

# New Evidence Supports Assessment that DarkSide Likely Responsible for Colonial Pipeline Ransomware Attack; Others Targeted

[securityscorecard.com/blog/new-evidence-supports-assessment-that-darkside-likely-responsible-for-colonial-pipeline-ransomware-attack-others-targeted](https://securityscorecard.com/blog/new-evidence-supports-assessment-that-darkside-likely-responsible-for-colonial-pipeline-ransomware-attack-others-targeted)



## Executive summary

On May 7, 2021, Colonial Pipeline issued a statement that, due to a cyber-attack, they had partially shut down operations of their pipeline that supplies almost 50% of gasoline to the eastern United States. The press later confirmed that the attack included ransomware. The FBI stated on May 10, 2021, that the DarkSide ransomware group -- also known as Carbon Spider -- was responsible for the attack.

SecurityScorecard conducted an analysis of the attack analyzing NetFlow data (data associated with data transfers on the Internet) and determined that a large amount of data was exfiltrated from Colonial Pipeline networks to IP addresses also associated with other ransomware attacks for which Carbon Spider has previously taken responsibility. Through this analysis, combined with identifying and deconstructing associated malware and correlation with other known victims, SecurityScorecard can confirm with moderate confidence that DarkSide also known as Carbon Spider was responsible for the Colonial Pipeline attack and potentially other ransomware attacks.

## Key findings

- 
- Through an ongoing investigation, SecurityScorecard has found with a moderate confidence level that the DarkSide ransomware group, also known as Carbon Spider, transferred data from Colonial Pipeline on May 6, 2021, to an external IP address, one day prior to public reports.
  - Through SecurityScorecard's analysis, we have identified other organizations that Carbon Spider has already claimed to have attacked as well as others that have not been previously identified.
  - SecurityScorecard's research indicates that Carbon Spider exfiltrated data from the Colonial Pipeline network likely for use in an extortion attempt, just as we see with many other ransomware groups.
  - SecurityScorecard did not find any evidence of direct disruption of the critical infrastructure owned and operated by Colonial Pipeline. However, it is plausible that Carbon Spider caused damage to other parts of the Colonial Pipeline network. DarkSide ransomware is designed to encrypt files that are often irreversible without a decrypter from the authors.
  - SecurityScorecard observed that this group has been operating since August 2020 through dark web leak postings.
  - The attribution analysis was made based on publicly available data in both clearweb and open access to dark web sources.

## Background

---

The DarkSide ransomware group, also known as Carbon Spider, is suspected to have breached Colonial Pipeline (Colonial). Carbon Spider is a Russian criminal group focused on developing and using DarkSide ransomware. This group follows a traditional Advanced Persistent Threat (APT) like pattern of intrusion (i.e. gain access to a network through a known vulnerability, perform reconnaissance within the network and identify targeted data for encryption/exfiltration) that we have seen in other targeted attacks. The following is an intelligence assessment from SecurityScorecard's Investigations & Analysis team.

## Investigation

---

Reviewing the techniques, tactics, and procedures used by this attacker, the threat actor utilized Cobalt Strike amongst many other tools. Cobalt Strike is a tool frequently used by Russian APTs and criminal groups involved in the distribution of ransomware. The Cobalt Framework is considered a file-less implant (residing in memory) of the infected victim and allows for the attacker to introduce additional malware.

SecurityScorecard's Investigations & Analysis team focused on understanding the actor's capability and intent. SecurityScorecard found that over 80GB of data was transferred from the Colonial Pipeline network to an external IP address. Based on our observations the actor exfiltrated data from the victim's network likely in an extortion attempt, like many other ransomware groups.

SecurityScorecard did not observe any evidence of direct disruption of the critical infrastructure owned and operated by Colonial that resulted in the shutdown of the pipeline. However, it is plausible that DarkSide caused damage to systems in parts of their network, as DarkSide is designed to encrypt files on disk which are often unrecoverable without a decrypter from the authors.

