CASE STUDY: DARKSIDE RANSOMWARE ATTACK ON COLONIAL PIPELINE

Cybersecurity for the Operational Technology Environment (CyOTE)

31 MARCH 2022

CyOTE Cybersecurity for the Operational Technology Environment

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

INL/RPT-22-67337

This document was prepared by Idaho National Laboratory (INL) under an agreement with and funded by the U.S. Department of Energy.

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

This *paper* is the product of *research* conducted by the Cybersecurity for the Operational Technology Environment (CyOTE) program and was funded by the Department of Energy Office of Cybersecurity, Energy Security and Emergency Response (DOE CESER). No updates have been made since the date of publication and no further funding has been approved.

TABLE OF CONTENTS

FIGURES

TABLES

CASE STUDY: DARKSIDE RANSOMWARE ATTACK ON COLONIAL PIPELINE

1. EXECUTIVE SUMMARY

The Darkside Ransomware Attack on Colonial Pipeline case study leverages publicly available information about the Colonial Pipeline cyber-attack and catalogs anomalous observables for each technique employed in the attack. This analysis is based upon the methodology of the Cybersecurity for the Operational Technology Environment (CyOTE) program.

On 7 May 2021, Colonial Pipeline Co., a Houston, Texas, based refined fuel pipeline operator, experienced a ransomware attack on their enterprise network, resulting in the company shutting down pipeline operations. Colonial's CEO, Joseph Blount, reported that an employee in the control center identified a ransom note on a system in the enterprise network that demanded payment to regain access to the system. The employee immediately notified the operations supervisor at the control center. The supervisor decided to halt operations to isolate the operational technology network from the attack.[1] This resulted in the shutdown of 5,500 miles of pipeline, which delivers refined fuel products to approximately 260 points across 13 states.[2] The outage impacted availability of commercial gasoline services, resulting in higher prices and consumer-driven shortages.[3] Shortly after discovering the ransomware note, Colonial paid a ransom of $4.4 million to the adversaries for a decryption tool.[4] The company restarted its pipeline operations on 12 May 2021, five days after the initial shutdown.[5]

Researchers and analysts identified 11 techniques utilized during the attack with a total of 68 observables using the MITRE ATT&CK® for Industrial Control Systems Matrix. The CyOTE program assesses observables accompanying techniques used prior to the triggering event to identify opportunities to observe malicious activity. If observables accompanying the attack techniques are perceived and investigated prior to the triggering event, earlier comprehension of malicious activity can take place. Nine of the identified techniques used during the Colonial cyber-attack were precursors to the triggering event. Case study analysis identified 45 observables associated with these precursor techniques, 24 of which were assessed to have an increased likelihood of being perceived in the nine days preceding the execution of the ransomware. The response and comprehension time could have been reduced to less than five days if the observables had been identified earlier.

The information gathered in this case study contributes to a library of observables tied to a repository of artifacts, data sources, technique detection capabilities, and procedural recipes to support the comprehension of indicators of attack. Asset owners and operators can use these products if they perceive similar observables, or to prepare for comparable scenarios.

2. INTRODUCTION

The Cybersecurity for the Operational Technology Environment (CyOTE) program developed capabilities for energy sector asset owners and operators (AOOs) to independently identify adversarial tactics and techniques within their operational technology (OT) environments.

Led by Idaho National Laboratory (INL) under the leadership of the Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), CyOTE is a partnership with energy sector owners and operators whose goal is to tie the impacts of a cyber-attack to anomalies in the OT environment to determine whether the anomalies have a malicious cyber cause.

2.1. APPLYING THE CYOTE METHODOLOGY

The CyOTE methodology, as shown in Figure 1, applies fundamental concepts of perception and comprehension to a universe of knowns and unknowns increasingly disaggregated into observables, anomalies, and triggering events. The program utilizes MITRE's ATT&CK® Framework for Industrial Control Systems (ICS) as a common lexicon to assess triggering events. By leveraging the CyOTE methodology with existing commercial monitoring capabilities and manual data collection, energy sector partners can understand relationships between multiple observables, which could represent a faint signal of an attack requiring investigation. CyOTE can assist AOOs in prioritizing their OT environment visibility investments.

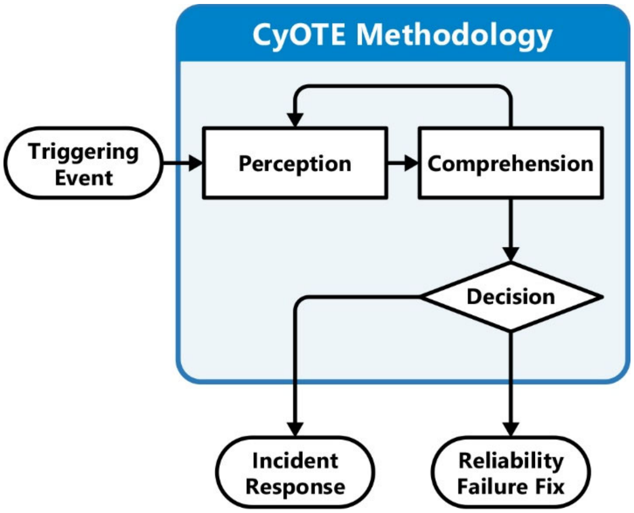


Figure 1. CyOTE Methodology

Case studies such as this one support continued learning through analysis of historical incidents that have impacted OT. This case study is based on publicly available reports and provides examples of how key concepts in the CyOTE methodology appear in the real world, providing insights on how similar novel attacks could be detected earlier and therefore mitigated. The analysis enables AOOs to independently identify observables associated with techniques known to be indicators of attack within OT environments. The identified observables highlight anomalous events for further investigation, which could enhance comprehension of malicious activity.

A timeline of events is created based on the CyOTE methodology and the attack-related observables. The timeline includes assessed dates for initial access, the triggering event, and the date the victim comprehended the malicious activity. The point on this timeline when each technique appears is critical to the AOO's ability to perceive and comprehend the associated malicious activity. Perception of techniques early in the timeline is critical, since responding to those techniques will generally have greater potential to limit damage to operations.

Each technique has an assessed perceivability. Perceivability is a function of the number of observables and the potential for AOOs to detect those observables. If a technique includes effects which AOOs may detect, such as deletion or modification of system files or required user execution, then the technique would be more perceivable.

Differences in infrastructure and system configurations may present different challenges and opportunities for observable detection. For example, architecture-wide endpoint monitoring is likely to improve the perceivability of techniques which modify host files, such as the Data Destruction technique (T0809) for Inhibit Response Function and Theft of Operational Information technique (T0882) for Impact. Network monitoring and log analysis capabilities are likely to improve perceivability of techniques which create malicious network traffic, such as the Standard Application Layer Protocol technique (T0869) for Command and Control, External Remote Services technique (T0822) for Initial Access, and Connection Proxy technique (T0884) for Command and Control. Alternatively, enhancing the monitoring parameters of system files would increase the perceivability of techniques such as Data from Information Repositories technique (T0811) for Collection and the Service Stop technique (T0881) for Inhibit Response Function.

The CyOTE program provides AOOs with a library of observables reported in each historical case. The library can be used in conjunction with a repository of artifacts, technique detection capabilities, and procedural recipes to support the comprehension of indicators of attack.

