**A Very Serious National Security Threat**

**Damage to any of our large energy networks will be very dangerous if they are disrupted in a time of crisis.**

The May 7, 2021 disruption to Colonial Pipeline illustrates how a foreign organization, purported to be merely a criminal ransomware hack, shut down a major energy pipeline for days even after a $4.4 million dollar ransom was paid immediately. 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. The decrypto keys provided to Colonial computer managers did not return full function to the network.

The Colonial Pipeline Company supplied gasoline, diesel, and jet fuel for civilian and government organizations from the Gulf Coast to New Jersey. Most gas stations ran out of gas in Washington D.C., and several states served by Colonial. Even our military stations, including Andrews AFB could not be serviced with fuel.

This created a mini-crisis when we were not in a major crisis. Had it occurred during a time of crisis, the harm could have been enormous.



**The Colonial Energy Network**

Who was responsible?

The FBI confirms that the **Darkside** ransomware is responsible for the compromise of the Colonial Pipeline network. DarkSide is a group believed to have been active since the summer of 2020. **DarkSide**'s malware is offered under a Ransomware-as-a-Service (RaaS) model, and once a system has been breached, ransomware payment demands can range from $200,000 to $2,000,000.

Over 100 billion bytes of data was stolen that revealed data from civilian d government clients of Colonial Pipeline.

**DarkSide** is either Russian or East European based organization. The criminal organization alleges it donates a small part of its ransom booty to charities. It claims no affiliation with any government which gives some plausible denial to Vladimir Putin.

It is logical to assume that these operations are in fact blessed or supported by the Kremlin (or maybe some other enemy). The magnitude of real and potential damage to America has occurred, and this is exactly what Putin wants for revenge for our economic sanctions. We have known of Russian, (and to a lesser degree, Chinese) digital probes of our utilities for several years.

These threatening hacks require a strong response from us, but we might be holding back and not reveal our capabilities, as playing our hand now, will give any opposition to develop a defense for our offensive capabilities. We demonstrated some of our offensive capabilities in the Stuxnet cyber operation against Iran in 2010.

===========================================================

[***https://www.zdnet.com/article/darkside-the-ransomware-group-responsible-for-colonial-pipeline-cyberattack-explained/***](https://www.zdnet.com/article/darkside-the-ransomware-group-responsible-for-colonial-pipeline-cyberattack-explained/)

**DarkSide explained: The ransomware group responsible for Colonial Pipeline attack**

**Updated: The group's existence is tied to a murky web of shorted stocks, criminality, and failed attempts to appear as Robin Hood.**

By Charlie Osborne for Zero Day | May 14, 2021 -- 12:05 GMT (05:05 PDT) | Topic: Security

When speaking to a cybersecurity expert concerning the Microsoft Exchange Server vulnerabilities several months ago and its impact on thousands of organizations worldwide, they asked, "What could possibly be worse this year?"

Perhaps the situation the United States found itself this week, with a major pipeline down due to ransomware, comes close.

Colonial Pipeline, which supplies 45% of the East Coast's fuel, revealed a ransomware outbreak on the company's systems which forced the suspension of operations and some IT systems last Friday, as previously reported by ZDNet.

Nearly a week following the May 7 attack, Colonial Pipeline restarted operations. The company said it will take "several days" for the pipeline's deliveries to return to normal.

Data breaches and security incidents taking place at enterprise organizations are commonplace and hardly a week goes by when we don't hear of yet another cyberattack on a well-known company -- but when core, critical utilities and country infrastructure is involved, things take an even more serious turn.

Colonial Pipeline says that a system restart plan is being "developed" and some small lateral lines are back in service. However, it may be days before full functions are restored, and in the meantime, gasoline futures are rising and there is concern that some parts of the US may experience fuel shortages.

Gasoline futures jumped to their highest level in three years due to the cyberattack.

Deploy solutions faster, more securely and at lower operational expense with IBM Cloud hosting services. Customize your server to meet your needs and get up to 20TB BW included.

