The New York Times

# U.S. Accuses Russian Military Hackers of Attack on Email Servers

Julian E. Barnes and David E. Sanger

May 28, 2020

WASHINGTON — The National Security Agency publicly accused Russian government hackers of targeting email servers around the world in an unusual announcement on Thursday, showing that the agency is becoming more aggressive in calling out Moscow's action as the presidential election approaches.

While the Trump administration has publicly attributed cyberattacks to Russia before — including for its 2016 election hack and for paralyzing Ukraine in 2017, which damaged the operations of the shippers Maersk and FedEx — this allegation was unusually specific. It singled out Russia's military intelligence unit, widely known as the G.R.U., demonstrating intelligence agencies' concern that Russia intends to interfere in the election only a little more than five months away.

But it also comes as President Trump has renewed his baseless claims that the investigation into Russia's activities was part of a "hoax" intended by Democrats to paralyze him. He has publicly questioned Russia's culpability in the election hacking and appeared to accept President Vladimir V. Putin's argument that Russia was so good at cyberoperations that it would never have been caught.

"There has been a reluctance to be critical of Russia because of echoes of investigations," said retired Gen. Martin E. Dempsey, the former chairman of the Joint Chiefs of Staff. "For the N.S.A. to do that, in this climate, they must have absolutely incontrovertible evidence."

The "Sandworm Team," a group of G.R.U. hackers, tried to use a vulnerability in computer networks to gain access to them, the National Security Agency said. It did not say which networks were compromised.

But the software targeted by the hackers, Exim, is a commonly used email transfer program, used by some Unix computers. Exim was developed at Cambridge University and is frequently used in Britain.

The vulnerability allowed attackers to execute commands and run their own code on compromised networks, a National Security Agency official said. It was, the agency said in its announcement, "pretty much any attacker's dream access."

The Russian Embassy in Washington did not respond to a request for comment.

Since before the 2018 midterm elections, the National Security Agency and its sister agency, United States Cyber Command, have stepped up efforts to identify and deter Russian interference. They have taken down internet networks used to spread divisive messages, warned the people behind troll farms against spreading disinformation and carried out other undisclosed operations. They also began an operation to put malware in the Russian electrical grid, as a warning about what kind of retaliation could happen if Moscow tried to attack the American grid.

The G.R.U.'s continued malicious activity shows that the American counterattacks have had only a modest effect, even as the National Security Agency persists in pressuring Russia. "When you are looking at some of the actions that have been done, they haven't quite made their mark," Scott Jasper, a lecturer at the U.S. Naval Postgraduate School and the author of a new book, "Russian Cyber Operations," said at a Cato Institute event on Thursday.

ackers from the G.R.U. were behind both the theft of documents on the Democratic National Committee's servers and the hack of Hillary Clinton's campaign in 2016. Russia publicly released those documents in an attempt to promote the election of Donald J. Trump, the United States government concluded.

The ability to exploit the software was first identified publicly in June 2019, and the G.R.U. team began using it two months later, targeting unpatched systems, according to the National Security Agency. The agency urged companies using the Exim software to update it to remove the vulnerability.

In February, the State Department called out the G.R.U. and the Sandworm Team, accusing them of conducting electronic attacks on the republic of Georgia in 2019 that defaced government websites and interrupted television broadcasts.

For the agency to accuse a Russian intelligence agency is a sign that, at least for now, it can operate outside of direct political pressure from Mr. Trump, former officials said.

National Security Agency officials have insisted that their agency is able to operate apolitically, without political influence changing their intelligence judgments. But that often involves acting against Russia without first seeking explicit permission from the president.

Under a presidential order issued in 2018, Gen. Paul M. Nakasone, the head of the agency and the commander of the United States Cyber Command, can operate on his own authority in operations short of war, including the kind that involve pushing back on Moscow.