

# Colonial Pipeline ransomware attack

On May 7, 2021, Colonial Pipeline, an American oil pipeline system that originates in Houston, Texas, and carries gasoline and jet fuel mainly to the Southeastern United States, suffered a ransomware cyberattack that impacted computerized equipment managing the pipeline.<sup>[4][5][6]</sup> The Colonial Pipeline Company halted all pipeline operations to contain the attack.<sup>[7][8][9][10]</sup> Overseen by the FBI, the company paid the amount that was asked by the hacker group (75 bitcoin or \$4.4 million) within several hours;<sup>[11][12]</sup> upon receipt of the ransom, an IT tool was provided to the Colonial Pipeline Company by DarkSide to restore the system. However, the tool had a very long processing time to help get the system back up in time.<sup>[12]</sup>

The Federal Motor Carrier Safety Administration issued a regional emergency declaration for 17 states and Washington, D.C., to keep fuel supply lines open on May 9.<sup>[13]</sup> It was the largest cyberattack on an oil infrastructure target in the history of the United States.<sup>[2]</sup> The FBI and various media sources identified the criminal hacking group DarkSide as the responsible party.<sup>[14]</sup> The same group is believed to have stolen 100 gigabytes of data from company servers the day before the malware attack.<sup>[1]</sup>

On June 7, the Department of Justice announced that it had recovered 63.7 of the bitcoins (approximately \$2.3 million) from the ransom payment.<sup>[15]</sup>

## Colonial Pipeline ransomware attack

<b>Date</b>	<ul style="list-style-type: none"> <li>May 6, 2021 (data stolen)<sup>[1]</sup></li> <li>May 7, 2021 (malware attack)</li> <li>May 12, 2021 (pipeline restarted)</li> </ul>
<b>Location</b>	United States
<b>Type</b>	Cyberattack, <u>data breach</u> , <u>ransomware</u>
<b>Target</b>	<u>Colonial Pipeline</u>
<b>Suspects</b>	<u>DarkSide</u> <sup>[2][3]</sup>

## Contents

### Background

### Impact

### Responses

#### Perpetrators

### Pipeline restart

### Investigations

#### Partial ransom recovery

### See also

### References

### External links

## Background

---

The Colonial Pipeline carries gasoline, diesel and jet fuel from Texas to as far away as New York. About 45% of all fuel consumed on the East Coast arrives via the pipeline system.<sup>[16]</sup> The attack came amid growing concerns over the vulnerability of infrastructure (including critical infrastructure) to cyberattacks after several high-profile attacks, including the 2020 SolarWinds hack that hit multiple federal government agencies, including the Defense, Treasury, State, and Homeland Security departments.<sup>[6][17]</sup>

## Impact

---

The primary target of the attack was the billing infrastructure of the company. The actual oil pumping systems was still able to work. According to CNN sources in the company, the inability to bill the customers was the reason for halting the pipeline operation.<sup>[18]</sup> Colonial Pipeline reported that it shut down the pipeline as a precaution due to a concern that the hackers might have obtained information allowing them to carry out further attacks on vulnerable parts of the pipeline. The day after the attack, Colonial could not confirm at that time when the pipeline would resume normal functions.<sup>[7]</sup> The attackers also stole nearly 100 gigabytes of data and threatened to release it on the internet if the ransom was not paid.<sup>[1]</sup> It was reported that within hours after the attack the company paid a ransom of nearly 75 Bitcoins (\$5 million) to the hackers in exchange for a decryption tool, which proved so slow that the company's business continuity planning tools were more effective in bringing back operational capacity.<sup>[19][20]</sup>

On May 9, Colonial stated they planned to substantially repair and restore the pipeline's operations by the end of the week.<sup>[21]</sup>

In response to fuel shortages at Charlotte Douglas International Airport caused by the pipeline shutdown, American Airlines changed flight schedules temporarily.<sup>[22]</sup> At least two flights (to Honolulu and London) had fuel stops or plane changes added to their schedules for a four-day period. The shortage also required Hartsfield–Jackson Atlanta International Airport to use other fuel suppliers, and there are at least five other airports directly serviced by the pipeline.<sup>[23]</sup>

