PRECURSOR ANALYSIS REPORT: KANSAS WATER UTILITY INSIDER CYBER ATTACK 2019

Cybersecurity for the Operational Technology Environment (CyOTE)

31 DECEMBER 2022

CyOTE Cybersecurity for the Operational Technology Environment

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

INL/RPT-22-70441

TABLE OF CONTENTS

FIGURES

TABLES

PRECURSOR ANALYSIS REPORT: KANSAS WATER UTILITY INSIDER CYBER ATTACK 2019

1. EXECUTIVE SUMMARY

The Kansas Water Utility Insider Cyber Attack 2019 Precursor Analysis Report leverages publicly available information about the Kansas Ellsworth County Rural Water District No. 1 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 the evening of 27 March 2019, the adversary – a former employee – gained unauthorized remote access to the operational technology (OT) network of the Kansas Ellsworth County Rural Water District No. 1 water treatment plant via the plant's remote desktop software using valid shared credentials that were not revoked following his separation from the company. He likely used the water utility's native systems to perform an unscheduled shutdown of the water treatment plant's processes and turned off one of its filters. Shutting down these systems had the potential to directly impact the facility's purification process; however, a customer service specialist at the water utility stated that the attack had no impact on customers' drinking water. While specific details about the attack's impact are not documented, CyOTE analysts assess that some systems may have been temporarily unavailable until restarted.

Researchers and analysts identified six unique techniques utilized during the attack with a total of 58 observables using MITRE ATT&CK® for Industrial Control Systems. The CyOTE program assesses observables accompanying techniques used prior to the triggering event to identify opportunities to detect 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. Four of the identified techniques used during the Kansas Ellsworth County Rural Water District No. 1 cyber attack were precursors to the triggering event. Analysis identified 56 observables associated with these precursor techniques, 48 of which were assessed to have an increased likelihood of being perceived in the minutes preceding the triggering event. The response and comprehension time could have been reduced if the observables had been identified earlier.

The information gathered in this report contributes to a library of observables tied to a repository of artifacts, data sources, and technique detection references for practitioners and developers to support the comprehension of indicators of attack. Asset owners and operators can use these products if they experience similar observables or to prepare for comparable scenarios.

2. INTRODUCTION

The Cybersecurity for the Operational Technology Environment (CyOTE) program developed capabilities for energy sector organizations to independently identify adversarial tactics and techniques within their operational technology (OT) environments. Led by Idaho National Laboratory (INL) under 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. CyOTE Methodology 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 organizations in prioritizing their OT environment visibility investments.

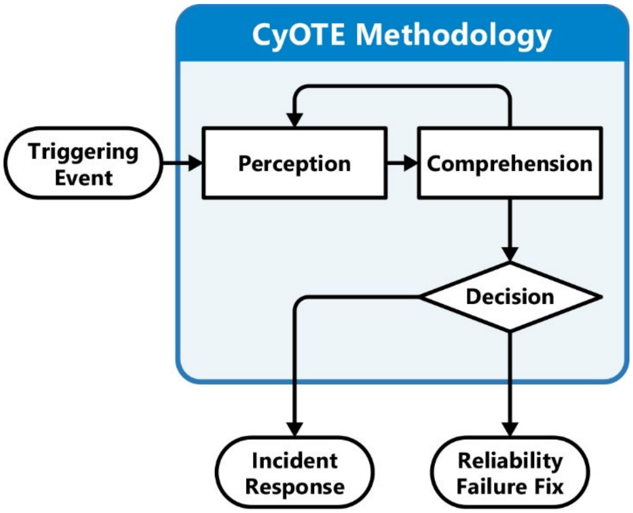


Figure 1. CyOTE Methodology

Historical case studies such as this one support continued learning through analysis of incidents that have impacted OT. This precursor analysis report 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 OT personnel 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 based on the CyOTE methodology portrays the attack-related observables associated with the precursor analysis report cyber attack. The timeline includes assessed dates, the triggering event, and comprehension of malicious activity by the organization. The point on this timeline when each technique appears is critical to the organization's ability to perceive and comprehend the associated malicious activity. Perception of techniques early in the timeline is critical, since halting those techniques will generally have greater potential to limit additional attack vectors using other techniques, defeat the cyber attack, and limit damage to operations.

Each technique has an assessed perceivability. Perceivability is a function of the number of observables and the potential for personnel to detect those observables. If a technique includes effects which personnel 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.