Additionally, using NetFlow analysis, the Investigations & Analysis team observed details around data exfiltration to understand connections made between the victim's network and the adversary's infrastructure. NetFlow data is similar to call detail records which record time, duration, routing details between phones, but not the content of the conversation. NetFlow data shows which IP addresses were connected, the Transmission Control Protocol (TCP) port that was used, and the number of packets and bytes that were transmitted. This is a key element of SecurityScorecard's investigation as it provides critical insight into victimology and enables us to link it back to Carbon Spider. NetFlow, like call detail records, does not include content of the transmission so we were unable to view the data exfiltrated. However, we can assume the data will be used to extort the victim. It is possible that sensitive data stolen from Colonial could make its way to Carbon Spider's leak site if the company does not pay.



## Get your instant security score

[Learn More](#)



### Malicious infrastructure

---

Using SecurityScorecard's in-house analysis methods, we were able to extract several configuration files relating to Cobalt Strike that provided additional insight into the adversaries' infrastructure. In any incident response investigation, understanding the infrastructure used by the threat actor will enable the discovery of additional indicators of compromise (IOC). Upon infecting victims a ransomware note is left on the victim's PC with instructions for payment.

```

----- [ Welcome to DarkSide ] ----->

What happend?
-----
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.
Follow our instructions below and you will recover all your data.

Data leak
-----
First of all we have uploaded more then 30GB data.

These files include:
- Accounting
- Finance
- Internal documents
- Insurance

Your personal leak page: http://darksidedxkcftrmga.onion/blog/article/id/88/EbDvhFDs\_z2hYxVROXHv4S3ZzHUrKh4rqa3bgZ44Qq-ORPqEAqM1zoTDuM46leXv
On the page you will find examples of files that have been downloaded.
The data is preloaded and will be automatically published if you do not pay.
After publication, your data will be available for at least 6 months on our tor cdn servers.

We are ready:
- To provide you the evidence of stolen data
- To delete all the stolen data.

What guarantees?
-----
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
We guarantee to decrypt one file for free. Go to the site and contact us.

How to get access on website?
-----
Using a TOR browser:
1) Download and install TOR browser from this site: https://torproject.org/
2) Open our website: http://darksidfgzcuhtk2.onion/KB0LXKYKN6E96Z7RFYWCEI6NM03TX93VZCL5EDA4IVFXUIQQ2BG22EG2692IFSFM

When you open our website, put the following data in the input form:
Key:
9mMrqcP7meAPxAvXF250NPJ4KqIozRuGzFKqvsN4XCuThdV2qteuONtFOu4gYqMxwUx5wELPmbMsI2CcmFySRZJDqPLc8rvxUGJg12wu2ki8EizCFaGSL8oQIfgOCvMrTkxmSmVhcSjQ

!!! DANGER !!!
DO NOT MODIFY or try to RECOVER any files yourself. We WILL NOT be able to RESTORE them.
!!! DANGER !!!

```

## DarkSide Ransom Note

From a malicious infrastructure perspective, there are several elements involved in this attack.

- Data exfiltration IPs
- Cobalt Strike beacons

## Cobalt strike beacons

Of the domains and IPs reported by the FBI, the following are verified to be active at the time of this writing:

- Openmsdn[.]xyz
- 45.153.184[.]167
- Security-desk[.]com
- 213.252.247[.]18

Beacon DLLs can be injected into the following legitimate Windows processes:

- Rundll32.exe
- svchost.exe

Hashes for these DLLs are:

- c1b288c1426bac664c6df61c10367ff71704213a
- 05233911465a0131ce15115df4807d8cd3024fd9
- 4bba9fc4a3b09cb8d3c206c9d8f5d5a6e9ec226c
- 535bb593b64b1c91327df657d776a573a8afc3f7
- Ee82c429fb3db89a61a222abe6458b604c3644a6
- bfb9a58aaba4198fc189e44bdcf397453efebdec

Possible User-agents these DLLs will use are:

- Mozilla/5.0 (Linux; Android 8.0.0; SM-G960F Build/R16NW) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202
- Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0; MDDCJS)

