#CYBER RISK

OCTOBER 5, 2017 / 8:28 PM / 6 DAYS AGO

# Russian hackers stole U.S. cyber secrets from NSA: media reports

Dustin Volz, Joseph Menn

WASHINGTON (Reuters) - Russian government-backed hackers stole highly classified U.S. cyber secrets in 2015 from the National Security Agency after a contractor put information on his home computer, two newspapers reported on Thursday.

An undated aerial handout photo shows the National Security Agency (NSA) headquarters building in Fort Meade, Maryland. NSA/Handout via REUTERS

As reported first by The Wall Street Journal, citing unidentified sources, the theft included information on penetrating foreign computer networks and protecting against cyber attacks

In a later story, The Washington Post said the employee had worked at the NSA's Tailored Access Operations unit for elite hackers before he was fired in 2015.

The NSA declined to comment, citing agency policy “never to comment on our affiliates or personnel issues.” Reuters was not able to independently verify the reports.

If confirmed, the hack would mark the latest in a series of breaches of classified data from the secretive intelligence agency, including the 2013 leaks of data on classified U.S. surveillance programs by contractor Edward Snowden.

Another contractor, Harold Martin, is awaiting trial on charges that he took classified NSA material home. The Washington Post reported that Martin was not involved in the newly disclosed case.

Republican U.S. Senator Ben Sasse, a member of the Senate Armed Services Committee, said in a statement responding to the Journal report that, if true, the details were alarming.

”The NSA needs to get its head out of the sand and solve its contractor problem,“ Sasse said. ”Russia is a clear adversary in cyberspace and we can’t afford these self-inflicted injuries.”

Tensions are already high in Washington over U.S. allegations of a surge in hacking of American targets by Russians, including the targeting of state election agencies and the hacking of Democratic Party computers in a bid to sway the outcome of the 2016 presidential election in favor of Republican Donald Trump.

Citing unidentified sources, both the Journal and the Post also reported that the contractor used antivirus software from Moscow-based Kaspersky Lab, the company whose products were banned from U.S. government networks last month because of suspicions they help the Kremlin conduct espionage.

Kaspersky Lab has strongly denied those allegations.

from the machine to Kaspersky computers.

Kaspersky said in a statement on Thursday that it found itself caught in the middle of a geopolitical fight.

“Kaspersky Lab has not been provided any evidence substantiating the company’s involvement in the alleged incident reported by the Wall Street Journal,” it said. “It is unfortunate that news coverage of unproven claims continue to perpetuate accusations about the company.”

The Department of Homeland Security on Sept. 13 banned Kaspersky products in federal networks, and the U.S. Senate approved a bill to ban them from use by the federal government, citing concerns the company may be a pawn of the Kremlin and poses a national security risk.

James Lewis, a cyber expert with the Washington-based Center for Strategic and International Studies, said the report of the breach sounded credible, though he did not have firsthand information on what had transpired.

“The baffling parts are that he was able to get stuff out of the building and that he was using Kaspersky, despite where he worked,” Lewis said. He said that intelligence agencies have considered Kaspersky products to be a source of risk for years.

Democratic Senator Jeanne Shaheen, who led calls in Congress to purge Kaspersky Lab products from government networks, on Thursday called on the Trump administration to declassify information about threats posed by Kaspersky Lab.

“It’s a disservice to the public and our national security to continue withholding this information,” Shaheen said in a statement.

Reporting by Dustin Volz and Joseph Menn; Additional reporing by Warren Strobel, John Walcott, Doina Chiacu; Editing by Jim Finkle, Jonathan Oatis and Grant McCool

*Our Standards:* *The Thomson Reuters Trust Principles.*

OCTOBER 11, 2017 / 3:51 AM / UPDATED 10 HOURS AGO

# Israeli spies found Russians using Kaspersky software for hacks: media

Reuters Staff

((This version of the story corrects to remove name of Kaspersky spokesperson cited by Washington Post in 15th paragraph. The story quoted a company statement).)

The logo of the anti-virus firm Kaspersky Lab is seen at its headquarters in Moscow, Russia September 15, 2017. REUTERS/Sergei Karpukhin

WASHINGTON (Reuters) - Israeli intelligence officials spying on Russian government hackers found they were using Kaspersky Lab antivirus software that is also used by 400 million people globally, including U.S. government agencies, according to media reports on Tuesday.

first reported the story. (nyti.ms/2yev8vj)

That led to a decision in Washington only last month to order Kaspersky software removed from government computers.

The Washington Post also reported on Tuesday that the Israeli spies had also found in Kaspersky′s network hacking tools that could only have come from the U.S. National Security Agency. wapo.st/2i2clXa

After an investigation, the NSA found that those tools were in possession of the Russian government, the Post said.

And late last month, the U.S. National Intelligence Council completed a classified report that it shared with NATO allies concluding that Russia’s FSB intelligence service had “probable access” to Kaspersky customer databases and source code, the Post reported.

That access, it concluded, could help enable cyber attacks against U.S. government, commercial and industrial control networks, the Post reported.

The New York Times said the Russian operation, according to multiple people briefed on the matter, is known to have stolen classified documents from a National Security Agency employee who had improperly stored them on his home computer, which had Kaspersky antivirus software installed on it.

It is not yet publicly known what other U.S. secrets the Russian hackers may have discovered by turning the Kaspersky software into a sort of Google search for sensitive information, the Times said.

The current and former government officials who described the episode spoke about it on condition of anonymity because of classification rules, the Times said.

The newspaper said the National Security Agency and the White House declined to comment, as did the Israeli Embassy, while the Russian Embassy did not respond to requests for comment.

Kaspersky Lab denied to the Times any knowledge of, or involvement in, the Russian hacking. “Kaspersky Lab has never helped, nor will help, any government in the world with its cyberespionage efforts,” the company said in a statement on Tuesday.

RELATED COVERAGE

Germany: 'No evidence' Kaspersky software used by Russians for hacks

Eugene Kaspersky, the company’s co-founder and chief executive, has repeatedly denied charges his company conducts espionage on behalf of the Russian government.

The company issued a statement saying that “as a private company, Kaspersky Lab does not have inappropriate ties to any government, including Russia, and the only conclusion seems to be that Kaspersky Lab is caught in the middle of a geopolitical fight,” the Washington Post reported. The company “does not possess any knowledge” of Israel’s hack, the Post cited the statement as saying.

U.S. intelligence agencies have concluded that Russian President Vladimir Putin ordered a multipronged digital influence operation last year in an attempt to help Donald Trump win the White House, a charge Moscow denies.

Reporting by Eric Walsh; Editing by Grant McCool and Bill Trott

*Our Standards:* *The Thomson Reuters Trust Principles.*

Apps Newsletters Reuters Plus Advertising Guidelines Cookies Terms of Use Privacy