MENU US

MUST READ: Python programming: We want to make the language twice as fast, says its creator

Colonial Pipeline attack: Everything you need to know

Updated: DarkSide has claimed responsibility for the catastrophic ransomware outbreak.

By Charlie Osborne for Zero Day | May 13, 2021 -- 07:17 GMT (00:17 PDT) | Topic: Security

The real-world consequences of a successful cyberattack have been clearly highlighted this week with the closure of one of the US' largest pipelines due to ransomware.

Here's everything we know so far.

On Friday, May 7, Colonial Pipeline said that a cyberattack (https://www.zdnet.com/article/colonial-pipeline-cyberattack-shuts-down-pipeline-that-supplies-45-of-east-coasts-fuel/) forced the company to proactively close down operations and freeze IT systems after becoming the victim of a cyberattack.

This measure "temporarily halted all pipeline operations" and cybersecurity firm FireEye (h om/article/usa-stocks-fireeye/fireeye-shares-jump-after-pipeline-cyberattackidUSL1N2MX19M), which operates the Mandiant cyberforensics team, was reportedly pulled in to assist.

What is Colonial Pipeline?

Founded in 1962 and headquartered in Alpharetta, Georgia, privately-held Colonial Pipeline (https://www.colpipe.com/) is one of the largest pipeline operators in the United States and provides roughly 45% of the East Coast's fuel, including gasoline, diesel, home heating oil, jet fuel, and military supplies.

The company says that it transports over 100 million gallons of fuel daily across an area spanning Texas to New York.

How did the Colonial Pipeline ransomware attack happen?

There are few concrete details on how the cyberattack took place, and it is likely that this will not change until Colonial Pipeline and the third-party company brought in to investigate have concluded their analysis of the incident.

However, what did occur was a ransomware outbreak, linked to the DarkSide group, that struck Colonial Pipeline's networks.

The initial attack vector isn't known, but it may have been an old, unpatched vulnerability in a system; a phishing email that successfully fooled an employee; the use of access credentials purchased or obtained elsewhere that were leaked previously, or any other number of tactics employed by cybercriminals to infiltrate a company's network.

It should be noted that DarkSide operators targeted the business side rather than operational systems, which implies the intent was money-orientated rather than designed to send the pipeline crashing down.

The oil giant said it "proactively took certain systems offline to contain the threat, which temporarily halted all pipeline operations, and affected some of our IT systems."

Colonial Pipeline's update, published on Monday 10 (https://www.zdnet.com/article/colonial-pipeline-aims-to-restore-operations-by-end-of-the-week-after-cyberattack/), said that remediation is ongoing and each system is being worked on in an "incremental approach."

"This plan is based on a number of factors with safety and compliance driving our operational d Manage Cookies goal of substantially restoring operational service by the end of the week," the company added.

In a further update, Colonial Pipeline said that one line is operating under manual control while supplies of gas are "available."

"While our main lines continue to be offline, some smaller lateral lines between terminals and delivery points are now operational as well. We continue to evaluate product inventory in storage tanks at our facilities and others along our system and are working with our shippers to move this product to terminals for local delivery."

Why does the Colonial Pipeline ransomware attack matter?

As shown in the company's operations map, by taking out the systems supporting and managing pipeline operation and fuel distribution, vast swathes of the US have been impacted.

At the time of the attack, supply shortage concerns prompted gasoline futures to reach their highest le (https://www.cnbc.com/2021/05/09/gasoline-futures-jump-as-much-of-vital-pipeline-remains-shutdownfollowing-cyberattack.html). Demand has risen, but drivers are being urged not to panic buy, as this could impact prices that have already increased due to the pipeline disruption by six cents (https://www.reuters.com/article/usa-gasoline-colonial-pipeline/us-pump-prices-head-for-highest-since-2014-as-hacked-fuel-pipeline-shut-idUSL1N2MX1NL) per gallon in the past week.

With normal operations not expected to resume until, at best, the end of the week, we are likely to see fluctuations -- and potentially further price increases -- in fuel supplies across impacted areas in the US.

US President Biden has also been briefed on the event. If anything highlights just how serious a cyberattack has become, it is this.

See also: Ransomware just got very real. And it's likely to get worse (https://www.zdnet.com/article/ransomware-just-got-very-real-and-its-likely-to-get-worse/)

Will there be gas shortages?

Patrick De Haan

Late Tuesday evening, White House press secretary Jen Psaki said the US government is "monitoring supply shortages in parts of the Southeast," as reported by (https://www.independent.co.uk/news/world/americas/us-politics/colonial-pipeline-gas-prices-white-house-b1845563.html) The Independent, and "are evaluating every action the Administration can take to mitigate the impact as much as possible."

In other words, it is possible. Disruption to the supply lines for potentially a full week, or more, could lead to supply problems for consumers, aviation, and the military -- especially if the security incident incites the former to panic-buy. Some gas stations have already begun running dry and panic buying has been reported (https://www.nytimes.com/2021/05/11/business/colonial-pipeline-shutdown-latest-news.html) in some areas.

On May 12, Colonial Pipeline said the company continues to "make forward progress in our around-the-clock efforts to return our system to service."

Additional lateral systems are now being operated manually to deliver supplies, with priority given to areas that are either not being supported by other fuel delivery services or currently experiencing shortages.

Over 50 members of staff are now walking or driving along over 5,000 miles of pipeline per day in addition to increased aerial patrols.

Since the pipeline system was taken offline, the company has delivered roughly 41 million gallons of fuel.

Colonial Pipeline is working with the US Department of Energy (DOE) to "evaluate market conditions" and deliver supplies to where they are needed most.

84 million gallons of fuel have been accepted from refineries for "deployment upon restart" of the firm's network.

On May 13, the company said (https://www.zdnet.com/article/colonial-pipeline-restarts-operations-brought-down-by-ransomware/) that operations had restarted, but it could take several days for the delivery supply chain to return to normal.

"Some markets served by Colonial Pipeline may experience, or continue to experience, intermittent service interruptions during the start-up period," Colonial Pipeline commented. "Colonial will move as much gasoline, diesel, and jet fuel as is safely possible and will continue to do so until markets return to

Manage Cookies

Have any agencies become involved?

FMCSA

To keep supplies flowing, the USDOT Federal Motor Carrier Safety Administration (FMCSA) issued a Regional Emergency Declaration (https://www.zdnet.com/article/pipeline-ransomware-attack-us-invokes-emergency-transport-rules-to-keep-fuel-flowing/) on Sunday 9, easing standard restrictions on the land transport of fuel and the permissible working hours of drivers.

"FMCSA is issuing a temporary hours of service exemption that applies to those transporting gasoline, diesel, jet fuel and other refined petroleum products to Alabama, Arkansas, District of Columbia, Delaware, Florida, Georgia, Kentucky, Louisiana, Maryland, Mississippi, New Jersey, New York, North Carolina, Pennsylvania, South Carolina, Tennessee, Texas and Virginia," the agency said (https://www.fmcsa.dot.gov/newsroom/fmcsa-responds-unanticipated-shutdown-colonial-pipeline).

The FBI

The US Federal Bureau of Investigation (FBI) is also aware of the incident. On May 10, the law enforcement agency said (https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks):

> "The FBI confirms that the Darkside ransomware is responsible for the compromise of the Colonial Pipeline networks. We continue to work with the company and our government partners on the investigation."

CISA

The Cybersecurity and Infrastructure Security Agency (CISA), together with the FBI, issued an alert (https://www.zdnet.com/article/fbi-cisa-publish-alert-on-darkside-ransomware/) warning organizations that DarkSide affiliates have "recently been targeting organizations across various CI sectors including manufacturing, legal, insurance, healthcare, and energy." Best practices and cybersecurity recommendations were also provided.

Who is DarkSide?

Manage Cookies

Sophos

DarkSide is a Ransomware-as-a-Service (RaaS) group (https://www.zdnet.com/article/darkside-the-ransomware-group-responsible-for-colonial-pipeline-cyberattack-explained/) that offers its own brand of malware to customers on a subscription basis. The ransomware is currently in version 2.