Fuel shortages began to occur at filling stations amid panic buying as the pipeline shutdown entered its fourth day.<sup>[24][25]</sup> Alabama, Florida, Georgia, North Carolina, and South Carolina all reported shortages.<sup>[24]</sup> Areas from northern South Carolina to southern Virginia were hardest hit, with 71% of filling stations running out of fuel in Charlotte on May 11<sup>[26]</sup> and 87 percent of stations out in Washington, D.C. on May 14.<sup>[27]</sup> Average fuel prices rose to their highest since 2014, reaching more than \$3 a gallon.<sup>[28]</sup>

## Responses

---



Panic buying caused widespread gasoline shortages



Some filling stations were without fuel for several days

U.S. President Joe Biden declared a state of emergency on 9 May 2021. During regular times there were limits on the amount of petroleum products that could be transported by road, rail, etc., domestically within the U.S mainland. However, with the declaration in place, these were temporarily suspended.<sup>[29]</sup>

On May 10, Georgia Governor Brian Kemp declared a state of emergency,<sup>[30]</sup> and temporarily waived collection of the state's taxes on motor fuels (diesel and gasoline).<sup>[31]</sup> In response to panic buying in the Southeast, U.S. Transportation Secretary Pete Buttigieg and U.S. Energy Secretary Jennifer Granholm on May 12 both cautioned against gasoline hoarding, reiterating that the United States was undergoing a "supply crunch" rather than a gas shortage.<sup>[32][33]</sup>

On May 12, the U.S. Consumer Product Safety Commission advised people to "not fill plastic bags with gasoline" or to use any containers not meant for fuel.<sup>[33]</sup>

Biden signed Executive Order 14028<sup>[34]</sup> on May 12, increasing software security standards for sales to the government, tighten detection and security on existing systems, improve information sharing and training, establish a Cyber Safety Review Board, and improve incident response. The United States Department of Justice also convened a cybersecurity task force to increase prosecutions.<sup>[35]</sup>

The Department of State issued a statement that a \$10,000,000 reward would be given out in case of information leading to the arrest of DarkSide members.<sup>[36]</sup>

## Perpetrators

DarkSide released a statement on May 9 that did not directly mention the attack, but claimed that "our goal is to make money, and not creating problems for society".<sup>[37][29]</sup>

## Pipeline restart

---

The restart of pipeline operations began at 5 p.m. on May 12,<sup>[38]</sup> ending a six-day shutdown, although Colonial Pipeline Company warned that it could take several more days for service to return to normal. The pipeline company stated that several markets that are served by the pipeline may experience, or continue to experience, intermittent service interruptions during the restart. The company also stated that they would move as much gasoline, diesel and jet fuel as safely possible until markets return to normal.<sup>[39][40]</sup> All Colonial Pipeline systems and operations had returned to normal by May 15.<sup>[38]</sup> After the shutdown, the average national cost rose to the highest it's been in over six years, to about an average of \$3.04 a gallon on May 18. The price increase was more pronounced in the southern states, with prices rising between 9 and 16 cents in the Carolinas, Tennessee, Virginia, and Georgia. Around 10,600 gas stations were still without gas as of May 18.<sup>[41][42][43]</sup>

In a May 19, 2021, interview with *The Wall Street Journal*, Joseph Blount said why he ultimately decided to pay a \$4.4 million ransom to hackers who breached the company's systems; "It was the right thing to do for the country." He also said, "I know that's a highly controversial decision".<sup>[44]</sup>

## Investigations

---

Biden said on May 10 that though there was no evidence that the Russian government was responsible for the attack, there was evidence that the DarkSide group is in Russia, and that thus, Russian authorities "have some responsibility to deal with this".<sup>[45][46]</sup> Independent cybersecurity

researchers have also stated the hacking group is Russian as their malware avoids encrypting files in a system where the language is set to Russian.<sup>[46][47]</sup>

In the aftermath of the attack, it was revealed at a Senate Armed Services cyber subcommittee hearing that the Department of Homeland Security was not alerted to the ransomware attack and that the Justice Department was not alerted to the ransom type or amount, prompting discussion about the numerous information silos in the government and difficulties of sharing.<sup>[48]</sup>

