THERE'S SOMETHING VERY WEIRD HAPPENING INSIDE RUSSIA'S CYBERSECURITY WORLD

-

27.01.2017

BuzzFeed Jan. 27, 2017

Sheera Frenkel

The arrest of several of Russias top cybersecurity figures has led to speculation that theres a shakeup inside the countrys national security service related to hacks surrounding the US election.

A series of surprising arrests of some of Russias top cybersecurity figures has left the international cybersecurity officials and analysts wondering whether Russia is cleaning house of suspected spies, or going through an internal shakeup of the FSB, Russias national security service.

At some point in December, Ruslan Stoyanov, a well-respected researcher with the Moscow-based Kaspersky Lab, and Sergei Mikhailov, head of the FSBs Center of information Security, were arrested by Russian police as part of what Russias Kommersant newspaper described as a probe into possible treason. No date of arrest has been made public, though Kommersant reported that Stoyanov last logged into his private social media account on December 4, and Mikhailov on December 5. The Moscow-based Novaya Gazeta newspaper cited sources as saying Mikhailov was arrested during a meeting with other FSB officers in Moscow, and was taken from the room with a sack over his head.

On Thursday, REN-TV, a privately-owned TV channel in Russia, said a second FSB officer had also been arrested in December. They identified the man as Major Dmitry Dokuchayev, and reported he had served under Mikhailov in the the Center for Information Security. In another indication that Russia was seeing a high-level shakedown at the FSB, Kommersant reported that on January 13, the director of the Center for Information Security, Andrei Gerasimov, was fired. He was described as having close ties to cybersecurity companies, including Kaspersky Lab.

Kaspersky Lab confirmed that Stoyanov was under investigation for activity during a period predating his employment at the company, and added, in a public statement, We do not possess details of the investigation. The work of Kaspersky Labs Computer Incidents Investigation Team is unaffected by these developments.

Stoyanovs LinkedIn page lists his previous employer as the Ministry of the Interiors Cyber Crime Unit.

Four intelligence officers working in various branches of the US government told BuzzFeed News this week that they had no insight into the arrests of Stoyanov and Mikhailov, with one explaining, its above my paygrade.

There are a small handful of people who would know if one or both of these men was a US asset or in any way involved in any intelligence operation, and Im not one of them, said the US intelligence officer, who asked not to be named due to the sensitivity of the story. Obviously, this could also be an internal struggle within the FSB, in which case we would have little daylight into what was happening.

The case against Stoyanov and Mikhailov has been filed in a secret military tribunal under Article 275 of the countrys constitution, which allows the government to investigate individuals they suspect of spying for a foreign state.

Whether or not their cases have anything to do with the Russias involvement in the hacks targeting the US 2016 elections remains unclear. Fancy Bear, the group named by US cybersecurity companies as being behind the hacking and leaking of damaging emails from top DNC officials, has been tied back to the GRU, Russias main foreign intelligence agency. Cozy Bear, a group also believed to have been within the DNCs system, has been linked to the FSB.

While most news reports do not directly tie the arrested men to the DNC hack, the Moscow Times reported that Mikhailovs arrest was due to suspicions that he tipped US officials off to the Russian server rental company King Servers which the Arlington-based ThreatConnect cybersecurity company identified last September as a nexus used by Russian hackers in attacks against the US.

In Russia, rumors about the arrested men are running rampant. Russias Tzargrad news site published a story claiming that Mikhailov had secretly been the leader of a notorious Russian hacking group called Shaltay-Boltay (or Humpty Dumpty), and that the group was secretly backed by the CIA. The article, which was shared widely within Russian social media, was suddenly taken off the site, though an archived version is still being shared.

Sheera Frenkel is a cybersecurity correspondent for BuzzFeed News based in San Francisco. She has reported from Israel, Egypt, Jordan and across the Middle East. Her secure PGP fingerprint is 4A53 A35C 06BE 5339 E9B6 D54E 73A6 0F6A E252 A50F

Contact Sheera Frenkel at Sheera.Frenkel@buzzfeed.com.

Kaynak/Source: