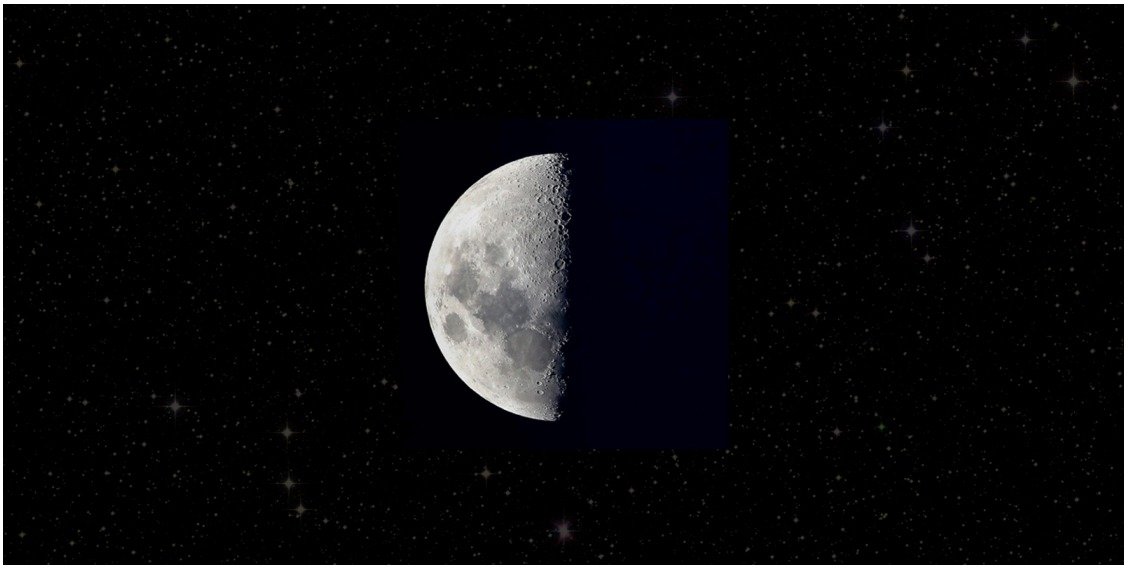
DarkSide: New targeted ransomware demands million dollar ransoms

By Lawrence Abrams

Published: 2020-08-21 · Archived: 2026-04-02 11:28:33 UTC



A new ransomware operation named DarkSide began attacking organizations earlier this month with customized attacks that have already earned them million-dollar payouts.

Starting around August 10th, 2020, the new ransomware operation began performing targeted attacks against numerous companies.

In a "press release" issued by the threat actors, they claim to be former affiliates who had made millions of dollars working with other ransomware operations.

