

Page, Lisa C. (OGC) (FBI)

From: Page, Lisa C. (OGC) (FBI)
Sent: Monday, May 01, 2017 6:34 PM
To: Strzok, Peter P. (CD) (FBI)
Subject: RE: Yahoo hack background

Oh yes, got it. Yeah, I wouldnt sweat that.

----- Original message -----

From: "Strzok, Peter P. (CD) (FBI)" [redacted]
Date: 05/01/2017 6:12 PM (GMT-05:00)
To: "Page, Lisa C. (OGC) (FBI)" [redacted]
Subject: RE: Yahoo hack background

b6 -1
b7C -1
b7E -6

Everyone was trying to remember who they were, particularly Andy, I said Belan and Dokuchaev. [redacted] thought it was someone else, it wasn't clear to who the D directed the comment. All good I'm sure, if you didn't remark on it, NP.

From: Page, Lisa C. (OGC) (FBI)
Sent: Monday, May 01, 2017 6:07 PM
To: Strzok, Peter P. (CD) (FBI) [redacted]
Subject: RE: Yahoo hack background

b6 -1
b7C -1
b7E -6

Not following. Which names?

----- Original message -----
From: "Strzok, Peter P. (CD) (FBI)" [redacted]
Date: 05/01/2017 6:04 PM (GMT-05:00)
To: "Page, Lisa C. (OGC) (FBI)" [redacted]
Subject: FW: Yahoo hack background

b6 -1
b7C -1
b7E -6

Below makes me happy. What did you make of D's comment about the names, after he said "it doesn't matter," when he then said, "it matters to him." Hope that wasn't negative. I assume/hope he values the attention to detail and getting the facts right...

From: Strzok, Peter P. (CD) (FBI)
Sent: Monday, May 01, 2017 6:03 PM
To: [redacted] (CD) (FBI) [redacted]
Subject: RE: Yahoo hack background

b6 -1
b7C -1
b7E -6

No problem at all. What you saw, for better or worse (and I think most definitely for the better), is that the D, DD, and EAD are all bright men with attention to detail and impressive memories.

From: [redacted] (CD) (FBI)
Sent: Monday, May 01, 2017 6:01 PM
To: Strzok, Peter P. (CD) (FBI) [redacted]
Subject: RE: Yahoo hack background

b6 -1
b7C -1
b7E -6

I now owe you some type of beverage.

I told Jon this and wanted to pass to you as well. Thanks for giving us the opportunity to see how these briefings work, and how you've done them, before we had to go prime time ourselves.

----- Original message -----

From: "Strzok, Peter P. (CD) (FBI)" [redacted]
 Date: 05/01/2017 5:49 PM (GMT-05:00)
 To: "Rybicki, James E. (DO) (FBI)" [redacted] "Page, Lisa C. (OGC) (FBI)"
 [redacted]
 Cc: "Priestap, E. W. (CD) (FBI)" [redacted] "Moffa, Jonathan C. (CD) (FBI)"
 [redacted] (CYD) (FBI) [redacted]
 (CD) (FBI) [redacted]
 Subject: Yahoo hack background

b6 -1
b7C -1
b7E -6

Follow up to a Q at the 4:45 session. Below from DOJ website – a redacted indictment was released on 3/15
U.S. CHARGES RUSSIAN FSB OFFICERS AND THEIR CRIMINAL CONSPIRATORS FOR HACKING YAHOO AND MILLIONS OF EMAIL ACCOUNTS

FSB Officers Protected, Directed, Facilitated and Paid Criminal Hackers

A grand jury in the Northern District of California has indicted four defendants, including two officers of the Russian Federal Security Service (FSB), for computer hacking, economic espionage and other criminal offenses in connection with a conspiracy, beginning in January 2014, to access Yahoo's network and the contents of webmail accounts. The defendants are Dmitry Aleksandrovich Dokuchaev, 33, a Russian national and resident; Igor Anatolyevich Sushchin, 43, a Russian national and resident; Alexsey Alexseyevich Belan, aka "Magg," 29, a Russian national and resident; and Karim Baratov, aka "Kay," "Karim Taloverov" and "Karim Ake Ahmet Tokbergenov," 22, a Canadian national and a resident of Canada.