These DLLs were found to have a heartbeat of:

- 60 +/- 0 seconds
- 59.290 +/- 22 seconds

```

] {
  "BeaconType": ["HTTPS"],
  "Port": 443,
  "SleepTime": 59290,
  "MaxGetSize": 1864740,
  "Jitter": 37,
  "MaxDNS": "Not Found",
  "PublicKey": "MIGfMA0GCSSqGSIb3DQEBAQUAA4GNADCBiQKBgQCFZx4kHSYdbimHECW7YugZlTqERDzUuUKCL
  "PublicKey_MD5": "96d31d30b4462635e6aae706172aaf49",
  "C2Server": "security-desk.com,/posting",
  "UserAgent": "Mozilla/5.0 (Linux; Android 8.0.0; SM-G960F Build/R16NW) AppleWebKit/537.
  "HttpPostUri": "/templates",
  "Malleable_C2_Instructions": ["Remove 600 bytes from the beginning", "Base64 decode", "
  "HttpGet_Metadata": {
    "ConstHeaders": ["Connection: close", "Accept: image/*"],
    "ConstParams": ["grant=true"],
    "Metadata": ["mask", "base64", "prepend \"wordpress_logged_in=\\\"", "header \"Cookie
    "SessionId": [],
    "Output": []
  },
  "HttpPost_Metadata": {
    "ConstHeaders": ["Connection: close", "Accept-Language: en-GB;q=0.9, *;q=0.7", "Con
    "ConstParams": [],
    "Metadata": [],
    "SessionId": ["base64", "prepend \"__session_id=\\\"", "header \"Cookie\\\"",
    "Output": ["netbios", "base64", "prepend \"grant=\\\"", "print"]
  }
}

```

*Cobalt Strike beacon configuration*

## Malicious C2 server

The FBI reported on May 10, 2021, that IP address 159.65.225.72 is affiliated with the DarkSide ransomware group as a data exfiltration destination. The address is hosted in DigitalOcean, an American cloud provider, in AS14061 within their NYC region. As of the last

SecurityScorecard scan on May 5, 2021, the only service running on the C2 IP was SSH (port 22). Our NetFlow analysis demonstrates that SSH was used as the data exfiltration method.

## Data exfiltration

---

SecurityScorecard can confirm reports in both media and by the FBI that the adversary was present in the Colonial Pipeline environment. We were able to identify a connection between the Colonial Pipeline network and a malicious asset associated with Carbon Spider.

The Investigations & Analysis team identified a connection between the victim's IP (198.154.26.212) and IP address 159.65.225.72, as mentioned above to be associated with the DarkSide ransomware group by the FBI. Our investigation confirmed the connection by cross-referencing the IPs with NetFlow data from our datasets. Based on our analysis at least 80GB+ of data was exfiltrated from Colonial and sent to the adversary between GMT: Thursday, 6 May 2021 10:31:22 and GMT: Thursday, 6 May 2021 12:22:20.

## Victimology

---

Beyond Colonial Pipeline, there are additional suspected victims of DarkSide ransomware that SecurityScorecard has identified based on NetFlow analysis.

