

Darkside Ransomware

Colonial Pipeline outage

<https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption>

On May 7, Colonial Pipeline Company learned it was the victim of a cybersecurity attack and has since determined that the incident involved ransomware. Quickly after learning of the attack, Colonial proactively took certain systems offline to contain the threat. These actions temporarily halted all pipeline operations and affected some of our IT systems, which we are actively in the process of restoring.

May 6, 2021

Earliest News

Sources told Bloomberg News that hackers stole nearly 100 gigabytes of data out of Colonial's network on Thursday before demanding a ransom.

<https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown>

May 7, 2021

Colonial Pipeline Offline

Colonial Pipeline shut down its entire pipeline network due to ransomware cyber attack

<https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption>

Actor attribution was unknown at the time, but information began to emerge of a threat actor named "DarkSide".

May 19, 2021

Latest Developments

Colonial pipeline restarted operations on May 12, taking a few days to ramp up to normal operations on or around May 15. It was reported DarkSide demanded \$5M ransom, but not confirmed how much was paid.

<https://www.cnn.com/2021/05/15/politics/colonial-pipeline-returns-normal-operations/index.html>

Following the restoration of Colonial, it was reported that DarkSide was shutting down operations.

<https://news.yahoo.com/darkside-claims-shutting-down-colonial-162049879.html>

FortiGuard Threat Signal report is available at:

<https://www.fortiguard.com/threat-signal-report/3943/colonial-pipeline-attack-attributed-to-darkside-ransomware-group>

Fortinet Products Summary

Services	Version	Other info	
FortiGate NGFW			
Anti-Virus	85.00092	NGAV Detects & Blocks malware file transfers	
DNS	FortiGuard DNS	Detects & Blocks DNS traffic to known malicious domains associated with this attack	
Botnet C&C	4.693	Detects & Blocks traffic to known C&C domains	
FortiClient			
Anti-Virus	85.00092	FortiGuard AV real-time protection blocks ransomware file	
Botnet C&C	4.693	Detects & blocks access to known C&C domains	
FortiEDR			
EDR	v4, v5	EDR behaviour detection & blocking of ransomware activity out of the box.	
Pre-execution	v4, v5	All related IOCs have been added to our Cloud intelligence for FortiEDR protection and will be blocked by FortinetCloudservices during pre-execution	
FortiSandbox			
Sandboxing	3.2+	Existing behaviour detection of the ransomware (launching files, visible windows, etc.).	
Pre-execution	85.00092	Detected by pre-filter or scan engines, as this is a known ransomware.	
FortiAI			
ANN	1.5+	Neural network / AI-based detection detects the ransomware	
Pre-filter	85.00092	Detected by pre-filter or scan engines, as this is a known ransomware.	
FortiMail FortiProxy FortiADC FortiCASB FortiCWP	Anti-Virus	85.00092	Detected by pre-filter or scan engines, as this is a known ransomware.
FortiDeceptor	Decoy	3.x	Use Decoys & Deception Lures (CACHE CREDENTIALS & SMB & RDP) to detect activities related to the DarkSide ransomware .
FortiAnalyzer	IOC	0.01868	Detected by FortiGuard IOC for post event analysis
	Event Handler	6.4+	Detects indicators attributed to the ransomware from Fabric products.
	Threat Hunting Report		
FortiSIEM	IOC	0.01868	Detected by FortiGuard IOC for post event analysis
	Rules	6.x+	Detects indicators attributed to the ransomware from Fabric products and 3rd party products.
	Threat Hunting Report		

Cyber Kill Chain



Reconnaissance



Weaponization



Delivery

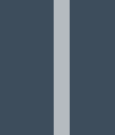


FortiGuard Anti-Malware Protection

FortiGate
FortiClient
FortiEDR
FortiMail
FortiSandbox
FortiAI
FortiCASB
FortiCWP

Version Info: 85.00092

Link: <https://www.fortiguard.com/updates/antivirus?version=85.00092>



FortiSandbox

Behavior Detection

Version Info: 3.2+

Link: <https://filestore.fortinet.com/fortiguard/downloads/9e779da82d86bcd4cc43ab29f929f73f.pdf>

Other Info: Existing behaviour detection of the ransomware (launching files, visible windows, etc.).



FortiAI

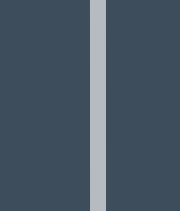
Artificial Neural Networks (ANN)

Version Info: 1.5+

Link: <https://filestore.fortinet.com/fortiguard/downloads/>

FortiAI%20Darkside%20VSA%20report_%20b278d7ec3681df16a541cf9e34d3b70a.pdf

Other Info: Neural network / AI-based detection detects the ransomware.



Exploitation



Installation



FortiEDR

Behavior Detection

Version Info: v4, v5

Link: https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKc&docType=kc&externalId=FD52267&sliceId=1&docTypeID=DT_KCARTICLE_1_1&dialogID=221610791&stateId=1%200%20221612085%27

Other Info: EDR behaviour detection & blocking of ransomware activity out of the box.



FortiDeceptor

Decoy VMs, Lure

Version Info: 3.x

Link: <https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKc&docType=kc&externalId=FD52296>

Other Info: Use FortiDeceptor Decoys & Deception Lures (CACHE CREDENTIALS & SMB & RDP) to detect activities related to the DarkSide ransomware malware attack.



C2



FortiGuard DNS

FortiGuard DNS

Version Info: 6.2+

Link: <https://www.fortiguard.com/learnmore#dns>

Other Info: Detects & Blocks DNS traffic to known malicious domains associated with this attack



FortiGuard Botnet C&C

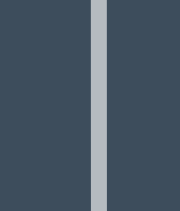
FortiGuard Botnet C&C (FortiGate)

FortiGuard Botnet Domain (FortiClient)

Version Info: 4.693

Link: <https://www.fortiguard.com/learnmore#botnet>

Other Info: Detects & Blocks traffic to known C&C domains



Action

Incident Response (Security Operations)

To help customers identify and protect vulnerable, FortiAnalyzer, FortiSIEM and FortiSOAR updates are available to raise alerts and escalate:

Analyzer / SIEM / SOAR Threat Hunting & Playbooks



FortiGuard IOC

FortiAnalyzer and FortiSIEM

Version Info: 0.01868

Link: <https://www.fortiguard.com/updates/ioc?version=0.01868>

Other Info: Detected by FortiGuard IOC for post event analysis



FortiAnalyzer

FortiAnalyzer Event Handlers & Reports

Version Info: 6.2+

Link: <https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKc&docType=kc&externalId=FD52270>

Other Info: Detects indicators attributed to the ransomware from Fabric products.



FortiSIEM

FortiSIEM Rules & Reports

Version Info: 6.x+

Link: <https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKc&docType=kc&externalId=FD52277>

Other Info: Detects indicators attributed to the ransomware from Fabric products and 3rd party products.