Blockchain analytics firm Elliptic published a bitcoin wallet report showing \$90 million in bitcoin ransom payments were made to DarkSide or DarkSide affiliates over the last year, originating from 47 distinct wallets. According to a DarkTracer release of 2226 victim organizations since May 2019, 99 organizations have been infected with the DarkSide malware – suggesting that approximately 47% of victims paid a ransom and that the average payment was \$1.9 million. The DarkSide developer had received bitcoins worth \$15.5 million (17%), with the remaining \$74.7 million (83%) going to the various affiliates.<sup>[49][50]</sup>

## Partial ransom recovery

The U.S. Department of Justice issued a press release on June 7, 2021, stating that it had seized 63.7 Bitcoins from the original ransom payment.<sup>[15]</sup> The value of the recovered Bitcoins was only \$2.3 million, because the trading price of Bitcoin had fallen since the date of the ransom payment. Through possession of the private key of the ransom account, the FBI was able to retrieve the Bitcoin, though it did not disclose how it obtained the private key.<sup>[51][52]</sup>

## See also

- Steamship Authority cyberattack
- Health Service Executive cyberattack



Warrant authorizing the seizure of 63.7 BTC by the FBI.

## References

- Robertson, Jordan; Turton, William (May 8, 2021). "Colonial Hackers Stole Data Thursday Ahead of Shutdown" (<https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown>). *Bloomberg News*. Archived (<https://web.archive.org/web/20210509150415/https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown>) from the original on May 9, 2021. Retrieved May 9, 2021.
- Gonzalez, Gloria; Lefebvre, Ben; Geller, Eric (May 8, 2021). "'Jugular' of the U.S. fuel pipeline system shuts down after cyberattack" (<https://www.politico.com/news/2021/05/08/colonial-pipeline-cyber-attack-485984>). *Politico*. Archived (<https://web.archive.org/web/20210509154120/https://www.politico.com/news/2021/05/08/colonial-pipeline-cyber-attack-485984>) from the original on May 9, 2021. Retrieved May 9, 2021. "The infiltration of a major fuel pipeline is "the most significant, successful attack on energy infrastructure we know of.""

3. Helmore, Edward (May 10, 2021). "FBI confirms DarkSide hacking group behind US pipeline shutdown" (<https://www.theguardian.com/us-news/2021/may/10/colonial-pipeline-shutdown-us-darkside-message>). *The Guardian*. Archived (<https://web.archive.org/web/20210512115806/https://www.theguardian.com/us-news/2021/may/10/colonial-pipeline-shutdown-us-darkside-message>) from the original on May 12, 2021. Retrieved May 10, 2021.
4. Bing, Christopher; Kelly, Stephanie (May 8, 2021). "Cyber attack shuts down top U.S. fuel pipeline network" (<https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/>). *Reuters*. Archived (<https://web.archive.org/web/20210508050319/https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/>) from the original on May 8, 2021. Retrieved May 8, 2021.
5. Segers, Grace (May 8, 2021). "Cyberattack prompts major pipeline operator to halt operations" (<https://www.cbsnews.com/news/colonial-pipeline-cyberattack-halt-operations/>). *CBS News*. Archived (<https://web.archive.org/web/20210508150203/https://www.cbsnews.com/news/colonial-pipeline-cyberattack-halt-operations/>) from the original on May 8, 2021. Retrieved May 8, 2021.
6. Peñaloza, Marisa (May 8, 2021). "Cybersecurity Attack Shuts Down A Top U.S. Gasoline Pipeline" (<https://www.npr.org/2021/05/08/995040240/cybersecurity-attack-shuts-down-a-top-u-s-gasoline-pipeline>). *NPR*. Archived (<https://web.archive.org/web/20210508181849/https://www.npr.org/2021/05/08/995040240/cybersecurity-attack-shuts-down-a-top-u-s-gasoline-pipeline>) from the original on May 8, 2021. Retrieved May 8, 2021.
7. Sanger, David; Krauss, Clifford; Perloth, Nicole (May 8, 2021). "Cyberattack Forces a Shutdown of a Top U.S. Pipeline" (<https://www.nytimes.com/2021/05/08/us/cyberattack-colonial-pipeline.html>). *New York Times*. Archived (<https://web.archive.org/web/20210508120639/https://www.nytimes.com/2021/05/08/us/cyberattack-colonial-pipeline.html>) from the original on May 8, 2021. Retrieved May 8, 2021.
8. Eaton, Collin; Volz, Dustin (May 8, 2021). "U.S. Pipeline Cyberattack Forces Closure" (<https://www.wsj.com/articles/cyberattack-forces-closure-of-largest-u-s-refined-fuel-pipeline-11620479737>). *Wall Street Journal*. Archived (<https://web.archive.org/web/20210508131722/https://www.wsj.com/articles/cyberattack-forces-closure-of-largest-u-s-refined-fuel-pipeline-11620479737>) from the original on May 8, 2021. Retrieved May 8, 2021.
9. Stracqualursi, Veronica (May 8, 2021). "Cyberattack forces major US fuel pipeline to shut down" (<https://www.cnn.com/2021/05/08/politics/colonial-pipeline-cybersecurity-attack/index.html>). *CNN*. Archived (<https://web.archive.org/web/20210508151906/https://www.cnn.com/2021/05/08/politics/colonial-pipeline-cybersecurity-attack/index.html>) from the original on May 8, 2021. Retrieved May 8, 2021.
10. "Colonial Pipeline blames ransomware for pipeline shutdown" (<https://www.nbcnews.com/news/us-news/cyberattack-forces-colonial-pipeline-shut-major-fuel-line-n1266737>). *NBC News*. May 8, 2021. Archived (<https://web.archive.org/web/20210508085111/https://www.nbcnews.com/news/us-news/cyberattack-forces-colonial-pipeline-shut-major-fuel-line-n1266737>) from the original on May 8, 2021. Retrieved May 8, 2021.
11. First on CNN: US recovers millions in cryptocurrency paid to Colonial Pipeline ransomware hackers (<https://www.cnn.com/2021/06/07/politics/colonial-pipeline-ransomware-recovered/index.html>) *CNN*
12. Turton, William; Riley, Michael; Jacobs, Jennifer (May 12, 2021). "Colonial Pipeline Paid Hackers nearly \$5 Million in Ransom" (<https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom>). *Bloomberg*.
13. "Emergency declaration issued in 17 states and D.C. over fuel pipeline cyberattack" (<https://news.yahoo.com/biden-admin-declares-state-emergency-011332752.html>). *Yahoo! News*. May 10, 2021. Retrieved May 10, 2021.