The defendants used unauthorized access to Yahoo's systems to steal information from about at least 500 million Yahoo accounts and then used some of that stolen information to obtain unauthorized access to the contents of accounts at Yahoo, Google and other webmail providers, including accounts of Russian journalists, U.S. and Russian government officials and private-sector employees of financial, transportation and other companies. One of the defendants also exploited his access to Yahoo's network for his personal financial gain, by searching Yahoo user communications for credit card and gift card account numbers, redirecting a subset of Yahoo search engine web traffic so he could make commissions and enabling the theft of the contacts of at least 30 million Yahoo accounts to facilitate a spam campaign.

The charges were announced by Attorney General Jeff Sessions of the U.S. Department of Justice, Director James Comey of the FBI, Acting Assistant Attorney General for National Security Mary McCord, U.S. Attorney Brian Stretch for the Northern District of California and Executive Assistant Director Paul Abbate of the FBI's Criminal, Cyber, Response and Services Branch.

"Cyber crime poses a significant threat to our nation's security and prosperity, and this is one of the largest

data breaches in history," said Attorney General Sessions. "But thanks to the tireless efforts of U.S. prosecutors and investigators, as well as our Canadian partners, today we have identified four individuals, including two Russian FSB officers, responsible for unauthorized access to millions of users' accounts. The United States will vigorously investigate and prosecute the people behind such attacks to the fullest extent of the law."

"Today we continue to pierce the veil of anonymity surrounding cyber crimes," said Director Comey. "We are shrinking the world to ensure that cyber criminals think twice before targeting U.S. persons and interests."

"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," said Acting Assistant Attorney General McCord. "Once again, the Department and the FBI have demonstrated that hackers around the world can and will be exposed and held accountable. State actors may be using common criminals to access the data they want, but the indictment shows that our companies do not have to stand alone against this threat. We commend Yahoo and Google for their sustained and invaluable cooperation in the investigation aimed at obtaining justice for, and protecting the privacy of their users."

"This is a highly complicated investigation of a very complex threat. It underscores the value of early, proactive engagement and cooperation between the private sector and the government," said Executive Assistant Director Abbate. "The FBI will continue to work relentlessly with our private sector and international partners to identify those who conduct cyber-attacks against our citizens and our nation, expose them and hold them accountable under the law, no matter where they attempt to hide."

"Silicon Valley's computer infrastructure provides the means by which people around the world communicate with each other in their business and personal lives. The privacy and security of those communications must be governed by the rule of law, not by the whim of criminal hackers and those who employ them. People rightly expect that their communications through Silicon Valley internet providers will remain private, unless lawful authority provides otherwise. We will not tolerate unauthorized and illegal intrusions into the Silicon Valley computer infrastructure upon which both private citizens and the global economy rely," said U.S. Attorney Stretch. "Working closely with Yahoo and Google, Department of Justice lawyers and the FBI were able to identify and expose the hackers responsible for the conduct described today, without unduly intruding into the privacy of the accounts that were stolen. We commend Yahoo and Google for providing exemplary cooperation while zealously protecting their users' privacy."

Summary of Allegations

According to the allegations of the Indictment:

The FSB officer defendants, Dmitry Dokuchaev and Igor Sushchin, protected, directed, facilitated and paid criminal hackers to collect information through computer intrusions in the U.S. and elsewhere. In the present case, they worked with co-defendants Alexsey Belan and Karim Baratov to obtain access to the email accounts of thousands of individuals.

Belan had been publicly indicted in September 2012 and June 2013 and was named one of FBI's Cyber Most Wanted criminals in November 2013. An Interpol Red Notice seeking his immediate detention has been lodged (including with Russia) since July 26, 2013. Belan was arrested in a European country on a request.

from the U.S. in June 2013, but he was able to escape to Russia before he could be extradited.

Instead of acting on the U.S. government's Red Notice and detaining Belan after his return, Dokuchaev and Sushchin subsequently used him to gain unauthorized access to Yahoo's network. In or around November and December 2014, Belan stole a copy of at least a portion of Yahoo's User Database (UDB), a Yahoo trade secret that contained, among other data, subscriber information including users' names, recovery email accounts, phone numbers and certain information required to manually create, or "mint," account authentication web browser "cookies" for more than 500 million Yahoo accounts.

Belan also obtained unauthorized access on behalf of the FSB conspirators to Yahoo's Account Management Tool (AMT), which was a proprietary means by which Yahoo made and logged changes to user accounts. Belan, Dokuchaev and Sushchin then used the stolen UDB copy and AMT access to locate Yahoo email accounts of interest and to mint cookies for those accounts, enabling the co-conspirators to access at least 6,500 such accounts without authorization.