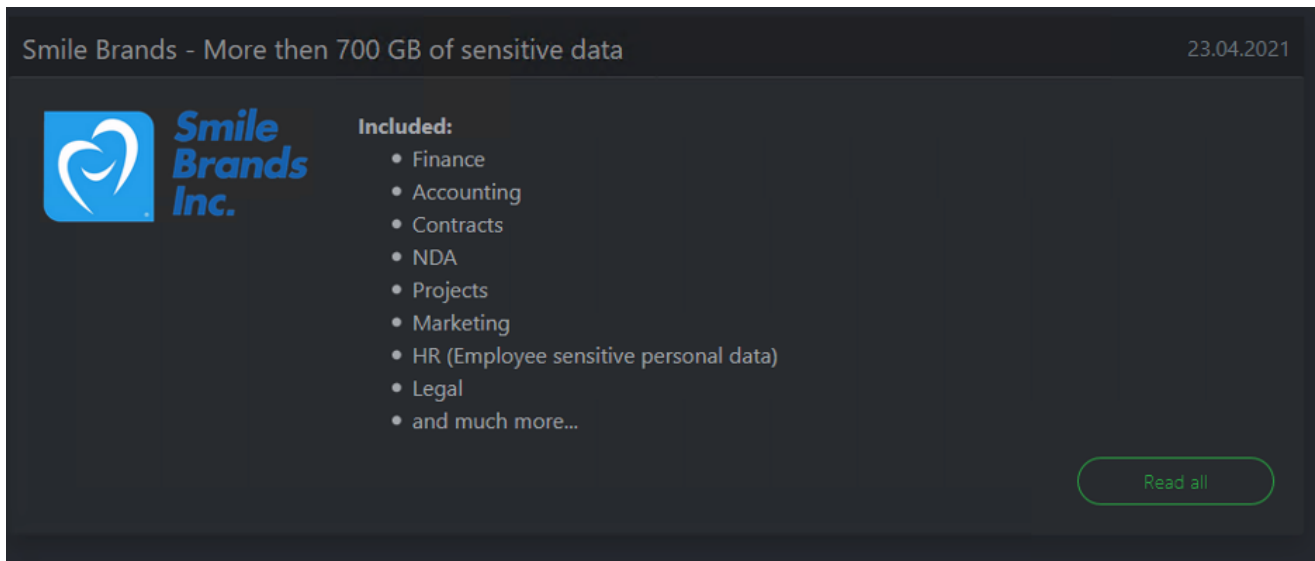
## Potential other victims

---


Victim	Date	Data Transfer
Large Retailer	5/6/2021	2117GB
Dedicated Cloud Solutions Provider	5/5/2021	1129GB
<u>Smilebrands</u>	4/24/2021	451GB
<u>Colonial Pipeline</u>	5/6/2021	87GB
Large Distribution Company	4/27/2021	50GB
Cloud Platform Provider	4/27/2021	117GB
<u>Homehardware</u>	2/18/2021	84GB

The attacker utilized the server in DigitalOcean to exfiltrate data from a number of entities, including Colonial Pipeline. Some of these addresses correlate with victims found on the

threat actor's own leak site, but others have not previously been identified as victims.



