Two Russian Nationals Working with Russia's Federal Security Service Charged with Global Computer Intrusion Campaign

Published: 2023-12-07 · Archived: 2026-04-05 13:50:47 UTC

A federal grand jury in San Francisco returned an indictment on Tuesday charging two individuals with a campaign to hack into computer networks in the United States, the United Kingdom, other North Atlantic Treaty Organization member countries and Ukraine, all on behalf of the Russian government.

According to court documents, Ruslan Aleksandrovich Peretyatko (Перетятько Руслан Александрович), an officer in Russia's Federal Security Service (FSB) Center 18, Andrey Stanislavovich Korinets (Коринец Андрей Станиславович) and other unindicted conspirators employed a sophisticated spear phishing campaign to gain unauthorized, persistent access (*i.e.*, "hack") into victims' computers and email accounts.

"The Russian government continues to target the critical networks of the United States and our partners, as highlighted by the indictment unsealed today," said Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division. "Through this malign influence activity directed at the democratic processes of the United Kingdom, Russia again demonstrates its commitment to using weaponized campaigns of cyber espionage against such networks in unacceptable ways. The Department of Justice will respond to such behavior with an even more determined commitment to disrupt those activities and to hold accountable the individuals responsible."

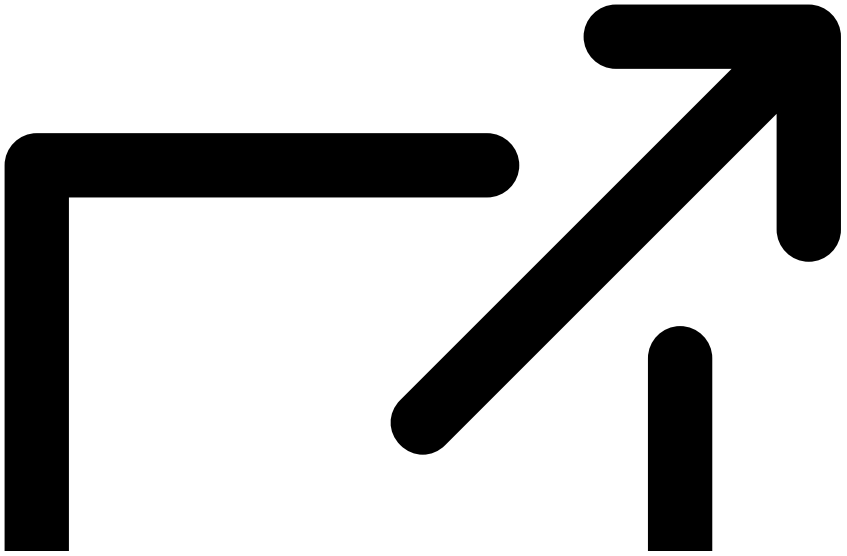
"Today's indictment is part of a coordinated international response to send a message to the conspirators that the whole of the United States government stands together and with our partners internationally to identify and disrupt cyber espionage actors, particularly those seeking to obtain government information and attempting to create chaos in democratic processes," said U.S. Attorney Ismail J. Ramsey for the Northern District of California. "We are grateful to all of our partners for their assistance in addressing these threats posed by the FSB's action in the Northern District of California, across the United States and around the world."

"The FBI will not stand idly by as Russia continues to perpetuate this type of targeted malicious activity," said Assistant Director Bryan Vorndran of the FBI's Cyber Division. "Russian interference through malign foreign influence campaigns is deplorable, and we will not tolerate it in the United States or directed against our foreign partners. The FBI is dedicated to combating this pervasive threat and will tirelessly seek to prevent and disrupt these criminal acts carried out by Russia."

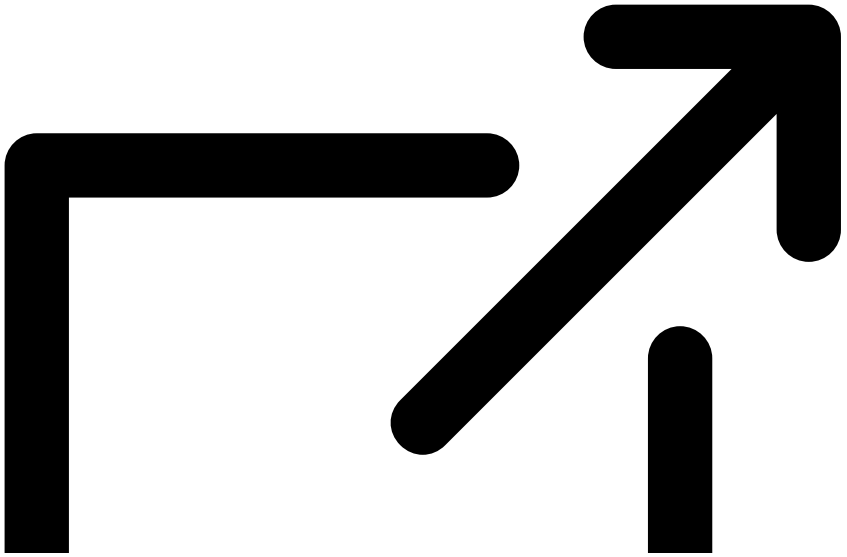
The indictment, which was unsealed today, alleges the conspiracy targeted current and former employees of the U.S. Intelligence Community, Department of Defense, Department of State, defense contractors, and Department of Energy facilities between at least October 2016 and October 2022. In addition, the indictment alleges the conspirators – known publicly by the name "Callisto Group" – targeted military and government officials, think tank researchers and staff, and journalists in the United Kingdom and elsewhere, and that information from certain of these targeted accounts was leaked to the press in Russia and the United Kingdom in advance of U.K. elections in 2019.

