

# The Ransomware Conundrum – A Look into DarkSide

deepinstinct.com/2021/06/04/the-ransomware-conundrum-a-look-into-darkside/

June 4, 2021



June 4, 2021 | [Bar Block](#)

By now most of you should be familiar with the Colonial Pipeline ransomware incident that shut down a mission-critical U.S. fuel pipeline. The breach and subsequent disruption of services took the company offline for days and a [\\$4.4M ransom](#) was paid.

Ransomware has been gaining attention both in the U.S. and around the world not only because of the severe business impact an attack can have on target companies, but also because the frequency and significance of these attacks are growing in scope and scale.

In this post we will provide context into the DarkSide attack.

## **DarkSide Ransomware-as-a-Service (RaaS) Takes Center Stage**

DarkSide has been observed in more than 15 countries since first being spotted in the wild in August 2020. DarkSide, sold using the nickname "Darksupp," is part of a disturbing – and growing – trend called Ransomware-as-a-Service (RaaS) where ransomware is sold on darknet sites. DarkSide itself was listed on Russian darknet forums exploit.in and xss.is. RaaS has been gaining momentum for the past several years with some of the most prolific ransomware attacks, including Satan, stemming from similar origins.

In this RaaS model, buyers or "affiliates," are provided an interface from which they can costume their own DarkSide variant, manage victims, and write content for the DarkSide blog, where victim information and data is published and where affiliates can pressure for payment. In exchange, affiliates give the malware creators a stake of the ransom payment, which varies in percentage based on the ransom request amount.

In reported attack scenarios, threat actors, which could be affiliates or the creators of DarkSide themselves, infiltrated an organization using various methods, including exploiting known organizational VPN vulnerabilities and using legitimate user credentials. Once the exploit has taken place, the DarkSide payload is downloaded and copied into different locations on local and network drives. Once the victim, patient zero,

has been fully infected, the threat actors set off on their quest to find the network's holy grail – the Domain Controller (DC). If they successfully reach their destination, the attackers then collect more sensitive information and files. They could also dump the SAM registry hive, to extract passwords.

When the exfiltration is completed, the DC is infected with the malware, as well as the associated network. The malicious actors can then use it later in the attack to infect other targets in the network. Finally, an execution mechanism, such as Windows Scheduled Task, runs the ransomware payload, which will be discussed in length later in this post.

Victims are informed of the attack by a ransom note, which is typically placed on the desktop and in affected folders. If victim companies refuse to pay the ransom their data remains encrypted and the attackers may make stolen artifacts available for public access.

### Bringing DarkSide into the Light – The Colonial Pipeline Attack and its Consequences

On May 7, 2021, the Colonial Pipeline Company was attacked by DarkSide. The pipeline the company operates (of the same name) carries 45 percent of the fuel used to supply the U.S. East Coast, so any disruption of this pipeline will invariably cause fuel and supply chain problems. The brunt of the attack impacted the company's data systems, but Colonial Pipeline chose to disable the operational technology systems as well to mitigate any larger damage or disruption – a decision which created its own set of compounding challenges. This decision may not have been taken if the company had a network isolation solution it could count on to prevent the ransomware from reaching the operational systems. Not only did this threaten the supply of fuel and gasoline to the most populous region of the U.S., but it also led to immediate gas shortages, long gas station lines, panic, and price hikes.

On the same day of the attack, Colonial Pipeline Company, which is a private company, chose to pay the ransom, about \$4.4 million USD in Bitcoin, despite the FBI's discouragement to do so (the logic being that large ransomware payments only incentivize more ransomware attacks and larger ransomware payouts).

On May 12, five days following the attack, the company successfully brought the pipeline back online, with normal activity resuming in the following days.

But the fallout from this attack will likely last much longer.