2.2. BACKGROUND ON THE ATTACK

Adversaries gained initial network access to the Colonial Pipeline Co. (Colonial) enterprise environment on 29 April 2021, nine days before they executed their ransomware attack (D-9). Colonial operates the largest refined pipeline in the United States, which supplies fuel and fuel services to 260 locations across 13 states from Texas to New Jersey. At approximately 5:00 AM on 7 May, the triggering event (D-0) occurred when a pipeline operator observed a ransom note on a system display. The note demanded $4.4 million in cryptocurrency. The operator quickly contacted their operations supervisor, who immediately began shutdown procedures along the 5,500-mile-long pipeline. By 6:10 AM the entire pipeline was shut down, although some operations continued under limited manual control between terminals and delivery points. Manual operation was utilized until 12 May (D+5) when automated systems were brought back online.[6]

A timeline of adversarial techniques is shown in Figure 2. The timeline includes the estimated number of days prior to and after the triggering event. The timeline after the triggering event includes the assessed victim comprehension timeline.

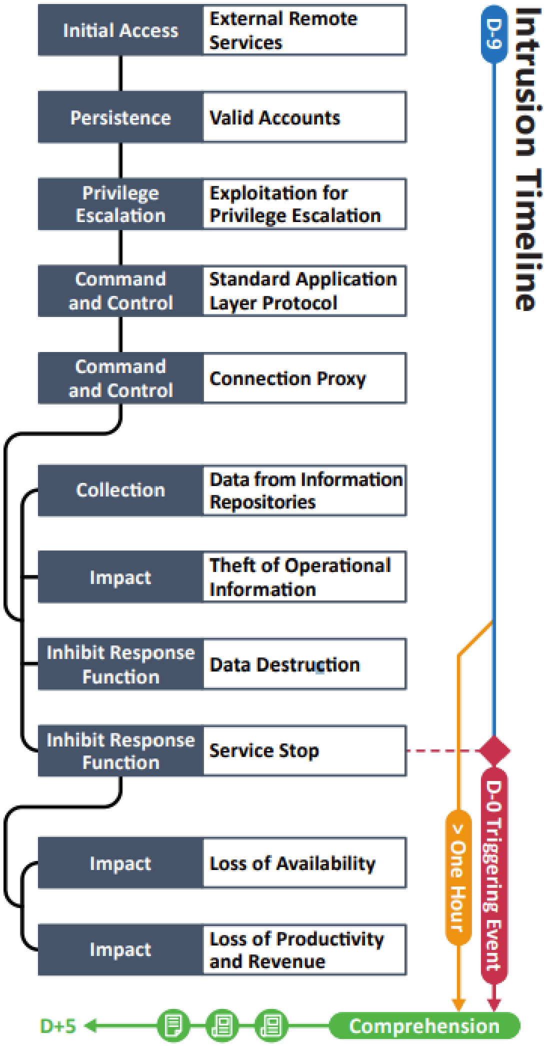


Figure 2. Colonial Pipeline Attack Timeline

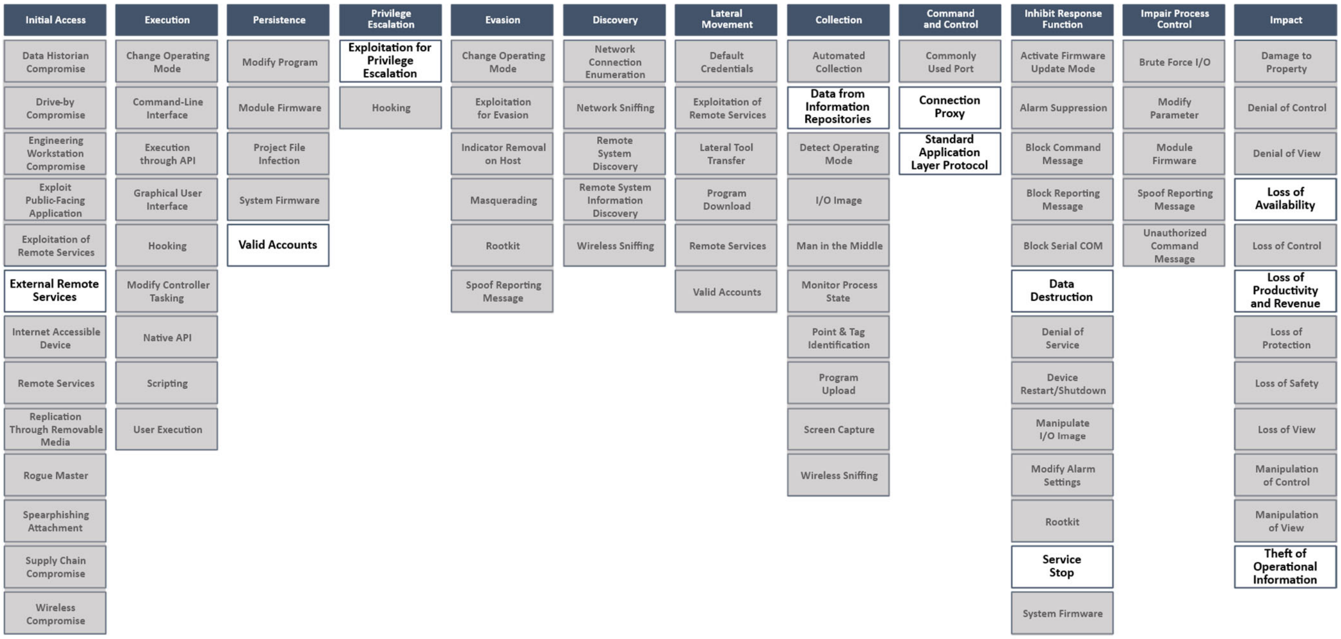
The adversaries gained initial access on 29 April through a virtual private network (VPN) connection with valid credentials from an expired account linked to a collection of leaked passwords on the dark web.[7] This occurred nine days (D-9) prior to the triggering event (D-0) when the ransom note was displayed and system files were encrypted. This nine-day gap allowed the adversaries to elevate privileges, deploy ransomware, and exfiltrate 100 GB of corporate data.[8,9]

The first details of the cyber-attack were reported on 7 May (D-0). Comprehension of the entire attack event occurred by 12 May (D+5) when Colonial brought all OT systems back online.

Mandiant assisted in the cyber-attack investigation and recovery effort. No technical reports on the cyber-attack were publicly released, resulting in CyOTE technical analysts having to rely on publicly available information and techniques previously associated with DarkSide ransomware. The DarkSide group provides this ransomware as ransomware-as-a-service (RaaS) to other entities willing to split profits from intended cyber-attacks.

Analysis identified 11 techniques in a sequence and timeframe likely used by adversaries during this cyber-attack (**Error! Reference source not found.**). These attack techniques are defined according to MITRE's ATT&CK® for ICS framework.

Table 1. Techniques Used in the Colonial Pipeline Cyber-Attack



Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Operating Mode	Modify Program	**Exploitation for Privilege Escalation**	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	**Data from Information Repositories**	**Connection Proxy**	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation Compromise	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	**Standard Application Layer Protocol**	Block Command Message	Module Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	**Loss of Availability**
Exploitation of Remote Services	Hooking	**Valid Accounts**		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
External Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		**Data Destruction**		**Loss of Productivity and Revenue**
Internet Accessible Device	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Remote Services	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Replication Through Removable Media	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Rogue Master							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Spearphishing Attachment									Rootkit		Manipulation of View
Supply Chain Compromise									**Service Stop**		**Theft of Operational Information**
Wireless Compromise									System Firmware		

Table 2. Case Study Quantitative Summary

Case Study Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	11
Technique Observables	68
Precursor Techniques	9
Precursor Technique Observables	45
Highly Perceivable Precursor Technique Observables	24

3. OBSERVABLE AND TECHNIQUE ANALYSIS

The following analysis may assist AOOs in identifying malicious cyber activity earlier and more effectively. The following techniques and observables were compiled from publicly available sources and correlated with expert analysis.