14. Javers, Eamon (May 10, 2021). "Here's the hacking group responsible for the Colonial Pipeline shutdown" (<https://www.cnbc.com/2021/05/10/hacking-group-darkside-reportedly-responsible-for-colonial-pipeline-shutdown.html>). *CNBC*. Archived (<https://web.archive.org/web/20210510145819/https://www.cnbc.com/2021/05/10/hacking-group-darkside-reportedly-responsible-for-colonial-pipeline-shutdown.html>) from the original on May 10, 2021. Retrieved May 11, 2021.
15. DOJ seizes millions in ransom paid by Colonial Pipeline (<https://abcnews.go.com/Politics/doj-seizes-millions-ransom-paid-colonial-pipeline/story?id=78135821>) ABC News
16. Walsh, Joe. "Ransomware Attack Shuts Down Massive East Coast Gasoline Pipeline" (<https://www.forbes.com/sites/joewalsh/2021/05/08/ransomware-attack-shuts-down-massive-east-coast-gasoline-pipeline/>). *Forbes*. Retrieved February 6, 2022.
17. Walton, Robert (May 11, 2021). "Colonial Pipeline hack highlights grid disruption risks even with IT-focused cyberattack, analysts say" (<https://www.utilitydive.com/news/colonial-pipeline-hack-highlights-grid-disruption-risks-even-with-it-focus/599942/>). *UtilityDive*.
18. Bertrand, Natasha; Perez, Evan; Cohen, Zachary; Sands, Geneva; Campbell, Josh. "Colonial Pipeline did pay ransom to hackers, sources now say" (<https://edition.cnn.com/2021/05/12/politics/colonial-pipeline-ransomware-payment/index.html>). *CNN*. Retrieved May 23, 2021.
19. Perlroth, Nicole (May 13, 2021). "Colonial Pipeline paid 75 Bitcoin, or roughly \$5 million, to hackers" (<https://www.nytimes.com/2021/05/13/technology/colonial-pipeline-ransom.html>). *The New York Times*. Retrieved May 13, 2021.
20. Turton, William; Riley, Michael; Jacobs, Jennifer (May 13, 2021). "Colonial Pipeline Paid Hackers Nearly \$5 Million in Ransom" (<https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom>). *Bloomberg News*. Retrieved June 8, 2021. "Once [Colonial] received the payment, the hackers provided the operator with a decrypting tool to restore its disabled computer network. The tool was so slow that the company continued using its own backups to help restore the system, one of the people familiar with the company's efforts said."
21. Bomey, Nathan. "Colonial Pipeline looking to 'substantially restore operations by end of week" (<https://www.usatoday.com/story/money/2021/05/10/gas-prices-colonial-pipeline-ransomware-attack-cyberattack/5019214001/>). *USA TODAY*. Archived (<https://web.archive.org/web/20210510143554/https://www.usatoday.com/story/money/2021/05/10/gas-prices-colonial-pipeline-ransomware-attack-cyberattack/5019214001/>) from the original on May 10, 2021. Retrieved May 10, 2021.
22. "American Airlines adds fuel stops to two flights after pipeline outage" (<https://www.reuters.com/business/energy/american-airlines-adds-fuel-stops-two-flights-after-pipeline-outage-2021-05-11/>). *Reuters*. May 11, 2021. Archived (<https://web.archive.org/web/20210512232950/https://www.reuters.com/business/energy/american-airlines-adds-fuel-stops-two-flights-after-pipeline-outage-2021-05-11/>) from the original on May 12, 2021. Retrieved May 11, 2021.
23. Josephs, Leslie (May 11, 2021). "Pipeline outage forces American Airlines to add stops to some long-haul flights" (<https://www.cnbc.com/2021/05/10/colonial-pipeline-shutdown-forces-airlines-to-consider-other-ways-to-get-fuel.html>). *CNBC*. Archived (<https://web.archive.org/web/2021051223057/https://www.cnbc.com/2021/05/10/colonial-pipeline-shutdown-forces-airlines-to-consider-other-ways-to-get-fuel.html>) from the original on May 12, 2021. Retrieved May 11, 2021.
24. "Gas Stations Run Dry as Pipeline Races to Recover From Hacking" (<https://www.bloomberg.com/news/articles/2021-05-09/u-s-fuel-sellers-scramble-for-alternatives-to-hacked-pipeline>). *Bloomberg News*. May 9, 2021. Archived (<https://web.archive.org/web/20210510055911/https://www.bloomberg.com/news/articles/2021-05-09/u-s-fuel-sellers-scramble-for-alternatives-to-hacked-pipeline>) from the original on May 10, 2021. Retrieved May 11, 2021.

