The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

U.S. Says 'Russia-Based' Group DarkSide Behind Pipeline Hack

By AFP

May 11, 2021



President Biden said a Russia-based group was behind the ransomware attack that shut down the largest oil pipeline in the eastern U.S. **Francois Picard / AFP**

President Joe Biden said Monday that a Russia-based group was behind the ransomware attack that forced the shutdown of the largest oil pipeline in the eastern United States.

The FBI identified the group behind the hack of Colonial Pipeline as DarkSide, a shadowy operation that surfaced last year and attempts to lock up corporate computer systems and force companies to pay to unfreeze them.

"So far there is no evidence ... from our intelligence people that Russia is involved, although there is evidence that actors, ransomware is in Russia," Biden told reporters.

"They have some responsibility to deal with this," he said.

Related article: Moscow Rejects U.S. Ransomware Attack Claims

Three days after being forced to halt operations, Colonial said Monday it was moving toward a partial reopening of its 5,500 miles (8,850 kilometers) of pipeline — the largest fuel network between Texas and New York.

At the White House, Deputy National Security Advisor Elizabeth Sherwood-Randall said Biden was being kept updated on the incident, which threatened to crimp supplies of gasoline, diesel fuel and jet fuel across much of the eastern United States.

Colonial said in a statement that "segments of our pipeline are being brought back online."

"Colonial has told us that it has not suffered damage and can be brought back online relatively quickly," Sherwood-Randall said, with no fuel disruptions so far.

Seeking ransom

The ransomware forced the company to shut down pipeline controls system for safety reasons.

DarkSide began attacking medium and large-sized companies mostly in Western Europe, Canada and the United States last year, reportedly asking for anywhere from a few hundred thousand dollars to a few million dollars, to be paid in Bitcoin.

In return, DarkSide supplies the company with a program that will unlock the its computing systems.

They also download and retain large amounts of data from the company, threatening to release it publicly if the company does not pay up.

In a statement on their website on the dark net, they rejected allegations that they had any official backing.

"We are apolitical, we do not participate in geopolitics, do not need to tie us with a defined government and look for other our motives," it said.

"Our goal is to make money, and not creating problems for society."

Dmitri Alperovitch, one of the foremost cybersecurity experts who cofounded the firm CrowdStrike, said his group believes DarkSide enjoys official protection in Russia.

"A ransomware group we believe is operating (and likely harbored) by Russia has shutdown a company that is moving 45% of petroleum supplying the East Coast. Is it a criminal act? Sure," he tweeted.

He said it also "undoubtedly" has "huge" national security implications, especially in US-Russia relations.

Another cybersecurity expert, Brett Callow of Emsisoft, told NBC News that an indication of the group's origins is that its software is designed to not work on computers whose default languages are Russian or several other eastern European languages.

“DarkSide doesn't eat in Russia,” Callow told NBC.

Anne Neuberger, deputy national security adviser for cyber, said most ransomware comes from transnational criminal groups.

Asked if Colonial Pipeline or other companies should pay the ransom, she said the Biden adminstration has not offered advice on that.

"They have to balance the cost-benefit when they have no choice with regard to paying a ransom," she said. "Typically that is a private sector decision."

Original url:
https://www.themoscowtimes.com/2021/05/11/us-says-russia-based-group-darkside-behind-pipeline-hack-a73858