Fortinet Outbreak Alert

DarkSide Ransomware

Colonial Pipeline offline due to ransomware attack

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.

Background

May 6 - 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 - Colonial Pipeline shut down its entire pipeline network due to ransomware cyber attack May 8 - Actor attribution was unknown at the time, but information began to emerge of a threat actor named "DarkSide".

Announced

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

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

Fortinet Products Summary

Fortinet Products Summary	Services	Version	Other Info
FortiGate	**AV**	*6.0+*	NGAV Detects & Blocks malware file transfers
	DNS Filter	*6.2+*	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	**AV**	*6.0+*	FortiGuard AV real-time protection blocks ransomware file
	Botnet C&C	*4.693*	Detects & Blocks traffic to known C&C domains
	Anti-Ransomware	*6.4.4+*	
FortiEDR	**EDR**	*v4v5*	EDR behaviour detection & blocking of ransomware activity out of the box.
FortiSandbox	**AV (Pre-Filter)**	*3.2+*	Detected by pre-filter or scan engines, as this is a known ransomware.
	Behavior Detection	*3.2+*	Existing behaviour detection of the ransomware (launching files, visible windows, etc.).
FortiAI	**AV (Pre-Filter)**	*85.00092*	Detected by pre-filter or scan engines, as this is a known ransomware.
	ANN	*1.5*	Neural network / AI-based detection
FortiDeceptor	**Lure**	*3.x*	Use FortiDeceptor Decoys & Deception Lures (CACHE CREDENTIALS & SMB & RDP) to detect activities related to the DarkSide ransomware malware attack.
	Decoy VM	*3.x*	Use FortiDeceptor Decoys & Deception Lures (CACHE CREDENTIALS & SMB & RDP) to detect activities related to the DarkSide ransomware malware attack.
FortiMail	**AV**	*85.00092*	Detected by pre-filter or scan engines, as this is a known ransomware.
FortiCASB	**AV**	*85.00092*	Detected by pre-filter or scan engines, as this is a known ransomware.
FortiCWP	**AV**	*85.00092*	Detected by pre-filter or scan engines, as this is a known ransomware.
FortiADC	**AV**	*85.00092*	Detected by pre-filter or scan engines, as this is a known ransomware.
FortiProxy	**AV**	*85.00092*	Detected by pre-filter or scan engines, as this is a known ransomware.
FortiAnalyzer	**IOC**	*0.01868*	Detected by FortiGuard IOC for post event analysis
	Event Handlers & Reports	*6.2+*	Detects indicators attributed to the ransomware from Fabric products.
FortiSIEM	**IOC**	*0.01868*	Detected by FortiGuard IOC for post event analysis
	Rules & Reports	*6.x+*	Detects indicators attributed to the ransomware from Fabric products and 3rd parties.

Cyber Kill Chain

Reconnaissance

Weaponization

Delivery

FortiGate
AV
Version Info: 85.00092
Link: https://www.fortiguard.com/updates/antivirus?version=85.00092

FortiClient
AV
Version Info: 85.00092
Link: https://www.fortiguard.com/updates/antivirus?version=85.00092

FortiSandbox
AV (Pre-Filter)
Version Info: 85.00092
Link: https://www.fortiguard.com/updates/antivirus?version=85.00092

Behavior Detection
Version Info: 3.2+
Link: https://filestore.fortinet.com/fortiguard/downloads/9e779da82d86bcd4cc43ab29f929f73f.pdf

FortiAI
AV (Pre-Filter)
Version Info: 85.00092
Link: https://www.fortiguard.com/updates/antivirus?version=85.00092

ANN
Version Info: 1.071
Link: https://filestore.fortinet.com/fortiguard/downloads/FortiAI%20Darkside%20VSA%20report_979692cd7fc638beea6e9d68c752f360.pdf https://filestore.fortinet.com/fortiguard/downloads/FortiAI%20Darkside%20VSA%20report_%20b278d7ec3681df16a541cf9e34d3b70a.pdf

FortiMail
AV
Version Info: 85.00092
Link: https://www.fortiguard.com/updates/antivirus?version=85.00092

FortiCASB
AV
Version Info: 85.00092
Link: https://www.fortiguard.com/updates/antivirus?version=85.00092

FortiCWP
AV
Version Info: 85.00092
Link: https://www.fortiguard.com/updates/antivirus?version=85.00092

FortiADC
AV
Version Info: 85.00092
Link: https://www.fortiguard.com/updates/antivirus?version=85.00092

FortiProxy
AV
Version Info: 85.00092
Link: https://www.fortiguard.com/updates/antivirus?version=85.00092

Exploitation

Installation

FortiClient
Anti-Ransomware
Version Info: 6.4.4+
Link: https://www.fortinet.com/products/endpoint-security/forticlient#overview

FortiEDR
EDR
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)

FortiDeceptor
Lure
Version Info: 3.x
Link: https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FD52296

Decoy VM
Version Info: 3.x
Link: https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FD52296

C2

Action

Endpoint

Incident Response (Security Operations)

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

Analyzer / SIEM / SOAR Threat Hunting & Playbooks

FortiAnalyzer
IOC
Version Info: 0.01868
Link: https://www.fortiguard.com/updates/ioc?version=0.01868

Event Handlers & Reports
Version Info: 6.2+
Link: https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FD52270

FortiSIEM
IOC
Version Info: 0.01868
Link: https://www.fortiguard.com/updates/ioc?version=0.01868

Rules & Reports
Version Info: 6.x+
Link: https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FD52277