3.1. EXTERNAL REMOTE SERVICES TECHNIQUE (T0822) FOR INITIAL ACCESS

Based on analysis conducted by Mandiant, the External Remote Services technique (T0822) was used to gain initial access through a VPN account, creating a tunnel directly to Colonial's enterprise network on 29 April 2021. With authenticated connection credentials, adversaries were able to maintain an unhindered connection to the enterprise environment.[10] IT staff, IT managers, and cybersecurity personnel may have been able to observe the creation of VPN connections.

With authentic credentials used to gain access to the enterprise environment, no alerts would have been raised unless parameters were previously set to trigger an alarm if a user logged in during unusual times or at an unusual location. The observables connected to this technique, due to its authorized nature, would coincide with permitted connectivity through VPN access.

A total of four observables were identified with the use of the External Remote Services Technique (T0822) and were likely present on victim networks for the longest period of time. These observables likely would have been visible to the network administrator, IT staff, and IT cybersecurity, and if identified and investigated earlier in the attack could have reduced comprehension time. This technique is important for investigation because it presents perceivable effects, such as user-privilege changes and event log creation from a legacy user. This technique also occurs early in the timeline and responding to this technique will effectively halt all future events. If the External Remote Services technique is detected and prevented, then subsequent techniques are not executed. Terminating the chain of techniques at the External Remote Services technique would prevent adversaries from accessing internal networks and delivering malicious payloads. Of the four observables associated with this technique, one of these observables is assessed to be highly perceivable (VPN Activity Timestamp).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 59 artifacts could be generated by the External Remote Services technique
Technique Observers[a]	IT Staff and IT Cybersecurity

[a] Observer titles are adapted from the Job Role Groupings listed in the SANS ICS Job Role to Competency Level Poster. CyOTE products utilize these job categories rather than organizational titles to both support comprehensive analysis and preserve anonymity within the victim organization. A complete list of potential observers can be found in Appendix C

3.2. VALID ACCOUNTS TECHNIQUE (T0859) FOR PERSISTENCE

Adversaries employed the Valid Accounts technique (T0859) by utilizing an employee's VPN account credentials found in a collection of leaked passwords on the dark web. This was a legacy account that was not deactivated and which the adversaries used to gain persistent access to the enterprise network.[11]

IT staff and IT cybersecurity would have been able to observe use of the Valid Accounts Technique if account login notification parameters had been set. Among the observables gathered from the Valid Accounts technique were account login logs that showed a legacy account was being used. When this account was being used to log on, during regular or unusual hours, is not known from publicly available information. However, system logs would have a record of any successful log-on events.

A total of four observables were identified with the use of the Valid Accounts technique (T0859). Two of these observables are assessed to be highly perceivable (Leaked Credentials and Passwords Found on the Internet, VPN Activity Timestamp).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 15 artifacts could be generated by the Valid Accounts technique
Technique Observers	IT Staff and IT Cybersecurity

3.3. EXPLOITATION FOR PRIVILEGE ESCALATION (T0890) FOR PRIVILEGE ESCALATION

The ransomware deployed by the adversaries after gaining access would then have checked to see if it was running on a system with elevated privileges. If it was not operating with administrator privileges, it would utilize the User Account Control (UAC) elevation technique to rerun itself, this time operating at an administrator level.[12]

The observers of this technique during the attack would be network administrators and IT personnel monitoring user privileges. Systems and network administrators may find artifacts associated with this technique in security event logs or alerts provisioned through Windows Defender event logs.

Malicious files or programs running under elevated user privileges have been found in similar cyber-attacks, along with the popular credential harvester tool Mimikatz. While its use in the attack against Colonial has not been confirmed, the popularity of Mimikatz is such that a number of observables and artifacts likely would coincide with its use. However, standard anti-virus software or other signature-based detection and prevention capabilities would have difficulty catching the use of this tool due to its changing of hash values.

A total of seven observables were identified with the use of the Exploitation for Privilege Escalation technique (T0890). Two of these observables are assessed to be highly perceivable (Security Event Log, Windows Defender Event Log).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 15 artifacts could be generated by the Exploitation for Privilege Escalation technique
Technique Observers	IT Staff and IT Cybersecurity

3.4. STANDARD APPLICATION LAYER PROTOCOL TECHNIQUE (T0869) FOR COMMAND AND CONTROL

After the DarkSide ransomware infects a network, it begins to gather information about the operating system and other aspects of the victim network. The ransomware then exfiltrates the data to the command-and-control (C2) server. During delivery, a hash is created within the HTTP packet and sent to the C2 server to uniquely identify and organize information about the victim's infected systems.[13]

Network administrators, IT cybersecurity, and IT Staff would likely observe communications with external IP addresses, as compromised systems would communicate with C2 servers using HTTP POST requests to potentially suspect IP addresses.

A total of six observables were identified with the use of the Standard Application Layer Protocol technique (T0869). These observables likely would have been visible to the network administrator, IT staff, and IT cybersecurity, and if identified and investigated earlier in the attack could have reduced comprehension time. This technique is important for investigation because it presents noticeable effects, such as generation of system logs and anomalous network traffic. This technique also occurs early in the timeline, and detection of this technique will effectively halt all future events. If the Standard Application Layer Protocol technique is detected and prevented, then subsequent techniques are not executed. Terminating the chain of techniques at the Standard Application Layer Protocol technique would limit operational damage. Of the six observables associated with this technique, four of these observables are assessed to be highly perceivable (Connection to External C2 Network, Unique Victim Hash Created and Sent to C2 Servers Via HTTP, HTTP POST Request to C2 IPs, Missing Files).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 11 artifacts could be generated by the Standard Application Layer Protocol technique
Technique Observers	IT Staff and IT Cybersecurity

3.5. CONNECTION PROXY TECHNIQUE (T0884) FOR COMMAND AND CONTROL

Adversaries have been known to use The Onion Router (TOR) to establish a multi-hop proxy network with layers of encryption to protect the routing information and data being exfiltrated.[14] TOR was used during the attack on Colonial, as the ransomware note left on the operator's computer directed the company to a TOR address with links to the exfiltrated data.[15]

Network administrators, IT staff, and IT cybersecurity personnel could likely observe unexpected application communication to the network proxy port, unusual processes accessing the network proxy port, observed via firewall logs, and a significant observable, unusual network or host communication identified in network proxy logs.

A total of five observables were identified with the use of the Connection Proxy technique (T0884). Four of these observables are assessed to be highly perceivable (Victim Connects to C2 Network via TOR, Unexpected Application Communication from the Victim to the Network Proxy Port, Unusual Processes Accessing Network Proxy Port, Firewall Logs).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 6 artifacts could be generated by the Connection Proxy technique
Technique Observers	IT Staff and IT Cybersecurity

3.6. DATA FROM INFORMATION REPOSITORIES TECHNIQUE (T0811) FOR COLLECTION

As the DarkSide ransomware proliferates through the victim's system, it collects data about the infected environment by loading the libraries instructed by the dynamic-link library (DLL).[16] The ransomware harvests standard information on the system, such as OS, username, hostname, domain, and OS architecture, then encrypts the data and sends it to the C2 server. The ransomware also performs a default language check: if the default language is Russian or another Eastern European language, it will initiate a stop protocol and self-delete, as the DarkSide actors allegedly will not attack Russian entities.[17]

System and network administrators in IT and OT environments may have had access to observables associated with systems infected with the DarkSide ransomware. This assessment is based on the responsibilities typically assigned to these job positions to investigate anomalous network and system activity.[18]

A total of three observables were identified with the use of the Data from Information Repositories technique (T0811). These observables might have been visible to the network administrator, IT staff, and IT cybersecurity, and if identified and investigated earlier in the attack could have reduced comprehension time. This technique is important for investigation because it presents perceivable effects, such as deletion of volume shadow copies. This technique also occurs in the middle of the timeline, and detection of this technique will effectively halt all future events. This technique collects the host operating system files and any files stored on local and external drives, resulting in the host being placed into a compromised state. If system backups are created after this technique is executed, data recovery and disaster recovery efforts will be impaired. None of the observables are highly perceivable.