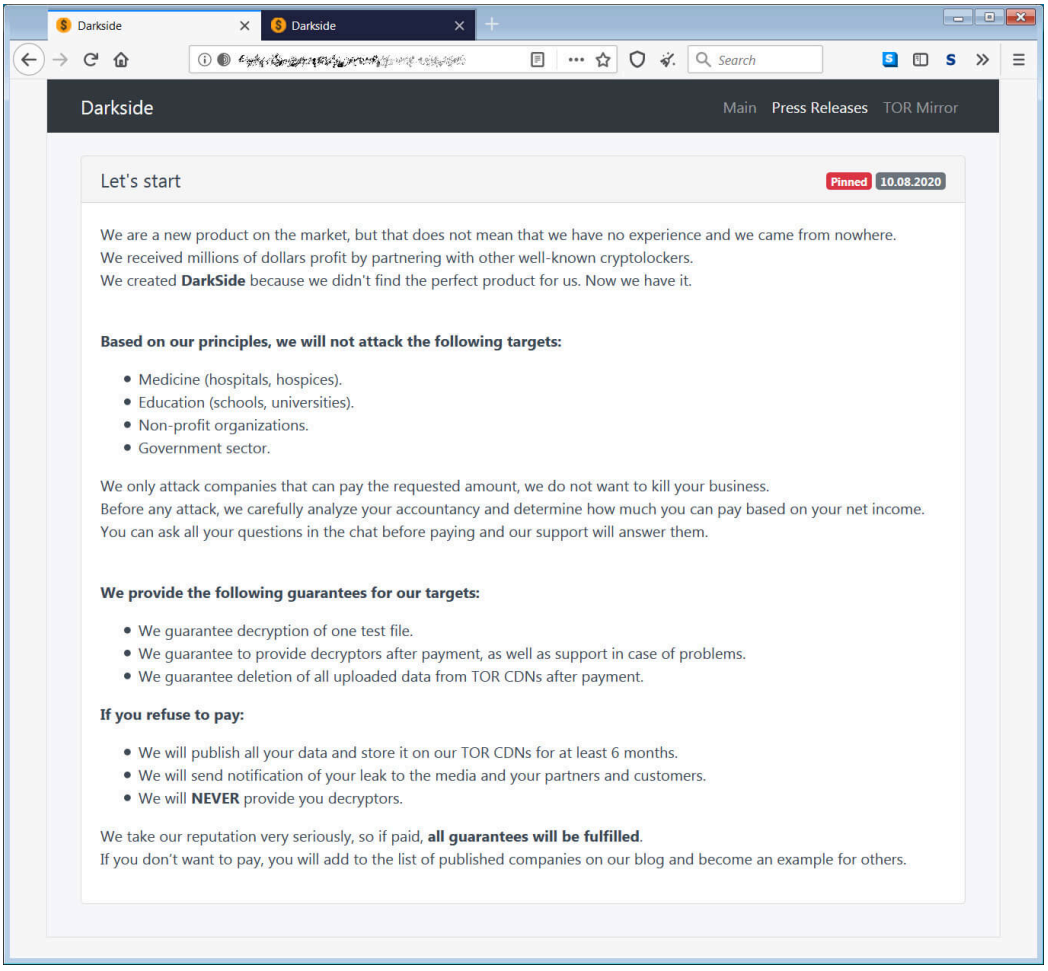

f5
Outlook
cisco
cisco

Visit Advertiser website[GO TO PAGE]

After not finding a "product" that suited their needs, they decided to launch their own operation.

"We are a new product on the market, but that does not mean that we have no experience and we came from nowhere.
We received millions of dollars profit by partnering with other well-known cryptolockers.
We created **DarkSide** because we didn't find the perfect product for us. Now we have it."

DarkSide states that they only target companies that can pay the specified ransom as they do not "want to kill your business."

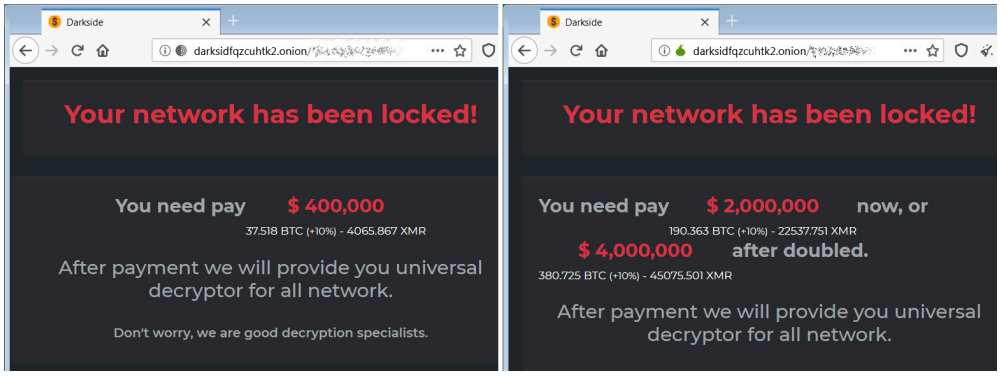


The threat actors have also stated that they do not target the following types of organizations.

- Medicine (hospitals, hospices).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

It is too soon to tell if they will honor this statement.

From victims seen by BleepingComputer, DarkSide's ransom demands range from $200,000 to $2,000,000. These numbers can likely be more or less depending on the victim.



Random demand ranges

At least one of the victims seen by BleepingComputer appears to have paid a million+ dollar ransom.