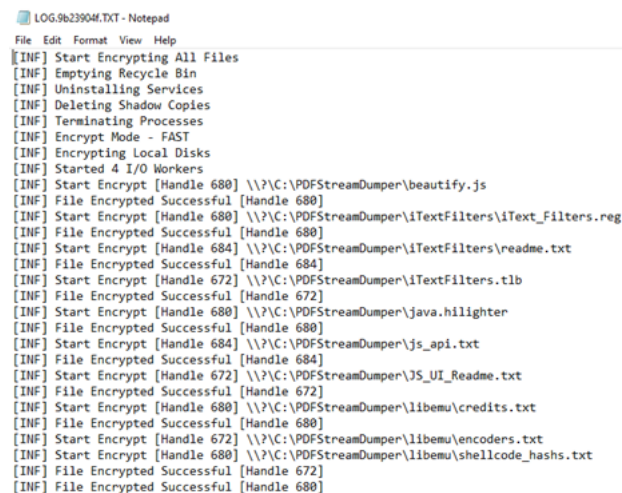
Given the high-profile nature of this attack, and the chain reaction it had on gas supply, business operations, consumer confidence, and the larger, interconnected supply chain, ransomware has gained the attention of business executives and the U.S. government alike. In the days following the attack, DarkSide became an immediate target of U.S. President Biden and the DarkSide website was shut down in short order. Fearing further repercussions and investigation, DarkSide and other ransomware groups, including Babuk, which had attacked the Washington D.C. police department in the same month, announced their dissolution later that week.

### An Analysis of a DarkSide Sample

DarkSide RaaS models provide affiliates with an infrastructure from which they can create their own ransomware builds and lead attacks at their own discretion. Using this console, affiliates can decide how their variant will act by choosing the encryption mode, deciding whether a language check will be performed to determine if the victim is from a CIS country, disabling or enabling network drives encryption, shadow copies deletion, and more.

The analyzed sample, which is referred to in this section, unless specified otherwise, has a SHA256 value of 6931b124d38d52bd7cdef48121fda457d407b63b59bb4e6ead4ce548f4bbb971.

When this DarkSide variant runs, it creates a file in which it logs its actions in the directory it runs from called LOG.victim\_extension.TXT. The "victim\_extension" is an 8-character pseudo-random string that DarkSide variants generate and use as the extension for encrypted files on infected machines. This string is also used in the names of the ransom and log files.



```
LOG.9b23904f.TXT - Notepad
File Edit Format View Help
[INF] Start Encrypting All Files
[INF] Emptying Recycle Bin
[INF] Uninstalling Services
[INF] Deleting Shadow Copies
[INF] Terminating Processes
[INF] Encrypt Mode - FAST
[INF] Encrypting Local Disks
[INF] Started 4 I/O Workers
[INF] Start Encrypt [Handle 680] \\?\C:\PDFStreamDumper\beautify.js
[INF] File Encrypted Successful [Handle 680]
[INF] Start Encrypt [Handle 680] \\?\C:\PDFStreamDumper\iTextFilters\iText_Filters.reg
[INF] File Encrypted Successful [Handle 680]
[INF] Start Encrypt [Handle 684] \\?\C:\PDFStreamDumper\iTextFilters\readme.txt
[INF] File Encrypted Successful [Handle 684]
[INF] Start Encrypt [Handle 672] \\?\C:\PDFStreamDumper\iTextFilters.tlb
[INF] File Encrypted Successful [Handle 672]
[INF] Start Encrypt [Handle 680] \\?\C:\PDFStreamDumper\java.highlighter
[INF] File Encrypted Successful [Handle 680]
[INF] Start Encrypt [Handle 684] \\?\C:\PDFStreamDumper\js_api.txt
[INF] File Encrypted Successful [Handle 684]
[INF] Start Encrypt [Handle 672] \\?\C:\PDFStreamDumper\JS_UI_Readme.txt
[INF] File Encrypted Successful [Handle 672]
[INF] Start Encrypt [Handle 680] \\?\C:\PDFStreamDumper\libemu\credits.txt
[INF] File Encrypted Successful [Handle 680]
[INF] Start Encrypt [Handle 672] \\?\C:\PDFStreamDumper\libemu\encoders.txt
[INF] Start Encrypt [Handle 680] \\?\C:\PDFStreamDumper\libemu\shellcode_hashes.txt
[INF] File Encrypted Successful [Handle 672]
[INF] File Encrypted Successful [Handle 680]
```