Comprehension can be further enhanced by technique artifacts created when adversaries employ certain attack techniques. The CyOTE program provides organizations with a library of observables reported in each historical case. The library can be used in conjunction with a repository of artifacts, data sources, and technique detection references for practitioners and developers to support the comprehension of indicators of attack.

2.2. BACKGROUND ON THE ATTACK

On the evening of 27 March 2019, a former employee gained unauthorized remote access to the OT network of the Ellsworth County Rural Water District No. 1 water treatment plant in Kansas (D-0).[1]

The adversary used his cellphone to connect to the plant's legitimate remote desktop software, GoToMyPC, using valid shared credentials that were not revoked following his separation from the company.[2] The GoToMyPC application utilizes an internet-based web service to provide remote access to hosts. As a result, the adversary employed both Internet Accessible Device and External Remote Services techniques to gain initial access.

Upon gaining access to the utility's control system environment, the adversary likely used native systems to unexpectedly shut down the water treatment plant's processes and turn off one of its filters.[a,3,4] Shutting down these systems had the potential to directly impact the facility's purification process; however, a customer service specialist at the water utility stated that the incident had no impact on customers' drinking water.[5]

Utility operators likely did not comprehend the facility was experiencing a cyberattack until after the triggering event was observed, which occurred when critical plant processes were unexpectedly shut off.

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.

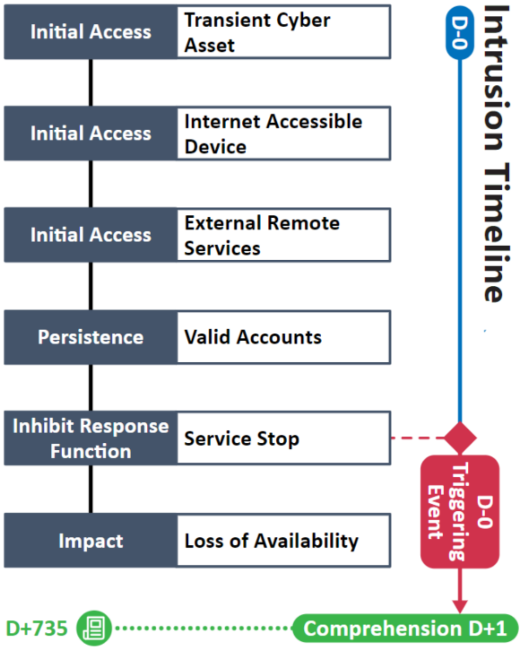


Figure 2. Intrusion Timeline

Shutting down these systems had the potential to directly impact the facility's purification process;[b] however, the incident had no impact on customers' drinking water.[6] Specific details about the attack's impact are not documented;

