Yahoo breach spotlights links between Russian spies, hackers

March 16 2017, by Howard Amos

Acting Assistant Attorney General Mary McCord, center, accompanied by U.S. Attorney for the Northern District Brian Stretch, left, and FBI Executive Director Paul Abbate, speaks during a news conference at the Justice Department in Washington, Wednesday, March 15, 2017. The Justice Department announced charges against four defendants, including two officers of Russian security services, for a mega data breach at Yahoo. (AP Photo/Susan Walsh)

A U.S. indictment of two Russian intelligence agents and two hackers

alleged to have stolen more than half a billion U.S. email accounts in 2014 has cast a spotlight on the intertwining of the Russian security services and the murky digital underworld.

The officers of the powerful FSB, Russia's Federal Security Service, are accused of employing cybercriminals to access Yahoo's systems and steal data on millions of ordinary users as well as U.S. and Russian officials, Russian journalists and executives at large companies.

Interviews with security experts, hackers and people close to the Russian cybercriminal world suggest that the FSB's ties to cybercrime date back years and are mediated through a web of intermediaries and lubricated by blackmail and cash.

"There has been a lot of piggy-backing by the Russian state on the activities of Russian organized cybercriminal groups and scooping up the fruits of their activities," said Nigel Inkster, director of Future Conflict and Cyber Security at the International Institute for Strategic Studies in London and a former British intelligence officer.

"The FSB know where these guys are and they know where they can find them," he said.

According to the indictment, FSB agents Igor Sushchin and Dmitry Dokuchaev ran two hackers during the Yahoo operation and paid them. The hackers were Aleksei Belan, a Russian national, and Karim Baratov, a Kazakh who lives in Canada. Belan also is alleged to have simultaneously used the data to run a spamming network to look for financial information for personal profit.

This Jan. 14, 2015, file photo shows a sign outside Yahoo's headquarters in Sunnyvale, Calif. In an indictment Wednesday, March 15, 2017, announcing charges against four Russians, U.S. officials describe how Russian hackers working with Russian intelligence officials broke into Yahoo's network, stole information on Yahoo user accounts and ultimately gained entry into other services used by individuals they were targeting. (AP Photo/Marcio Jose Sanchez, File)

Dokuchaev, a 33-year-old major in the FSB's Information Security Center, was arrested in December as part of a treason case, Russian media have reported. The U.S. Justice Department would not confirm that account.

In 2011, Dokuchaev was identified by the pseudonym "Forb" in the Russian-language magazine Hacker. In a 2004 interview with the Russian newspaper Vedomosti, Forb boasted of making money from credit-card fraud and breaking into U.S. government websites. Little is