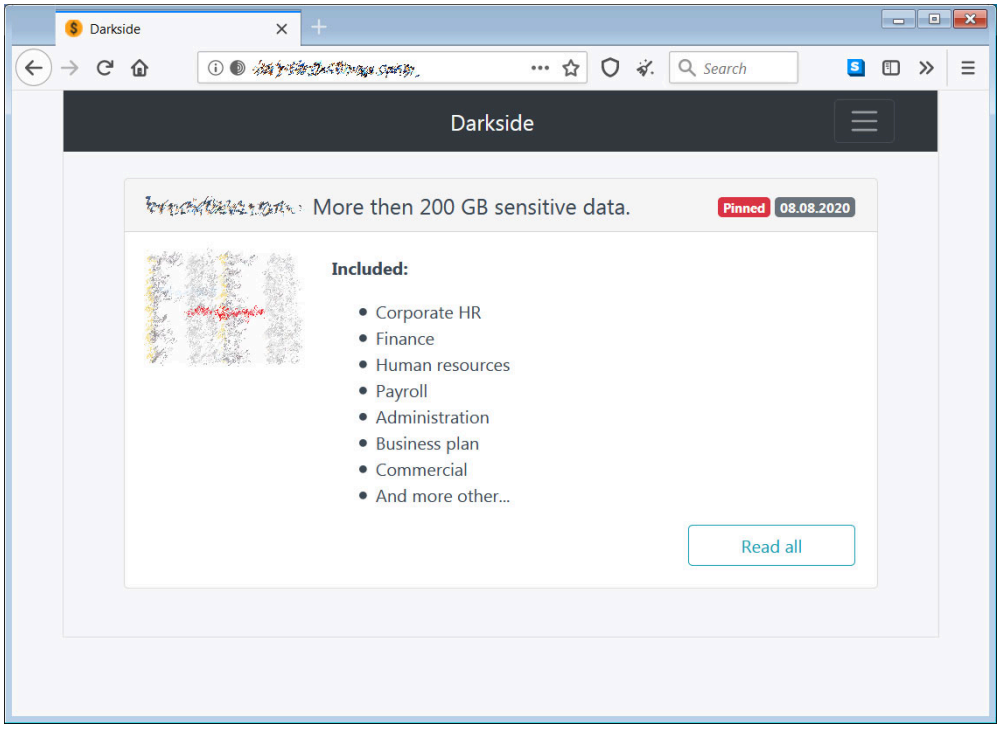
DarkSide steals data before encrypting victims

Like other human-operated ransomware attacks, when the DarkSide operators breach a network, they will spread laterally throughout a network until they gain access to an administrator account and the Windows domain controller.

While they spread laterally, the attackers will harvest unencrypted data from the victim's servers and upload it to their own devices.

This stolen data is then posted to a data leak site under their control and used as part of the extortion attempt.

When data is posted to the leak site, the threat actors will list the company name, the date they were breached, how much data was stolen, screenshots of the data, and the types of stolen data.



DarkSide data leak site

DarkSide states that if a victim does not pay, they will publish all of the data on their website for at least six months.

This extortion strategy is designed to scare a victim into paying the ransom even if they can recover from backups.

If a victim pays the ransom, DarkSide states that they will remove the stolen data from their leak site.

For the victim that had paid the ransom, their data has already been removed from the site.

Customized ransomware attacks

When performing attacks, DarkSide will create a customized ransomware executable for the specific company they are attacking.

When executed, the ransomware will execute a PowerShell command that deletes Shadow Volume Copies on the system so that they cannot be used to restore files.

According to Advanced Intel's Vitali Kremez, it then proceeds to terminate various database, office applications, and mail clients to prepare the machine for encryption.

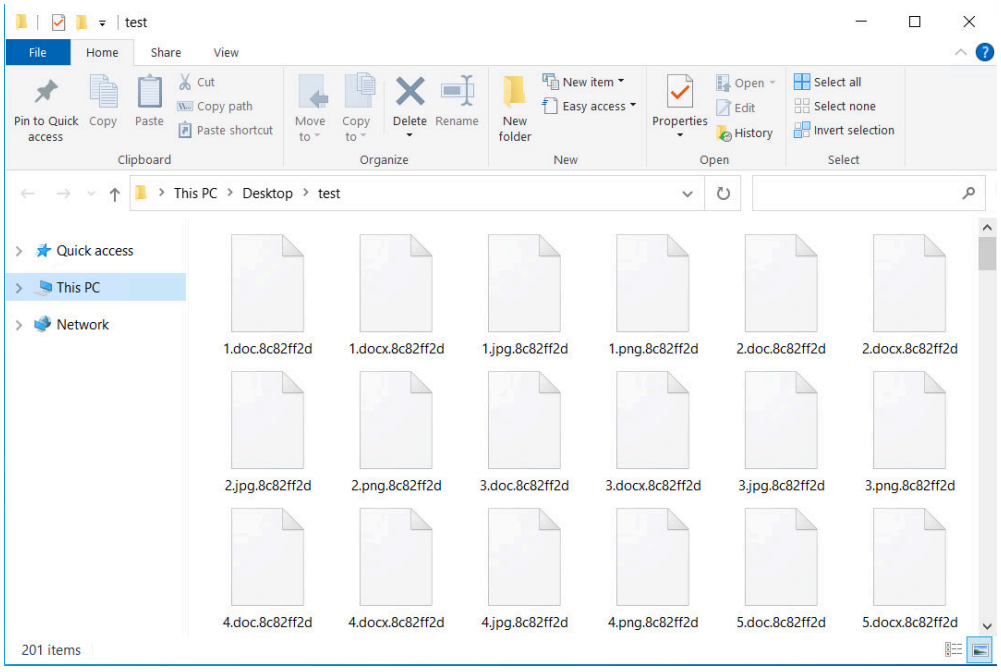
When encrypting a computer, DarkSide will avoid terminating certain processes.

```
 vmcompute.exe
vmms.exe
vmwp.exe
svchost.exe
TeamViewer.exe
explorer.exe
```