**White Papers provided by IBM**

The USDOT Federal Motor Carrier Safety Administration (FMCSA) agency has issued a Regional Emergency Declaration to try and push back against the supply disruption through temporary exemptions for fuel transport on the road and the permissible hours that drivers are allowed to work for. The FBI said on May 10 that the agency is working with Colonial to investigate the incident.

But who is responsible? According to the FBI, the DarkSide ransomware group.

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

DarkSide is a group believed to have been active since the summer of 2020. DarkSide's malware is offered under a Ransomware-as-a-Service (RaaS) model, and once a system has been breached, ransomware payment demands can range from $200,000 to $2,000,000.

The group has previously been connected to "big game" hunting methods, in which large organizations are targeted -- which would fit with the Colonial Pipeline incident.

Other cybercriminal organizations follow the same path, including Hades ransomware operators, which appear to specifically target companies with annual revenue of at least $1 billion.

DarkSide 2.0, the latest version of the ransomware, was recently released under an affiliates program. According to FireEye, affiliates are required to pay up to 25% of ransom payments under $500,000, and 10% of any successful extortion attempts over $5 million.

===========================================

[***https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/***](https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/)

**Colonial Pipeline attack: Everything you need to know**

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

Charlie Osborne

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 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, 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 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, 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 decisions, and the 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?**



**Colonial-pipeline-system-map.jpg**

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 level in three years. 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 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.

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 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 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 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 normal."

Have any agencies become involved?

**FMCSA**

To keep supplies flowing, the USDOT Federal Motor Carrier Safety Administration (FMCSA) issued a Regional Emergency Declaration 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.

**The FBI**

The US Federal Bureau of Investigation (FBI) is also aware of the incident. On May 10, the law enforcement agency said:

"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 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?**

DarkSide is a Ransomware-as-a-Service (RaaS) group 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, 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 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 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.

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 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.

**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 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 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, and back in 2016, the city of Kieve, in Ukraine, lost all power for an hour due to Industroyer malware.

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 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.

===================================

**Colonial Pipeline paid close to $5 million in ransomware blackmail payment**

The payment was reportedly made soon after the attack began. It wasn’t enough to stop the disruption.

Colonial Pipeline reportedly paid the ransomware group responsible for a cyberattack last week close to $5 million to decrypt locked systems.

On Thursday, Bloomberg reported that two people close to the matter said a blackmail demand was agreed to within hours of the cyberattack that has impacted the fuel giant's systems for close to a week.

On May 7, Colonial Pipeline experienced a ransomware attack which forced the company to temporarily close down its operations and freeze IT systems to isolate the infection.

However, the decryptor was reported to be "so slow" that backups were also used in restoration efforts.

Meet The Infrastructure For Smarter Business

Find the right IaaS solutions for your business requirements. Deploy, control and manage your workloads in more than 60 IBM Cloud Data Centers.

White Papers provided by IBM

The cyberattack was the work of DarkSide, a ransomware-as-a-service (RaaS) outfit. The DarkSide ransomware variant is provided to affiliates who sign up, and in return, partner groups give the malware's developers a slice of any profits made through successful ransomware extortion attempts.

DarkSide affiliates may also use double-extortion tactics, in which corporate files are also stolen during an attack. If a company refuses to pay up to decrypt their systems, they are then threatened with the public leak of stolen data.

FireEye researchers say that DarkSide's developers take a profit cut of 25% for ransom payments under $500,000, and this reduces to 10% for payments made over $5 million.

The FBI and Cybersecurity and Infrastructure Security Agency (CISA) issued an alert this week warning businesses of the ongoing threat of RaaS operations. Federal agencies do not condone paying ransom demands made by cybercriminals.

According to Reuters, Colonial Pipeline has cyber insurance coverage of at least $15 million.

On Thursday, the organization said in an update that it "has made substantial progress in safely restarting our pipeline system and can report that product delivery has commenced in a majority of the markets we service."