25. "Petrol shortages sweep US as Colonial Pipeline remains down" (<https://www.aljazeera.com/economy/2021/5/11/petrol-shortages-sweep-us-as-colonial-pipeline-remains-down>). *Al Jazeera*. Archived (<https://web.archive.org/web/20210511182941/https://www.aljazeera.com/economy/2021/5/11/petrol-shortages-sweep-us-as-colonial-pipeline-remains-down>) from the original on May 11, 2021. Retrieved May 11, 2021.
26. Lee, Ron (May 11, 2021). "GasBuddy reports 71% of gas stations without fuel in Charlotte metro amid Colonial Pipeline shutdown" (<https://www.wbtv.com/2021/05/11/long-lines-charlotte-gas-supply-squeezed/>). *WBTV*. Charlotte, NC. Archived (<https://web.archive.org/web/20210512233023/https://www.wbtv.com/2021/05/11/long-lines-charlotte-gas-supply-squeezed/>) from the original on May 12, 2021. Retrieved May 12, 2021.
27. Shah, Jill R. (May 15, 2021). "Gasoline pinch to continue with truck shortage". *The Charlotte Observer*. p. A4 – via *Bloomberg News*.
28. Englund, Will; Nakashima, Ellen (May 12, 2021). "Panic buying strikes Southeastern United States as shuttered pipeline resumes operations" (<https://www.washingtonpost.com/business/2021/05/12/gas-shortage-colonial-pipeline-live-updates/>). *Washington Post*. Retrieved May 13, 2021.
29. "US fuel pipeline hackers 'didn't mean to create problems' " (<https://www.bbc.com/news/business-57050690>). *BBC News*. May 10, 2021. Archived (<https://web.archive.org/web/20210510000238/https://www.bbc.com/news/business-57050690>) from the original on May 10, 2021. Retrieved May 10, 2021.
30. Mahtani, Melissa; Macaya, Melissa; Hayes, Mike; Rocha, Veronica (May 11, 2021). "Latest on the US gas demand spikes" (<https://www.cnn.com/us/live-news/us-gas-demand-hack-05-11-21/index.html>). *CNN*. Archived (<https://web.archive.org/web/20210512233023/https://www.cnn.com/us/live-news/us-gas-demand-hack-05-11-21/index.html>) from the original on May 12, 2021. Retrieved May 12, 2021.
31. "Kemp extends Georgia gas tax waiver due to pipeline outage" (<https://apnews.com/article/georgia-hacking-technology-government-and-politics-business-bc290931a741d6d0b897423b91b0c6d4>). *Associated Press*. May 14, 2021.
32. Wagner, Meg; Macay, Melissa; Hayes, Mike; Mahtani, Melissa; Rocha, Veronica. "Gas shortages at some US stations: Live updates" (<https://www.cnn.com/business/live-news/us-gas-demand-05-12-21/index.html>). *CNN*. Archived (<https://web.archive.org/web/20210512233040/https://www.cnn.com/business/live-news/us-gas-demand-05-12-21/index.html>) from the original on May 12, 2021. Retrieved May 12, 2021.
33. Brito, Christopher (May 12, 2021). "Officials warn people not to fill plastic bags with gasoline amid panic over gas shortage" (<https://www.cbsnews.com/news/gas-shortage-plastic-bags-warning/>). *CBS News*. Archived (<https://web.archive.org/web/20210512192916/https://www.cbsnews.com/news/gas-shortage-plastic-bags-warning/>) from the original on May 12, 2021. Retrieved May 13, 2021.
34. Executive Order on Improving the Nation's Cybersecurity (<https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>) (full text)
35. Biden Adviser On Cyber Threats And The New Executive Order To Combat Them (<https://www.npr.org/2021/05/13/996617560/biden-advisor-on-cyber-threats-and-the-new-executive-order-to-combat-them>)
36. "Reward Offers for Information to Bring DarkSide Ransomware Variant Co-Conspirators to Justice" (<https://www.state.gov/reward-offers-for-information-to-bring-darkside-ransomware-variant-co-conspirators-to-justice/>). *United States Department of State*. Retrieved December 31, 2021.




