phones to discuss details of the negotiations. Kaspersky didn't identify the hotels, though most talks have taken place in Austria and Switzerland.

Spyware also was found to have targeted people attending the 70th anniversary event of the liberation of Poland's Auschwitz-Birkenau death camp, Kaspersky said.

Iran says its program is solely for peaceful energy, medical and research purposes, though many governments fear it harbors nuclear weapons ambitions.

President Barack Obama and others have said a failure to address the standoff through diplomacy could lead to military confrontation.

Highlighting ongoing American intelligence concerns, the former chief of the Defense Intelligence Agency told a House subcommittee

Wednesday that the proposed deal "suffers from serious deficiencies," including the intelligence community's inability to verify full Iranian compliance.

"The intelligence community does not have complete 'eyes on' the totality of the Iranian nuclear program, nor can it guarantee that we have identified all of Iran's nuclear facilities and processes," Michael Flynn testified. He said it was prudent to conclude "that there are elements of Iran's nuclear program that still remain hidden from view."

Citation: Cybersecurity firm says spying campaign targeted Iran talks (Update) (2015, June 10) retrieved 5 May 2024 from https://phys.org/news/2015-06-worm-enabled-spying-iran.html