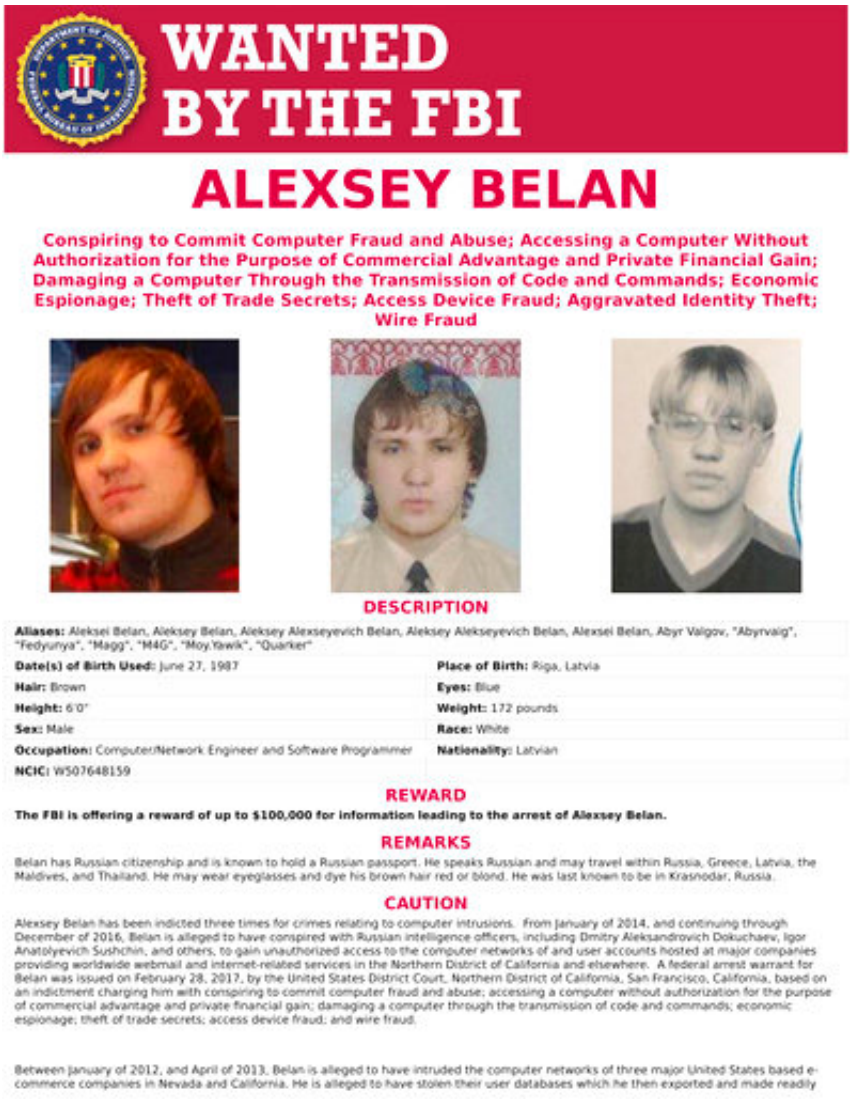
known about the nature of the treason charge.

In announcing the indictment that included Dokuchaev and Sushchin, Acting Assistant Attorney General Mary McCord noted that their department was "the FBI's point of contact in Moscow for cybercrime matters."

"The involvement and direction of FSB officers with law enforcement responsibilities makes this conduct that much more egregious," she said.

President Vladimir Putin's spokesman Dmitry Peskov said the Kremlin learned about the indictments from the media and hasn't received any official information. He also reaffirmed Russia's denial of any official involvement in hacking.

"We have repeatedly said that there absolutely can't be any talk about any Russian agency's official involvement, including the FSB, in any illegal actions in cyberspace," he said.



WANTED
BY THE FBI

ALEXSEY BELAN

Conspiring to Commit Computer Fraud and Abuse; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging a Computer Through the Transmission of Code and Commands; Economic Espionage; Theft of Trade Secrets; Access Device Fraud; Aggravated Identity Theft; Wire Fraud

DESCRIPTION

Aliases: Aleksei Belan, Aleksey Belan, Aleksey Alexseyevich Belan, Aleksey Alekseyevich Belan, Alexsei Belan, Abyr Valgov, "Abyrvalg", "Fedyunya", "Magg", "M4G", "Moy.Yawik", "Quarker"

Date(s) of Birth Used: June 27, 1987	**Place of Birth:** Riga, Latvia
Hair: Brown	**Eyes:** Blue
Height: 6'0"	**Weight:** 172 pounds
Sex: Male	**Race:** White
Occupation: Computer/Network Engineer and Software Programmer	**Nationality:** Latvian
NCIC: W507648159	

REWARD

The FBI is offering a reward of up to $100,000 for information leading to the arrest of Alexsey Belan.

REMARKS

Belan has Russian citizenship and is known to hold a Russian passport. He speaks Russian and may travel within Russia, Greece, Latvia, the Maldives, and Thailand. He may wear eyeglasses and dye his brown hair red or blond. He was last known to be in Krasnodar, Russia.