Some victim accounts were of predictable interest to the FSB, a foreign intelligence and law enforcement service, such as 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. However, other personal accounts belonged to employees of commercial entities, such as 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.

During the conspiracy, the FSB officers facilitated Belan's other criminal activities, by providing him with sensitive FSB law enforcement and intelligence information that would have helped him avoid detection by U.S. and other law enforcement agencies outside Russia, including information regarding FSB investigations of computer hacking and FSB techniques for identifying criminal hackers. Additionally, while working with his FSB conspirators to compromise Yahoo's network and its users, Belan used his access to steal financial information such as gift card and credit card numbers from webmail accounts; to gain access to more than 30 million accounts whose contacts were then stolen to facilitate a spam campaign; and to earn commissions from fraudulently redirecting a subset of Yahoo's search engine traffic.

When Dokuchaev and Sushchin learned that a target of interest had accounts at webmail providers other than Yahoo, including through information obtained as part of the Yahoo intrusion, they tasked their co-conspirator, Baratov, a resident of Canada, with obtaining unauthorized access to more than 80 accounts in exchange for commissions. On March 7, the Department of Justice submitted a provisional arrest warrant to Canadian law enforcement authorities, requesting Baratov's arrest. On March 14, Baratov was arrested in Canada and the matter is now pending with the Canadian authorities.

An indictment is merely an accusation, and a defendant is presumed innocent unless proven guilty in a court of law.

The FBI, led by the San Francisco Field Office, conducted the investigation that resulted in the charges announced today. The case is being prosecuted by the U.S. Department of Justice National Security Division's

Counterintelligence and Export Control Section and the U.S. Attorney's Office for the Northern District of California, with support from the Justice Department's Office of International Affairs.

Defendants: At all times relevant to the charges, the indictment alleges as follows:

- **Dmitry Aleksandrovich Dokuchaev**, 33, was an officer in the FSB Center for Information Security, aka "Center 18." Dokuchaev was a Russian national and resident.
- **Igor Anatolyevich Sushchin**, 43, was an FSB officer, a superior to Dokuchaev within the FSB, and a Russian national and resident. Sushchin was embedded as a purported employee and Head of Information Security at a Russian investment bank.
- **Alexsey Alexseyevich Belan**, aka "Magg," 29, was born in Latvia and is a Russian national and resident. U.S. Federal grand juries have indicted Belan twice before, in 2012 and 2013, for computer fraud and abuse, access device fraud and aggravated identity theft involving three U.S.-based e-commerce companies and the FBI placed Belan on its "Cyber Most Wanted" list. Belan is currently the subject of a pending "Red Notice" requesting that Interpol member nations (including Russia) arrest him pending extradition. Belan was also one of two criminal hackers named by President Barack Obama on Dec. 29, 2016, pursuant to Executive Order 13694, as a Specially Designated National subject to sanctions.
- **Karim Baratov**, aka "Kay," "Karim Taloverov" and "Karim Akehmet Tokbergenov," 22. He is a Canadian national and a resident of Canada.

Victims: Yahoo; more than 500 million Yahoo accounts for which account information about was stolen by the defendants; more than 30 million Yahoo accounts for which account contents were accessed without authorization to facilitate a spam campaign; and at least 18 additional users at other webmail providers whose accounts were accessed without authorization.

Time Period: As alleged in the indictment, the conspiracy began at least as early as 2014 and, even though the conspirators lost their access to Yahoo's networks in September 2016, they continued to utilize information stolen from the intrusion up to and including at least December 2016.

Crimes:

Count (s)	Defendant (s)	Charge	Statute U.S.C.	18	Conduct	Maximum Penalty
1.	All	Conspiring to commit computer fraud and abuse	§ 1030(b)		Defendants conspired to hack into the computers of Yahoo and accounts maintained by Yahoo, Google and other providers to steal information from them. First, Belan gained access to Yahoo's servers and stole information that allowed him, Dokuchaev, and Sushchin to gain unauthorized access to individual Yahoo user	10 years

accounts.

