6 Russian military officers charged in vast hacking campaign

Associated Press

The Justice Department announced charges Monday against Russian intelligence officers in cyberattacks that targeted a French presidential election, the Winter Olympics in South Korea and American businesses. The case implicates the same Kremlin unit that interfered in the 2016 U.S. elections, but is not related to the November vote.

© Andrew Harnik/AP Photo

A poster showing six wanted Russian military intelligence officers is displayed as Assistant Attorney General for the National Security Division John Demers, left, takes the podium to speak at a news conference at the Department of Justice on Oct. 19.

The indictment accuses the six defendants, all said to be current and former officers in the Russian military intelligence agency known as the GRU, of hacks that prosecutors say were aimed at furthering the Kremlin's geopolitical interests and in destabilizing or punishing perceived enemies.

All told, the attacks caused billions of dollars in losses and disrupted a broad cross-section of life, including health care in Pennsylvania, a power grid serving hundreds of thousands of customers in Ukraine and a French election that saw the late-stage disclosure of hacked emails.

The seven-count indictment is the most recent in a series of Justice Department prosecutions of Russian hackers, often working on behalf of the government.

Past cases have focused on attacks against targets like internet giant Yahoo and the 2016 presidential contest, when Russian hackers from the GRU stole Democratic emails that were released online in the weeks before the election.

The attacks in this case are "some of the most destructive, most costly, most egregious cyber attacks ever known," said Scott Brady, the U.S. Attorney for the Western District of Pennsylvania, where the 50-page indictment was filed.

"Time and again, Russia has made it clear: They will not abide by accepted norms, and instead, they intend to continue their destructive, destabilizing cyber behavior," said FBI Deputy Director David Bowdich.

The indictment does not charge the defendants in connection with interference in American elections, though the officers are part of the same intelligence unit that prosecutors say interfered in the 2016 U.S. election.

One of the six charged in the case announced Monday was among the Russian military intelligence officers charged with hacking in special counsel Robert Mueller's investigation into Russian election interference.

The timing of the indictment was unrelated to the upcoming election in the U.S., said Assistant Attorney General John Demers.

He said that despite ongoing warnings of Russian interference in the election, Americans "should be confident that a vote cast for their candidate will be counted for that candidate."

The hacking targets described in Monday's case are diverse, with the indictment fleshing out details about attacks that in some instances had already received significant attention because of the havoc they had caused.

The indictment accuses the officers, for instance, of hacking into the 2018 Winter Olympics in South Korea after Russia was punished by the International Olympic Committee for a vast doping conspiracy.

It also says the Tokyo 2020 Olympics were targeted. Those Olympics have been postponed until next year.

The Japanese government's chief Cabinet secretary Katsunobu Kato declined to comment on specifics. "We cannot overlook malicious cyberattacks that could shake the foundation of democracy," he said.

Tokyo 2020 in a statement said "no significant impact has been observed in our operations." It said it has been taking "countermeasures" but declined to disclose them.
Prosecutors say the hackers unleashed a devastating malicious software attack during the opening ceremony in February 2018 that deleted data from thousands of computers related to the event and left them inoperable. Russia then tried to pin blame on North Korea in what prosecutors say was a failed "false flag" attempt.

Another attack was aimed at disrupting the 2017 presidential election in France through hacks that targeted local government entities, campaigns and political parties, including the party of current President Emmanuel Macron.

The controversy known as the "Macron Leaks" involved the leak of over 20,000 emails linked to Macron's campaign in the days before his victory. The involvement of bots raised questions about the possible involvement of Vladimir Putin and the Russian government.

The leaks, which gained huge media attention in France, were shared by WikiLeaks and several alt-right activists on Twitter, Facebook and others.

Other attacks targeted international investigators looking into the suspected nerve agent poisoning of former Russian spy Sergei Skripal and his daughter in the United Kingdom, as well as the country of Georgia, where roughly 15,000 websites were defaced.

"In many cases," the indictment says, "the Conspirators replaced website home pages with an image of a former Georgian president, who was known for his efforts to counter Russian influence in Georgia, along with the caption, 'I'll be back.'"

Beyond that, though, the hacks had harmful impacts on quality-of-life for everyday citizens. The attacks in Ukraine, for instance, disrupted the power supply in the middle of winter for hundreds of thousands of customers, officials say.

And the global malware attack known as NotPetya that infected computers across the world harmed the operations of the Heritage Valley Heath System, which prosecutors say serves tens of thousands of people in western Pennsylvania.

Work stations were locked, hard drives encrypted, laboratory records and other files were inaccessible, and Heritage Valley temporarily lost access to critical computer systems related to medical care.

Robert Lee, a security researcher who helped uncover the malware used in one of the Ukraine hacks, said U.S. and European political leaders should have done more at the time to call out Russia and make clear that attacks on power grids are unacceptable.

But Lee, CEO of security firm Dragos, also welcomed the indictment as an important message before the U.S. presidential election about American officials' resolve to fight back against attacks on elections and civic infrastructure.
"This is a broad signal from U.S. intelligence to say, 'We're watching you and we're willing to burn our resources to burn your resources,'" Lee said. "Leading up to the election, I think that's an important signal to send."

© Provided by CBS News Russian intelligence operatives indicted by the U.S. for malware and hacking campaigns. Clockwise, from top left: Petr Nikolayevich Pliskin, Artem Valeryevich Ochichenko, Pavel Valeryevich Frolov, Yuriy Sergeyevich Andrienko, Sergey Vladimirovich Detistov and Anatoliy Sergeyevich Kovalev. / Credit: Justice Department / CBS News

The six defendants face charges including conspiracy to conduct computer fraud and abuse, wire fraud and aggravated identity theft. None is currently in custody, but the Justice Department in recent years has eagerly charged foreign hackers in absentia in countries including Russia, China and Iran with the goal of creating a message of deterrence.

“No country has weaponized its cyber capabilities as maliciously and irresponsibly as Russia, wantonly causing unprecedented collateral damage to pursue small tactical advantages as fits of spite," said Demers, the Justice Department's top national security official.