GlobalResearch
Center for Research on Globalization

Israel Spied on Hotels Used for P5+1 Iran Nuclear Talks

By Stephen Lendman
Global Research, June 11, 2015

Region: Middle East & North Africa, USA
Theme: Intelligence, Militarization and WMD

It's not the first time Israeli spying on Iran nuclear talks was discovered. An earlier article discussed the following:

On March 23, the Wall Street Journal headlined "Israel Spied on Iran Nuclear Talks with US," saying:

Washington and other P5+1 nations learned Israel spied on their closed-door talks all along.

It was part of Netanyahu's scheme "to penetrate the negotiations and then help build a case against the emerging terms of the deal," the Journal cited current and former US officials saying.

Israel "eavesdropp(ed), acquired information from confidential US briefings, informants and diplomatic contacts in Europe."

White House officials were angered because Israel "share(d) inside information with US lawmakers and others" to scuttle any prospective Iranian deal reached.

According to an unnamed senior US official:

> "It is one thing for the US and Israel to spy on each other. It is another thing for Israel to steal (its) secrets and play them back to (congressional) legislators to undermine US diplomacy."

It's well known Israel spies on America more aggressively than any of its other allies. It's been caught red-handed numerous times. Its lies claiming otherwise don't wash.

A leading cybersecurity firm caught Israel red-handed again. Kaspersky Lab ZAO discovered it was hacked last year by a virus used by Israeli spies. In checking others targeted, it learned three luxury European hotels used for Iranian nuclear talks were hit.

According to the Journal, "(t)he spyware…was an improved version of Duqu, a virus first identified by cybersecurity experts in 2011."

"Current and former US officials and many cybersecurity experts believe Duqu was designed to carry out Israel's most sensitive intelligence-collection operations."

> "Kaspersky's findings…shed new light on the use of a stealthy virus in the

> spying efforts. The revelations also could provide what may be the first concrete evidence that the nuclear negotiations were targeted and by whom."

Israel prioritizes spying on Iran – especially ahead of an agreed June 30 final agreement deadline.

Kaspersky didn't identify Israel by name. It's not its policy to do so. But company researchers indicated an Israeli connection.

Their report is titled "The Duqu Bet." Bet is the Hebrew language's second letter. Many questions remain unanswered, said the Journal.

It's unclear how the virus was used and what information Israel obtained. Possibly it was "able to eavesdrop on conversations and steal electronic files by commandeering the hotel systems that connect to computers, phones, elevators and alarms, allowing them to turn them on and off at will to collect information," said the Journal citing Kaspersky researchers.

Israel declined comment on what the cybersecurity company learned. The FBI is reviewing its analysis, said the Journal. US officials weren't surprised to learn about Israeli spying, it added.

An unnamed senior congressional aide briefed on what happened said "(w)e take this seriously." Kaspersky's findings are credible.

The company protects hundreds of millions of computers from hackers. It took over six months to realize its own computers were accessed.

The Journal explained as follows, saying:

> "Costin Raiu, director of the global research and analysis team at Kaspersky, said the attackers first targeted a Kaspersky employee in a satellite office in the Asia Pacific region, likely through email that contained an attachment in which the virus was hidden."
>
> "By opening the attachment, the employee inadvertently would have allowed the virus to infect his computer through what Kaspersky believes was a hacking tool called a 'zero day exploit.' "

These devices penetrate security holes. They undermine software companies' ability to prevent hacking.

They're sophisticated and expensive to create. They generally only work once. "After that, companies can build up digital antibodies through software patches," said the Journal.

"US intelligence agencies view Duqu infections as Israeli spy operations," the Journal cited former US officials saying.

It "could not have been created by anyone without access to the original Duqu source code," the Kaspersky report explained – meaning it clearly bore Israeli fingerprints.

A Kaspersky employee discovered the virus on a company computer believed bug-free. A

special team was established to monitor its action – learn how it worked and what it was designed to do.

According to the Journal, "(i)t It jumped from one system to another, slowly attacking an increasing number of computers."

> "The virus sought to cover its tracks, abandoning machines the attackers deemed of no additional interest, while leaving a small file that would allow them to return later."

Kaspersky expects intrusions but nothing this sophisticated. It calls the improved virus Duqu 2.0.

It ran tests to learn if any of its 270,000 corporate clients were infected. It found a limited number in Western Europe, Asia and the Middle East – none in America.

Kaspersky didn't identify the three hotels hacked. Those used for talks include the Beau-Rivage Palace in Lausanne, Switzerland, the Intercontinental in Geneva, the Palais Coburg in Vienna, the Hotel President Wilson in Geneva, the Hotel Bayerischer Hof in Munich and Royal Plaza Montreux in Montreux, Switzerland, the Journal explained.

Kaspersky said the virus used employed over 100 separate "modules" able to:

- compress video feeds including from surveillance cameras;
- target telephonic and Wi-Fi networks communications;
- steal electronic files;
- operate two-way microphones in hotel computers, elevators and alarm systems; and
- penetrate front desk computers to learn who occupied what rooms – then target their communications.

Small reconnaissance files were embedded in hacked computers to ensure monitoring and ability to access contents later on, the Journal explained.

Stephen Lendman *lives in Chicago. He can be reached at lendmanstephen@sbcglobal.net.*

His new book as editor and contributor is titled "Flashpoint in Ukraine: US Drive for Hegemony Risks WW III."

http://www.claritypress.com/LendmanIII.html

Visit his blog site at sjlendman.blogspot.com.

Listen to cutting-edge discussions with distinguished guests on the Progressive Radio News Hour on the Progressive Radio Network.

It airs three times weekly: live on Sundays at 1PMCentral time plus two prerecorded archived programs.

Articles by: **Stephen Lendman**

About the author:

Stephen Lendman lives in Chicago. He can be reached at lendmanstephen@sbcglobal.net. His new book as editor and contributor is titled "Flashpoint in Ukraine: US Drive for Hegemony Risks WW III." http://www.claritypress.com/LendmanIII.html Visit his blog site at sjlendman.blogspot.com. Listen to cutting-edge discussions with distinguished guests on the Progressive Radio News Hour on the Progressive Radio Network. It airs three times weekly: live on Sundays at 1PM Central time plus two prerecorded archived programs.