According to IBM X-Force (https://exchange.xforce.ibmcloud.com/collection/06d0917405c36ca91f5db1fe0c01d1ad), the malware, once deployed, steals data, encrypts systems using Salsa20 and RSA-1024 encryption protocols, and executes an encoded PowerShell command to delete volume shadow copies.

SecureWorks tracks them as Gold Waterfall (https://www.secureworks.com/research/threat-profiles/gold-waterfall) and attributes the group as a Russian-speaking past affiliate of the REvil ransomware RaaS service.

A decryptor for DarkSide malware on Windows machines was released by Bitdefender in January (https://www.zdnet.com/article/free-decrypter-released-for-victims-of-darkside-ransomware/) 2021. In response, the group said the decryptor was based on a key previously purchased and may no longer work as "this problem has been fixed."

Bitdefender told ZDNet that the decryption tool, unfortunately, does not work with the latest version of DarkSide malware.

"We're constantly working on new versions of our tools as cybercriminals fix vulnerabilities that make decryption possible," the firm added.

While believed to be relatively new to the ransomware scene, first spotted in the summer of 2020, DarkSide has already created a leak website used in double-extortion campaigns, in which victim companies are not only locked out of their systems, but also have their information stolen.

If these organizations refuse to pay up, stolen data may be published on the platform and made available to the public.

DarkSide isn't just content in making money from ransomware demands, however, as the group has indicated it will happily work with competitors or investors before leaks are published.

"If the company refuses to pay, we are ready to provide information before the publication, so that it would be possible to earn in the reduction price of shares," the group says.

Read on: **DarkSide explained: the ransomware group responsible for Colonial Pipeline cyberattack** (https://www.zdnet.com/article/darkside-the-ransomware-group-responsible-for-colonial-pipeline-cyberattack-explained/)

Perhaps unusually, however, DarkSide also appears to be trying to cultivate a Robin Hood and good-guy image -- stealing from the rich (the so-called 'big game' targets) and giving a portion of the criminal proceeds to charity.

Charities reportedly offered donations in stolen Bitcoin (BTC) have, so far, refused to accept them.

The RaaS service operators have also tried to distance themselves from the incident by vaguely implying it was a customer at fault and that the cyberattack doesn't fit the DarkSide ethos.

"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," DarkSide said on May 10. "Our goal is to make money, and not creating problems for society. We [will] introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future."

FireEye has released the results (https://www.zdnet.com/article/researchers-track-down-five-affiliates-of-darkside-ransomware-service/) of an investigation into DarkSide affiliates. Sophos says that the cybersecurity company has been called in at least five times to deal with suspected DarkSide infections and has published research on the group's typical attack methods and tools (https://news.sophos.com/en-us/2021/05/11/a-defenders-view-inside-a-darkside-ransomware-attack/).

What happens next?

As a group known to double-extort victims, Colonial Pipeline could be the next company to face the threat of the leak of data unless they give in to blackmail and pay the attackers. It may be, however, that DarkSide could choose not to pursue this usual tactic due to the aforementioned "social" problems caused by the ransomware.

Bloomberg says (https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown) that during the attack, over 100GB in corporate data was stolen in just two hours.

As of May 11, Colonial Pipeline has not been added to the DarkSide leak site.

On May 13, Bloomberg reported (https://www.zdnet.com/article/colonial-pipeline-paid-close-to-5-million-in-ransomware-blackmail-payment/) that the company paid a ransom demand of close to $5 million in return for a decryption key.

This appears to be one of the largest and most successful cyberattacks on a critical component of a country's infrastructure to date -- but it is not the first.

In February, a cyberattacker attempted to add dangerous levels of a chemical to a city in Florida's drinking water system (https://www.zdnet.com/article/hacker-modified-drinking-water-chemical-levels-in-a-us-city/), and back in 2016, the city of Kieve, in Ukraine, lost all power for an hour due to Industroyer malware (https://www.zdnet.com/article/industroyer-an-in-depth-look-at-the-culprit-behind-ukraines-power-grid-blackout/).

