What We Know About the DarkSide Ransomware and the US Pipeline Attack

May 12, 2021

Updated May 17, 2021, 3:25 a.m. Eastern Time: This article has been updated to add references to the DarkSide victim data.

On May 7, a ransomware attack forced Colonial Pipeline, a company responsible for nearly half the fuel supply for the US East Coast, to proactively shut down operations. Stores of gasoline, diesel, home heating oil, jet fuel, and military supplies had been so heavily affected that the Federal Motor Carrier Safety Administration (FMCSA) declared a state of emergency in 18 states to help with the shortages.

It has been five days since the shutdown prompted by the attack, but Colonial Pipeline is still unable to resume full operations. Outages have already started affecting motorists. In metro Atlanta, 30% of gas stations are without gasoline, and other cities are reporting similar numbers. To keep supplies intact for essential services, the US government has issued advisories against hoarding.

The FBI has confirmed that DarkSide, a cybercriminal group believed to have originated in Eastern Europe, is behind the attack. The ransomware used by the group is a relatively new family that was first spotted in August 2020, but the group draws on experience from previous financially successful cybercrime enterprises.

Apart from locking Colonial Pipeline's computer systems, DarkSide also stole over 100 GB of corporate data. This data theft is all the more relevant in light of the fact that the group has a history of doubly extorting its victims — not only asking for money to unlock the affected computers and demanding payment for the captured data, but also threatening to leak the stolen data if the victims do not pay. As we will cover later, DarkSide shows a level of innovation that sets it apart from its competition, being one of the first to offer what we call "quadruple extortion services."

The group announced on May 12 that it had three more victims: a construction company based in Scotland, a renewable energy product reseller in Brazil, and a technology services reseller in the US. The DarkSide actors claimed to have stolen a total of 1.9 GB of data from these companies, including sensitive information such as client data, financial data, employee passports, and contracts.

Since Darkside is a ransomware-as-a-service (RaaS), it is possible that three different affiliate groups are behind these three attacks. Even the DarkSide actors themselves admit that they just buy access to company networks — they have no idea how access was acquired.

Trend Micro Research found dozens of DarkSide ransomware samples in the wild and investigated how the ransomware group operates and what organizations it typically targets.

The DarkSide ransomware

DarkSide offers its RaaS to affiliates for a percentage of the profits. The group presents a prime example of modern ransomware, operating with a more advanced business model. Modern ransomware identifies high-value targets and involves more precise monetization of compromised assets (with double extortion as an example). Modern ransomware attacks are also typically done by several groups who collaborate and split profits. These attacks may look more like advanced persistent threat (APT) attacks than traditional ransomware events.

Here is a short timeline of DarkSide activity compiled from publicly available reports:

- August 2020: DarkSide introduces its ransomware.
- October 2020: DarkSide donates US$20,000 stolen from victims to charity.
- November 2020: DarkSide establishes its RaaS model. The group invites other criminals to use its service. A DarkSide data leak site is later discovered.
- November 2020: DarkSide launches its content delivery network (CDN) for storing and delivering compromised data.
- December 2020: A DarkSide actor invites media outlets and data recovery organizations to follow the group’s press center on the public leak site.
- March 2021: DarkSide releases version 2.0 of its ransomware with several updates.
- May 2021: DarkSide launches the Colonial Pipeline attack. After the attack, Darkside announces it is apolitical and will start vetting its targets (possibly to avoid raising attention to future attacks).

Initial access

In our analysis of DarkSide samples, we saw that phishing, remote desktop protocol (RDP) abuse, and exploiting known vulnerabilities are the tactics used by the group to gain initial access. The group also uses common, legitimate tools throughout the attack process to remain undetected and obfuscate its attack.

Throughout the reconnaissance and gaining-entry phases, we saw these legitimate tools used for specific purposes:

- PowerShell: for reconnaissance and persistence
- Metasploit Framework: for reconnaissance
- Mimikatz: for reconnaissance
- BloodHound: for reconnaissance
- Cobalt Strike: for installation

For modern ransomware like DarkSide, gaining initial access no longer immediately leads to ransomware being dropped. There are now several steps in between that are manually executed by an attacker.