As a common example, the conspirators used “spoofed” email accounts designed to look like personal and work-related email accounts of the group’s targets. The conspirators allegedly also sent sophisticated looking emails that appeared to be from email providers suggesting users had violated terms of service. These messages were designed to trick victims into providing their email account credentials to false login prompts. Once the conspirators fraudulently obtained the victim’s credentials, they were able to use those credentials to access the victims’ email accounts at will.

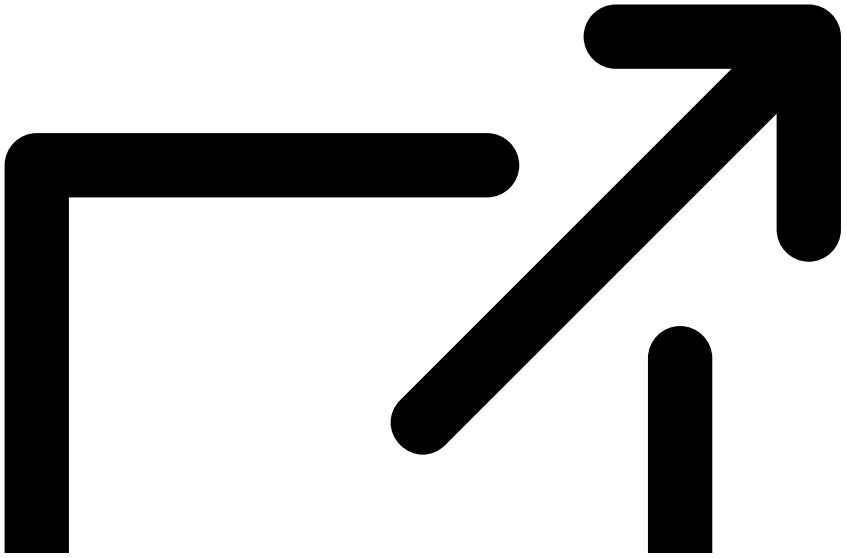
In addition to the indictment, the Department of the Treasury’s Office of Foreign Assets Control (OFAC)



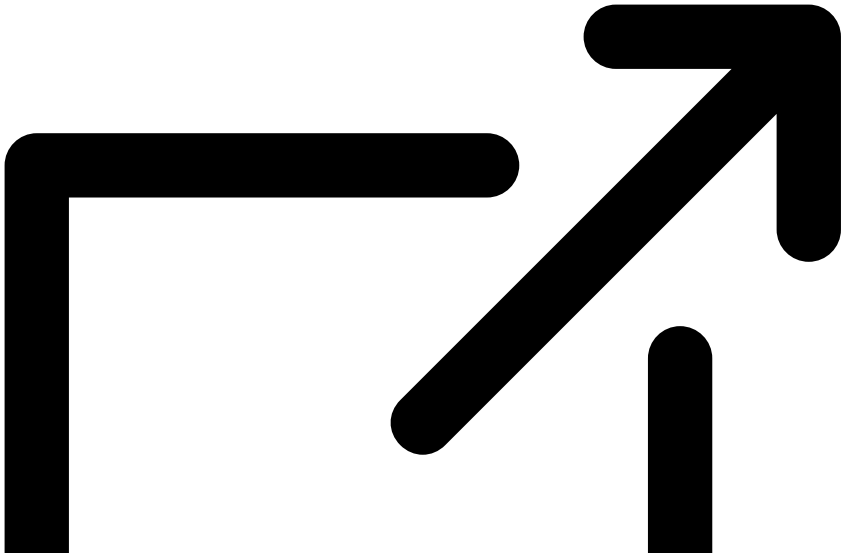
announced that it has sanctioned both Peretyatko and Korinets for their roles in malicious cyber-enabled activity. Moreover, the United Kingdom has issued sanctions



of its own, and the U.S. Department of State announced rewards of up to $10 million for information leading to the identification or location of Peretyatko



and Korinets



, as well as their conspirators.

In addition to the name “Callisto Group,” FSB Center 18 is known by cybersecurity investigators as “Dancing Salome” by Kaspersky Labs, “STAR BLIZZARD” by Microsoft Threat Intelligence Center and “COLDRIVER” by Google’s Threat Analysis Group.

The defendants are each charged with one count of conspiracy to commit an offense against the United States, namely, computer fraud, which carries a maximum sentence of five years in prison for PERETYATKO, and up to 10 years for KORINETS. The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only, as any sentencings of the defendants will be determined by the assigned judge.

The investigation was conducted jointly by the U.S. Attorney's Office for the Northern District of California, the National Security Cyber Section of the Justice Department's National Security Division and the FBI San Francisco Field Office. The FBI's Cyber Division, Cyber Assistant Legal Attachés, and Legal Attachés in countries around the world provided essential support. Numerous victims cooperated and provided valuable assistance in the investigation.

An indictment is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Note: *This release has been updated to reflect the correct criminal offense and statutory penalties.*
