

Working group of US intelligence agencies asserts Russia is “likely” behind SolarWinds hack

Kevin Reed
8 January 2021

A working group of four US intelligence agencies has issued a press release declaring that hackers behind the unprecedented cyberattack on hundreds of government and corporate users of the SolarWinds Orion platform were “likely Russian in origin.”

The joint statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI) and the National Security Agency (NSA) was first published on Tuesday afternoon on the website of the ODNI.

The statement says that the Trump administration’s National Security Council has created a task force called the cyber Unified Coordinating Group (UCG) composed of the four agencies to organize “the investigation and remediation of this significant cyber incident involving federal government networks.” It says that the UCG is “still working to understand the scope of the incident but has the following updates on its investigative and mitigation efforts.”

The press release is the first official statement by any US government agency to claim that Russians carried out the hack, saying the work of the UCG “indicates that an Advanced Persistent Threat (APT) actor, likely Russian in origin, is responsible for most or all of the recently discovered, ongoing cyber compromises of both government and non-governmental networks.”

Up to this point, accusations that Russian intelligence carried out the “supply chain attack”—in which the hackers embedded malicious code into multiple software updates and users unwittingly downloaded it into their Orion network administration platform—were made by the corporate media based on anonymous sources as well as the comments of individual political

figures.

Like the previous claims—such as that of Secretary of State Mike Pompeo that it was “pretty clear that it was the Russians”—the US intelligence task force presents no evidence or proof of its claim that Russia organized the SolarWinds hack.

The US intelligence task force statement mentions Russia only once and does not refer to the Russian intelligence service SVR or go into any details about the hacking group Cozy Bear which the corporate media has repeatedly stated is behind the breach.

The UCG statement also reveals that “fewer than 10 U.S. government agencies” have been compromised by the hack, although it does not say which ones. Media reports have indicated that among these agencies are: Department of State, Department of Homeland Security, National Institutes of Health, The Pentagon, Department of Energy, Department of the Treasury and Department of Commerce, as well as state and local government bodies.

Few details have been revealed about the impact of the hack on the government entities. Some reports have said that email messages were being monitored for months and that information or data may have been stolen.

An earlier statement on December 16 by the newly-formed UCG, that did not include an assertion of Russian involvement, is very similar to the document published on Tuesday. According to a report in the *New York Times*, the statement was modified “after Mr. Trump erupted at his intelligence briefers and said they had no evidence to link the action to Russia.” President Trump has consistently suggested on Twitter that the hack was carried out by China, not Russia.

While it is impossible—based upon presently available information—to determine precisely who is behind the SolarWinds cyberattack, the issuing of the latest UCG statement shows a growing consensus within the US intelligence community and political establishment that a renewed geostrategic offensive by US imperialism against Russia is a top priority of the incoming Biden administration.

As the *New York Times* indicated in its report by David Sanger and Julian. E Barnes late Tuesday, the UCG statement, “however carefully worded, the formal conclusion sets the stage for retaliation, most likely by President-elect Joseph R. Biden Jr. after he takes office. Mr. Biden, unlike Mr. Trump, has declared that whoever was behind the operation would pay a steep price.”

It is significant that the UCG statement was issued two days after the *New York Times* published a major front-page story in its Sunday edition—co-written by Sanger, Barnes and Nicole Perlroth—that ratcheted up the hysteria about the unproven “Russian hacking” of SolarWinds Orion and said absolutely nothing about the ongoing criminal cyberwarfare activities of the US intelligence agencies against the people of the world.

Based upon interviews with “key players investigating what intelligence agencies believe to be an operation by Russia’s SVR intelligence service,” the *Times* provided six bullet points. Among these are that the hackers “managed their intrusion from servers inside the United States, exploiting legal prohibitions on the National Security Agency from engaging in domestic surveillance and eluding cyberdefenses deployed by the Department of Homeland Security.”

In other words, with Biden in White House, the drive by US imperialism to “retaliate” against Russia will be accompanied by an intensification of NSA cyber surveillance and further attacks on the democratic rights of the public within the borders of the US.



To contact the WSWWS and the
Socialist Equality Party visit:

wsws.org/contact