Lateral movement and privilege escalation

Lateral movement is a key discovery phase in the modern ransomware process. In general, the goal is to identify all critical data within the victim organization, including the target files and locations for the upcoming exfiltration and encryption steps.

In the case of DarkSide, we confirmed reports that the goal of lateral movement is to gain Domain Controller (DC) or Active Directory access, which will be used to steal credentials, escalate privileges, and acquire other valuable assets for data exfiltration. The group then continues its lateral movement through the system, eventually using the DC network share to deploy the ransomware to connected machines. Some of the known lateral movement methods deployed by DarkSide use PSExec and RDP. But as we previously noted, a modern ransomware group behaves with methods more commonly associated with APT groups — it adapts its tooling and methods to the victim's network defenses.

Exfiltration

As is common practice with double extortion ransomware, critical files are exfiltrated prior to the ransomware being launched. This is the riskiest step so far in the ransomware execution process, as data exfiltration is more likely to be noticed by the victim organization's security team. It is the last step before the ransomware is dropped, and the attack often speeds up at this point to complete the process before it is stopped.

For exfiltration, we saw the following tools being used:

- 7-Zip: a utility used for archiving files in preparation for exfiltration
- Rclone and Mega client: tools used for exfiltrating files to cloud storage
- PuTTy: an alternative application used for network file transfer

DarkSide uses several Tor-based leak sites to host stolen data. The file-sharing services used by the group for data exfiltration include Mega and PrivatLab.

Execution and impact

The execution of the actual ransomware occurs next. The DarkSide ransomware shares many similarities with REvil in this step of the process, including the structure of ransom notes and the use of PowerShell to execute a command that deletes shadow copies from the network. It also uses the same code to check that the victim is not located in a Commonwealth of Independent States (CIS) country.

In addition to PowerShell, which is used to install and operate the malware itself, the group reportedly uses Certutil and Bitsadmin to download the ransomware. It uses two encryption methods, depending on whether the target operating system is Windows or Linux: A ChaCha20 stream cipher with RSA-4096 is used on Linux, and Salsa20 with RSA-1024 is used on Windows.

The following figure shows a sample ransom note from DarkSide.

Conclusion

Ransomware is an old but persistently evolving threat. As demonstrated by the recent activities of DarkSide, modern ransomware has changed in many aspects: bigger targets, more advanced extortion techniques, and farther-reaching consequences beyond the victims themselves.

Ransomware actors are no longer content with simply locking companies out of their computers and asking for ransom. Now they are digging deeper into their victims' networks and looking for new ways to monetize their activities. For example, a compromised cloud server can go through a complete attack life cycle, from the initial compromise to data exfiltration to resale or use for further monetization. Compromised enterprise assets are a lucrative commodity on underground markets; cybercriminals are well aware of how to make money from attacking company servers.

In the Colonial Pipeline attack, DarkSide used double extortion. But some ransomware actors have gone even further. Jon Clay, Director of Global Threat Communications at Trend Micro, outlines the phases of ransomware:

- Phase 1: Just ransomware. Encrypt the files, drop the ransom note, and wait for the payment.
- Phase 2: Double extortion. Phase 1 + data exfiltration and threatening data release. Maze was one of the first documented cases of this.
- Phase 3: Triple extortion. Phase 1 + Phase 2 + threatening DDoS. SunCrypt, RagnarLocker, and Avaddon were among the first groups documented doing this.
- Phase 4: Quadruple extortion. Phase 1 (+ possibly Phase 2 or Phase 3) + directly emailing the victim's customer base or having contracted call centers contact customers.

In fact, as detailed in security reports, DarkSide offers both the DDoS and call center options. The group is making quadruple extortion available to its affiliates and showing a clear sign of innovation. In cybercrime, there are no copyright or patent laws for tools and techniques. Innovation is as much about quickly and completely copying others' best practices as it is about coming up with new approaches.