If the prospect of fuel shortages, the invoking of emergency powers, and the briefing of a president is anything to go by, we may see a more urgent review of cybersecurity procedures and practices in the US soon -- and perhaps the implementation of severe punitive actions to companies that do not maintain a strong security posture.

However, cyberthreats continue to evolve and, either way, this is unlikely to be the last time we see such severe social disruption caused by cyberattackers just in it for the money.

"This incident is not the first and will definitely not be the last, as US critical infrastructure spans across an entire continent and relies on engineers in remote places to log in and perform maintenance when needed," Bitdefender commented. "It is common for ransomware operators to probe networks for such points of entry or even to buy phished credentials to remote desktop instances that they can use to mount an attack. Critical infrastructure is becoming increasingly appealing to ransomware operators -- particularly those who are involved in Ransomware-as-a-Service schemes."

Update 13/5: On Wednesday, US President Biden signed an executive order (h

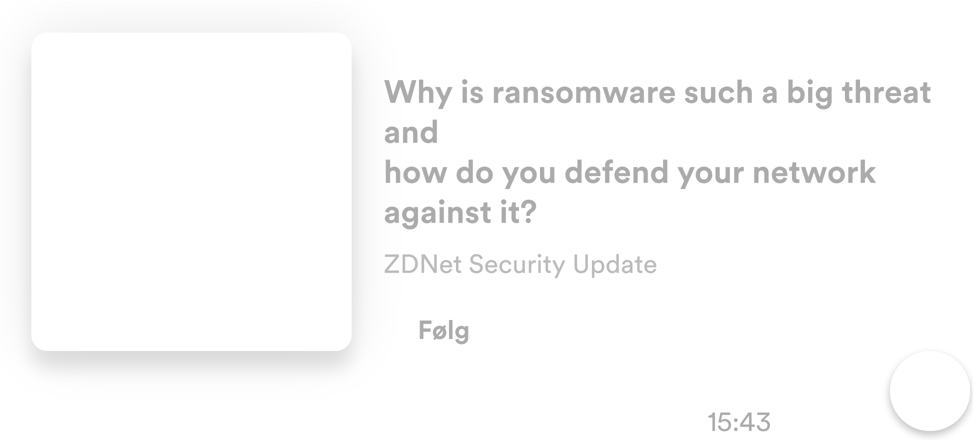
article/biden-signs-order-boosting-us-cyber-posture-saying-incremental-improvements-are-not-enough/)

to improve federal cybersecurity, noting that agencies need to "lead by example."

The order includes a shift to multi-factor authentication, data encryption both at rest and in transit, a zero-trust security model, and improvements in endpoint protection and incident response.

A Cybersecurity Safety Review Board will also be established.

"Incremental improvements will not give us the security we need; instead, the federal government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life," the order reads.



Why is ransomware such a big threat and
how do you defend your network against it?

ZDNet Security Update

Følg

15:43

PREVIOUS AND RELATED COVERAGE

- Ransomware just got very real. And it's likely to get worse (https://www.zdnet.com/article/ransomware-just-got-very-real-and-its-likely-to-get-worse/)
- Pipeline ransomware attack: US invokes emergency transport rules to keep fuel flowing (https://www.zdnet.com/article/pipeline-ransomware-attack-us-invokes-emergency-transport-rules-to-keep-fuel-flowing/)
- DarkSide explained: the ransomware group responsible for Colonial Pipeline cyberattack (https://www.zdnet.com/article/darkside-the-ransomware-group-responsible-for-colonial-pipeline-cyberattack-explained/)

Have a tip? Get in touch securely via WhatsApp | Signal at +447713 025 499, or over at Keybase: charlie0

MORE COVERAGE

Everything you need to know about the Colonial Pipeline attack (https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/)

Ransomware just got very real. And it's likely to get worse (https://www.zdnet.com/article/ransomware-just-got-very-real-and-its-likely-to-get-worse/)

S Manage Cookies **ng the guy next to you** (https://www.zdnet.com/article/ransomware-survive-by-outrunning-the-gu