Spy Virus Linked to Israel Targeted Hotels Used for Iran Nuclear Talks

Cybersecurity firm Kaspersky Lab finds three hotels that hosted Iran talks were targeted by a virus believed used by Israeli spies

By Adam Entous And Danny Yadron

June 10, 2015

When a leading cybersecurity firm discovered it had been hacked last year by a virus widely believed to be used by Israeli spies, it wanted to know who else was on the hit list.

The Moscow-based firm, Kaspersky Lab ZAO, checked millions of computers world-wide and three luxury European hotels popped up. The other hotels tested—thousands in all—were clean.

Researchers at the firm weren't sure what to make of the results. Then they realized what the three hotels had in common. Each was infiltrated by the virus before hosting high-stakes negotiations between Iran and world powers over curtailing Tehran's nuclear program.

The spyware, the firm has now concluded, was an improved version of Duqu, a virus first identified by cybersecurity experts in 2011, according to a Kaspersky report and outside security experts. Current and former U.S. officials and many cybersecurity experts say they believe Duqu was designed to carry out Israel's most sensitive intelligence-collection operations.

Senior U.S. officials learned Israel was spying on the nuclear talks in 2014, a finding first reported by The Wall Street Journal in March. Officials at the time offered few details about Israel's tactics.

U.S. Secretary of State John Kerry, right, talks to Iranian Foreign Minister Mohammad Javad Zarif on May 30 in Geneva

Kaspersky's findings, disclosed publicly in a report on Wednesday, 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.

No intelligence-collection effort is a higher priority for Israel's spy agencies than Iran, including the closed-door talks which have entered a final stage. Israeli leaders say the emerging deal could allow Iran to continue working toward building nuclear weapons, something Iran denies it is trying to do.

Kaspersky, in keeping with its policy, doesn't identify Israel by name as the country responsible for the hacks. But researchers at the company indicate that they suspect an Israeli connection in subtle ways.

For example, the version of the company's report viewed by the Journal before its release was titled "The Duqu Bet." Bet is the second letter of the Hebrew alphabet. Kaspersky revised the title in the final version of the report released Wednesday, removing the "Bet" reference.

Israeli Prime Minister Benjamin Netanyahu, center-left, speaks to his cabinet on May 31, hours after warning against making concessions to Iran in the nuclear talks

Researchers at the company acknowledge that many questions remain unanswered about how the virus was used and what information may have been stolen. Among the possibilities, the researchers say, the intruders might have been 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.

Israeli officials have denied spying on the U.S. or other allies, although they acknowledge conducting close surveillance on Iranians generally. Israeli officials declined to comment specifically on the allegations relating to the Duqu virus and the hotel intrusions.

The Federal Bureau of Investigation is reviewing the Kaspersky analysis and hasn't independently confirmed the firm's conclusions, according to people familiar with the discussions. U.S. officials, though, said they weren't surprised to learn about the reported intrusions at the hotels used for the nuclear talks.

A senior congressional aide briefed on the matter said Kaspersky's findings were credible.

"We take this seriously," the aide said.

Kaspersky, which protects hundreds of millions of computers from intruders, didn't realize its own computers were compromised for more than six months after the 2014 breach. Hackers and intelligence agencies have long targeted security companies, given the valuable information they can learn about the Internet's defenses.

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." Such tools take advantage of previously unknown security holes—giving software companies no opportunity to prevent hackers from sneaking in through them. Kaspersky says the hackers used up to two more "zero day exploits" to work further into Kaspersky's system.

That alone, Kaspersky and outside experts say, offers evidence of the hackers' sophistication. These kinds of tools are expensive to create and are guaranteed to work only the first time they are used. After that, companies can build up digital antibodies through software patches.

Security researchers such as Kaspersky's Mr. Raiu often strive not just to find hackers, but also to find links between breaches through digital detective work. It is a mix of computer science, instinct and luck. In this case, Mr. Raiu saw links between this new virus and Duqu.

U.S. intelligence agencies view Duqu infections as Israeli spy operations, former U.S. officials said. While the new virus bore no overt links to Israel, it was so complex and borrowed so heavily from Duqu that it "could not have been created by anyone without access to the original Duqu source code," Kaspersky writes in its report.