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 34 artifacts could be generated by the Data from Information Repositories technique
Technique Observers	OT Staff, OT Cybersecurity, IT Staff, and IT Cybersecurity

3.7. THEFT OF OPERATIONAL INFORMATION TECHNIQUE (T0882) FOR IMPACT

Adversaries not only encrypt system files and restrict access to vital databases, but may also exfiltrate data to the C2 server and threaten to release the stolen information if the victim refuses to pay the ransom. DarkSide ransomware uses Salsa20 and RSA-1024 encryption to guarantee the victim will not be able to decrypt the data without the adversary's decryption tool, which is provided upon payment of the ransom.[19] Not only are local files at risk, but any connected directories and removeable disks can become targets of the DarkSide ransomware. Within each encrypted directory, a README.TXT file is created housing a copy of the ransom note.[20,21]

In the case of Colonial, adversaries were able to encrypt the victim's system files and exfil more than 100 GB of company data. The adversary threatens to publicly release the data if the company refuses to pay the ransom.

System and network administrators in IT and OT environments along with onsite operators may have had access to observables associated with systems infected with the DarkSide ransomware. This assessment is based on the responsibilities typically assigned to these job positions to investigate anomalous network and system activity.

Observables associated with theft of operational information for DarkSide ransomware are captured in Yara rules, as follows:[22]

```
1A700F845849E573AB3148DAEf1A3B0B
7CDAC4B82A7573AE825E5EDB48F80BE5
```

A total of five observables were identified with the use of the Theft of Operational Information technique (T0882). These observables likely would have been visible to the network administrator, OT staff, OT cybersecurity, IT staff, and IT cybersecurity, and if identified and investigated earlier in the attack would have reduced comprehension time. This technique is important for investigation because it presents noticeable effects, such as large amounts of data being packaged, a surge in data upload size, and generation of malicious network traffic regarding the exfiltration of host data. This technique occurs in the middle of the intrusion timeline. All five of these observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 3 artifacts could be generated by the Theft of Operational Information technique
Technique Observers	OT Staff, OT Cybersecurity, IT Staff, and IT Cybersecurity

3.8. DATA DESTRUCTION TECHNIQUE (T0809) FOR INHIBIT RESPONSE FUNCTION

Adversaries employed the use of the Data Destruction technique (T0809) by using a DarkSide ransomware variant in the cyber-attack which emptied Recycle Bins of infected systems and removed shadow copies of files to ensure data recovery was unavailable to the victim. If the victim system was running windows system WOW64, the ransomware would execute a PowerShell command intended to delete shadow copies of the file system to prevent recovery.[23,24]

System and network administrators in IT environments may have had access to observables associated with systems infected with the DarkSide ransomware. This assessment is based on the responsibilities typically assigned to these job positions to investigate anomalous network and system activity.

A total of 11 observables were identified with the use of the Data Destruction technique (T0809). These observables likely would have been visible to the network administrator, IT staff, and IT cybersecurity, and if identified and investigated earlier in the attack would have reduced comprehension time. This technique is important for investigation because of its significant impact to the operational capabilities of a host through program execution and memory corruption. This technique is the most devastating and inhibits recovery attempts made by the victim through its file encryption and recovery attempt failure observables. Detection of this technique would enable a response to be made by the victim before significant file encryption spreads throughout the host network. System backups taken after this technique is executed will impact data recovery and disaster recovery efforts. Of the 11 observables associated with this technique, six of these observables are assessed to be highly perceivable (Removes Volume Shadow Copies, File Encryption, Missing Files, Memory Corruption, System Application Interruption, Event Log Creation).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 26 artifacts could be generated by the Data Destruction technique
Technique Observers	IT Staff and IT Cybersecurity

3.9. SERVICE STOP TECHNIQUE (T0881) FOR INHIBIT RESPONSE FUNCTION

The DarkSide ransomware kills targeted running Windows services and operating processes to eliminate file handles used by services throughout the system.[25] Applications stopped across infected systems would have been an observable both IT and OT personnel would have been able to see. However, with it being at the end of the cyber kill chain, any defensive measures taken would have to be deployed immediately.

There is no publicly available information concerning the specific services stopped. DarkSide ransomware variants have targeted the following services: vss, sql, svc$, memtas, mepocs, sophos, veeam, and backup. Not only are these services stopped but they are deleted to prevent any possibility of data recovery outside of the decryption tool sold by the adversary.

A total of 11 observables were identified with the use of the Service Stop technique (T0881). All of these observables would likely be perceived.

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 12 artifacts could be generated by the Service Stop technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, IT Staff, IT Cybersecurity, Management, Support Staff

3.10. LOSS OF AVAILABILITY TECHNIQUE (T0826) FOR IMPACT

The Colonial cyber-attack produced a unique look into the Loss of Availability technique (T0826) and the impact it had on the OT sector strictly from the IT side. The OT segments of the network were left intact and operational; however, Colonial deemed it unsafe to continue automated operations and shut down the pipeline to prevent the spread of the ransomware infection from the IT to the OT network.[26]

Once the DarkSide ransomware had encrypted system files across the IT network, operators were unable to access required information to continue business operations. As operators attempted to start normal functions, they found applications failing to run, user data missing, and system files that were inaccessible due to modification. The information servers connected to the SCADA systems on the OT network, where critical process information is stored, were unavailable due to encryption by the ransomware.[27] These systems were taken offline until a secure operational process could be guaranteed, effectively halting automated processes until limited manual operations could be initiated.

A total of eight observables were identified with the use of the Loss of Availability technique (T0826). Seven of these observables are assessed to be highly perceivable (Inability to Utilize Services within the IT Network, Inability to Access Systems within the OT Network, Encrypted System Files, Failed Attempt to Start Normal Functions, Application Failing to Run, Missing User Data, Inaccessible System Files Due to Modification).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 8 artifacts could be generated by the Loss of Availability technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, IT Staff, IT Cybersecurity, Management, Support Staff

3.11. LOSS OF PRODUCTIVITY AND REVENUE (T0828) FOR IMPACT

Under normal operations Colonial, the largest refined product pipeline in the United States, supplies nearly 2.5 million barrels per day of fuel to 260 locations along its run from Texas to the East Coast. In 2020 the company generated a net income of $420 million on $1.3 billion in revenues. A week's loss from the DarkSide ransomware attack equates to roughly $8 million in net income and $25 million in revenues.[28] In addition, the adversaries demanded a ransom of $4.4 million in cryptocurrency on 7 May, which Colonial paid the following day. This loss, however, was partially mitigated when federal authorities recovered $2.3 million in early June.[29]

A total of four observables were identified with the use of the Loss of Productivity and Revenue technique (T0828). All of the observables are assessed to be highly perceivable (Loss of Productivity, Loss of Net Income, Loss of Revenue, Loss of Ransom Payment).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 5 artifacts could be generated by the Loss of Productivity and Revenue technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, IT Staff, IT Cybersecurity, Management, Support Staff

