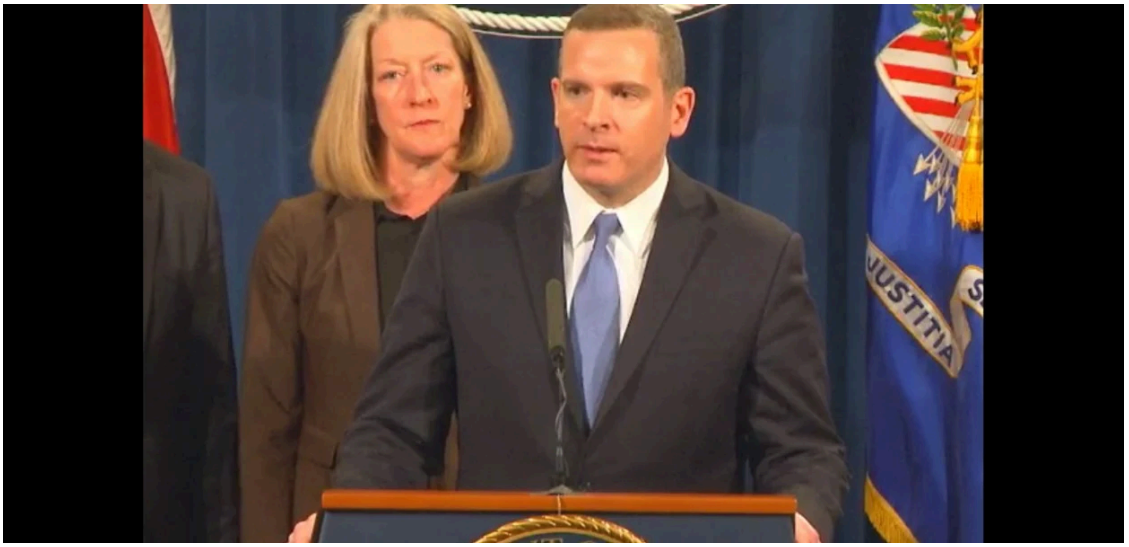
US Charges Four Hackers in Yahoo 2014 Security Breach, Including Two FSB Agents