To check his conclusions, Mr. Raiu a few weeks ago emailed his findings to a friend, Boldizsár Bencsáth, a researcher at Budapest University of Technology and Economics' Laboratory of Cryptography and System Security. Mr. Bencsáth in 2011 helped discover the original Duqu virus.

"They look extremely similar," Mr. Bencsáth said in an interview Tuesday. He estimated a team of 10 people would take more than two years to build such a clean copycat, unless they were the original author.

In the early spring, Kaspersky found itself on the other side of the digital intrusions it investigates.

A Kaspersky employee in Moscow discovered the virus while testing a new security program on a company computer he assumed was bug-free.

Rather than try to kick the hackers out, the company set up a special team to monitor the virus in action to figure out how it worked and what it was designed to do.

The way the virus operated took the team by surprise. 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.

Mr. Raiu said the company had been bracing for cyber intrusions but didn't expect anything this sophisticated. The attackers moved slowly through Kaspersky's systems to avoid attracting attention. Mr. Raiu concluded that they probably valued stealth more than anything else.

The company dubbed the new-and-improved virus Duqu 2.0.

In a written statement with the report that was reviewed by the Journal, Kaspersky said it didn't expect the incident to make customers more vulnerable to hackers.

"Kaspersky Lab is confident that its clients and partners are safe and that there is no impact on the company's products, technologies and services," it said.

The company ran tests to determine if any of its 270,000 corporate clients world-wide had been infected. Kaspersky's list of corporate clients includes big energy companies, European banks and thousands of hotels.

It found infections on a limited number of clients in Western Europe, Asia and the Middle East. None of Kaspersky's clients in the U.S. were targeted. A targeted cyberattack against a hotel struck researchers as unusual but not unprecedented.

The first hotel with Duqu 2.0 on its computers piqued Mr. Raiu's interest right away, in light of the revelations he read in the Journal about Israeli spying efforts, he said. The hotel, he said, was a well-known venue for the nuclear negotiations. But he wasn't sure if it was an isolated case.

Soon thereafter, Kaspersky found the same virus at a second luxury hotel. Initially, Mr. Raiu didn't see a connection between the hotel and the nuclear talks. Then, a couple of weeks after the discovery of the second hotel, he learned that the nuclear negotiations would take place there. His team was "shocked," Mr. Raiu recalled. In both cases, the hotels were infected about two to three weeks before the negotiators convened.

Kaspersky provided information about Duqu 2.0 to one of its partners, which did its own round of tests. That search turned up a third infected hotel which hosted the nuclear talks. Mr. Raiu said the third hotel was discovered last but appeared to have been infected first, sometime in 2014. Kaspersky declined to identify the three hotels.

Hotels that served as venues for the 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.

A Beau-Rivage spokeswoman said the hotel was unaware of being hacked. A manager on duty at the Intercontinental said he also was unaware of such an incident.

The management team at the Royal Plaza said: "Our internal policy doesn't allow us to deliver any information."

The others didn't respond to requests for comment.

In addition to the three hotels reported to have been hacked, the virus was found in computers at a site used to commemorate the 70th anniversary of the liberation of the Nazi death camp at Auschwitz. Some world leaders had attended events there.

A former U.S. intelligence official said it was common for Israel and other countries to target such international gatherings.

“The only thing that’s unusual now is you hear about it,” the official said.

Mr. Raiu said Kaspersky doesn’t know what was stolen from the three hotels or from the other venues. He said the virus was packed with more than 100 discrete “modules” that would have enabled the attackers to commandeer infected computers.

One module was designed to compress video feeds, possibly from hotel surveillance cameras. Other modules targeted communications, from phones to Wi-Fi networks. The attackers would know who was connected to the infected systems, allowing them to eavesdrop on conversations and steal electronic files. The virus could also enable them to operate two-way microphones in hotel elevators, computers and alarm systems. In addition, the hackers appeared to penetrate front-desk computers. That could have allowed them to figure out the room numbers of specific delegation members.

The virus also automatically deposited smaller reconnaissance files on the computers it passed through, ensuring the attackers can monitor them and exploit the contents of those computers at a later date.