CAUTION

Alexsey Belan has been indicted three times for crimes relating to computer intrusions. From January of 2014, and continuing through December of 2016, Belan is alleged to have conspired with Russian intelligence officers, including Dmitry Aleksandrovich Dokuchaev, Igor Anatolyevich Sushchin, and others, to gain unauthorized access to the computer networks of and user accounts hosted at major companies providing worldwide webmail and internet-related services in the Northern District of California and elsewhere. A federal arrest warrant for Belan was issued on February 28, 2017, by the United States District Court, Northern District of California, San Francisco, California, based on an indictment charging him with conspiring to commit computer fraud and abuse; accessing a computer without authorization for the purpose of commercial advantage and private financial gain; damaging a computer through the transmission of code and commands; economic espionage; theft of trade secrets; access device fraud; and wire fraud.

Between January of 2012, and April of 2013, Belan is alleged to have intruded the computer networks of three major United States based e-commerce companies in Nevada and California. He is alleged to have stolen their user databases which he then exported and made readily

This wanted poster provided by the FBI shows Alexsey Alexseyevich Belan, aka "Magg," 29, a Russian national and resident. The United States announced charges Wednesday, March 15, 2017, against two Russian intelligence officers and two hackers, including Belan, accusing them of a mega data breach at Yahoo that affected at least a half billion user accounts. (FBI via AP)

The FSB press service had no immediate comment on the indictment, and the agency did not reply to earlier faxed questions about its broader contacts with hackers.

Along with Dokuchaev, at least three other men reportedly were arrested in the treason case, including Col. Sergei Mikhailov, the deputy head of the FSB's Information Security Center. Although details are sparse, that case has highlighted apparent links between the FSB and cybercrime.

Russia has long been known for its dynamic cybercriminal underworld, which is fueled by high technical standards and the opportunity for significant financial rewards.

That makes it a fertile recruiting ground for the intelligence services.

"It's all about outsourcing," said Andrei Soldatov, an expert on the Russian security services and co-author of "Red Web," a book about Kremlin attempts to control the internet.

Soldatov pointed to the Russian military operations in Ukraine that used local proxies and private contractors, describing it as a tactic helpful to Kremlin officials "because it allows them to deny responsibility."

WANTED BY THE FBI

DMITRY ALEKSANDROVICH DOKUCHAEV

Conspiring to Commit Computer Fraud and Abuse; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging a Computer Through the Transmission of Code and Commands; Economic Espionage; Theft of Trade Secrets; Access Device Fraud; Aggravated Identity Theft; Wire Fraud

DESCRIPTION

Aliases: Dmitriy Aleksandrovich Dokuchayev, "Patrick Nag"

Date(s) of Birth Used: February 28, 1984 **Place of Birth:** Russia

Hair: Brown **Eyes:** Blue

Sex: Male **Race:** White

Occupation: Russian Federal Security Service (FSB) Officer **Nationality:** Russian

REMARKS

Dokuchaev is alleged to be an officer of the Russian FSB, assigned to FSB Center 18. He has Russian Citizenship and was last known to be in Moscow, Russia.

CAUTION

From at least January of 2014, continuing through December of 2016, Dmitry Aleksandrovich Dokuchaev is alleged to have conspired with, among others, known and unknown FSB officers, including Igor Sushchin, to protect, direct, facilitate, and pay criminal hackers, including Alexsey Belan. Dokuchaev and his conspirators allegedly agreed to, and did, gain unauthorized access to the computer networks of and user accounts hosted at major companies providing worldwide webmail and internet-related services in the Northern District of California and elsewhere.

A federal arrest warrant for warrant for Dmitry Aleksandrovich Dokuchaev was issued on February 28, 2017, by the United States District Court, Northern District of California, San Francisco, California. That warrant was based on an indictment charging him with conspiring to commit computer fraud and abuse; accessing a computer without authorization for the purpose of commercial advantage and private financial gain; damaging a computer through the transmission of code and commands; economic espionage; theft of trade secrets; access device fraud; aggravated identity theft; and wire fraud.

