

Corporate media, Democrats escalate claims of Russian hacking of US government agencies

Kevin Reed

17 December 2020

The Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security issued a warning on Thursday that the recently reported hack of “US government agencies, critical infrastructure entities, and private sector organizations” was carried out by “an advanced persistent threat (APT) actor beginning in at least March 2020.”

The CISA technical announcement makes no reference to the widely reported assertion that the hack was carried out by Russian intelligence. This claim, which has yet to be backed up by any proof or evidence, is being shamelessly repeated by nearly every corporate news organization in the US based upon the statements of unnamed cybersecurity experts and government officials.

The assertion that Russian intelligence is behind the hack has been picked up by Republican Senator Chuck Grassley of Iowa and Democratic Senator Ron Wyden of Oregon, who sent a letter to IRS Commissioner Charles Rettig on Thursday raising concerns that personal taxpayer information may have been stolen in the breach. The senators demanded details about IRS measures being taken to ensure that the hackers did not “still have access to internal IRS systems.”

After attending a Senate Armed Services Committee briefing, Democratic Senator Richard Blumenthal of Connecticut tweeted, “Russia’s cyberattack left me deeply alarmed, in fact downright scared. Americans deserve to know what’s going on.” While he said he would push to make more information public, Blumenthal failed to give any facts to substantiate the claim of Russian participation in the hacking operation.

Although he did not mention Russia, President-elect Joe Biden issued a statement that the breaches were “a

matter of great concern” and that he would impose “substantial costs on those responsible for such malicious attacks.”

“We have learned in recent days of what appears to be a massive cybersecurity breach affecting potentially thousands of victims, including U.S. companies and federal government entities,” Biden said. “I have instructed my team to learn as much as we can about this breach, and Vice President-elect Harris and I are grateful to the career public servants who have briefed our team on their findings, and who are working around-the-clock to respond to this attack.”

Although the scale and scope of the hack are still being investigated—and may never be fully disclosed to the public—the CISA alert states that the months-long breach “poses a grave risk to the Federal Government, local, tribal, and territorial governments” as well as civilian organizations and companies responsible for US telecommunications and energy infrastructure.

The CISA alert states that the threat actor “has demonstrated patience, operational security, and complex tradecraft in these intrusions,” and the agency “expects that removing this threat actor from compromised environments will be highly complex and challenging for organizations.”

While the US government itself has not publicly accused Russia of the intrusion, news sources have been reporting that hacker groups named Berserk Bear and Cozy Bear connected with the Russian Foreign Intelligence Service (SVR) are behind the intrusion into the enterprise IT software systems sold by SolarWinds of Austin, Texas.

CISA confirmed on Sunday that government and corporate IT systems based on the SolarWinds Orion

Platform had been hacked by exploiting vulnerabilities in the software pushed out to the government agencies and corporations during routine system updates. CISA states that these “supply chain attacks” used sophisticated methods to insert malicious code and mimic legitimate activity on the SolarWinds platform in order to monitor activity on the system and avoid detection.

The Trojan horse-style intrusion reportedly enabled the hackers to gain access to email traffic on the SolarWinds network management and infrastructure monitoring systems.

Among the government organizations named by the media as having been hit by the hack are the Treasury Department, the Commerce Department, the State Department, the Department of Homeland Security, the Justice Department, the Pentagon, the National Security Agency, the Energy Department, the US Postal Service and the National Institute of Health.

The corporate and private entities reportedly impacted by the SolarWinds exploit were many Fortune 500 companies in the US such as Microsoft Corporation and the ten largest US telecommunications providers.

Bloomberg reported on Thursday that the National Nuclear Security Administration, responsible for maintaining the US nuclear stockpile, was targeted as part of the hack. However, an investigation has found the “mission-essential national security functions” had not been impacted by the intrusion, according to Shaylyn Hynes, a Department of Energy spokeswoman. “At this point, the investigation has found that the malware has been isolated to business networks only,” Hynes said.

The combination of the way in which the hack was initially reported and the subsequent unfounded claims of its Russian source—as well as the timing just days after the Electoral College officially declared Joe Biden as president-elect—gives the events of the past few days an especially smelly character.

The same newspapers, and even the same state-connected “journalists,” like David Sanger of the *New York Times*, are peddling ever more elaborate tales of the gigantic Russian bogeyman, without a shred of factual substantiation. But readers are urged to draw the conclusion that Russia remains, along with China, the greatest threat to the US “national interest.” Happily

for the military-intelligence apparatus, this is exactly the perspective outlined by the Pentagon in its most recent national security documents, which declared the main focus of US military security policy had shifted from the “war on terror” to “great-power conflicts,” particularly with those two countries.

Once again, the Democrats and the intelligence community are firing up the engine of anti-Russia propaganda to manipulate public opinion for purposes connected with the foreign policy and geostrategic aims of US imperialism. Having passed through the experience of more than two years of the Mueller probe into “Russian interference” in the 2016 elections—which ended without proving that the regime of Vladimir Putin manipulated the presidential election in favor of Donald Trump—workers and young people must reject this latest propaganda exercise in the lead-up to Inauguration Day.



To contact the WSWS and the
Socialist Equality Party visit:

wsws.org/contact