

## National Security

# Court document points to Kaspersky Lab's cooperation with Russian security service

---

By **Ellen Nakashima** December 13

Kaspersky Lab, a Russian cybersecurity firm, has long asserted its independence of the Russian government. But a court document posted on the Facebook page of a Russian criminal suspect this year shows what appears to be an unusual degree of closeness to the FSB, the country's powerful security service.

The suspect, Konstantin Kozlovskiy, was arrested in the summer of 2016 in connection with several cyber heists of Russian banks, and he is in a Moscow jail awaiting trial. From his cell, he posted documents related to his case.

One of them shows that in April 2015, an FSB agent inside the office of Kaspersky Lab in Moscow gave a company technician a password for a suspected Russian cyber criminal's computer. The technician gained access to the computer and obtained decrypted documents for the agent.

The agent, A.V. Kutasevich, worked side-by-side with the Kaspersky technician, Ruslan Sabitov, in the "information retrieval" operation, according to the document, dated April 28, 2015.

Though American cybersecurity firms sometimes provide technical assistance to the FBI in criminal investigations, the close cooperation between Kaspersky Lab and the FSB raises eyebrows at a time when the Russian firm's software products have been banned by the U.S. government out of concern they can be exploited as a platform for Russian spying.

The FSB used the information Kaspersky obtained to help make its case against Kozlovskiy, who is a member of the criminal group Lurk.

Kaspersky previously had publicized its help in bringing down Lurk, which allegedly stole up to \$45 million from Russian companies and banks. But it was not known that Kaspersky allowed an FSB agent to be inside its Moscow office to supervise the operation.

"The most interesting thing is that Kaspersky's experts were not asked to provide expertise," said Andrei Soldatov, an expert on Russian surveillance and co-author of The Red Web. "They actively and secretly participated in an ongoing FSB operation,

which makes them look like assets rather than experts.”

Though authorized by a Moscow court, “this kind of ‘joint operation’ raises a question whether the company went too far in its cooperation with the Russian secret services,” Soldatov said.

The firm said in a statement that as part of its technical assistance in taking down Lurk, it served “as a third party expert source for a specified task, as granted by the court. The work completed by a Kaspersky Lab expert was requested by law to ensure that no modifications of any information received from the server were made, and also to assist in the translation of technical data obtained during the procedure into language that could be understood in a legal setting. In addition, this investigation procedure was completed in the presence of an FSB agent and two civil witnesses, and it is important to note that Kaspersky Lab products or services were not used.”

A former FBI special agent who worked a number of high-profile cyber cases said such an arrangement in the United States would be unusual and “outside the realm of something the bureau would approve.”

The optics are poor, said Milan Patel, co-head of managed services at BlueVoyant, a cybersecurity company. It’s one thing to ask a firm to provide intelligence on a particular hacker it has researched, he said. It’s another to ask that firm to help the FBI get “live access to” a computer “that might have that information.” With a court order, the FBI would conduct the surveillance on its own.

A senior executive at a major cyber firm, who spoke on the condition of anonymity to avoid being seen as criticizing another security firm, said: “For any commercial security vendor to be overtly involved in work like that is extremely unusual. You’re basically doing an offensive cyber operation, targeting an individual system’s people on behalf of an intelligence organization.”


The company’s founder, Eugene Kaspersky, graduated from a KGB-supported cryptography school and had worked in Russian military intelligence. He insists the firm has “never helped” espionage agencies. “It doesn’t matter if they’re Russians or from any other nation,” he said recently in London. He added that “If the Russian government comes to me and asks me to do anything wrong — or my employees — I will move the business out of Russia.”

The company said it has also provided technical assistance for national and international law enforcement agencies, including Interpol, Europol and the London police.

“In addition, it’s common for law enforcement agencies to work together with cybersecurity companies to effectively fight cybercrime,” the company said.

Koslovskiy has placed other documents on his Facebook page that have sparked concerns. In August, he posted a letter in which he states he hacked the U.S. Democratic National Committee’s computers on orders from the FSB. The assertion is dubious, senior intelligence officials said, especially as it was two other Russian spy agencies that penetrated the DNC system.

 **21 Comments**

Ellen Nakashima is a national security reporter for The Washington Post. She covers cybersecurity, surveillance, counterterrorism and intelligence issues.  Follow @nakashimae

### Share news tips with us confidentially

Do you have information the public should know? Here are some ways you can securely send information and documents to Post journalists.

**[Learn more](#)**