Then, Dokuchaev and Sushchin tasked Baratov with gaining access to individual user accounts at Google and other Providers (but not Yahoo) and paid Baratov for providing them with the account passwords. In some instances, Dokuchaev and Sushchin tasked Baratov with targeting accounts that they learned of through access to Yahoo's UDB and AMT (e.g., Gmail accounts that served as a Yahoo user's secondary account).

2	Dokuchaev Sushchin Belan	Conspiring to engage in economic espionage	§ 1831(a)(5)	<p>Starting on Nov. 4, 2014, Belan stole, and the defendants thereafter transferred, received and possessed the following Yahoo trade secrets:</p> <ul style="list-style-type: none"> • the Yahoo UDB, which was proprietary and confidential Yahoo technology and information, including subscriber names, secondary accounts, phone numbers, challenge questions and answers; • the AMT, Yahoo's interface to the UDB; and • Yahoo's cookie "minting" source code, which enabled the defendants to manufacture account cookies to then gain access to individual Yahoo user accounts. 	15 years
3	Dokuchaev Sushchin Belan	Conspiring to engage in theft of trade secrets	§ 1832(a)(5)	See Count 2	10 years
4-6	Dokuchaev Sushchin Belan	Economic espionage	§§ 1831(a)(1), (a)(4), and 2	See Count 2	15 years (each count)

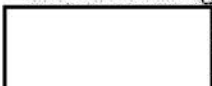
7-9	Dokuchaev Sushchin Belan	Theft of trade secrets	§§ 1832(a)(1), and 2	See Count 2	10 years (each count)
10	Dokuchaev Sushchin Belan	Conspiring to commit wire fraud	§ 1349	The defendants fraudulently schemed to gain unauthorized access to Yahoo's network through compromised Yahoo employee accounts and then used the Yahoo trade secrets to gain unauthorized access to valuable non-public information in individual Yahoo user accounts.	20 years
11-13	Dokuchaev Sushchin Belan	Accessing (or attempting to access) a computer without authorization to obtain information for the purpose of commercial advantage and private financial gain.	§§ 1030(a)(2)(C), 1030(c)(2)(B)(i)-(iii), and 2	The defendants gained unauthorized access to Yahoo's corporate network and obtained information regarding Yahoo's network architecture and the UDB.	5 years (each count)
14-17	Dokuchaev Sushchin Belan	Transmitting code with the intent to cause damage to computers.	§§ 1030(a)(5)(A), 1030(c)(4)(B), and 2	During the course of their unauthorized access to Yahoo's network, the defendants transmitted code on Yahoo's network in order to maintain a persistent presence, to redirect Yahoo search engine users and to mint cookies for individual Yahoo accounts.	10 years (each count)
18-24	Dokuchaev Sushchin Belan	Accessing (or attempting to access) a computer without authorization to obtain information for the	§§ 1030(a)(2)(C), 1030(c)(2)(B)(i)-(iii), and 2	Defendants obtained unauthorized access to individual Yahoo user accounts.	5 years (each count)

purpose or commercial advantage and private financial gain.

25-36	Dokuchaev Sushchin Belan	Counterfeit access device fraud	§§ 1029(a)(1), 1029 (b)(1), and 2	Defendants used minted cookies to gain unauthorized access to individual Yahoo user accounts.	10 years (each count)
37	Dokuchaev Sushchin Belan	Counterfeit access device making equipment	§§ 1029(a)(4)	Defendants used software to mint cookies for unauthorized access to individual Yahoo user accounts.	15 years
38	Dokuchaev Sushchin Baratov	Conspiring to commit access device fraud	§§ 1029(b)(2)	Defendants Dokuchaev and Sushchin tasked Baratov with gaining unauthorized access to individual user accounts at Google and other Providers and then paid Baratov for providing them with the account passwords. In some instances, Dokuchaev and Sushchin tasked Baratov with targeting accounts that they learned of through access to Yahoo's UDB and AMT (e.g., Gmail accounts that served as a Yahoo user's secondary account).	7 ½ years.
39	Dokuchaev Sushchin Baratov	Conspiring to commit wire fraud	§ 1349	See Count 38	20 years
40-47	Dokuchaev Baratov	Aggravated identity theft	§ 1028A(a)(1)	See Count 38	2 years

The language of this release was updated to reflect the current citizenship of Karim Baratov.

Peter P. Strzok II
Deputy Assistant Director, Branch I
Counterintelligence Division

 (O)
(C)

b6 -1
b7C -1