WORLD

Another Russian Hacker Claims He's The One Who Hacked The DNC

Konstantin Kozlovskiy's purported confession in a Russian court has triggered skepticism among experts.

Posted on December 14, 2017, at 6:32 p.m.


Jane Lytvynenko
BuzzFeed News Reporter


Kevin Collier
BuzzFeed News Cybersecurity Correspondent

Facebook Screenshot

A Russian hacker issued a stunning confession in a Moscow courtroom earlier this year claiming that he hacked the Democratic National Committee on orders from the FSB, according to a courtroom recording that's been posted on Facebook. But as cybersecurity experts try to parse the supposed confession — and why it's only coming to light now — some are casting doubt on the hacker's assertion.

The hacker's name is Konstantin Kozlovskiy. He is on trial alongside 50 other people for allegedly creating a virus called "Lurk" that targeted banking systems and allegedly stole 1.7 billion rubles (USD $28.7 million) from Russian banks. The hackers were caught in May 2016 after a joint investigation by the cybersecurity firm Kaspersky Lab, Russia's Ministry of Internal Affairs, and the Federal Security Bureau or FSB, one of the successor agencies to the Soviet-era KGB intelligence service. Kozlovskiy is considered one of the leaders of the hacking group and faces 12 to 20 years in prison if found guilty of cybercrime and organizing a criminal group.

News reports at the time made no suggestion that Kozlovskiy worked for the FSB. Kozlovskiy exercised his right against self-incrimination and did not testify in the case, though he told the court that he was aware the authorities had been monitoring his actions for some time. The operation itself was massive. Authorities arrested people from 15 different regions of the country in an investigation that began in 2012, four years before the 50 arrests were

Share Share

Kozlovskiy came back into the spotlight with a report by the Bell, an independent Russian media organization run by a former editor-in-chief of Forbes Russia. The report cited a previously unnoticed Facebook page seemingly belonging to Kozlovskiy that included legitimate-looking official documents, a handwritten letter, and a post addressed directly to Special Counsel Robert Mueller, the former FBI director who is now investigating Russian meddling in last year's US presidential election.

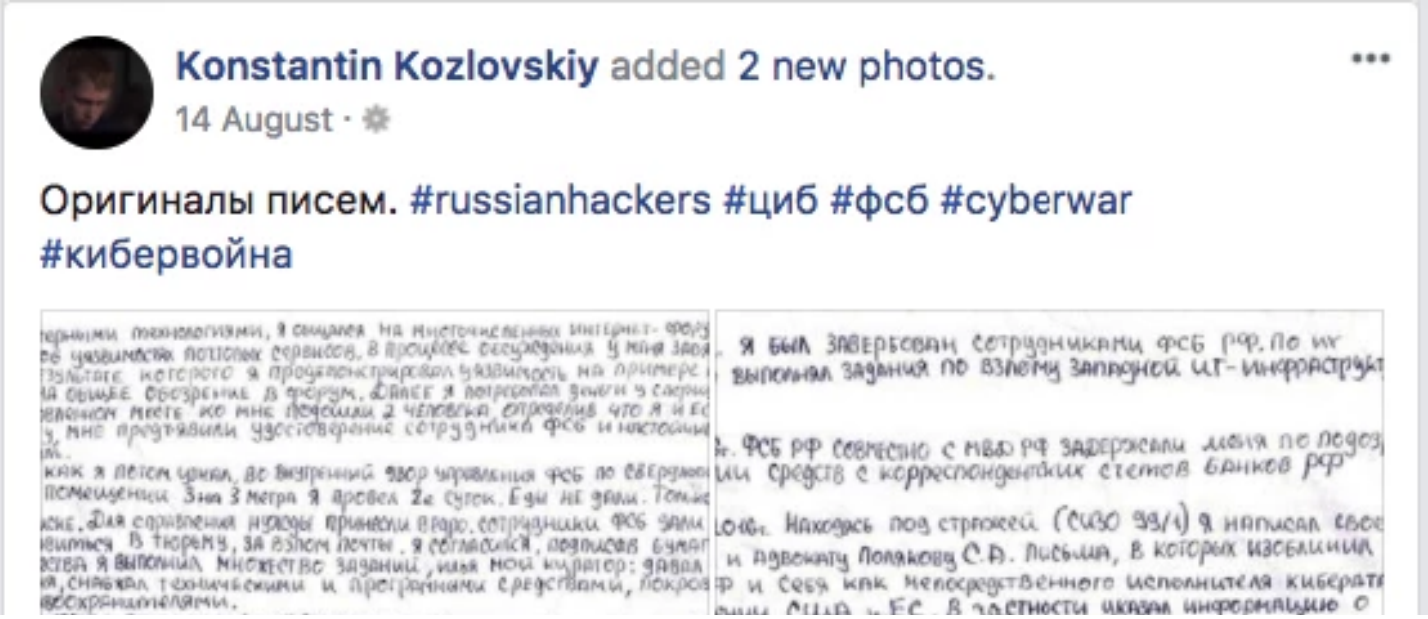
In the court recording posted on the page, purportedly from an Aug. 15 hearing, Kozlovskiy claims that he hacked into the DNC servers at the direction of the FSB. "If I'm guilty of anything, I'm guilty of working for this government," he said.

