Colonial Pipeline cyber attack

- Name: Aravinth TM
- Registration Number: 19BCE7415

Supervisory control And Data Acquisition(SCADA) systems monitor and control infrastructure like nuclear power plants, municipal drinking water systems, gas pipelines and power grids. They are notorious for running outdated, vulnerable software and are easy targets for cyber criminals.

On May 7, 2021, an American oil pipeline system situated in Houston, Texas came under a ransomware attack. It's responsible for ferrying gas and jet fuel to Southeastern parts of the US. The Colonial Pipeline Company company paid the 75 bitcoin ransom to restore operations of the pipeline. This amount was partially recovered after the criminal group called DarkSide's servers were seized.

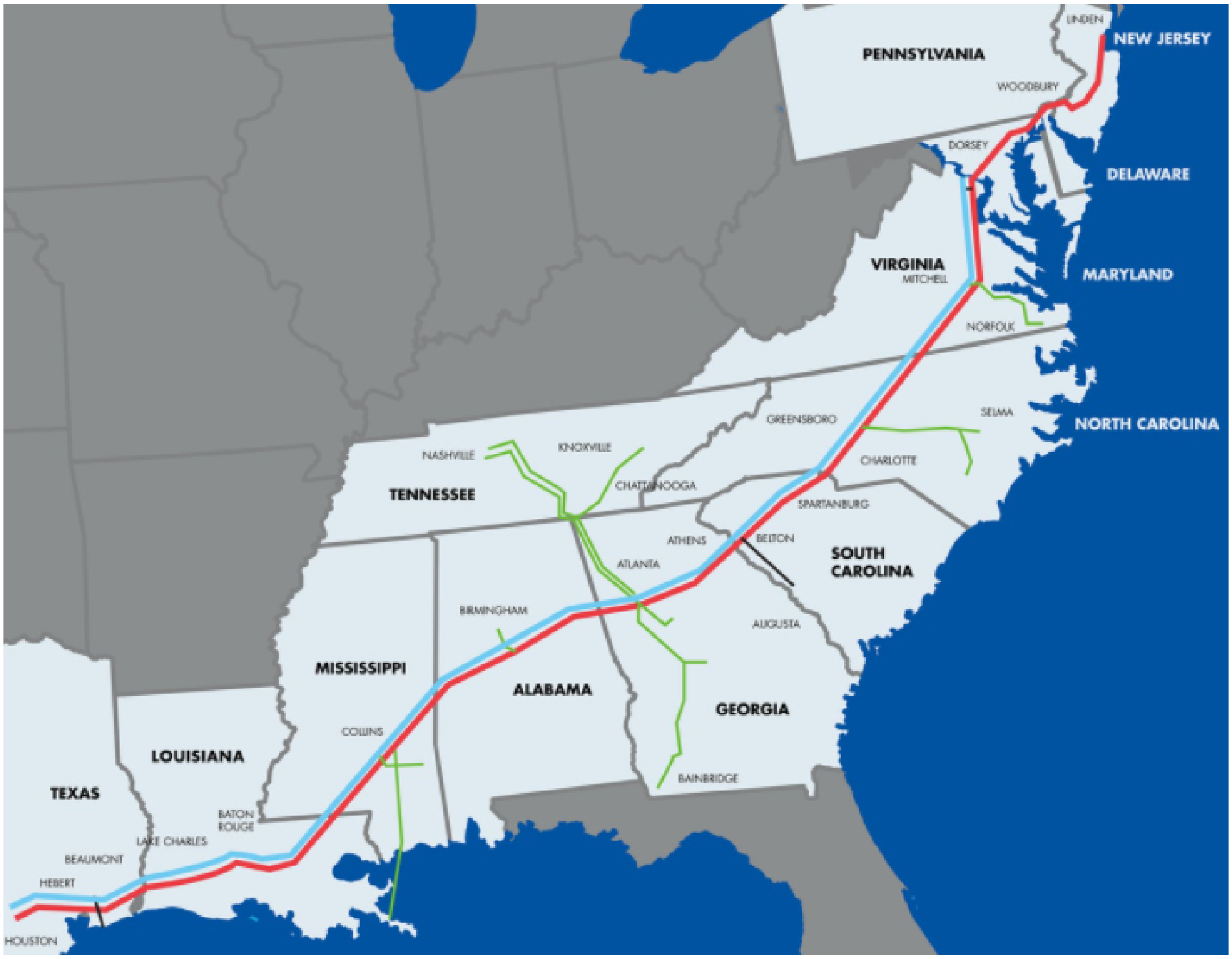
It is believed that the attacker stole 100 GB of data from company servers before the attack.