Ransomware will only continue to evolve. Organizations therefore need to take the time to put in place an incident response plan focused on the new model of ransomware attacks. Unfortunately, some organizations may be putting cybersecurity on the back burner. For example, some security experts noted that Colonial Pipeline was using a previously exploited vulnerable version of Microsoft Exchange, among other cybersecurity lapses. A successful attack on a company providing critical services will have rippling effects that will harm multiple sectors of society, which is why protecting these services should be a top priority.

In a US Senate hearing on cybersecurity threats, Senator Rob Portman of Ohio described the strike on Colonial Pipeline as “potentially the most substantial and damaging attack on US critical infrastructure ever.” This attack is a call to action for all organizations to harden their networks against attacks and improve their network visibility.

Trend Micro has a multilayered cybersecurity platform that can help improve your organization’s detection and response against the latest ransomware attacks and improve your organization’s visibility. Visit the Trend Micro Vision One™ website for more information. Detailed solutions can be found in our knowledge base article on DarkSide ransomware.

It is interesting to note that DarkSide’s ransom note is similar to that of Babuk, which might indicate that these two families share a link.

DarkSide ransomware targets

Based on the group’s Tor leak sites, DarkSide determines whether to pursue targeting a potential victim organization by primarily looking at that organization’s financial records. It also uses this information to determine the amount of ransom to demand, with a typical ransom demand amounting to anywhere between US$200,000 and US$2 million.

Reports say that, based on the leak sites, there are at least 90 victims affected by DarkSide. In total, more than 2 TB of stolen data is currently being hosted on DarkSide sites, and 100% of victims’ stolen files are leaked.

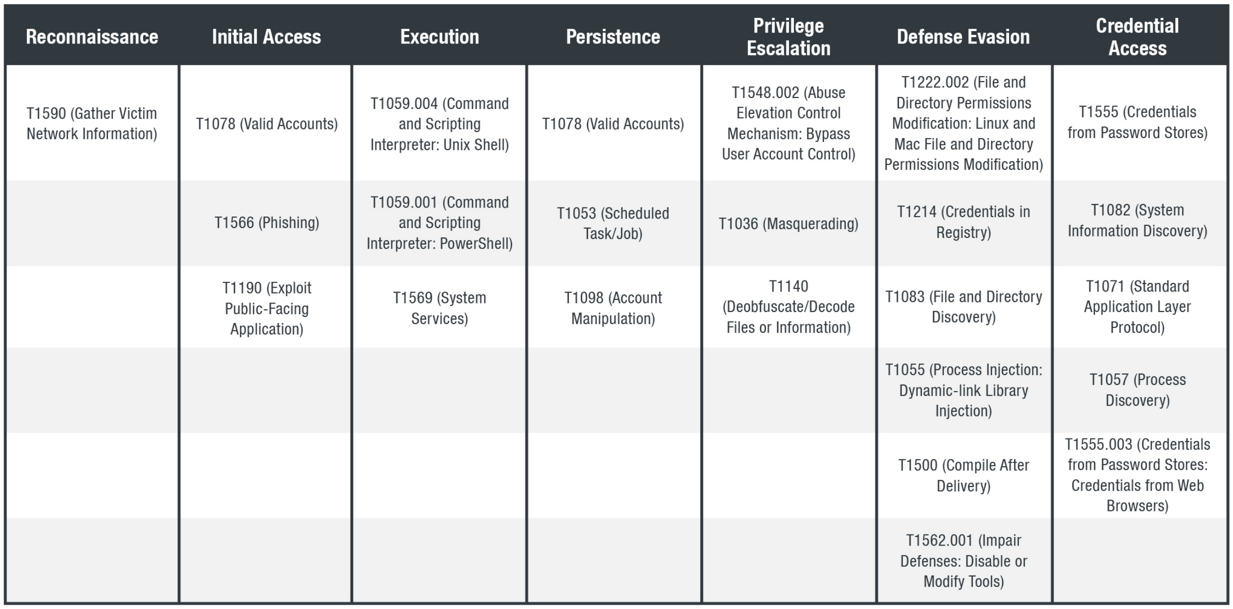
The actors behind Darkside have stated that they avoid targeting companies in certain industries, including healthcare, education, the public sector, and the nonprofit sector. Organizations in manufacturing, finance, and critical infrastructure have been identified in Trend Micro data as targets.