By Catalin Cimpanu

Published: 2017-03-15 · Archived: 2026-04-05 23:00:56 UTC

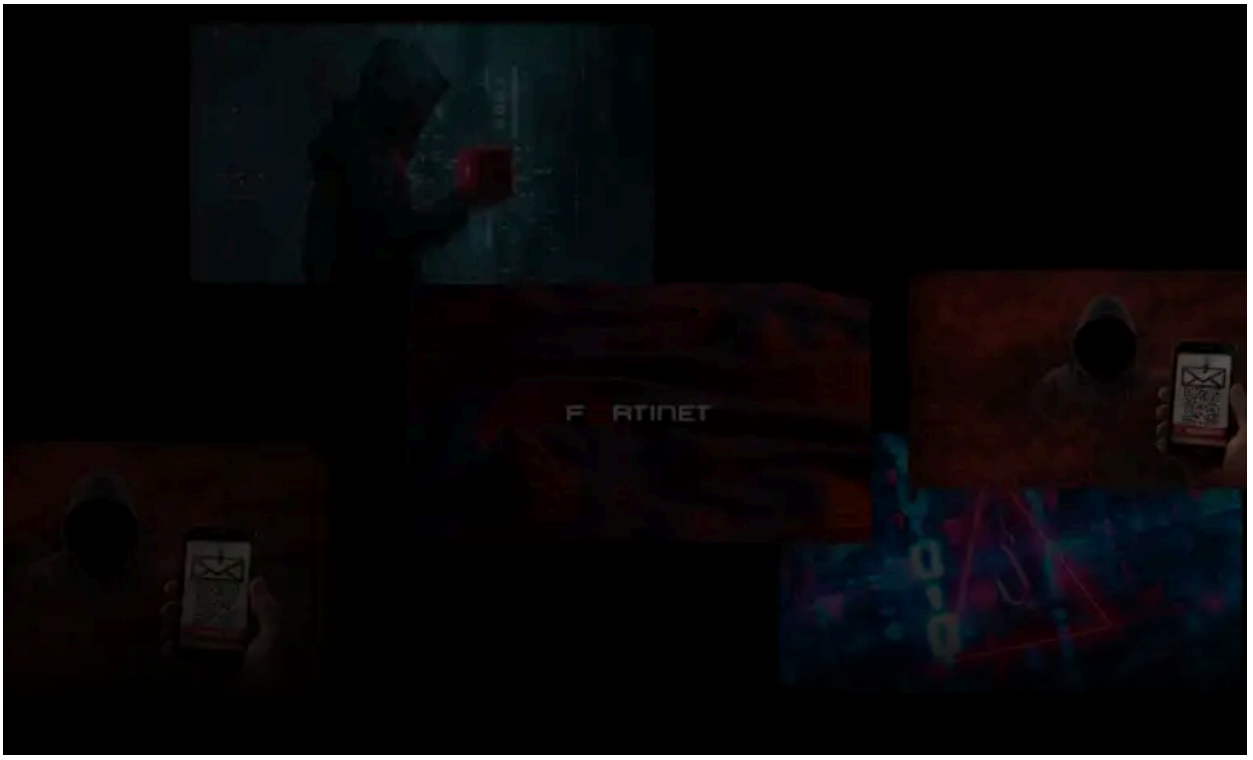


The US Department of Justice (DoJ) charged four suspects today for orchestrating the 2014 Yahoo data breach during which attackers stole details for over 500 million Yahoo users.

In a press conference today, officials from the DoJ and FBI said that two of the suspects are members of the Russian Federal Security Service (FSB), who "protected, directed, facilitated and paid criminal hackers" to breach Yahoo's network in 2014.

DoJ: Two FSB agents orchestrated the hack

The two FSB agents behind the Yahoo 2014 hack are Igor Anatolyevich Sushchin, 43, and Dmitry Aleksandrovich Dokuchaev, 33.


F RTINET

The two hackers who carried out the attacks are Alexsey Alexseyevich Belan, aka "Magg," 29, a Russian national, and Karim Baratov, aka "Kay," 22, a Canadian and Kazakh national, currently living in Canada. Of all, only Baratov is under custody, after Canadian police arrested him last week.

The other hacker, Belan, was previously charged with breaching three US tech companies in 2012 and stealing details for over 200 million users. Belan is also on the FBI's Cyber Most Wanted list, and he's been on the list since its creation a few years back.

FSB agents worked for Center 18

Authorities have little hope of arresting and extraditing the other three, and for a good reason.

"The FSB unit that the defendants worked for, the Center for Information Security, also known as Center 18, is also the **FBI's point of contact in Moscow for cyber-crime matters**," Acting Assistant Attorney General Mary McCord of the National Security Division explains.

In fact, the FBI says they reached out to FSB's Center 18 in 2014 and asked for Belan's extradition. The FSB never answered.

"Instead of acting on the U.S. government's [Interpol] Red Notice and detaining Belan after his return, **Dokuchaev and Sushchin subsequently used him to gain unauthorized access to Yahoo's network**," US officials said.

Yahoo was right. It was a "state-sponsored actor"

The indictment also proves Yahoo was right when it said last September that a "state-sponsored actor" was behind the attack, a claim very few people believed.

According to official documents detailing the attacks, the hack took place just as Yahoo described in recent SEC filings.

Belan, at the behest of the two FSB agents, breached Yahoo's network, from where he stole names, recovery email accounts, phone numbers, and data necessary to craft account browser cookies.

Furthermore, Belan also gained access to Yahoo's Account Management Tool (AMT), a system that allowed the hacker and the two FSB agents to craft the browser cookies necessary to access Yahoo accounts without a cleartext password.

FSB agents breached political targets, Belan hacked for profit

The US alleges the three accessed around 6,500 user accounts via this method. Targets included Russian journalists, Russian and US government officials, employees of a prominent Russian cybersecurity company, and numerous employees of web providers whose networks the three wanted to exploit.

Besides these targets, of clear interest for intelligence gathering, Belan also accessed accounts for personal gains. This included the personal accounts of employees at commercial entities, such as a Russian investment banking firm, a French transportation company, US financial services and private equity firms, a Swiss Bitcoin wallet and banking firm, and a US airline.

In addition, Belan also used his access to Yahoo email accounts to steal gift cards and credit card numbers from people's inboxes.

Furthermore, US officials say Belan stole the private contacts from 30 million Yahoo accounts, which he used to earn commissions from spam campaign and fraudulent search engine traffic.

DoJ: FSB agents protected Belan

US officials allege that for his work, the two FSB agents provided Belan with information necessary to avoid detection by US investigators.

It is very important for corporations around the country to know that when you are going against the resources and backing of a nation state, it is not a fair fight, and it is not a fight your are likely to win.
- Acting Assistant Attorney General Mary McCord

Baratov was only a second-stage pawn

Baratov, who was a hacker very active on the Dark Web under the alias of "Four," entered the scheme later on, when the two FSB agents couldn't gain access to email accounts at other email providers.

According to the indictment, using data from the Yahoo breach, the FSB agents asked Baratov to hack into more than 80 accounts. Investigators say Baratov stood to gain various commissions for providing the two FSB agents with passwords to desired accounts.

According to US officials, Google detected some of these attempted intrusions against Gmail accounts and also filed a complaint with authorities.

The official indictment is available for download here (PDF). Yahoo also issued a short statement on the hacks. An audio of the press conference is available below.
