The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Russia's Kaspersky Lab Says Cyberattack Targeted Iran Talks Venue

June 11, 2015



Employees working at the main office of Kaspersky Lab in Moscow.

A computer virus was used to hack into venues linked to international talks on Iran's nuclear program, Russian computer security company Kaspersky Lab said on Wednesday.

Kaspersky said it found the software in three European hotels used in the negotiations involving Iran and six world powers and also on Kaspersky's own computers.

Both Kaspersky and U.S. security company Symantec said the virus shared some programming with previously discovered espionage software called Duqu, which security experts believe to have been developed by Israelis.

"Most notably, some of the new 2014-2015 infections are linked to the P5+1 events and venues related to the negotiations with Iran about a nuclear deal," the statement said.

"P5+1" refers to the six world powers negotiating with Iran on curbs to its disputed nuclear program — the United States, Russia, China, Britain, France and Germany. The talks have

been held in Geneva, Lausanne, Montreux, Munich and Vienna.

In February, the United States accused Israel of using selective leaks from the talks to distort the U.S. position.

Israel has denounced the diplomatic opening to Iran, saying it doubts any agreement arising from the talks will sufficiently restrain the nuclear programme of its arch-enemy.

The West suspects Iran wants to develop a nuclear weapons capability from its enrichment of uranium. Iran says it wants nuclear energy only for electricity and medical isotopes.

During various rounds of the talks, Israeli officials said they knew what was being discussed from various sources including intelligence gathering and information relayed by allies.

The officials did not elaborate on the latter, but asserted that Israel never spied on the United States, its closest ally.

Other victims of what Kaspersky called "Duqu 2.0" had been found in Western countries, the Middle East and Asia.

Another attack, Kaspersky said, was carried out "in relation to" the commemoration of the 70th anniversary in January this year of the liberation of the Auschwitz-Birkenau Nazi concentration camp in Poland.

That ceremony was attended by the heads of state of Germany, France, Britain and other nations.

Kaspersky said the new software included commands for an unknown type of control software that could have been used at the hotels for conferencing tools.

Duqu Similar to Stuxnet Worm

Kaspersky said Duqu 2.0 had evolved from the earlier Duqu, which had been deployed against unidentified targets for years before it was discovered in 2011.

Symantec and Kaspersky analysts have said there was overlap between Duqu and Stuxnet, a U.S.-Israeli project that sabotaged Iran's nuclear program in 2009-2010 by destroying a thousand or more centrifuges that were enriching uranium.

Kaspersky said Duqu 2.0 used three previously unknown flaws in Microsoft Corp Inc software to infect machines and spread, including a problem with Software Installer files, which are commonly used by technical administrators to install and update software on Windows computers within an organization.

The attack left almost no traces.

Microsoft said it fixed the last of those flaws on Tuesday.

Moscow-based Kaspersky, a supplier of anti-virus software and other security tools, said it

discovered the advanced malware earlier in the spring as a result of attacks it had seen on a number of organizations, including itself.

At a news conference in London, Chief Executive Eugene Kaspersky said malicious software designed by cyberspies often finds its way into the hands of cybercriminals, and thereby poses a far wider threat in a world that now relies on the Internet.

"Cybercriminals are copying the technologies from the state-sponsored attacks. They educate the bad guys," Kaspersky said.

As a top research firm that shares its findings with the rest of the security industry, knowing what Kaspersky knew would allow cyberspies to craft fresh attacks to evade detection for new campaigns.

Kaspersky has uncovered a number of advanced cyber-espionage campaigns, including several from the West, making it a tempting target for spies who want to know what it knows.

Though known attacks on security firms are still rare, the industry has become increasingly fragmented along geopolitical lines.

Original url:
https://www.themoscowtimes.com/2015/06/11/russias-kaspersky-lab-says-cyberattack-targeted-iran-talks-venue-a47322