

4-NBC News-Russian Spies Charged

Tech News

Russian Spies Charged in Massive Yahoo Email Hack

Justice Department officials announced indictments against four suspects in hacking attacks on Yahoo, including two Russian intelligence officials.

FBI Criminal Cyber, Response and Services Branch Executive Assistant Director Paul Abbate speaks during a press conference to announce criminal charges against three Russians for the 2014 hacking of Yahoo at the Department of Justice on March 15, 2017 in Washington. Brendan Smialowski / AFP - Getty Images

Link copied

By Ken Dilanian

The Justice Department announced charges Wednesday against two Russian spies and two hackers behind the 2014 theft of data connected to half a billion Yahoo accounts, which officials called one of the largest known data breaches in American history.

The four men together face 47 criminal charges, including conspiracy, computer fraud, economic espionage, theft of trade secrets and aggravated identity theft, the Justice Department said in a news release.

One of them, Karim Baratov, 22, a Canadian and Kazakh national and a resident of Canada, was arrested in Canada on Tuesday, said Mary McCord, acting assistant attorney general for national security.

Yahoo Hack: Russian Spies Charged by U.S. Over Hack of 500M Accounts

March 15, 2017 02:58

Also charged were two agents of Russia's Federal Security Service, known as the FSB. They are Dmitry Aleksandrovich Dokuchaev, 33, a Russian national and resident, and Igor Anatolyevich Sushchin, 43, a Russian national and resident.

The other defendant, Alexsey Alexseyevich Belan, 29, a Russian national and resident, was already among the FBI's most wanted cyber criminals, McCord said.

Related: Were Russians Behind Massive Yahoo Email Hack?

"The criminal conduct at issue, carried out and otherwise facilitated by officers from an FSB unit that serves as the FBI's point of contact in Moscow on cybercrime matters, is beyond the pale," McCord said in a statement. [Anger]

At a news conference, she and other officials described a widespread and complex scheme that allowed the Russian spies to gather intelligence, while the hackers "lined their pockets."

Related: You Could Have a Yahoo Account and Not Know It

U.S. officials did not detail everything the Russian spy service gleaned from its massive haul of email data, but the Justice Department news release noted that "some victim accounts were of predictable interest to the FSB."

That included "personal accounts belonging to Russian journalists; Russian and U.S. government officials; employees of a prominent Russian cybersecurity company; and numerous employees of other providers whose networks the conspirators sought to exploit."

Russian Agents and Criminal Hackers Charged in Yahoo Hack

March 15, 2017 01:52

Other compromised accounts belonged to "a Russian investment banking firm, a French transportation company, U.S. financial services and private

equity firms, a Swiss bitcoin wallet and banking firm and a U.S. airline.”

Justice Department officials said the FSB officers facilitated Belan’s criminal activities by providing him with sensitive information that would have helped him avoid detection by U.S. and other law enforcement agencies outside Russia, including law enforcement techniques for identifying criminal hackers.

Related: Your Yahoo Account Was Probably Hacked

Belan used his access to Yahoo accounts to steal credit card numbers, officials said, and he also stole contacts from 30 million accounts for a spam campaign. He also earned commissions from fraudulently redirecting a subset of Yahoo’s search engine traffic, prosecutors alleged.

The two FSB officers worked in a section devoted to cyber security, McCord said.

“These are the very people that we are supposed to work with, cooperatively, in law enforcement channels.” McCord said.
[Disappointment]

Alexsey Alexseyevich Belan, 29, a Russian national and resident.FBI

Yahoo disclosed in September that hackers breached its network in late 2014 and stole personal data associated with more than 500 million users. The 2014 incident was in addition to a much larger theft that Yahoo disclosed in December and that dated back to 2013.

The two largest hacks, and Yahoo’s much-criticized slow response and disclosure, forced a discount of \$350 million in what had been a \$4.83 billion deal to sell Yahoo’s main assets to Verizon.

A high-level source familiar with Yahoo’s views on the hacking called the indictment a “vindication” [Positive] for the company, and cited comments by McCord that no company can defend itself against a concerted cyber attack from a nation-state.

“We work hard and diligently every day to protect Yahoo’s infrastructure, [Reinforce]” the source said. “This demonstrates the threat that Yahoo and other providers face from state sponsored actors and cyber mercenaries.” [Reinforce]

How To Protect Yourself From Cyber Hacking

March 15, 2017 01:44

In a statement, Chris Madsen, Yahoo’s assistant general counsel and head of global security, thanked law enforcement agencies for their work.

“We’re committed to keeping our users and our platforms secure and will continue to engage with law enforcement to combat cybercrime,” he said. [Rebuild]

Ken Dilanian is a correspondent covering intelligence and national security for the NBC News Investigative Unit.

Jo Ling Kent contributed.