

# UK, US, Canada accuse Russia of hacking virus vaccine trials

July 16 2020, by Jill Lawless and Danica Kirka

---



In this March 16, 2020 file photo, a subject receives a shot in the first-stage safety study clinical trial of a potential vaccine by Moderna for COVID-19, the disease caused by the new coronavirus, at the Kaiser Permanente Washington Health Research Institute in Seattle. Britain, the United States and Canada accused Russia on Thursday July 16, 2020, of trying to steal information from researchers seeking a COVID-19 vaccine. (AP Photo/Ted S. Warren, File)

Britain, the United States and Canada accused Russia on Thursday of trying to steal information from researchers seeking a COVID-19 vaccine.

The three nations alleged that hacking group APT29, also known as Cozy Bear and said to be part of the Russian intelligence service, is attacking academic and pharmaceutical research institutions involved in coronavirus vaccine development.

Britain's National Cybersecurity Centre made the announcement, which was coordinated with authorities in the U.S. and Canada.

"It is completely unacceptable that the Russian Intelligence Services are targeting those working to combat the coronavirus pandemic," British Foreign Secretary Dominic Raab said in a statement. "While others pursue their selfish interests with reckless behaviour, the U.K. and its allies are getting on with the hard work of finding a vaccine and protecting global health."

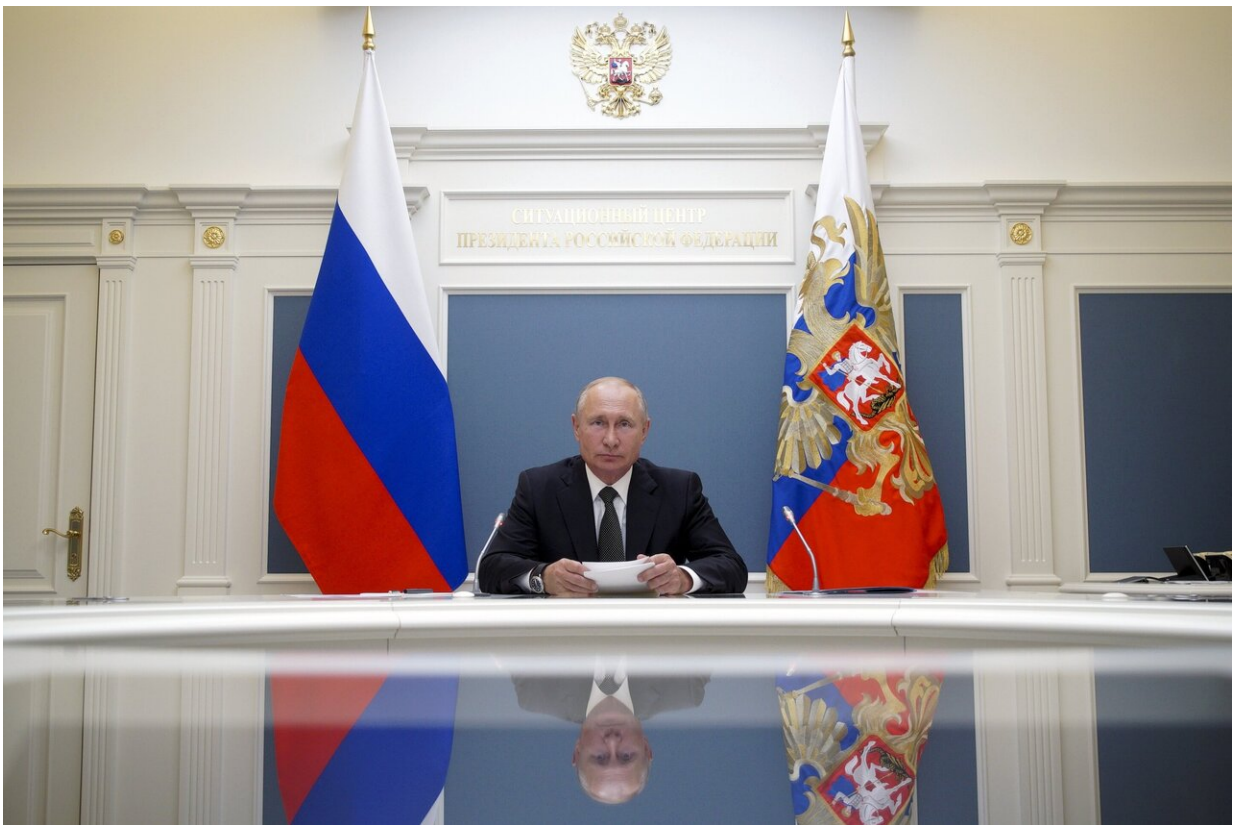
The persistent and ongoing attacks are seen by [intelligence officials](#) as an effort to steal intellectual property, rather than to disrupt research. The campaign of "malicious activity" is ongoing and includes attacks "predominantly against government, diplomatic, think-tank, healthcare and energy targets," the National Cybersecurity Centre said in a statement.

It was unclear whether any information actually was stolen but the center says individuals' confidential information is not believed to have been compromised. The Russian Foreign Ministry did not immediately respond to a request for comment.

Cozy Bear, also known as the "dukes," has been identified by Washington as one of two Russian government-linked hacking groups

that broke into the Democratic National Committee computer network and stole emails ahead of the 2016 presidential election. The other group is usually called Fancy Bear.

The director of operations for the British cybersecurity center, Paul Chichester, urged "organizations to familiarize themselves with the advice we have published to help defend their networks."



Russian President Vladimir Putin attends a video call with Defense Minister Sergei Shoigu in Moscow, Russia, Tuesday, June 30, 2020. Shoigu reported to Putin that the Defense Ministry plans to complete clinical tests of a coronavirus vaccine next month. (Alexei Druzhinin, Sputnik, Kremlin Pool Photo via AP)

The statement did not say whether Russian President Vladimir Putin knew about the vaccine research hacking, but British officials believe such intelligence would be highly prized.

A 16-page advisory prepared by the U.S. National Security Agency and made public by Britain, the U.S. and Canada on Thursday accuses Cozy Bear of using custom malicious software to target a number of organizations globally. The malware, called WellMess and WellMail, has not previously been associated with the hacking group, the advisory said.

"In recent attacks targeting COVID-19 vaccine research and development, the group conducted basic vulnerability scanning against specific external IP addresses owned by the organizations. The group then deployed public exploits against the vulnerable services identified," the advisory said.

The U.S. Department of Homeland Security's cybersecurity agency warned in April that cybercriminals and other groups were targeting COVID-19 research, noting at the time that the increase in people teleworking because of the pandemic had created potential avenues for hackers to exploit.

Vulnerable targets include health care agencies, pharmaceutical companies, academia, medical research organizations, and local governments, security officials have said.

The global reach and international supply chains of these organizations also make them vulnerable, the U.S. Cybersecurity and Infrastructure Security Agency said in an alert published in conjunction with its counterparts in Britain.

CISA said it and the British cybersecurity agency have detected the threat groups scanning the external websites of targeted companies and looking

for vulnerabilities in unpatched software. It did not name any of the targeted companies.

U.S. authorities have for months leveled similar accusations against China. FBI Director Chris Wray said last week, "At this very moment, China is working to compromise American health care organizations, [pharmaceutical companies](#), and academic institutions conducting essential COVID-19 research."

© 2020 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed without permission.

Citation: UK, US, Canada accuse Russia of hacking virus vaccine trials (2020, July 16) retrieved 10 April 2024 from <https://techxplore.com/news/2020-07-uk-canada-accuse-russia-hacking.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--