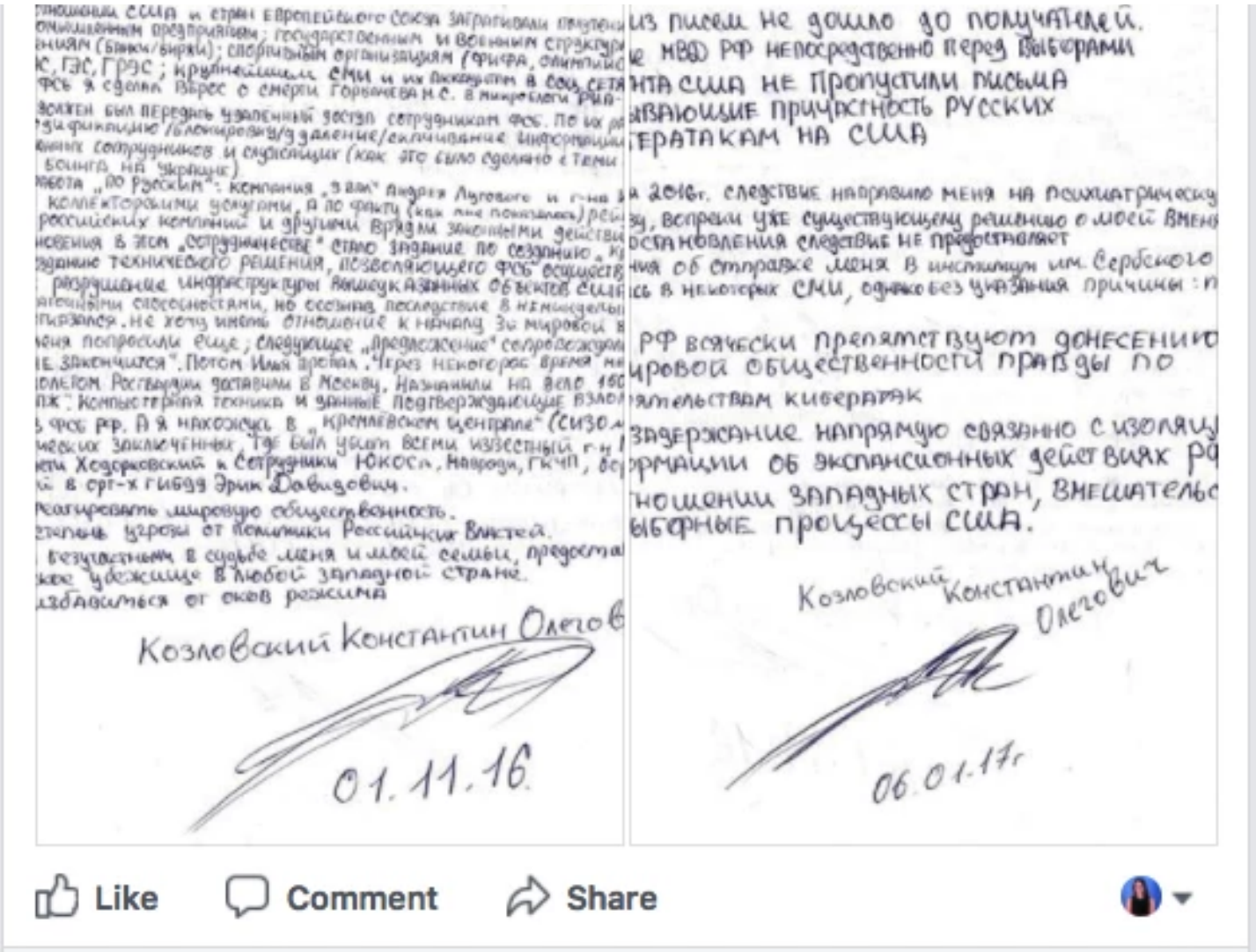
The Bell quoted two sources as confirming the authenticity of the Facebook page and the documents posted there, though BuzzFeed News couldn't independently verify that the page belongs to Kozlovskiy. Kozlovskiy's wife, Anya, told BuzzFeed News only that the page is run by a "trusted person." Kozlovskiy's lawyer declined to comment.