Impact

The company's payment infrastructure was compromised while the operational technology systems remained functional. Due to this, the company wasn't able to process payments so they decided to halt the pipeline operation.

A fuel shortage situations resulted in airports that were serviced by the pipeline company several airline companies had to change their flight schedule.

Average fuel prices rose to their highest since 2014, reaching more than $3 a gallon.

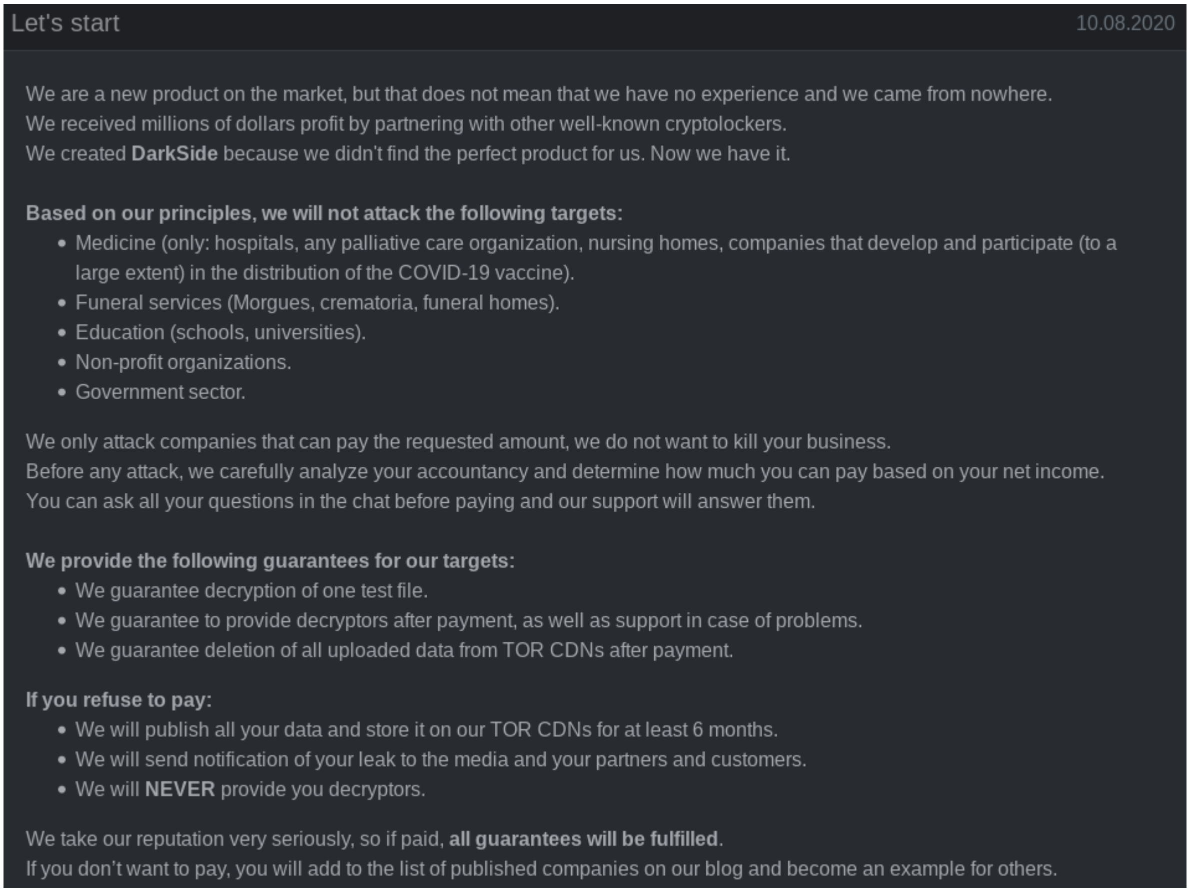


Colonial Pipeline coverage

This cyber attack is very new and forensics are just getting started. The rest of the report will focus on how DarkSide functions.

DarkSide's modus operandi

- DarkSide's doesn't have a nation state backing them, they are a randomware gang.
- They are apolitical: their actions are monetary rewards
- Their behaviour is inline with other ransomware gangs: 1. They encrypt their victims data 2. They steal their victims data And hold their victims ransom for both of them in different stages and there by committing double extortion.



Let's start 10.08.2020

We are a new product on the market, but that does not mean that we have no experience and we came from nowhere.
We received millions of dollars profit by partnering with other well-known cryptolockers.
We created **DarkSide** because we didn't find the perfect product for us. Now we have it.