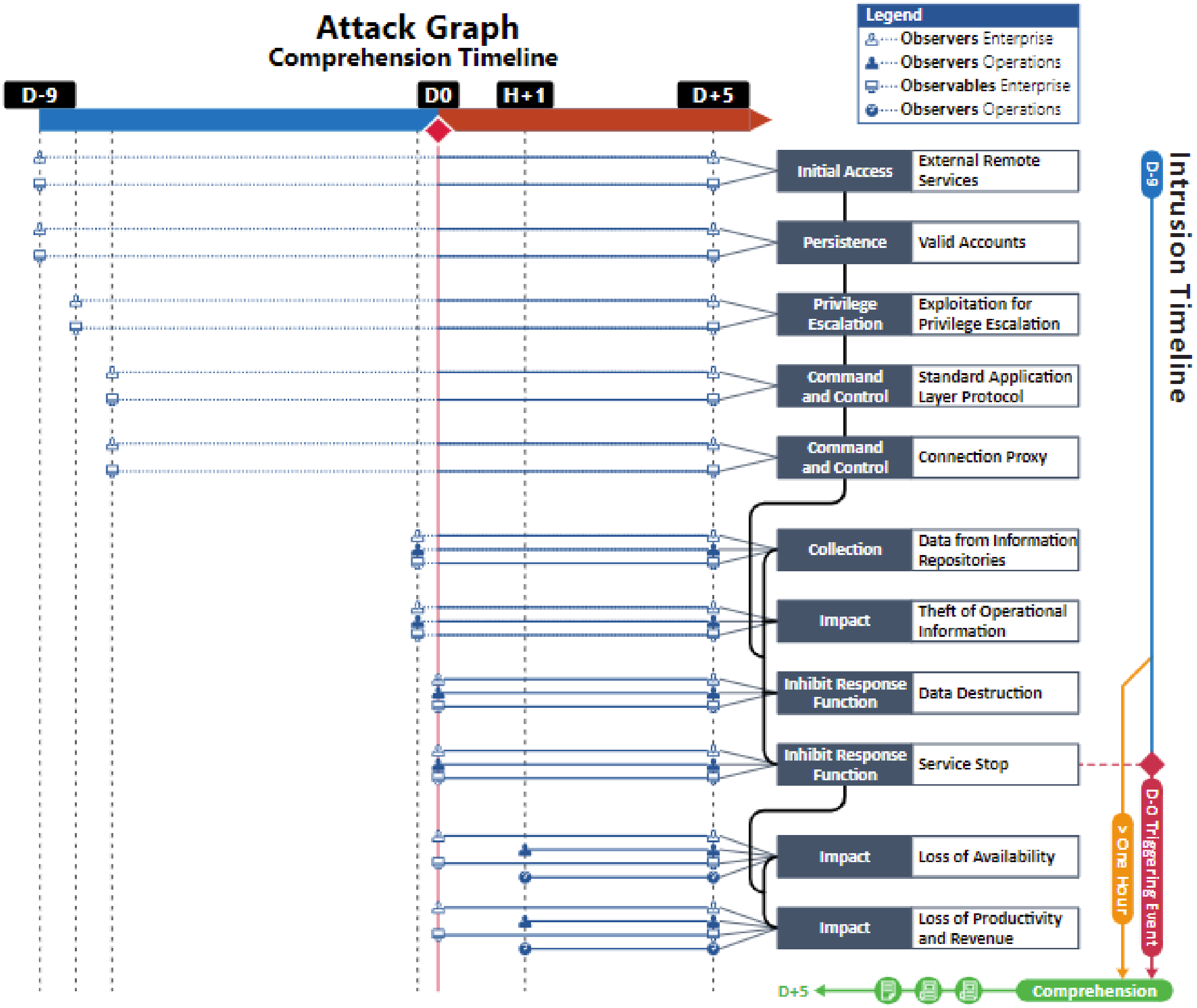


Figure 3. Attack Graph

APPENDIX A: OBSERVABLES LIBRARY

The observables listed here were associated or believed to be associated with the ransomware attack on Colonial.

Observables Associated with External Remote Services (T0822)	
Observable 1	VPN Account Usage
Observable 2	VPN Connection to Internal Enterprise Network
Observable 3	VPN Authentication Log
Observable 4	VPN Activity Timestamp

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1	Leaked Credentials and Passwords Found On Internet
Observable 2	VPN Legacy Account Usage
Observable 3	VPN Authentication Log
Observable 4	VPN Activity Timestamp

Observables Associated with Exploitation for Privilege Escalation Technique (T0890)	
Observable 1	Security Event Log
Observable 2	Malware Checking for Administration Privileges
Observable 3	User Account Control (UAC) Running with Administrator Privileges
Observable 4	Programs Running with Elevated Privileges
Observable 5	Application Execution Log
Observable 6	System Log with Elevated Privileges
Observable 7	Windows Defender Event Log

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 1	Ransomware Gathers Victim System Information and Other Identifiable Information
Observable 2	Connection to External C2 Network
Observable 3	Unique Victim Hash Created and Sent to C2 Servers via HTTP
Observable 4	Communications with External Ips
Observable 5	HTTP POST Request to C2 IPs
Observable 6	Missing Files

Observables Associated with Connection Proxy Technique (T0884)	
Observable 1	Victim Connects to C2 Network via TOR
Observable 2	Encrypted Data Being Exfiltrated
Observable 3	Unexpected Application Communication from The Victim to The Network Proxy Port
Observable 4	Unusual Processes Accessing Network Proxy Port
Observable 5	Firewall Logs

Observables Associated with Data from Information Repositories Technique (T0811)	
Observable 1	Victim Data Collection via DLL Execution
Observable 2	Ransomware Gathers Victim System Information and Other Identifiable Information
Observable 3	Ransomware Checks Victim Language, and Halts if Language Is Russian

Observables Associated with Theft of Operation Information Technique (T0882)	
Observable 1	Encryption of Victim Files Using Salsa20 And RSA-1024
Observable 2	Exfil Victim Data to C2 Network
Observable 3	Creation of README.TXT File Containing Ransom Note
Observable 4	Yara Rule String: 1A700F845849E573AB3148DAEf1A3B0B
Observable 5	Yara Rule String: 7CDAC4B82A7573AE825E5EDB48F80BE5

Observables Associated with Data Destruction Technique (T0809)	
Observable 1	Recycle Bin Emptied
Observable 2	Removes Volume Shadow Copies
Observable 3	Check if Victim Is Running a 64-Bit Windows OS
Observable 4	Delete Shadow Copies of File System if OS Is 64-Bit Windows
Observable 5	Recovery Attempt Failures
Observable 6	File Encryption
Observable 7	Missing Files
Observable 8	Memory Corruption
Observable 9	System Calls
Observable 10	System Application Interruption
Observable 11	Event Log Creation

Observables Associated with Service Stop Technique (T0881)	
Observable 1	Services Stopped
Observable 2	vss stop
Observable 3	sql stop
Observable 4	svc$ stop
Observable 5	memtas stop
Observable 6	mepocs stop
Observable 7	sophos stop
Observable 8	veeam stop
Observable 9	backup stop
Observable 10	Running Processes Killed
Observable 11	Deletion of Services

Observables Associated with Loss of Availability Technique (T0826)	
Observable 1	Inability to Utilize Services Within the IT Network
Observable 2	Inability to Access Systems Within the OT Network
Observable 3	Encrypted System Files
Observable 4	Unable to Access Required Information
Observable 5	Failed Attempt to Start Normal Functions
Observable 6	Application Failing to Run
Observable 7	Missing User Data
Observable 8	Inaccessible System Files Due to Modification