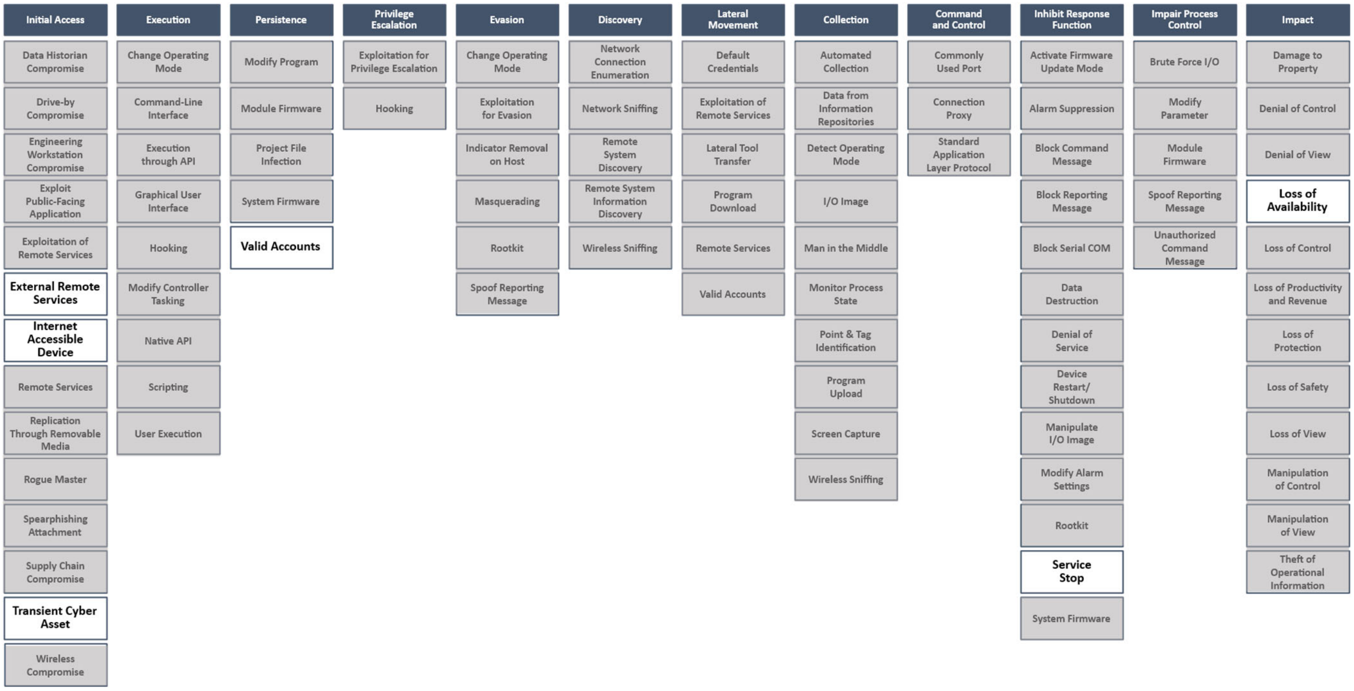
[a] According to the U.S. Centers for Disease Control and Prevention (CDC), water treatment plants use filters, consisting of different materials, to remove dust, chemicals, parasites, bacteria, and viruses from the water.

[b] Water treatment plants use different cleaning procedures although plants often use a series of steps to provide safe drinking water. These steps include coagulation, flocculation, sedimentation, filtration, and disinfection, according to the CDC. Coagulation involves introducing chemicals to cause particles to bind together. Coagulation is supported by flocculation, which is the process of mixing water to further stimulate particle coalescence, resulting in the formation of larger particles. Following these steps, the sedimentation process occurs, which allows larger particles to settle to the bottom of the water. The filtration process involves passing clean water through filters to further remove dissolved particles. The final step in the process involves disinfecting clean water of remaining parasites, bacteria, and viruses using chemical disinfectants. The Ellsworth County Rural Water District No. 1 water treatment plant uses chlorine dioxide as the primary disinfectant; however, it also uses chloramines, which are chemical compounds that contain chlorine and ammonia.

however, CyOTE analysts assess that some systems may have been temporarily unavailable until they were restarted.

Analysis identified six unique techniques in a sequence and timeframe likely used by adversaries during this cyber attack (Table 1). These attack techniques are defined according to MITRE's ATT&CK® for ICS framework.

Table 1. Techniques Used in the Kansas Water Utility 2019 Insider 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
Transient Cyber Asset									System Firmware		
Wireless Compromise											

Table 2. Precursor Analysis Report Quantitative Summary

Precursor Analysis Report Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	**6**
Technique Observables	**58**
Precursor Techniques	**4**
Precursor Technique Observables	**56**
Highly Perceivable Precursor Technique Observable	**48**

3. OBSERVABLE AND TECHNIQUE ANALYSIS

The following analysis may assist organizations 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. TRANSIENT CYBER ASSET (T0864) FOR INITIAL ACCESS

A former employee used his cellphone to gain unauthorized remote access to the OT network of the Kansas Ellsworth County Rural Water District No. 1 water treatment plant on the evening of 27 March 2019.[7,8] The adversary logged into the facility's legitimate remote desktop software, GoToMyPC, which likely was installed on his cellphone. GoToMyPC utilizes an internet-based web service to provide remote access to hosts. GoToMyPC requires outbound communications from the remotely accessed host, and access was granted to the adversary by connecting to the GoToMyPC website to obtain host IP and keys.

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe this activity in system or event logs; however, it is unlikely authenticated access would be flagged as malicious because a shared account was used, which could be associated with multiple authorized personnel. Additionally, since GoToMyPC is part of the utility's standard business processes, it would likely not be flagged as anomalous.

A total of three observables were identified with the use of the Transient Cyber Asset technique (T0864). This technique is important for investigation, as it establishes the initial access vector that was used to gain access to the utility's environment. The access vector is an important consideration for preventing similar attacks in the future. This technique appears early in the attack and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would limit an adversary's access.

