Exclusive: Russian hackers targeted California, Indiana Democratic parties

reuters.com/article/us-usa-election-cyber-russia-exclusive-idUSKBN27F1CP

Raphael Satter, Christopher Bing, Joel Schectman

Cyber Risk
Updated

By Raphael Satter, Christopher Bing, Joel Schectman

6 Min Read

WASHINGTON (Reuters) - The group of Russian hackers accused of meddling in the 2016 U.S. presidential election earlier this year targeted the email accounts of Democratic state parties in California and Indiana, and influential think tanks in Washington and New York, according to people with knowledge of the matter.

The Center for Strategic and International Studies (CSIS) is seen through the rain in Washington, D.C., October 29, 2020. REUTERS/Raphael Satter

The attempted intrusions, many of which were internally flagged by Microsoft Corp MSFT.O over the summer, were carried out by a group often nicknamed "Fancy Bear." The hackers' activity provides insight into how Russian intelligence is targeting the United States in the run-up to the Nov. 3 election.

The targets identified by Reuters, which include the Center for American Progress, the Council on Foreign Relations and the Washington-based Carnegie Endowment for International Peace, said they had not seen any evidence of successful hacking attempts.

Fancy Bear is controlled by Russia's military intelligence agency and was responsible for hacking the email accounts of Hillary Clinton's staff in the run-up to the 2016 election, according to a Department of Justice indictment filed in 2018.

News of the Russian hacking activity follows last month's announcement here by Microsoft that Fancy Bear had attempted to hack more than 200 organizations, many of which the software company said were tied to the 2020 election. Microsoft was able to link this year's cyber espionage campaign to the Russian hackers through an apparent programming error that allowed the company to identify a pattern of attack unique to Fancy Bear, according to a Microsoft assessment reviewed by Reuters.

Microsoft declined to comment on Reuters' findings, citing customer privacy. But Tom Burt, corporate vice president, customer security and trust, said in a statement that the company - and the U.S. government - "have been working hard to keep this election safe and secure."

The thrust of espionage operations could not be determined by Reuters. The Office of the Director of National Intelligence said in August here that Russian operations were attempting to undermine the campaign of presidential candidate Joe Biden.

Democratic National Committee spokesman Chris Meagher said it was "no surprise" that foreign actors were attempting to interfere with the election.

The Russian Embassy in Washington said it does not interfere in America's internal affairs and denied any link to "Fancy Bear," calling the allegation "fake news."

The Trump campaign did not return messages.

Over the summer, a specialized cybersecurity unit at Microsoft and federal law enforcement agents notified many of the targets who were in Fancy Bear's crosshairs, according to six people with knowledge of the matter. Reuters last month identified SKDKnickerbocker, a lobbying firm allied with Biden, as one of them.

The targeting of Democrats in Indiana and California - confirmed by four people familiar with the matter - suggests that the Russians are "casting their net wide," said Don Smith of cybersecurity company Secureworks.

The Indiana Democratic Party said in a statement it was “unaware of any successful intrusions.” California Democratic Party Chair Rusty Hicks acknowledged being targeted, but stopped short of naming Fancy Bear, saying in an email that “the effort by the foreign entity was unsuccessful.”

The FBI declined comment.

ATTACKS ON INFLUENTIAL NON-PROFITS Fancy Bear also targeted think tanks and foreign policy organizations that hold sway in Washington and have, in the past, provided staff for presidential administrations.

Among them was the Center for American Progress (CAP), a left-leaning group whose founder, John Podesta, was at the center of the 2016 Russian hack and leak operation, according to a person with direct knowledge of the incident.

A CAP spokesperson said the organization had not been breached and declined further comment. The Open Society Foundations, one of the first organizations to see its correspondence leaked to the public by Fancy Bear in 2016, was targeted by the Kremlin again earlier this year, according to two people briefed on the matter. The group’s founder, George Soros, has provided substantial funding to pro-democracy causes and is a regular target of Russian disinformation as well as domestic conspiracy theories.

In a statement, the Open Society said “obviously tensions are extraordinarily high heading into this election, and we are taking many steps to ensure the safety of our staff.”

Others targeted by Fancy Bear in 2020 included the New York-based Council on Foreign Relations (CFR), the Washington-based Carnegie Endowment, and the Center for Strategic and International Studies (CSIS) - all of whom were notified by Microsoft, according to people familiar with the respective organizations.

A CSIS spokesman declined comment on the hacking activity. A Carnegie spokeswoman confirmed the targeting, but declined to provide further detail. A spokeswoman with the Council on Foreign Relations said they had not been breached.

Editing by Jonathan Weber, Chris Sanders, Edward Tobin and Sonya Hepinstall

Our Standards: The Thomson Reuters Trust Principles.