This wanted poster provided by the FBI shows Dmitry Aleksandrovich Dokuchaev, 33, a Russian national and resident. The United States announced charges Wednesday, March 15, 2017, against two Russian intelligence officers, including Dokuchaev, and two hackers, accusing them of a mega data breach at Yahoo that affected at least a half billion user accounts. (FBI via AP)

The most talented Russian hackers work for groups that carry out big financial heists, said Alexander Gostev, chief security expert at Kaspersky Lab, a cybersecurity firm. This community is run by about 20 kingpins who have technical skills but are more notable for their

management abilities and contact networks, he said.

"Any hacking group can be hired for an attack on whatever you want," Gostev said.

The FSB is the leading Russian intelligence agency engaged in cyber operations, but it competes with the military intelligence service, known as the GRU, and the Foreign Intelligence Service, or SVR, according to Mark Galeotti, an expert on the Russian security services and a senior researcher at the Institute of International Relations in Prague.

Rivalries between these groups mean they are constantly vying for the Kremlin's favor. "They are like a collection of cats wanting to bring the dead mouse to the master's kitchen," Galeotti said.

Outgoing U.S. President Barack Obama imposed sanctions in December on both the FSB and the GRU for their role in what U.S. intelligence services concluded was Russian interference in the 2016 election campaign.

The FSB is more aggressive than the military and foreign intelligence agencies, which run more traditional intelligence operations, according to Galeotti.

This wanted poster provided by the FBI shows Igor Anatolyevich Sushchin, 43, a Russian national and resident is seen. The United States announced charges Wednesday, March 15, 2017, against two Russian intelligence officers, including Sushchin, and two hackers, accusing them of a mega data breach at Yahoo that affected at least a half billion user accounts. (FBI via AP)

"The FSB are secret policemen who are used to operating with absolute impunity and they freely use heavy-handed tactics like blackmail," he said.

Russian programmer Dmitry Artimovich, who was convicted in 2013 of hacking offenses, said the FSB had made repeated attempts to recruit him.

The first time, he said, was via his cellmate when he was in prison awaiting trial. Artimovich said he refused the offer, preferring to spend time in prison.

"Why would I do it?" he said. "I served one and a half years. Now I am free and don't owe anyone anything. But if you agree to this, you can't go anywhere. You can't have any career growth. It's real dependency."

Since being released, Artimovich said he has been asked dozens of times to carry out hacking operations, offers he said are designed to tempt him to break the law and become vulnerable to FSB pressure. Artimovich shared screenshots of some of these proposals with The Associated Press, which were made via social networking sites.

Alexander Glazastikov, a member of a hacking group that blackmailed top Russian officials after stealing personal details, said earlier this year that the group, known as Humpty Dumpty, cooperated with the FSB. In exchange for protection, Humpty Dumpty handed the FSB compromising material from hacked email accounts.

FBI Special Agent in Charge Jack Bennett speaks about a Yahoo security breach during a news conference Wednesday, March 15, 2017, in San Francisco. Two Russian intelligence agents and two hackers have been charged in a devastating breach at Yahoo that affected at least a half billion user accounts, the Justice Department said Wednesday in bringing the first case of its kind against Russian government officials. (AP Photo/Eric Risberg)

Security analysts also highlight the case of Yevgeny Bogachyov, a Russian programmer with a $3 million FBI bounty on his head. He is thought to be behind one of the most successful viruses, Zeus, which siphoned off hundreds of millions of dollars from bank accounts worldwide. U.S. officials have said that Bogachyov lives a luxurious life in a southern Russian resort on the Black Sea.

Bogachyov is one of the kingpins in Russia's cyber community, according to Kaspersky Lab's Gostev. "He is clearly not a programmer,"

Gostev said.

Since he was named publicly in 2010, Bogachyov has been linked to intelligence-gathering operations targeting the security services of Turkey, Georgia and Ukraine. Many experts assume his talents have been utilized by Russian intelligence agencies.