Based on Trend Micro data, the US is by far DarkSide’s most targeted country, at more than 500 detections, followed by France, Belgium, and Canada. As previously mentioned, DarkSide avoids victimizing companies in CIS countries. Part of the ransomware execution code checks for the geolocation of potential victims to avoid companies in these countries, although the group would likely be aware of the location of a target organization long before the ransomware is executed. That the group admittedly spares companies in CIS countries could be a clue to where DarkSide actors are residing. It is possible that they do this to avoid law enforcement action from these countries, since the governments of some of these countries do not persecute criminal acts such as DarkSide’s if they are done on foreign targets.

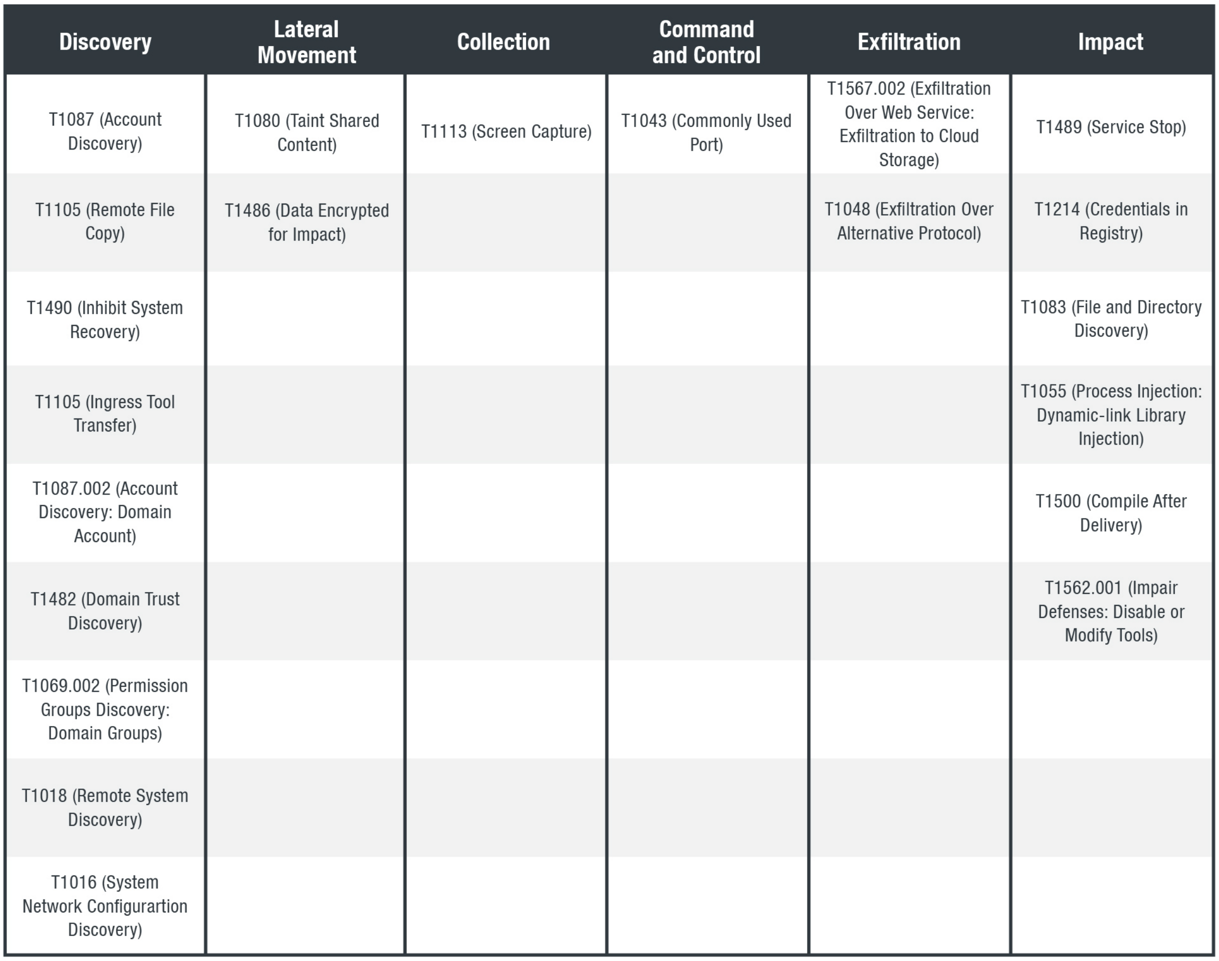
After the Colonial Pipeline attack, DarkSide released a statement on one of its leak sites clarifying that the group did not wish to create problems for society and that its goal was simply to make money. There is no way to verify this statement, but we know that the group is still quite active. As previously mentioned, DarkSide actors announced that they had stolen data from three more victims since the Colonial Pipeline attack.