Figure 1: DarkSide's log file

As can be seen in the above image, before starting the encryption, DarkSide took some measures to ensure the encrypted files could not be replaced by local backups – it uninstalled backup services, terminated certain processes that had handles on files it wished to encrypt, emptied the recycle bin, and for the final nail in the coffin, deleted the shadow copies using the following PowerShell command:

```
powershell -ep bypass -c "(0..61)%{$s+=[char][byte]
('0x'+4765742D576D694F626A6563742057696E33325F53686E1646F77636F7079207C20466F72456163682D4F626A656374207B245F2E44656
$s"
```

Variable “s” contained the following: `Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}`

Next, DarkSide began encrypting all the files on the file system, except those which resided in certain directories, such as “Windows,” “ProgramData,” and “AppData,” were of specified types, for example: “exe,” “bat,” and “bin,” or had one of a set of names to ignore, such as “thumbs.db” and “netuser.dat.”

The following ransom note was dropped in all the directories the ransomware had visited:

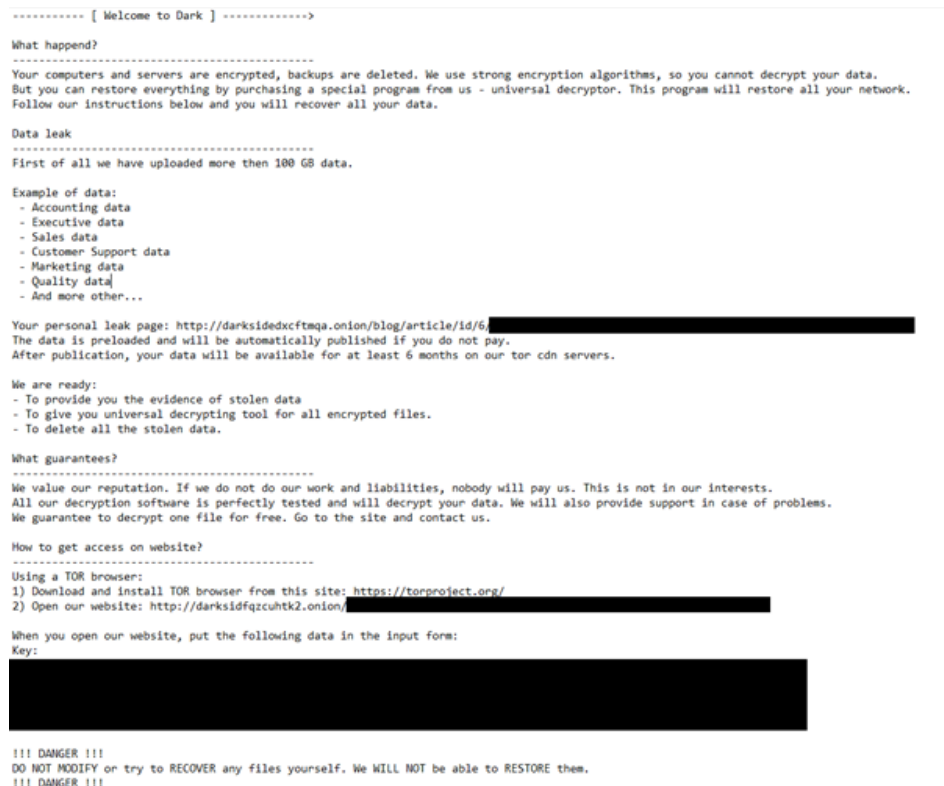


Figure 2: DarkSide's ransom note

As previously mentioned, DarkSide's website had been taken down, therefore the automatically generated URLs did not lead to any page and no data was actually exfiltrated. In any case, even if the servers were still up, 100GB of data could not have been stolen, since the used file system did not contain this amount of data and no attempts to connect to a remote server were observed during the analysis. It is safe to say this number is fixed, at least per variant (other analyzed samples mentioned different amounts of stolen data, such as 400GB), and cannot be counted on to estimate the amount of stolen data.