37. "DarkSide hackers behind Colonial Pipeline attack say they wanted cash, not chaos" (<https://www.abc.net.au/news/2021-05-11/darkside-says-aim-as-cash-no-chaos-colonial-pipeline/100130020>). *Australian Broadcasting Corporation*. May 10, 2021. Archived (<https://web.archive.org/web/20210512233040/https://www.abc.net.au/news/2021-05-11/darkside-says-aim-as-cash-no-chaos-colonial-pipeline/100130020>) from the original on May 12, 2021. Retrieved May 10, 2021.
38. Lyons, Kim (May 15, 2021). "Colonial Pipeline says operations back to normal following ransomware attack" (<https://www.theverge.com/2021/5/15/22437730/colonial-pipeline-normal-ransomware-attack-fuel>). *The Verge*.
39. Egan, Matt; Duffy, Clare. "Colonial Pipeline launches restart after six-day shutdown" (<https://www.cnn.com/2021/05/12/business/colonial-pipeline-restart/index.html>). *CNN Business*. Archived (<https://web.archive.org/web/20210512233024/https://www.cnn.com/2021/05/12/business/colonial-pipeline-restart/index.html>) from the original on May 12, 2021. Retrieved May 12, 2021.
40. Krauss, Clifford. "Colonial Pipeline Begins to Restart Flow of Fuel" (<https://www.nytimes.com/2021/05/12/business/energy-environment/pipeline-shutdown-latest-news.html>). *The New York Times*. Archived (<https://web.archive.org/web/20210512221720/https://www.nytimes.com/2021/05/12/business/energy-environment/pipeline-shutdown-latest-news.html>) from the original on May 12, 2021. Retrieved May 12, 2021.
41. Eaton, Collin (May 18, 2021). "Colonial Pipeline Still Moving Fuel Despite Disruptions to Orders System" (<https://www.wsj.com/articles/colonial-pipeline-ordering-system-disrupted-but-still-moving-fuel-11621358203>). *Wall Street Journal*. ISSN 0099-9660 (<https://www.worldcat.org/issn/0099-9660>). Retrieved May 19, 2021.
42. "Gas hits highest price in 6 years, fuel outages persist despite Colonial Pipeline restart" (<https://abcnews.go.com/US/gas-hits-highest-price-years-fuel-outages-persist/story?id=77735010>). *ABC News*. Retrieved May 19, 2021.
43. "Colonial Pipeline's Computer Network Temporarily Goes Dark" (<https://www.bloomberg.com/news/articles/2021-05-18/colonial-shippers-say-pipeline-communication-system-is-down>). *www.bloomberg.com*. Archived (<https://web.archive.org/web/20210518153516/https://www.bloomberg.com/news/articles/2021-05-18/colonial-shippers-say-pipeline-communication-system-is-down>) from the original on May 18, 2021. Retrieved May 19, 2021.
44. Eaton, Collin; Volz, Dustin (May 19, 2021). "Colonial Pipeline CEO Tells Why He Paid Hackers a \$4.4 Million Ransom" (<https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hacker-s-a-4-4-million-ransom-11621435636>). *The Wall Street Journal*. Retrieved May 20, 2021.
45. "Biden Says Russia Has 'Some Responsibility' In Pipeline Ransomware Attack" (<https://www.rferl.org/a/fbi-confirms-darkside-hacker-group-pipeline-cyberattack-russia/31248174.html>). *Radio Free Europe*. May 10, 2021. Archived (<https://web.archive.org/web/20210512233023/https://www.rferl.org/a/fbi-confirms-darkside-hacker-group-pipeline-cyberattack-russia/31248174.html>) from the original on May 12, 2021. Retrieved May 11, 2021.
46. "US fuel pipeline hackers 'didn't mean to create problems' " (<https://www.bbc.com/news/business-57050690>). *BBC News*. May 10, 2021. Archived (<https://web.archive.org/web/20210510172239/https://www.bbc.com/news/business-57050690>) from the original on May 10, 2021. Retrieved May 12, 2021.
47. Rivero, Nicolás. "Hacking collective DarkSide are state-sanctioned pirates" (<https://qz.com/2007399/the-darkside-hackers-are-state-sanctioned-pirates/>). *Quartz (publication)*. Archived (<https://web.archive.org/web/20210512233022/https://qz.com/2007399/the-darkside-hackers-are-state-sanctioned-pirates/>) from the original on May 12, 2021. Retrieved May 12, 2021.
48. "Lawmakers Grill Pentagon Officials on How to Prevent Another Colonial Pipeline-Style Attack" (<https://news.usni.org/2021/05/18/lawmakers-grill-pentagon-homeland-security-officials-on-how-to-prevent-another-colonial-pipeline-style-attack>). *USNI News*. May 18, 2021.