Specifically avoiding TeamViewer is not common, if ever seen with ransomware, and could indicate that the threat actors are using it for remote access to computers.

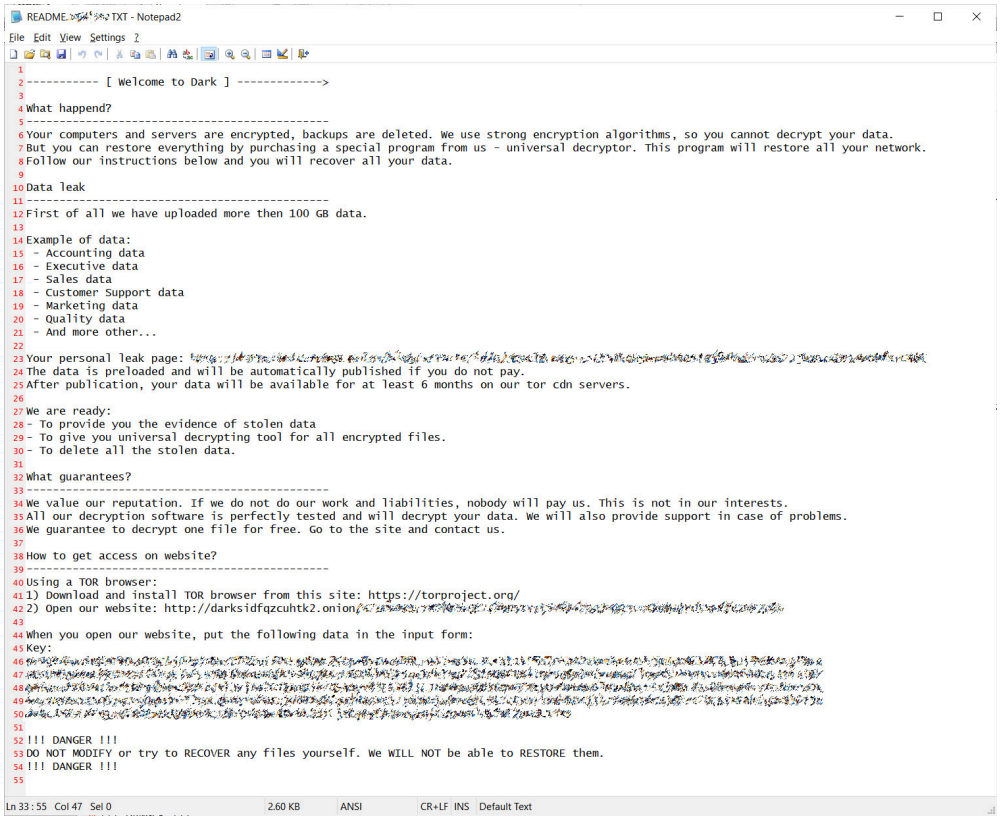
Michael Gillespie, who analyzed the encryption process, told BleepingComputer that the ransomware utilizes a SALSA20 key to encrypt files. This key is then encrypted with a public RSA-1024 key included in the executable.

Each victim will also have a custom extension created using a custom checksum of the victim's MAC address.



DarkSide encrypted files

Each executable is customized to include personalized "Welcome to Dark" ransom note, which will include the amount of data that was stolen, the type of data, and a link to their data on the data leak site.



