The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Russia 'Likely' Behind SolarWinds Hack – U.S. Intelligence Agencies

By AFP

January 06, 2021

Russia previously denied it was involved in the SolarWinds hack. **Christopher Schirner / Flickr (CC BY-SA 2.0)**

U.S. intelligence and law enforcement agencies said Tuesday that Russia was probably behind the massive SolarWinds hack that has shaken government and corporate security, contradicting President Donald Trump, who had suggested China could be to blame.

A joint statement by the FBI, Directorate of National Intelligence, the National Security Agency and Cybersecurity and Infrastructure Security Agency outlined their findings in what experts have called the most devastating break in U.S. computer security in years.

Their investigation "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," they said.

Trump, who over four years has steadfastly avoided criticizing Moscow, has refused to finger Russia in the hacking case.

"Russia, Russia, Russia is the priority chant when anything happens," he tweeted about the hack in December, adding that the media were, "for mostly financial reasons, petrified of discussing the possibility that it may be China (it may!)."

Both Secretary of State Mike Pompeo and then-Attorney General Bill Barr have also previously pointed to Moscow as the culprits.

Related article: Pompeo Blames Russia for Massive U.S. Cyberattack

According to CISA, the hack is focused on the Orion security software produced by the U.S. firm SolarWinds, widely found in government and private sector computers across the globe.

Some 18,000 public and private customers of SolarWinds would be vulnerable to the hack, the statement said.

But it said that out of that number, "a much smaller number have been compromised by follow-on activity on their systems."

So far investigators have found less than 10 U.S. government agencies whose systems were compromised, the statement said.

The statement did not identify which agencies. But some have admitted they were targets, including the State Department, Commerce Department, Treasury, Homeland Security Department, Defense Department, and the National Institutes of Health.

The intrusion, which began earlier this year, only became public in December, revealed by private security consultants.

It sparked concerns that those behind it may have been able to access highly classified government secrets.

Related article: Russia Denies Role in U.S. Cyber Attacks

The three agencies said that they believe the hack "was, and continues to be, an intelligence gathering effort," rather than an effort to steal corporate secrets or wreak damage on IT systems.

"This is a serious compromise that will require a sustained and dedicated effort to remediate," they said.

The wording in the attribution, that it was "likely" a breach by Russians, came under fire from a senior lawmaker who had already been briefed by U.S. intelligence in December on it.

"It's unfortunate that it has taken over three weeks after the revelation of an intrusion this significant for this Administration to finally issue a tentative attribution," said Senator Mark

Warner, vice chairman of the Senate Intelligence committee.

"I would hope that we will begin to see something more definitive," he said.

"We need to make clear to Russia that any misuse of compromised networks to produce destructive or harmful effects is unacceptable and will prompt an appropriately strong response."