Observables Associated with Loss of Productivity and Revenue Technique (T0828)	
Observable 1	Loss of Five Days of Productivity
Observable 2	Approximately $8 Million Lost in Net Income
Observable 3	Approximately $25 Million Lost in Revenue
Observable 4	Loss of $4.4 Million for Ransom Payment

APPENDIX B: ARTIFACTS LIBRARY

Artifacts Associated with External Remote Services (T0822)	
Artifact 1	Remote Services Protocols
Artifact 2	Remote Vendor Connections
Artifact 3	Session Authentication
Artifact 4	Failed Logons Event ID 4625
Artifact 5	Session Timestamp
Artifact 6	Logon Event Type 3
Artifact 7	Logon Event Type 10
Artifact 8	Logon Event Type 11
Artifact 9	Remote Session Key
Artifact 10	System Registry Network Interfaces
Artifact 11	Remote Services Logon
Artifact 12	Remote Services Logon
Artifact 13	Session Logoff Event ID 4634/4647
Artifact 14	Domain Controller Log
Artifact 15	User Account Name
Artifact 16	User Client Address
Artifact 17	Security Account Manager Registry Entries
Artifact 18	Dialog Box Pop-Up
Artifact 19	Mouse Movement
Artifact 20	Command Prompt Window Opened
Artifact 21	Security Account Manager Registry Password Hashes
Artifact 22	External IP Address
Artifact 23	External IP Address
Artifact 24	User Privileges Change
Artifact 25	Blocked Incoming Connections Event ID 5031
Artifact 26	Blocked Incoming Packet Event ID 5152
Artifact 27	Encrypted Network Traffic
Artifact 28	Mouse Movement
Artifact 29	Cursor Movement

Artifacts Associated with External Remote Services (T0822)	
Artifact 30	Keyboard Entries
Artifact 31	Application Execution Via Input Devices
Artifact 32	Prefetch Files Created
Artifact 33	External MAC Address
Artifact 34	External MAC Address
Artifact 35	RDP Connections
Artifact 36	Program Executions
Artifact 37	Code Injections
Artifact 38	Host-Screen Adjustments
Artifact 39	Screen Resolution Changes
Artifact 40	SSH Connections
Artifact 41	Process Creations
Artifact 42	Service Creation
Artifact 43	Service Modification
Artifact 44	Event Log Creation
Artifact 45	Event Log Creation
Artifact 46	Jumplist Creation
Artifact 47	Shellbag Creation
Artifact 48	System Resource Use Management Changes
Artifact 49	Network Connection Durations
Artifact 50	Changes in Bytes Sent and Received
Artifact 51	Increase CPU Cycles
Artifact 52	Host System Crash
Artifact 53	Application Usage Increase
Artifact 54	Network Bandwidth Changes
Artifact 55	Logon Event ID 4624
Artifact 56	Logon Event ID 4624
Artifact 57	SMB Port 445
Artifact 58	RDP Port 3389
Artifact 59	SSH Port 22

Artifacts Associated with Valid Accounts (T0859)	
Artifact 1	Logons
Artifact 2	Application Log
Artifact 3	Domain Permission Requests
Artifact 4	Permission Elevation Requests
Artifact 5	Application Use Times
Artifact 6	Configuration Changes
Artifact 7	Prefetch Files Created After Execution
Artifact 8	Logon Session Creation
Artifact 9	User Account Creation
Artifact 10	Authentication Creation
Artifact 11	System Logs
Artifact 12	Successful Logon Event ID 4624
Artifact 13	Failed Logons Event ID 4625
Artifact 14	Logon Timestamp
Artifact 15	Logon Type Entry

Artifacts Associated with Exploitation for Privilege Escalation (T0890)	
Artifact 1	Unexpected Process Crash
Artifact 2	Unusual Process Activity
Artifact 3	Sysmon Event 8 CreateRemoteThread Process Injection Detected
Artifact 4	Unusual Command Line History Associated with Known CVE Techniques
Artifact 5	Suspicious File Write to System Directory Followed by Privileged Execution of File
Artifact 6	Execution of a Suspicious File in System32 or Windows Directory at Privileged Level
Artifact 7	Unusual or Unexpected Kerberos Ticket Requests
Artifact 8	Suspicious Files Written to Disk
Artifact 9	Suspicious Program Running Under SYSTEM or Other Elevated Account
Artifact 10	Driver Loaded
Artifact 11	Network Traffic Matching Vulnerability
Artifact 12	Abnormal Reads/Writes Between Processes
Artifact 13	Unusual Command Line Arguments to Application

Artifacts Associated with Exploitation for Privilege Escalation (T0890)	
Artifact 14	Artifacts Associated with Known Privilege Escalation CVEs
Artifact 15	Unusual or Unexpected Child Process Running at Elevated Privileges

Artifacts Associated with Standard Application Layer Protocol (T0869)	
Artifact 1	External Network Connections
Artifact 2	Increase In Number of External Connections
Artifact 3	Network Content Metadata
Artifact 4	Network Connection Times
Artifact 5	HTTP Traffic Port 80
Artifact 6	DNS Traffic Port 53
Artifact 7	SMB Traffic Port 445
Artifact 8	HTTPS Traffic Port 443
Artifact 9	RDP Traffic Port 3389
Artifact 10	HTTP Post Request
Artifact 11	External IP Addresses

Artifacts Associated with Connection Proxy (T0884)	
Artifact 1	Unexpected Application Communication to Network Proxy Port in Command Line Output
Artifact 2	Unexpected Process Usage of Network Proxy Port Observed Via Memory
Artifact 3	Unexpected Process Usage of Network Proxy Port Observed Via OS Logs
Artifact 4	Unexpected Process Usage of Network Proxy Port Observed Via Firewall Logs
Artifact 5	Unexpected Host Communicating with Network Proxy Port on Industrial Asset
Artifact 6	Unusual Network or Host Communications Identified in Network Proxy Log

Artifacts Associated with Data from Information Repositories (T0884)	
Artifact 1	Database Request
Artifact 2	Authentication Attempts
Artifact 3	Authentication Success
Artifact 4	Authentication Failure

Artifacts Associated with Data from Information Repositories (T0884)	
Artifact 5	RDP Traffic Port 3389
Artifact 6	SSH Traffic Port 22
Artifact 7	VNC Traffic Port 5900
Artifact 8	FTP Traffic Port 21
Artifact 9	SFTP Traffic Port 22
Artifact 10	Telnet Traffic Port 23
Artifact 11	MSSQL Traffic
Artifact 12	MSSQL Traffic
Artifact 13	HTTPS Traffic Port 443
Artifact 14	HTTP Traffic Port 80
Artifact 15	Engineering Workstation Application Log
Artifact 16	Operational Database Logons
Artifact 17	Operational Database Data Modification
Artifact 18	File Access
Artifact 19	File Modification
Artifact 20	MRU List Change
Artifact 21	Recent Search List
Artifact 22	Remote Procedure Calls
Artifact 23	Remote Procedure Calls
Artifact 24	Jump Host Credentials Accessed
Artifact 25	Personnel List Files Accessed
Artifact 26	Traffic Timestamps
Artifact 27	Design Documentation Manipulation
Artifact 28	Design Documentation Access
Artifact 29	TDS Port 1433
Artifact 30	Application Logon
Artifact 31	User Session Creation
Artifact 32	Data Bytes Sent
Artifact 33	Project File Modification
Artifact 34	SMB Traffic

