US charges two Russian spies in massive Yahoo cyberattack (Update)

March 15 2017

Russian agents Dmitry Dokuchaev and Igor Sushchin, indicted in the US over a massive Yahoo hack, were part of the successor to the KGB

Two Russian intelligence agents and a duo of hackers were indicted Wednesday over a data breach that compromised 500 million Yahoo accounts in one of the largest cyberattacks in history.

The indictment announced by the US Justice Department links Russia's

top spy agency, the FSB, to the massive hacking operation which began in 2014 with the twin goals of espionage and financial gain.

It comes amid a high-stakes investigation into Russian cyber-meddling in the US election, potentially aimed at boosting the campaign of President Donald Trump.

The Russian agents were identified as Dmitry Dokuchaev and Igor Sushchin, both members of the successor agency to Russia's KGB.

Dokuchaev was an officer in the FSB Center for Information Security, known as "Center 18," which is tasked with investigating hacking and is the FBI's point of contact in Moscow for cyber crimes.

The 33-year-old Dokuchaev was reported to have been arrested in Moscow earlier this year on treason charges. He is accused of directing the Yahoo hack along with his superior, the 43-year-old Sushchin.

The two officers "protected, directed, facilitated and paid criminal hackers to collect information through computer intrusions in the United States and elsewhere," acting assistant attorney general Mary McCord told reporters.

They are accused of hiring hackers Alexsey Belan and Karim Baratov to carry out the attacks, which continued until late 2016.

Targets of the Yahoo breach included both Russian and US government officials, including cyber security, diplomatic and military personnel, according to McCord, who said it aimed to gather information "clearly some of which has intelligence value."

She added that "the criminal hackers used this to line their own pockets for private financial gain," seeking to cash in on the breach by accessing

stolen credit or gift card numbers, and through a series of spam marketing schemes.

Journalists, diplomats targeted

The US indictment includes 47 criminal charges including conspiracy, computer fraud, economic espionage, theft of trade secrets and identity theft.

Asked if there were any links between the Yahoo hack and the wider question of Russian interference, McCord said, "We don't have anything that suggests... any relationship," but added that the election case "is an ongoing investigation."

The US statement said some targets were "of predictable interest" to the Russian spy agency including Russian and US government officials and employees of a prominent Russian cybersecurity company.

The Yahoo breach, McCord said, "also targeted Russian journalists; numerous employees of other providers whose networks the conspirators sought to exploit; and employees of financial services and other commercial entities."

Other accounts compromised by the hackers belonged to employees of 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, according to the Justice Department.

Acting Assistant US Attorney General Mary McCord told a news conference that two Russian spies directed the cyberattack on Yahoo

Baratov, a 22-year-old Canadian-Kazakh national, was arrested this week on a US warrant in Canada, she said.

Belan, 29, has been indicted twice in US cases involving the hacking of e-commerce companies, and is listed as one of the FBI's "Cyber Most Wanted criminals."

'State-sponsored'

FBI executive assistant director Paul Abbate said the agency has asked Moscow for assistance in apprehending the suspects but noted that "we have had limited cooperation with that element of the Russian government."

In Russia a high-level official quoted by Russian news agencies said that "Washington did not communicate with Moscow about this issue through the available channels set up to address issues related to cybersecurity."

The source added that "the absence of specifics in this case suggests this is the latest twist in the use of the subject of Russian hackers in the internal political struggle in the US."

The attack on Yahoo, disclosed last year, was one of the largest ever data breaches and at the time was blamed on a "nation-state" attacker.

Yahoo's assistant general counsel Chris Madsen said in a statement that the indictment "unequivocally shows the attacks on Yahoo were state-sponsored."

Chief executive Marissa Mayer tweeted that Yahoo was "very grateful to the FBI & DOJ" for their work.

The internet pioneer, which is in the process of selling its core assets, has been rocked by the disclosure of the breach and a separate case that affected one billion users.

Cookies, erectile dysfunction

The indictment unsealed in federal court in San Francisco showed a series of techniques used by the hackers in accessing user accounts.

In some cases, they used emails disguised as legitimate messages, a technique known as "phishing."

Another scheme directed users searching for erectile dysfunction medications to a fake website that included malicious software.

The hackers were also able to produce forged "cookies" or bits of software used to authenticate users, and used stolen Yahoo credentials to compromise accounts of other webmail providers, including Google.

These efforts enabled the hackers to obtain a backup copy of Yahoo's user database and eventually its "account management tool" that controlled passwords and other personal information, the indictment said.