FORTINET

OUTBREAK ALERTS

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

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Reconnaissance

Lure

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

FortiDeceptor
v3.0+

Decoy VM

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

FortiDeceptor
v3.0+

Weaponization

Delivery

AV

Detects & Blocks malware file

FortiGate	FortiWeb	FortiClient	FortiSASE	FortiMail	FortiCASB	FortiCWP
DB 85.00092	*DB 85.00092*	*DB 85.00092*	*DB 85.00092*	*DB 85.00092*	*DB 85.00092*	*DB 85.00092*

FortiADC	FortiProxy
DB 85.00092	*DB 85.00092*

AV (Pre-filter)

Detects & Blocks malware file

FortiEDR	FortiSandbox	FortiNDR
DB 85.00092	*DB 85.00092*	*DB 85.00092*

Behavior Detection

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

FortiSandbox
v4.0+

Exploitation

Installation

C2

Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Threat Hunting

FortiEDR
FortiSIEM
v6.0+

Outbreak Detection

FortiAnalyzer
v6.2+

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

NSE Training
Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.

Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Security Rating

Vulnerability Management

Reduce the attack surface on software vulnerabilities via systematic and automated patching.

FortiEDR

Additional Resources

World Pipelines https://www.worldpipelines.com/special-reports/07052023/colonial-pipeline-attack-2-year-anniversary/

Learn more about FortiGuard Outbreak Alerts