49. "DarkSide Ransomware has Netted Over \$90 million in Bitcoin" (<https://www.elliptic.co/blog/darkside-ransomware-has-netted-over-90-million-in-bitcoin>). *Elliptic.co*. May 18, 2021.
50. "Colonial Pipeline hacker Darkside reaped \$90M from 47 victims" (<https://www.foxbusiness.com/money/colonial-pipeline-hacker-darkside-reaped-90m-from-victims>). *FOX Business*. May 18, 2021.
51. @dnvolz (June 7, 2021). "The FBI seized \$2.3 million, roughly 64 bitcoin, from a bitcoin wallet said to contain proceeds from the ransom pay..." (<https://twitter.com/dnvolz/status/1401986721810718725>) (Tweet) – via [Twitter](#).
52. "U.S. seizes \$2.3 mln in bitcoin paid to Colonial Pipeline hackers" (<https://www.reuters.com/business/energy/us-announce-recovery-millions-colonial-pipeline-ransomware-attack-2021-06-07/>). *Reuters*. June 7, 2021. Retrieved June 7, 2021.

## External links

---

-  Media related to [Colonial Pipeline cyberattack](#) at Wikimedia Commons
- 

Retrieved from "[https://en.wikipedia.org/w/index.php?title=Colonial\\_Pipeline\\_ransomware\\_attack&oldid=1092151580](https://en.wikipedia.org/w/index.php?title=Colonial_Pipeline_ransomware_attack&oldid=1092151580)"

---

**This page was last edited on 8 June 2022, at 13:35 (UTC).**

Text is available under the Creative Commons Attribution-ShareAlike License 3.0; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.