### Deep Instinct vs DarkSide

Deep Instinct's endpoint solution prevents DarkSide variants execution both statically, via our deep learning brain, and dynamically via our behavioral analysis mechanisms. As such, Deep Instinct offers the world's most advanced prevention against all known and unknown ransomware attacks.

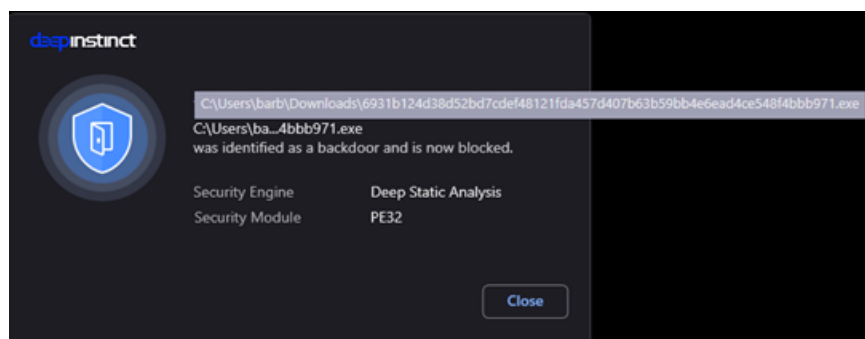


Figure 3: static prevention event on DarkSide

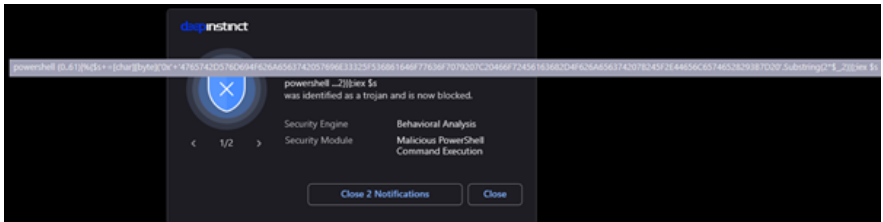


Figure 4: the PowerShell command used to delete shadow copies was identified as malicious and prevented.

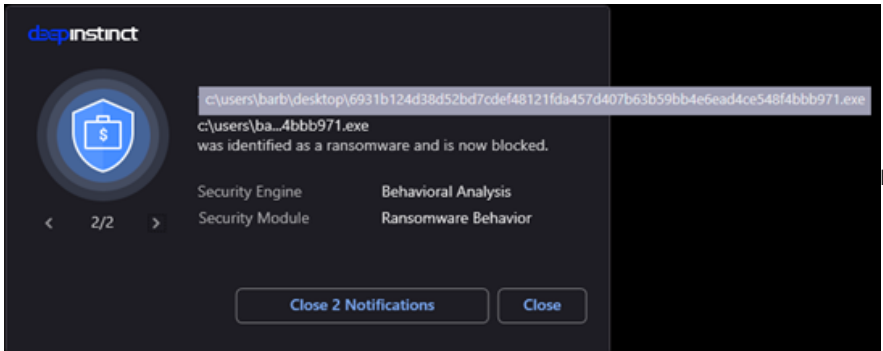


Figure 5: DarkSide was prevented due to

identified ransomware behavior, before any file was encrypted.

### Conclusion

RaaS-based attacks are far from over. As the technology and the expertise of lone hackers or larger syndicates grow in sophistication, we are likely to see more diverse and sinister ransomware attacks. And their profile companies could move upstream, impacting global brands with larger purses from which to pay ransoms.

But there is a solution to ransomware – using Deep Instinct to predict and prevent ransomware, stopping it before it can impact your system and operations. DarkSide has left a permanent mark on Colonial Pipeline Company and cost it dearly in revenue and reputation. Invest in your security posture and better prepare your network defense to prevent ransomware.

If you'd like to learn more about our industry-leading approach to stopping malware, backed by a \$3M guarantee, please download our new eBook, [Ransomware: Why Prevention is better than the Cure](#).