Based on our principles, we will not attack the following targets:

- Medicine (only: hospitals, any palliative care organization, nursing homes, companies that develop and participate (to a large extent) in the distribution of the COVID-19 vaccine).
- Funeral services (Morgues, crematoria, funeral homes).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the requested amount, we do not want to kill your business.
Before any attack, we carefully analyze your accountancy and determine how much you can pay based on your net income.
You can ask all your questions in the chat before paying and our support will answer them.

We provide the following guarantees for our targets:

- We guarantee decryption of one test file.
- We guarantee to provide decryptors after payment, as well as support in case of problems.
- We guarantee deletion of all uploaded data from TOR CDNs after payment.

If you refuse to pay:

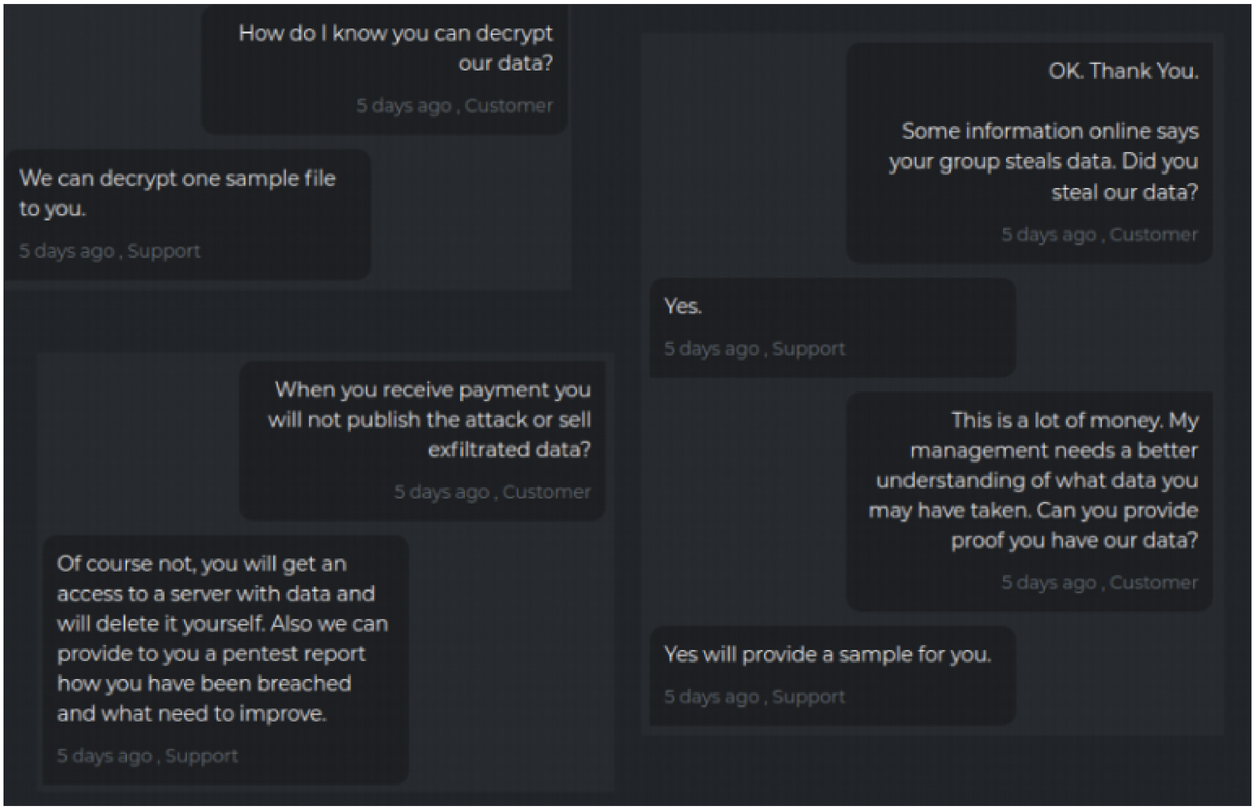
- We will publish all your data and store it on our TOR CDNs for at least 6 months.
- We will send notification of your leak to the media and your partners and customers.
- We will **NEVER** provide you decryptors.

We take our reputation very seriously, so if paid, **all guarantees will be fulfilled**.
If you don't want to pay, you will add to the list of published companies on our blog and become an example for others.

DarkSide philosophy

- The DarkSide core team is believed to be originated from an othe ransomeware gang called "REvil" so they share similar modus operandi

DarkSide infrastructure's and modus operandi is sophisticated. They have dedicated support teams and payment systems.



