Hack Brief: Russian Hackers Release Apparent IOC Emails in Wake of Olympics Ban

wired.com/story/russian-fancy-bears-hackers-release-apparent-ioc-emails/

Louise Matsakis January 10, 2018

On Wednesday, in the wake of Russia's December ban from the 2018 Winter Olympics, a Russia-linked group calling itself "Fancy Bears" published a set of apparently stolen emails. They purportedly belong to officials from the International Olympic Committee, the United States Olympic Committee, and third-party groups associated with the organizations. It's not the first time Russia has lashed out at the IOC and the anti-doping agencies in the last few years. And with a month left until the games begin, it may not be the last.

The Hack

The emails appear to span from the end of 2016 to the spring of 2017, and focus on correspondence between antidoping investigators who helped uncover a wide-scale, systematic doping scheme carried out by Russian athletes. It's not clear yet whether the emails are entirely authentic; Russian hacking groups have snuck false information into their leaks before. But the World Anti-Doping Agency Wednesday indirectly acknowledged that the emails were real, but not current.

"The Fancy Bears are a criminal organization which seeks to undermine the work of WADA and its partners," says WADA spokesperson Maggie Durand. "Everything that they have posted today is dated."

The hack appears to be retaliation for kicking the Russia out of 2018 PyeongChang games, at which only a handful of the country's athletes will be allowed to compete.

Fancy Bears—assumed to be the same hacking group known previously as Fancy Bear—has been linked to Russia's primary intelligence agency, the Main Intelligence Directorate (abbreviated GRU) by American intelligence officials. On its official website, the hackers portrayed the stolen emails as evidence that "the Europeans and the Anglo-Saxons are fighting for power and cash in the sports world." In other words, this hack looks like an attempt revive Russian claims that Westerners are attempting to disenfranchise the country by exposing its systemic cheating.

Who's Affected?

It's not clear whose email account Fancy Bears may have breached, nor how many accounts were affected. In the past, the group has often relied on phishing schemes to infiltrate targeted email accounts.

Fancy Bears has shown particular interest in discrediting Richard McLaren, a Canadian lawyer and professor who spent over a year investigating Russia's widespread cheating techniques. McLaren's findings provided the basis for banning Russia from the games, though his reports did not explicitly recommend Russia's removal.

In one message obtained by Fancy Bears and reviewed by *The New York Times*, IOC lawyer Howard Stupp complained that the WADA published McLaren's investigations about Russian doping without having discussed them with sports officials first. McLaren did not immediately return a request for comment.

Fancy Bears also singles out Richard Young, a Colorado lawyer who worked on McLaren's team. Young tells WIRED he hasn't yet authenticated the emails, because they are still being reviewed by his law firm's IT department. He says that from what he had heard about them, it was possible that they were legitimate. The IOC also did not immediately respond a request for comment.

How Serious Is This?

WIRED hasn't reviewed the entire contents of the emails, but upon first glance many appear to be routine logistical communications, despite Fancy Bears' efforts to sensationalize the correspondence. This isn't the first time the hacking group has tried to stir up controversy about the Olympics. In 2016, after the Summer Games in Rio de Janeiro, Fancy Bear published stolen medical records belonging to mostly British and American athletes on the same website it published this new hack.

Back then, the group attempted to discredit prominent competitors like gymnast Simone Biles for having taken banned medications. But Biles and others had received special permission to take the contraband drugs to treat legitimate medical conditions. None of the

athletes had actually committed a violation.

The hack also serves as a reminder that Russian hackers remain seemingly as active as ever. Security researchers believe Fancy Bear was one of two Russian hacking teams to break into to Democratic National Committee's files in 2016. It's also believed to be behind other prominent hacks, both in the US and abroad.

So far, Fancy Bears obtained a small number of emails from individuals associated with the Olympics, though it's possible the group chose to publish only a handful of what it had obtained. A Twitter message sent to Fancy Bears went unanswered.

Overall, Russia's latest attempt to save face on the international sports stage is far from convincing. Unlike the DNC hack, which helped to sway the US presidential election, it doesn't appear these emails will change the IOC's decision to ban the country.