Artifacts Associated with Theft of Operational Information (T0822)	
Artifact 1	Exfiltration of Endpoint Host Data (Spreadsheets, Diagrams, Documents, Configurations, Etc.) Via Standard Protocols
Artifact 2	Exfiltration From Database Via Standard Queries
Artifact 3	Exfiltration of Operational Info Via Phishing

Artifacts Associated with Data Destruction (T0809)	
Artifact 1	Program Execution
Artifact 2	SFTP Port 22
Artifact 3	FTPS Port 990
Artifact 4	SMB Port 139, 445
Artifact 5	HTTP Port 80
Artifact 6	HTTPS Port 443
Artifact 7	Command Line Arguments
Artifact 8	SCP Port 22
Artifact 9	Memory Corruption
Artifact 10	Files Moved to Recycle Bin
Artifact 11	Non-Native Files
Artifact 12	Non-Native Files
Artifact 13	External Network Connections
Artifact 14	Local Network Connections
Artifact 15	Host System Reboot Failure
Artifact 16	Process Logic Failure
Artifact 17	Event Log Creation
Artifact 18	System Call
Artifact 19	System Application Interruption
Artifact 20	Device Failure
Artifact 21	Recovery Attempt Failure
Artifact 22	File Encryptions
Artifact 23	Missing Files
Artifact 24	Use of File Transfer Protocols
Artifact 25	FTP Port 20, 21

Artifacts Associated with Data Destruction (T0809)	
Artifact 26	TFTP Port 60

Artifacts Associated with Service Stop (T0881)	
Artifact 1	Process Failure
Artifact 2	Sysinternals Logs
Artifact 3	Application Error Messages
Artifact 4	Process Error Messages
Artifact 5	Application Service Stop
Artifact 6	OS Service Stop
Artifact 7	System Event Logs
Artifact 8	Application Event Logs
Artifact 9	OS API Call
Artifact 10	Command Line System Argument
Artifact 11	System Resource Usage Manager Application Usage Change
Artifact 12	Registry Change HKLM\System\CurrentControlSet\Services

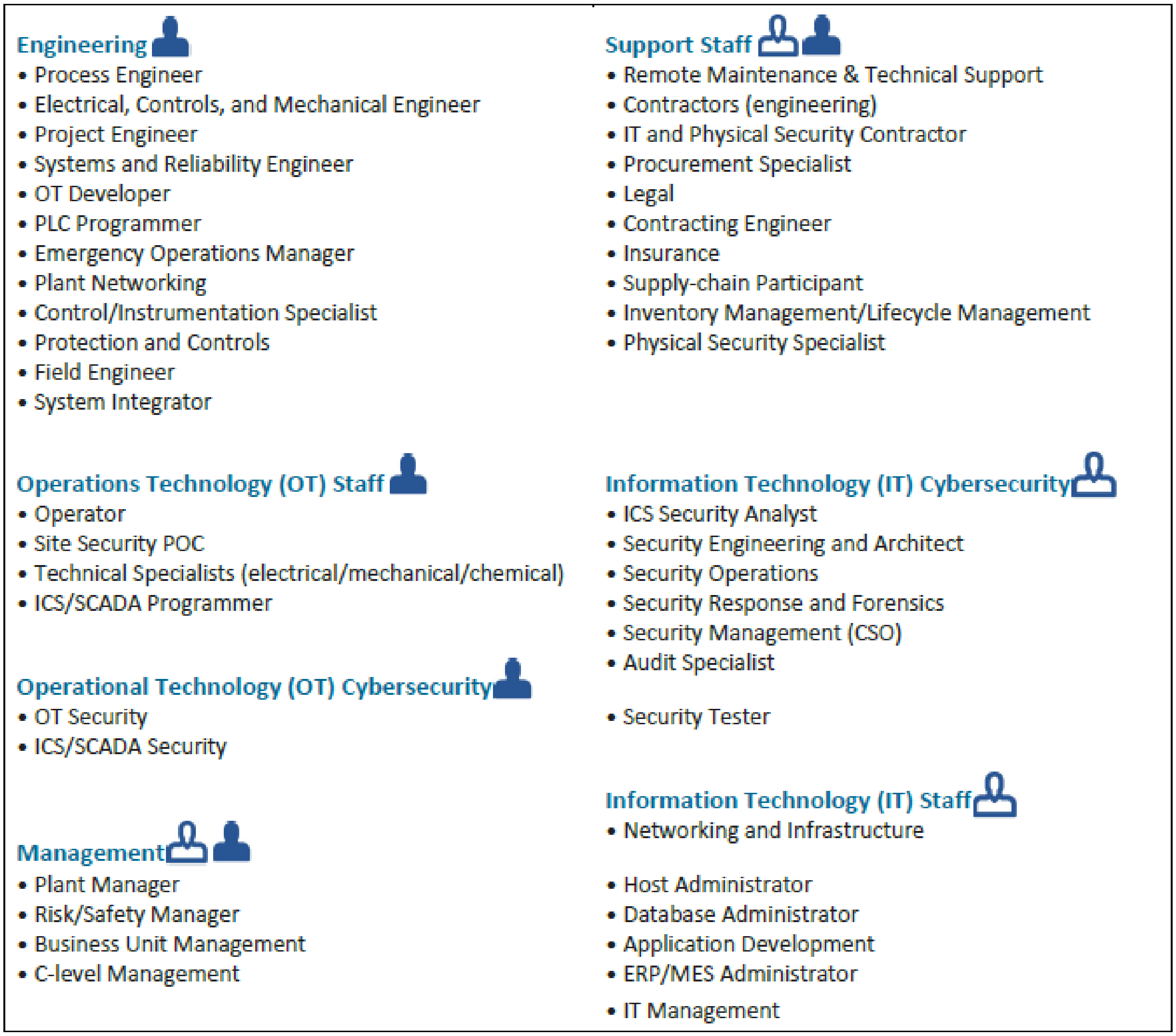
Artifacts Associated with Loss of Availability (T0826)	
Artifact 1	Operator or User Discovery of Encrypted or Inoperable Systems
Artifact 2	Significant Logged Usage of Native Crypto Functions or Presence of Import of Crypto Functions in Binaries
Artifact 3	Significant Reduction or Increase in Network Traffic Due to Malware Propagation of Disappearance of Services
Artifact 4	Unexplained Loss of Application Data
Artifact 5	Unexplained Loss of User Data
Artifact 6	Process Failure Due to Loss of Required Network or System Dependency
Artifact 7	Changes In Network Routing or Usage of Redundant Control System Network Connection Due to Failed Network Path
Artifact 8	File System Modification Artifacts Might Be Present on Disk

Artifacts Associated with Loss of Productivity and Revenue (T0828)	
Artifact 1	Loss of Confidence in a Safety System Due to Unreliability Might Result in a Risk Management Driven Shutdown of a Plant

Artifacts Associated with Loss of Productivity and Revenue (T0828)	
Artifact 2	Worms or Other Types of Rapidly Propagating Malware Might Result in the Shutdown of a Plant to Prevent Ransomware or Other Destructive Attacks
Artifact 3	Extortion Attempts Might Lead to Reduced Operations Due to Potential Presence of Malicious Attackers
Artifact 4	Loss of Control of Critical Systems Due to Ransomware or Loss of Confidence Might Lead to a Degraded Productivity or Revenue Operating State
Artifact 5	File System Modification Artifacts Might be Present on Disk

APPENDIX C: OBSERVERS

This is a collection of standardized potential observers that work in operational technology organizations. It has been slightly modified by the CyOTE team from the Job Role Groupings listed in the SANS ICS Job Role to Competency Level Poster to communicate the categories of potential observers during cyber events.