Smile Brands - More than 700 GB of sensitive data 23.04.2021

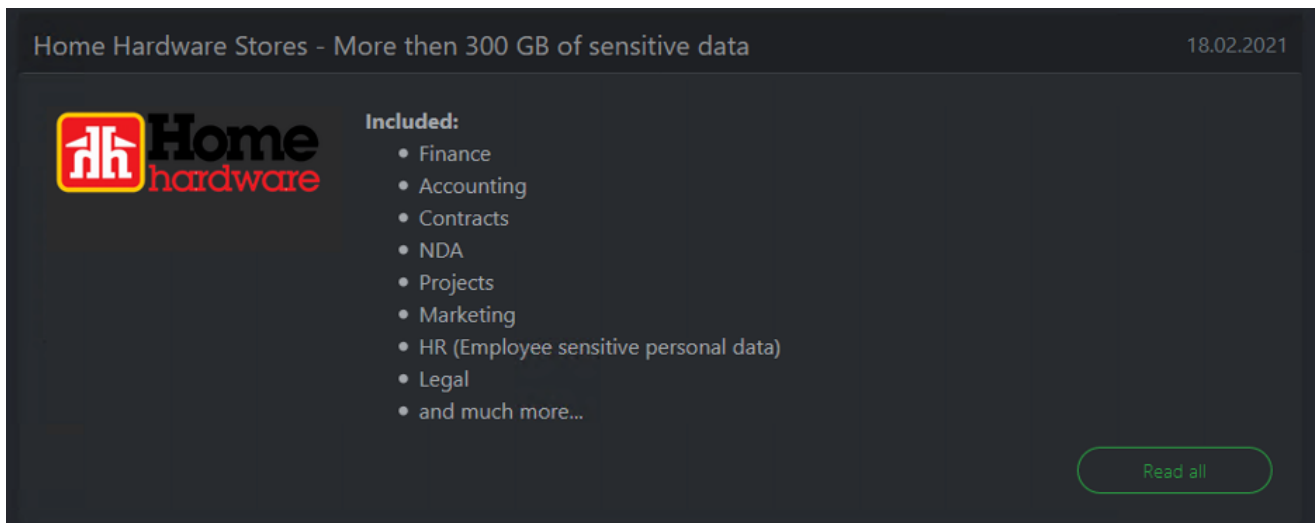
 **Smile Brands Inc.**

**Included:**


- Finance
- Accounting
- Contracts
- NDA
- Projects
- Marketing
- HR (Employee sensitive personal data)
- Legal
- and much more...

[Read all](#)

*SmileBrands leaked on TOR site*



Home Hardware Stores - More than 300 GB of sensitive data 18.02.2021

 **Home hardware**

**Included:**

- Finance
- Accounting
- Contracts
- NDA
- Projects
- Marketing
- HR (Employee sensitive personal data)
- Legal
- and much more...

[Read all](#)

*Homehardware*

To find potential victims, SecurityScorecard collected the unique IP addresses that communicated with the data exfiltration IP address on port 22 and had more than 1000 packets in the past three months. Some IP addresses communicated with the data exfiltration server for an unusually long period of time compared to Colonial, where the data was exfiltrated in 2 hours. We suspect those IP addresses may have been used by the attackers reviewing and downloading the data exfiltrated from victims' networks. We have also observed many IP addresses that have very few flows, which might suggest attackers could have used proxies to connect to the data exfiltration servers.

- DarkSide has stored their leaked data here
  - 542lsflqr4hgurjx.onion
  - Ru4rkIde4l4sgghf.onion
  - Erc4xzvrchka5izw.onion
  - lxltdyumdlthrtgx.onion
  - Fylszpcqfel7joif.onion
  - Gtmx56k4hutn3ikv.onion
  - hxt254aygrsziejn.onion
- DarkSide Ransomware [press site](#)

## Attribution

---

Attribution is often difficult and requires much analysis to attribute any cyber-attack to a specific group with any degree of certainty. SecurityScorecard concludes, because of the Analysis of Competing Hypotheses below, that the most likely scenario is that Carbon Spider conducted the attack. Our analysis supports the hypothesis, based on the correlation of NetFlow data with reported victims in the Carbon Spider’s leak site, that the Colonial Pipeline attack was conducted by this adversary.

SecurityScorecard can also confirm the Colonial Pipeline attack involves DarkSide ransomware and not another family of malware.

## Analysis of completing hypothesis (in progress)

---

In intelligence analysis, we use a model known as the analysis of competing hypotheses. This is a model designed to rank evidence against multiple hypotheses; in this case, we had several likely scenarios connected with this incident.

Evidence	Hypothesis 1	Hypothesis 2	Hypothesis 3	Hypothesis 4	Hypothesis 5
Evidence points	Was DarkSide Ransomware gang responsible for the Colonial breach?	Was another Ransomware actor responsible for the breach?	Was the APT actor responsible for the breach?	Is this a false flag operation, masquerading as a Ransomware group (cover for APT operation)	A DarkSide RAAS affiliate is responsible for this breach.



---

DarkSide Ransomware news leak site indicates they do not wish to cause problems in society

Is this a false flag operation, masquerading as a Ransomware group?

A DarkSide RAAS affiliate is responsible for this breach.

---

OSINT reporting is indicating DarkSide Ransomware group is responsible.

Was DarkSide Ransomware gang responsible for the Colonial breach?

---

FBI Confirms DarkSide was behind the Colonial according to Chris Bing.

Was DarkSide Ransomware gang responsible for the Colonial breach?

Download the blog post as a PDF.

[Download](#)