

Russian hackers may be behind Texas natural gas plant explosion: report

By Ryan Morgan

Published: 2022-06-24 · Archived: 2026-04-06 01:01:04 UTC

A Russian hacking group may have targeted the industrial controls at a liquefied natural gas plant in Texas, leading to its explosion on June 8, a new report revealed this week.

On June 8, an explosion erupted at the Freeport Liquefied Natural Gas (Freeport LNG) liquefaction plant and export terminal on Texas' Quintana Island and damaged the facility. According to a June 14 [statement](#) by the company, the incident was caused by "overpressure and rupture of a segment of an LNG transfer line, leading to the rapid flashing of LNG and the release and ignition of the natural gas vapor cloud." The company didn't explain why safety systems didn't kick in.

Two LNG pipeline experts who [spoke with](#) the Washington Times national security writer Tom Rogan on Tuesday said such pipelines should have had extensive safety mechanisms in place. One of the sources said he is confident pipeline flows at the facility would be undertaken from a networked control facility.

Based on assessments of these two LNG pipeline experts and multiple other sources, Rogan theorized this week that the industrial safety controls at the natural gas facility could have been hacked and turned off by malicious actors. Since 2017, western intelligence officials and cybersecurity experts have been aware of a set of malware tools known as TRITON or TRISIS. A hacking group of suspected Russian origins, known as XENOTIME, has used these tools to shut off safety instrumented systems to damage industrial facilities.

On March 24 the U.S. Department of Justice [brought](#) charges against four Russian nationals suspected of using TRITON malware in cyber attacks on behalf of the Russian government between 2012 and 2018. That same day, the FBI issued an [advisory](#) warning that TRITON malware tools still remain a major threat to industrial systems around the world.

Rogan theorized that the June 8 explosion at the Freeport LNG facility could be consistent with this type of hacking behavior. Freeport LNG has denied Rogan's theory, saying, "While our ongoing investigation continues, a cyberattack was ruled out as the cause within days of the incident. After a thorough assessment of our network, our internal cyber detection systems have been confirmed to have been functioning properly and do not indicate any manipulation or compromise of our security solutions."

While Freeport LNG denied the hacking theory overall, Rogan wrote that the company does not employ the Operation Technology/Industrial Control Systems network detection systems necessary to determine whether they were targeted with TRITON or similar malware. Rogan noted that in response to this line of questioning Freeport LNG only said that their original dismissal of the hacking theory "Stands" adding "Nothing further."

“Unless Freeport LNG has OT/ICS network detection systems deployed appropriately and has completed a forensics investigation, a cyberattack cannot be ruled out,” Rogan wrote.

In addition to possessing the means to carry out such an attack, Rogan noted Russia also possesses the motive.

Two more sources who spoke with Rogan said that around the time of Russia launched its invasion of Ukraine, a cyber unit of Russia’s GRU military intelligence service conducted targeting-reconnaissance operations against Freeport LNG.

Rogan also noted that U.S. LNG exports have long been a concern of Russia’s as they undercut Russia’s own gas exports throughout the European market. Ever since Russia launched its invasion of Ukraine, the U.S. and its allies have tried to [cut off the flow of Russian oil and gas products](#). Rogan wrote that European gas prices spiked after the June 8 explosion at the Freeport LNG facility.

The June 8 incident will also have a lasting impact on Freeport LNG’s operations. In their June 14 statement, Freeport LNG said that with the damage caused by the explosion, it won’t be finished with all of its necessary repairs and return to operations until the end of 2022.

Source: <https://americanmilitarynews.com/2022/06/russian-hackers-may-be-behind-texas-natural-gas-plant-explosion-report/>