Engineering

- Process Engineer
- Electrical, Controls, and Mechanical Engineer
- Project Engineer
- Systems and Reliability Engineer
- OT Developer
- PLC Programmer
- Emergency Operations Manager
- Plant Networking
- Control/Instrumentation Specialist
- Protection and Controls
- Field Engineer
- System Integrator

Operations Technology (OT) Staff

- Operator
- Site Security POC
- Technical Specialists (electrical/mechanical/chemical)
- ICS/SCADA Programmer

Operational Technology (OT) Cybersecurity

- OT Security
- ICS/SCADA Security

Management

- Plant Manager
- Risk/Safety Manager
- Business Unit Management
- C-level Management

Support Staff

- Remote Maintenance & Technical Support
- Contractors (engineering)
- IT and Physical Security Contractor
- Procurement Specialist
- Legal
- Contracting Engineer
- Insurance
- Supply-chain Participant
- Inventory Management/Lifecycle Management
- Physical Security Specialist

Information Technology (IT) Cybersecurity

- ICS Security Analyst
- Security Engineering and Architect
- Security Operations
- Security Response and Forensics
- Security Management (CSO)
- Audit Specialist
- Security Tester

Information Technology (IT) Staff

- Networking and Infrastructure
- Host Administrator
- Database Administrator
- Application Development
- ERP/MES Administrator
- IT Management

REFERENCES

[1] [U.S. Senate Committee on Homeland Security and Governmental Affairs | Joseph Blount | “Testimony of Joseph Blount, President and Chief Executive Officer Colonial Pipeline Company” | https://www.hsgac.senate.gov/imo/media/doc/Testimony-Blount-2021-06-08.pdf | 8 June 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[2] [Bloomberg | William Turton and Kartikay Mehrotra | “Hackers Breached Colonial Pipeline Using Compromised Password” | https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password | 4 June 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[3] [Bloomberg | William Turton and Kartikay Mehrotra | “Hackers Breached Colonial Pipeline Using Compromised Password” | https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password | 4 June 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[4] [Bloomberg | William Turton and Kartikay Mehrotra | “Hackers Breached Colonial Pipeline Using Compromised Password” | https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password | 4 June 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[5] [Colonial Pipeline | “A Message to Our Customers and Those Who Depend on Us.” | https://www.colpipe.com/safe-operations/cybersecurity-response?gclid=Cj0KCQjwh_eFBhDZARIsALHjIKcFyX6srFFwyDhqviGH4ViV05Ib7YG0b2ZazA1NCijn6ivM7ezYaqcaAswHEALw_wcB | 13 May 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[6] [U.S. Senate Committee on Homeland Security and Governmental Affairs | Joseph Blount | “Testimony of Joseph Blount, President and Chief Executive Officer Colonial Pipeline Company” | https://www.hsgac.senate.gov/imo/media/doc/Testimony-Blount-2021-06-08.pdf | 8 June 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[7] [Bloomberg | William Turton and Kartikay Mehrotra | “Hackers Breached Colonial Pipeline Using Compromised Password” | https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password | 4 June 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[8] [Trend Micro | “What We Know About the DarkSide Ransomware and the US Pipeline Attack” | https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-DarkSide-ransomware-and-the-us-pipeline-attac.html | 12 May 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[9] [U.S. Senate Committee on Homeland Security and Governmental Affairs | Joseph Blount | “Testimony of Joseph Blount, President and Chief Executive Officer Colonial Pipeline Company” | https://www.hsgac.senate.gov/imo/media/doc/Testimony-Blount-2021-06-08.pdf | 8 June 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[10] [Bloomberg | William Turton and Kartikay Mehrotra | “Hackers Breached Colonial Pipeline Using Compromised Password” | https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password | 4 June 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[11] [Bloomberg | William Turton and Kartikay Mehrotra | “Hackers Breached Colonial Pipeline Using Compromised Password” | https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password | 4 June 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[12] [Virsec | “Virsec Analysis of the Colonial Pipeline Attack” | https://www.virsec.com/blog/virsec-analysis-of-the-colonial-pipeline-attack | 11 May 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[13] [Virsec | “Virsec Analysis of the Colonial Pipeline Attack” | https://www.virsec.com/blog/virsec-analysis-of-the-colonial-pipeline-attack | 11 May 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[14] [Cybersecurity and Infrastructure Security Agency | “DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks” | https://www.cisa.gov/uscert/ncas/alerts/aa21-131a | Revised 8 July 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[15] [Cybersecurity and Infrastructure Security Agency | “MAR-10337802-1.v1: DarkSide Ransomware” | https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-189a | 8 July 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[16] [Cybersecurity and Infrastructure Security Agency | “MAR-10337802-1.v1: DarkSide Ransomware” | https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-189a | 8 July 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[17] [Virsec | “Virsec Analysis of the Colonial Pipeline Attack” | https://www.virsec.com/blog/virsec-analysis-of-the-colonial-pipeline-attack | 11 May 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[18] [Mandiant | Jordan Nuce and others | “Shining a Light on DARKSIDE Ransomware Operations” | https://www.mandiant.com/resources/shining-a-light-on-DarkSide-ransomware-operations | 11 May 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[19] [Cybersecurity and Infrastructure Security Agency | “MAR-10337802-1.v1: DarkSide Ransomware” | https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-189a | 8 July 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[20] [Cybersecurity and Infrastructure Security Agency | “DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks” | https://www.cisa.gov/uscert/ncas/alerts/aa21-131a | Revised 8 July 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[21] [Mandiant | Jordan Nuce and others | “Shining a Light on DARKSIDE Ransomware Operations” | https://www.mandiant.com/resources/shining-a-light-on-DarkSide-ransomware-operations | 11 May 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[22] [Mandiant | Jordan Nuce and others | “Shining a Light on DARKSIDE Ransomware Operations” | https://www.mandiant.com/resources/shining-a-light-on-DarkSide-ransomware-operations | 11 May 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[23] [Virsec | “Virsec Analysis of the Colonial Pipeline Attack” | https://www.virsec.com/blog/virsec-analysis-of-the-colonial-pipeline-attack | 11 May 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[24] [Cybersecurity and Infrastructure Security Agency | “DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks” | https://www.cisa.gov/uscert/ncas/alerts/aa21-131a | Revised 8 July 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[25] [Virsec | “Virsec Analysis of the Colonial Pipeline Attack” | https://www.virsec.com/blog/virsec-analysis-of-the-colonial-pipeline-attack | 11 May 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[26] [U.S. Senate Committee on Homeland Security and Governmental Affairs | Joseph Blount | “Testimony of Joseph Blount, President and Chief Executive Officer Colonial Pipeline Company” | https://www.hsgac.senate.gov/imo/media/doc/Testimony-Blount-2021-06-08.pdf | 8 June 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[27] [Virsec | “Virsec Analysis of the Colonial Pipeline Attack” | https://www.virsec.com/blog/virsec-analysis-of-the-colonial-pipeline-attack | 11 May 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[28] [Forbes | Christopher Helman | “Cyber-Ransom Of $5m ‘Nothing’ To Colonial Pipeline, Which Has Paid Hundreds Of Millions In Dividends To Billionaire Koch Family” | https://www.forbes.com/sites/christopherhelman/2021/05/14/cyber-ransom-of-5m-nothing-to-colonial-pipeline-which-has-paid-hundreds-of-millions-in-dividends-to-billionaire-koch-family/?sh=54a3131c2e6e | 14 May 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[29] [NPR | Vanessa Romo | “How A New Team Of Feds Hacked The Hackers And Got Colonial Pipeline's Ransom Back” | https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac | 8 June 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]