But other Russian sources have pointed out oddities about the page and the confession. In a report for the independent news outlet Novaya Gazeta, special correspondent Irek Murtazin wondered how Kozlovskiy's Facebook page could have gone unnoticed by reporters for months. Murtazin said he routinely monitors social media for the hashtags and topics that appear on the page, but he didn't see any of the posts.

It's not clear how the posts could have remained hidden from the public. There's no indication they were backdated, but most have the custom audience setting turned on. Facebook doesn't specify which demographics are excluded from seeing a post with a custom audience setting, but that could be one possible explanation for their going unnoticed.

Kozlovskiy also confessed to hacking Democratic emails in a handwritten letter posted on the page and dated Nov. 1, 2016. The letter was translated into English in a subsequent post. "I have successfully completed the task to hack the Democratic National Committee and personal correspondence of Hilary [*sic*] Clinton," the translation says. "I gave the result to Ilia, Federal Security Service of Russian Federation officer (approximately 850Gb of archived video of the process)."




Козловский Константин Олегович
01.11.16.
Козловский Константин Олегович
06.01.17г
Like Comment Share

Facebook: permalink.php

It's not clear which DNC hack Kozlovskiy was referring to. The cybersecurity firm CrowdStrike, which the Democratic Party hired to investigate the intrusions, found that DNC servers were hacked by two separate Russian entities, the first some time prior to September 2015 and then again in April 2016. Kozlovskiy was taken into custody on May 18, 2016, which means it's possible that he could have been involved with either. But his reference to hacking Clinton's correspondence adds to the mystery: Clinton's email is not known to have been hacked, though some of her messages were captured when presumed Russian hackers pirated the email of her campaign chairman, John Podesta.

Murtazin also questioned how the documents ended up on Facebook at a time when Kozlovskiy was in FSB custody on the hacking charges. In an interview, Murtazin told BuzzFeed News that he believes there could be ulterior motives to Kozlovskiy's confession, including a possibility he's working with the FSB.

In the letter, Kozlovskiy also details how he came to work for the FSB, saying the FSB threatened to prosecute him in 2008 for hacking unless he agreed to work for it—a common Russian government recruiting technique.

Kozlovskiy identifies his FSB handler as Maj. Dmitry Dokuchaev and says Dokuchaev ordered him to hack American and EU officials, government and military organizations, financial institutions, sports organizations, major media outlets, and their social media accounts. In it, he also claims responsibility for hacking the Twitter account of

Russia's RIA news agency in 2013 and falsely announcing Gorbachev's death. Russian authorities arrested Dokuchaev last December and charged him with treason.

In subsequent posts, Kozlovskiy also implicated Ruslan Stoyanov, formerly a top investigator at Russia's Kaspersky Lab. A post on the Facebook page says Kozlovskiy hacked computer servers in Germany, France, and Great Britain on FSB's orders. Like Dokuchaev, Stoyanov was also arrested on treason charges.

