https://www.wsj.com/articles/yahoo-hacking-charges-cast-new-light-on-ties-between-russias-fsb-cybercriminals-1489615891

WORLD

# Yahoo Hacking Charges Cast New Light on Ties Between Russian Intelligence, Cybercriminals

U.S. indictments overlap with major cybercrime scandal that rocked Russian political establishment


FSB officer Dmitry Dokuchaev, who was named in the U.S. indictment Wednesday, was also named in arrests earlier this year related to a major cybercrime scandal in Russia. *PHOTO: ANDREW HARRER/BLOOMBERG NEWS*

By **NATHAN HODGE**

March 15, 2017 6:11 p.m. ET

MOSCOW—The U.S. government's indictment of Russian government officials in connection with the hacking of Yahoo Inc. casts new light on the nexus between Russia's intelligence services and the world of cybercriminals.

The Justice Department on Wednesday alleged two officers of Russia's Federal Security Service, the successor agency to the Soviet-era KGB, recruited hackers to breach the Yahoo's networks.

It isn't the first time the U.S. government has accused Russia's spies of tapping the expertise of hackers. U.S. intelligence agencies last year accused the Russian government of trying to interfere in the 2016 U.S. presidential elections by orchestrating the hacking of emails from the Democratic National Committee and other entities. The Russians have consistently denied any interference in U.S. domestic politics.

> "Washington did not communicate with Moscow through the channels available to address issues related to cybersecurity in this case," a Russian official said

Wednesday following the Justice Department's allegations. "This fact, as well as the lack of specifics in this case, suggest the next round of raising the theme of 'Russian hackers' in the domestic political squabbles in the U.S."

The new U.S. indictments also appear to overlap with a major cybercrime scandal that has rocked the Russian political establishment.

Earlier this year, Russian news media were abuzz over the news of arrests tied to a high-profile treason case. Those arrested included at least two intelligence officials at the FSB and an employee at Kaspersky Lab, Russia's most prominent cybersecurity firm. The Russian government provided little official confirmation, but investigative reports and Russian news media speculated the arrests were tied to a hacking collective named "Shaltai Boltai," a shadowy group that earned notoriety in Russia by leaking the private correspondence of high-ranking government officials.

MORE

- Two Russian Spies Charged in Yahoo Hack
- Alleged Hacker Karim Baratov Flaunted Wealth
- Yahoo Hack: Are You Still at Risk?
- Read the Indictment

The FSB hasn't spoken publicly about the treason case and couldn't be reached about the charges announced Wednesday.

Much as WikiLeaks has become a headache for successive U.S. administrations, Shaltai Boltai revealed compromising information and hacked the accounts of prominent individuals, including the Twitter account of Prime Minister Dmitry Medvedev.

Adding to the sensation of the case, two of the individuals named late last year in the arrests were Russian intelligence officers charged with battling cybercrime: They worked in the Information Security Center, the FSB's cybersecurity wing. One of those two officers was Dmitry Dokuchaev, who was also charged in the U.S. government indictment Wednesday.

Mr. Dokuchaev couldn't be reached for comment. He is believed to be in Russia.

Andrei Soldatov, an expert on Russia's internet, said Mr. Dokuchaev, who went by the online alias Forb, according to Russian media, was recruited into the security services for his skills and contacts in the darker corners of the web.

"He had some knowledge about the digital underground, that's something really important," Mr. Soldatov said. "For the FSB, it was the perfect thing to try to get."

Mark Galeotti, senior researcher at the Institute of International Relations Prague, said Russian spy agencies had employed "a degree of outsourcing of capacity" for cyber operations, turning to groups that use hacking for criminal enterprises such as fraud and online scams.

"The Americans outsource [cyber capabilities], but they tend not to go to criminals," he said. "The Russians have a more pragmatic approach."

Several countries caught up in confrontation with Russia have been on the receiving end of cyberattacks in recent years. Cyber attackers traced to Russia carried out attacks on Estonian websites in 2007, temporarily taking down much of the country's online traffic. During a brief war between Russia and Georgia the following year, hackers traced to Russia attacked and defaced Georgian sites.

In recent years, however, Mr. Galeotti said Russian intelligence agencies have built up their own in-house cyberattack capabilities, recruiting hackers and putting them directly in government employ.

But when they need “surge capacity,” such as during the conflict with Ukraine, Mr. Galeotti added, “they have gone to the private sector—the criminal private sector.”

**Write to** Nathan Hodge at nathan.hodge@wsj.com