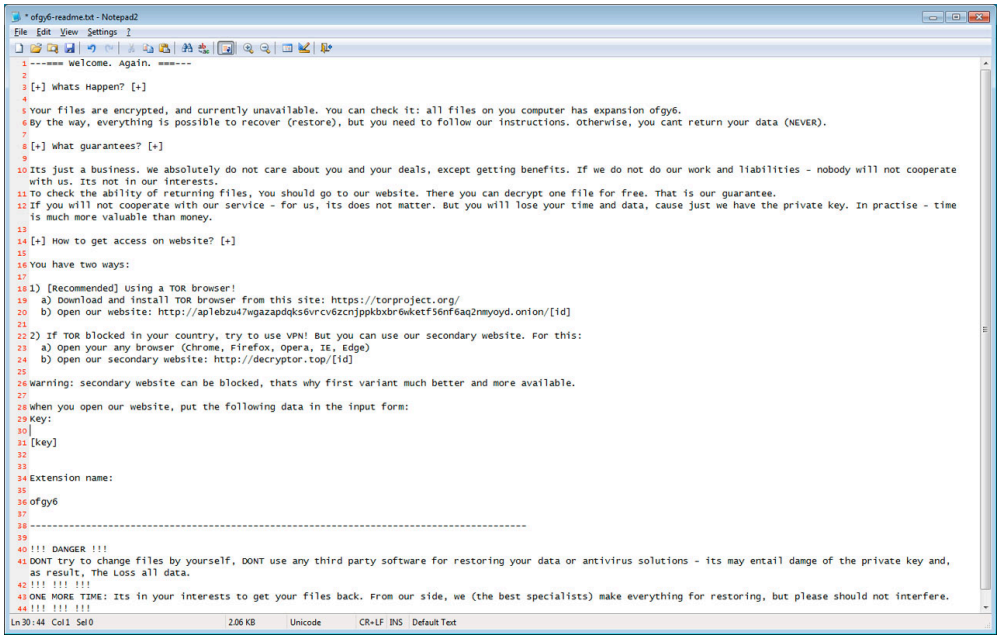
DarkSide Ransom Note

At this time, the ransomware looks secure, and there is no way to recover files for free.

Possible connection to REvil

When analyzing DarkSide, it was discovered that it has some similarities with the REvil ransomware.

The most obvious similarity is the ransom note, which uses almost the same template, as shown in the REvil ransom note below.



REvil Ransom Note

In BleepingComputer's behavioral analysis of DarkSide, we noticed that it would execute an encoded PowerShell script when first executed.

```
powershell -ep bypass -c
"(0..61)|%{$s+=[char][byte]('0x'+'4765742D576D694F626A6563742057696E33325F536
861646F77636F7079207C20466F72456163682D4F626A656374207B245F2E44656C6574652829
3B7D20'.Substring(2*$_,2))};iex $s"
```

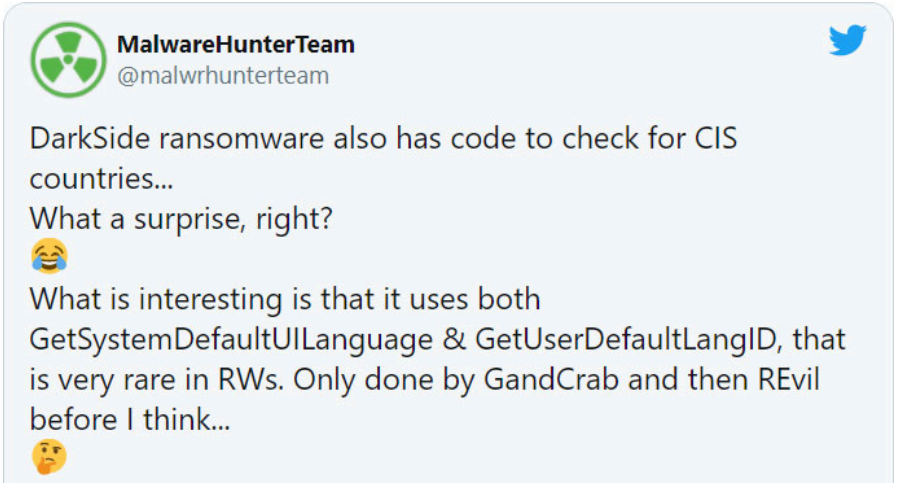
Executed PowerShell command

When deobfuscated, we can see that this PowerShell command is used to delete Shadow Volume Copies on the machine before encrypting it.

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

Using PowerShell to execute the above command is the same method used by REvil.

Finally, MalwareHunterTeam found that DarkSide purposely avoids infecting victims in CIS countries. The code to do this is similar to what is used in REvil and also GandCrab.



While these connections are tenuous, it is something that should be monitored.

Update 8/21/20: Added further technical information from Vitali Kremez and Michael Gillespie.

Source: https://www.bleepingcomputer.com/news/security/darkside-new-targeted-ransomware-demands-million-dollar-ransoms/