"The investigation is for a period predating his employment at Kaspersky Lab and we do not possess details of the investigation," a Kaspersky Lab spokesperson told BuzzFeed News.

FSB Col. Sergey Mikhailov and tech entrepreneur Georgy Fomchenkov were also part of those arrests, which were marked as secret by the court.

The Bell previously reported the men are suspected of leaking information to the US about the hacking attacks. As the former head of FSB's Information Security Center, it's Mikhailov who's suspected of being in charge.

That gives rise to another theory about the Facebook page: that it's part of a complicated FSB plot to bolster the idea that the DNC hacks were really the work of Mikhailov acting on instructions from the United States. In his Novaya Gazeta article, Murtazin writes that Kozlovskiy's "confession" could be an FSB "operational game."

Shaun Walker
@shaunwalker7

Novaya Gazeta suggests the hacker who said he hacked the DNC for the FSB could be leaking as part of an FSB plot to suggest US intelligence ordered a US agent inside the FSB to hack the DNC novayagazeta.ru/articles/2017/… Does your head hurt yet?

10:16 AM - Dec 12, 2017

Троянский червь сомнений

Константин Козловский, фото с «личной страницы» в фейсбуке Год спустя после возбуждения уголовного дела о

novayagazeta.ru

The credibility of the confession is also called into question by a post Kozlovskiy addressed to Mueller. In it, the hacker claims the FSB has created an astoundingly powerful hacking tool, one that makes it possible to distort what users see on their screens, no matter which device — phone, laptop, desktop, or tablet — a person might be using.

"It just doesn't make technical sense," said Ben Read, the manager of cyberespionage analysis at the cybersecurity firm FireEye. "You have some people using Internet Explorer, some people using Chrome. It would need a lot of capabilities to do this across all of the websites you use. Are you using Tweetdeck? Are you on Facebook, Google News? There are so many avenues that it becomes prohibitive to do at the scale being described."

Read also said it's impossible to believe that such malware would have escaped the notice of cyber sleuths in the highly competitive cybersecurity industry.

Raphael Satter @razhael 11 Dec
Replying to @razhael
Back in July we examined several of those cases, obtaining or reviewing court documents from Spain, Czechia, US and Russia: apnews.com/8b1b362ec75649…

Raphael Satter
@razhael

Several defendants had made claims that they were mixed up in the DNC hack. Take alleged spam lord Pyotr Levashov. His arrest made headlines when his wife told Russian media his arrest was linked to Trump's win. But when we finally spoke to her months later, she backpedaled: pic.twitter.com/oZwfKkRRzJ
6:33 PM - Dec 11, 2017

When Levashov was finally caught, his wife Maria drew international attention when she was quoted as saying the arrest was "linked to Trump's win." But in a conversation with The Associated Press in Madrid on Wednesday, she pulled back from those comments.

"I think there are some political reasons in this case, but I'm not sure," she said. "I don't have any evidence."

Levashov's lawyer, Margarita Repina, offered a similar qualification to her assertion that U.S. officials were "just taking hackers with any excuse to see if any of them admits involvement in the Trump issue."

"This is just an opinion," she said. "We have no evidence."

Kozlovskiy's claim of involvement with the DNC hack isn't the first "confession" by a Russian hacker. An AP reporter in Moscow, Raphael Satter, noted in a Twitter thread that several other defendants have claimed a role in the attacks.

CORRECTION

December 15, 2017, at 12:57 p.m.

Dmitry Dokuchaev's name was misspelled in an earlier version of this post.

Jane Lytvynenko is a reporter for BuzzFeed News and is based in Toronto, Canada. PGP fingerprint: A088 89E6 2500 AD3C 8081 BAFB 23BA 21F3 81E0 101C.
Contact Jane Lytvynenko at jane.lytvynenko@buzzfeed.com.

Kevin Collier is a cybersecurity correspondent for BuzzFeed News and is based in New York.
Contact Kevin Collier at kevin.collier@buzzfeed.com.

Got a confidential tip? Submit it here.