How do I know you can decrypt our data?

5 days ago , Customer

We can decrypt one sample file to you.

5 days ago , Support

When you receive payment you will not publish the attack or sell exfiltrated data?

5 days ago , Customer

Of course not, you will get an access to a server with data and will delete it yourself. Also we can provide to you a pentest report how you have been breached and what need to improve.

5 days ago , Support

OK. Thank You.

Some information online says your group steals data. Did you steal our data?

5 days ago , Customer

Yes.

5 days ago , Support

This is a lot of money. My management needs a better understanding of what data you may have taken. Can you provide proof you have our data?

5 days ago , Customer

Yes will provide a sample for you.

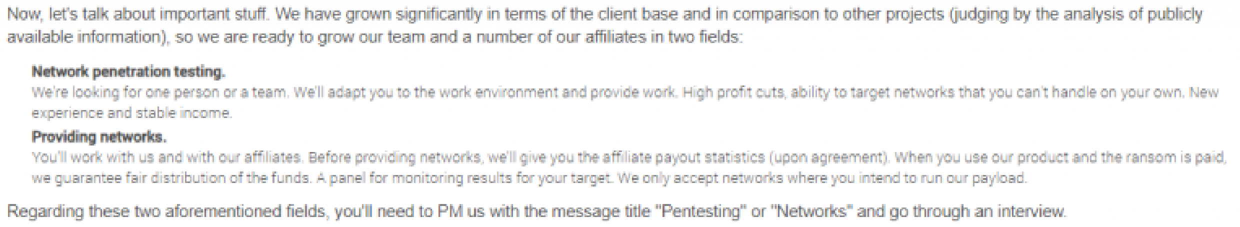
5 days ago , Support

DarkSide support team

They also take part “ransomware as a service”, which as the name suggests, helps other cyber criminal groups to offload certain aspects of the attack to ransomware specialists. This offering includes:

- customer support for both the victim and the criminal group
- payments gateway access with money laundering capabilities
- Tor based CDNs to distribute stolen data.

DarkSide also claims to be “growing” and as a result is looking to contract independent cyber criminals to assist them with their criminal endeavours.



Now, let's talk about important stuff. We have grown significantly in terms of the client base and in comparison to other projects (judging by the analysis of publicly available information), so we are ready to grow our team and a number of our affiliates in two fields:

Network penetration testing.
We're looking for one person or a team. We'll adapt you to the work environment and provide work. High profit cuts, ability to target networks that you can't handle on your own. New experience and stable income.

Providing networks.
You'll work with us and with our affiliates. Before providing networks, we'll give you the affiliate payout statistics (upon agreement). When you use our product and the ransom is paid, we guarantee fair distribution of the funds. A panel for monitoring results for your target. We only accept networks where you intend to run our payload.

Regarding these two aforementioned fields, you'll need to PM us with the message title "Pentesting" or "Networks" and go through an interview.

Job listing:

“There is huge insider information on the companies which we target, including information if there are tape drives and clouds (for example, Datto that is built to last, etc.), which significantly affects the scale of the conversion rate.

Requirements: – experience with cloud storage, ESXi. – experience with Active Directory. – privilege escalation on accounts with limited rights.

- Serious level of insider information on the companies with which we work. There are proofs of large payments, but only for verified LEADs.
- There is also a private MEGA INSIDE , which I will not write about here in public, and it is only for experienced LEADs with their teams.
- We do not look at REVENUE / NET INCOME / Accountant reports, this is our MEGA INSIDE, in which we know exactly how much to confidently squeeze to the maximum in total

Earlier, a cyber criminal's activities can be tracked with the money trail that they leave behind or their unique signature in the way they interact with the world but the trade of expertise among cyber criminals will both increase the lethality of cyber attacks and eliminate traditional avenues of forensic investigation. This is going to become characteristic of future cyber attacks.

How to protect against ransomware attacks?

1. SCADA systems should be isolated: systems that don't require a network to function should be taken off the network.

2. Use VPNs to implement access control: Access control is hard to implement. Private companies already follow this mechanism to isolate their private infrastructure from the larger internet. Rather than rolling out their own access control mechanism, they offload it to standardised VPN software like Wireguard, which offers cryptographically sound and fine grained access control mechanisms.

3. Regular backups: Post infection, ransom payment can be avoided if the organisation has current, functional backups. They could simple wipe their systems clean and restore it from backups.

4. Policy creation: policies must be created beforehand to deal with data leaks, ransomware attacks and other kinds of security breaches so first responders will have a framework to work from. This results in a more effective response that is well organised.