MITRE ATT&CK tactics and techniques

The following are the MITRE ATT&CK tactics and techniques associated with DarkSide.



Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
T1590 (Gather Victim Network Information)	T1078 (Valid Accounts)	T1059.004 (Command and Scripting Interpreter: Unix Shell)	T1078 (Valid Accounts)	T1548.002 (Abuse Elevation Control Mechanism: Bypass User Account Control)	T1222.002 (File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification)	T1555 (Credentials from Password Stores)
	T1566 (Phishing)	T1059.001 (Command and Scripting Interpreter: PowerShell)	T1053 (Scheduled Task/Job)	T1036 (Masquerading)	T1214 (Credentials in Registry)	T1082 (System Information Discovery)
	T1190 (Exploit Public-Facing Application)	T1569 (System Services)	T1098 (Account Manipulation)	T1140 (Deobfuscate/Decode Files or Information)	T1083 (File and Directory Discovery)	T1071 (Standard Application Layer Protocol)
					T1055 (Process Injection: Dynamic-link Library Injection)	T1057 (Process Discovery)
					T1500 (Compile After Delivery)	T1555.003 (Credentials from Password Stores: Credentials from Web Browsers)
					T1562.001 (Impair Defenses: Disable or Modify Tools)	



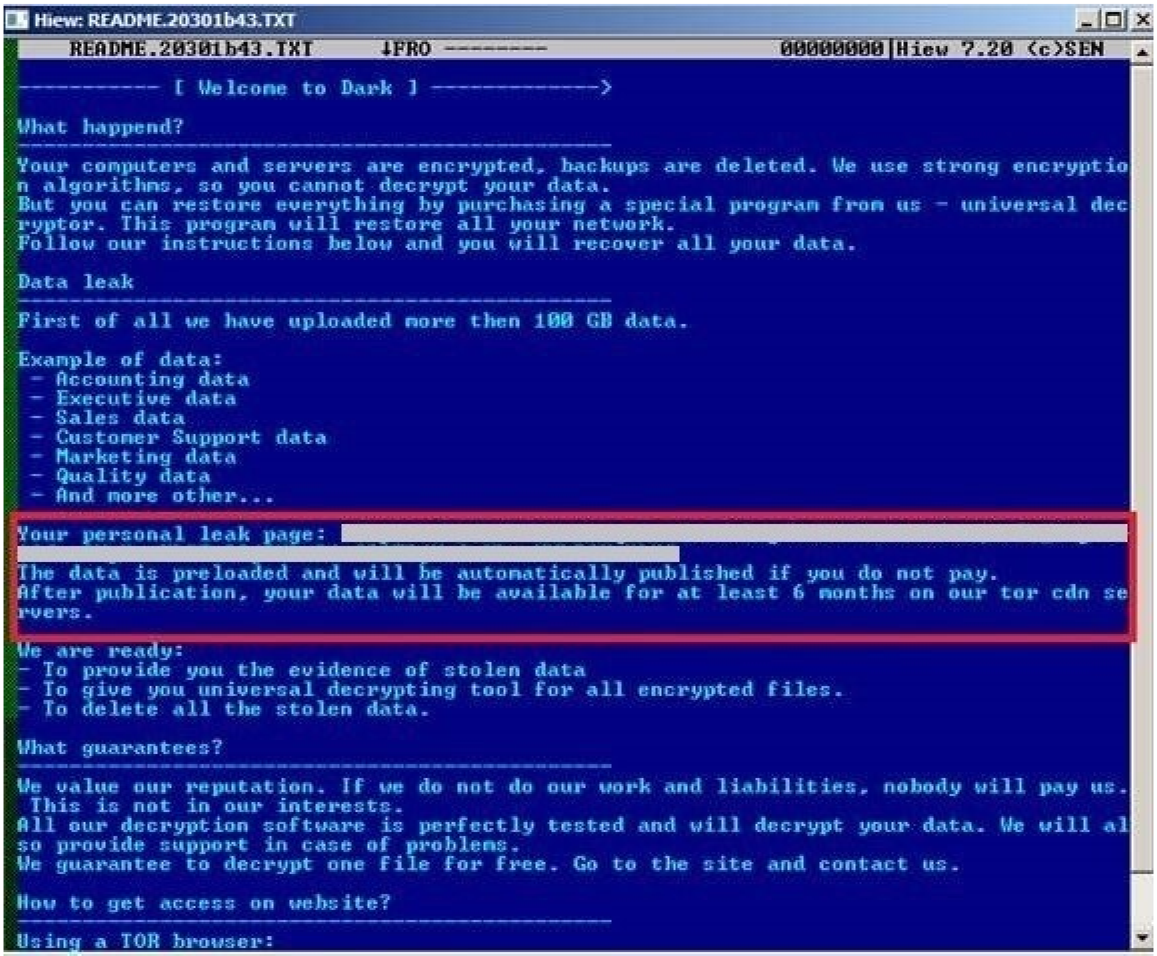
Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
T1087 (Account Discovery)	T1080 (Taint Shared Content)	T1113 (Screen Capture)	T1043 (Commonly Used Port)	T1567.002 (Exfiltration Over Web Service: Exfiltration to Cloud Storage)	T1489 (Service Stop)
T1105 (Remote File Copy)	T1486 (Data Encrypted for Impact)			T1048 (Exfiltration Over Alternative Protocol)	T1214 (Credentials in Registry)
