3-CNET-Yahoos

Featured Politics Social Media Privacy Misinformation

Yahoo’s massive hack blamed on Russian spies

Justice Department indicts four men, including two who worked for the KGB’s successor, for allegedly pulling off the second-largest online breach in history.

Alfred Ng

March 15, 2017 8:42 a.m. PT

Alfred Ng

Senior Reporter / CNET News

Alfred Ng was a senior reporter for CNET News. He was raised in Brooklyn and previously worked on the New York Daily News’s social media and breaking news teams.

Now playing: Watch this: DOJ charges Russian spies with Yahoo hack

1:22

The Yahoo hacking drama just swerved into James Bond territory.

The Justice Department on Wednesday said it’s indicted four hackers responsible for the second-largest online breach in history. Two of the alleged hackers were Russian spies under the Federal Security Service — the country’s FBI equivalent that’s better known as the FSB — while the other two were identified as hired criminals.

The spies wanted dirt on politicians, while the hackers for hire scavenged through the spoils for profits, the Justice Department said. The four were charged with wire fraud, trade secret theft and economic espionage.

Karim Baratov, one of the alleged hackers based in Canada, was arrested on Tuesday, while the other three Russian hackers could be protected from a complicated extradition process.

“The involvement and direction of FSB officers with law enforcement responsibilities makes this conduct that much more egregious,” said Acting Assistant Attorney General Mary McCord during a press conference on Wednesday. “There are no free passes for foreign state-sponsored criminal behavior.”

The indictments offer a tiny measure of closure for Yahoo *[Hope]*, which has wrestled over the last several months with revelations of massive security breaches. When Yahoo in September disclosed a 2014 hack , it was deemed the worst cyberattack ever. But three months later, the company outdid itself by disclosing a separate incident from 2013 that left 1 billion — yes, billion — accounts exposed.

The Russia angle

Beyond that, Wednesday’s news marks yet another incident involving Russia hackers, who are also believed to have meddled in the presidential election last year by accessing emails from the Democratic National Committee, Democratic presidential nominee Hillary Clinton and her campaign manager, John Podesta. It was enough that former President Barack Obama leveled sweeping sanctions against Russia for its cyberattacks.

A two-year investigation by the FBI’s San Francisco branch found evidence of Russian spies Dmitry Dokuchaev and Igor Sushchin helping to break into Yahoo to steal information from US government officials, Russian dissidents and journalists. The Yahoo breach is the largest hacking case ever handled by the US government.

Other victims of the hacks included employees of a Russian cybersecurity company, a Russian investment banking firm, a French transportation company, US financial firms, a Swiss bitcoin wallet and a US airline. Investigators said the spies also hacked their victims' spouses and children's emails to dig up extra dirt.

The Russian spies allegedly left the spoils for Baratov and hacker-for-hire Aleksey Belan, letting the two use the emails for profit.

Belan is already one of the FBI's most wanted cybercriminals , with the agency offering a $100,000 reward for his arrest. The FBI accused Belan of hacking into three major e-commerce companies between 2012 and 2013, allegedly stealing millions of accounts and selling the information. He was also sanctioned by the Obama administration in connection with Russian hackers meddling in the 2016 election.

"Belan used his access to Yahoo to search for and steal financial information such as gift cards and credit card numbers from user's email accounts," McCord said.

The Russian hacker used 30 million stolen Yahoo accounts as part of his own personal spam network, according to the indictment (PDF).

A toolbox of techniques

From left: Igor Sushchin, Alexsy Belan and Karim Baratov. The three Russian-sponsored actors are allegedly behind Yahoo's massive breach. (Not pictured is Dmitry Dokuchaev, whose mugshot was not of high-enough quality to republish.)

FBI

The four hackers used "a variety of techniques" to amass their stash of hacked accounts, FBI Assistant Director Paul Abbate said. Those techniques included spear-phishing , registering thousands of fake emails to fool users and downloading malware on Yahoo's network.

The hackers are said to have covered up their tracks by leasing servers in the US and creating fake authentication cookies to gain access. Yahoo's network had been breached in early 2014, after Belan allegedly stole a backup copy of Yahoo's user database and accessed its account management tools.

Yahoo earlier had described the 2014 breach as a "state-sponsored" attack, but didn't specify from what country . While financial data and clear-text passwords were safe, information stolen in the breach included names, email addresses, phone numbers, birth dates, encrypted passwords and, in some cases, security questions and answers.

"The indictment unequivocally shows the attacks on Yahoo were state-sponsored," Chris Madsen, Yahoo's head of security and safety said in a blog post. "We are deeply grateful to the FBI for investigating these crimes and the DOJ for bringing charges against those responsible."

Yahoo told lawmakers in a letter on Feb. 23 that the company was working with US and foreign governments to help find the hackers responsible for the 2014 attack *[Rebuild]*. The company also hired forensic firms Stroz Friedberg and Mandiant to investigate both breaches. *[Rebuild]*

The controversy surrounding Yahoo's hacks also cost the company $350 million in its pending sale to Verizon *[Anger]* . The telecommunications giant had plans to buy Yahoo's core internet business — assets including Yahoo Mail and Yahoo Finance — for $4.83 billion, but dropped the price to $4.48 billion in February. *[Anger]*

Verizon didn't respond to requests for comments.

As part of the reorganized deal, Verizon agreed to share the legal and regulatory burdens from the hacks, but Yahoo will have to handle any shareholder lawsuits on its own. Yahoo will also pay half for any non-Securities and Exchange Commission investigations and lawsuits related to the hacks.

The company is currently under investigation by the SEC for taking too long to report its 2013 and 2014 hacks to investors . *[Legal Action]*

Sen. Mark Warner, vice chairman of the Senate Committee on Intelligence, said he still believes Yahoo should have been more forthcoming about the breaches sooner. *[Disappointment]*

“Today’s indictments shed a light on the close and mutually beneficial tires between the cyber underworld and Russia’s government and security services,” Warner said in an emailed statement.

First published March 15 at 8:42 a.m. PT.

Updated at 9:05 a.m. PT: To add comments from Yahoo, at 11:30 a.m. PT: to include alleged hackers’ photos and at 12:55 p.m. PT: To add comments from Sen. Mark Warner.

Life, disrupted : In Europe, millions of refugees are still searching for a safe place to settle. Tech should be part of the solution. But is it?

Technically Incorrect : Bringing you a fresh and irreverent take on tech.