T1490 (Inhibit System Recovery)					T1083 (File and Directory Discovery)
T1105 (Ingress Tool Transfer)					T1055 (Process Injection: Dynamic-link Library Injection)
T1087.002 (Account Discovery: Domain Account)					T1500 (Compile After Delivery)
T1482 (Domain Trust Discovery)					T1562.001 (Impair Defenses: Disable or Modify Tools)
T1069.002 (Permission Groups Discovery: Domain Groups)					
T1018 (Remote System Discovery)					
T1016 (System Network Configurartion Discovery)					

Ransomware

Trend Micro Research found dozens of DarkSide ransomware samples in the wild and investigated how the ransomware group operates and what organizations it typically targets.

By: Trend Micro Research May 12, 2021 Read time: (words)

Content added to Folio



```
   README.20301b43.TXT     ↓FRO ---------              00000000|Hiew 7.20 (c)SEN

----------- [ Welcome to Dark ] ------------->

What happend?
----------------------------------------------
Your computers and servers are encrypted, backups are deleted. We use strong encryptio
n algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal dec
ryptor. 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 100 GB data.

Example of data:
 - Accounting data
 - Executive data
 - Sales data
 - Customer Support data
 - Marketing data
 - Quality data
 - And more other...

Your personal leak page: [redacted]

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 se
rvers.

We are ready:
- To provide you the evidence of stolen data
- To give you universal decrypting tool for all encrypted files.
- 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 al
so 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:
```

Figure 1. A Darkside ransom note