Of the three observables associated with this technique, one is assessed to be highly perceivable, as access logs would likely be generated, and is italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 39 artifacts could be generated by the Transient Cyber Asset technique
Technique Observers[c]	IT Cybersecurity, OT Cybersecurity

[c] 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. INTERNET ACCESSIBLE DEVICE TECHNIQUE (T0883) FOR INITIAL ACCESS

A former employee gained unauthorized remote access to the OT network of the water treatment plant through an internet accessible device.[9,10] The adversary gained initial access to the plant's environment by using the facility's legitimate remote desktop software, GoToMyPC, as described in the Transient Cyber Asset (T0864) technique.

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe this activity, possibly via unconfirmed logging; however, it is unlikely authenticated access would be flagged as malicious because a shared account was used, which could be associated with multiple authorized personnel. Additionally, since GoToMyPC is part of the utility's standard business processes, it would likely not be flagged as anomalous.

A total of 17 observables were identified with the use of the Internet Accessible Device technique (T0822). This technique is important for investigation, as it establishes the initial vector used to gain access to the utility's environment. This technique appears early in the attack and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would limit an adversary's access.

Of the 17 observables associated with this technique, 15 are assessed to be highly perceivable, as access logs would likely be generated, and are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 23 artifacts could be generated by the Internet Accessible Device technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

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

The adversary gained initial access to the plant's OT environment from the Internet by using the facility's legitimate remote access desktop software, GoToMyPC. The adversary accessed the plant's GoToMyPC application by using valid shared credentials.[11]

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe this activity, possibly via unconfirmed logging; however, it is unlikely authenticated access would be flagged as malicious because a shared account was used, which could be associated with multiple authorized personnel.

A total of 18 observables were identified with the use of the External Remote Services technique (T0822). This technique is important for investigation, as it establishes the initial vector that was used to gain access to the utility's environment. This technique appears early in the attack and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent adversaries from gaining access to internal operational networks and shutting down the purification process.

Of the 18 observables associated with this technique, 16 are assessed to be highly perceivable, as access logs would likely be generated, and are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 28 artifacts could be generated by the External Remote Services technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

3.4. VALID ACCOUNTS TECHNIQUE (T0859) FOR PERSISTENCE

The adversary used valid shared credentials to remotely access the water treatment plant's environment via the GoToMyPC application.[12] Upon gaining access to the utility's environment, the adversary used a shared pass code to access the facility's control software.[13] The utility's shared credentials were not changed after the employee separated from the utility.[14]

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe the initial access, possibly via unconfirmed logging; however, it is unlikely the adversary's authenticated access would be flagged as malicious because he used shared accounts, which can be used by multiple authorized personnel.

A total of 18 observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation, as it establishes persistent access to the utility's environment. This technique appears near the midpoint in the attack and responding to it will limit persistence via adversary-created credentials and access to protected systems. Terminating the chain of techniques at this point would protect the control systems network from further unauthorized access.

Of the 18 observables associated with this technique, 16 are assessed to be highly perceivable and are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 16 artifacts could be generated by the Valid Accounts technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

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

With access to the water utility's native systems, the adversary shut down the water treatment plant's processes and turned off one of its filters.[15] Shutting down these systems had the potential to directly impact the facility's purification process.[16] The time it took for utility personnel to discover that plant systems were offline and to restore operations is not known.

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, and Support Staff may have been able to observe plant systems being shut down.

One observable was identified with the use of the Service Stop technique (T0881). This technique is important for investigation because it demonstrates adversary intentions and can assist in reconstructing part of the attack, which can be helpful in addressing impacts and assigning mitigations to protect the environment from future incidents. This technique appears late in the attack timeline. Terminating the chain of techniques at this point would likely have minimal influence on preventing an impact; however, rapid response may reduce impact severity.

The one observable is assessed to be highly perceivable and is italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 13 artifacts could be generated by the Service Stop technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff

3.6. LOSS OF AVAILABILITY TECHNIQUE (T0826) FOR IMPACT

The plant's water purification control systems were unavailable to plant personnel for an unspecified length of time before the systems were brought back online. An unscheduled shutdown of the water treatment plant's systems had the potential to impact the facility's purification process; however, a customer service specialist at the water utility indicated the incident had no impact on customers' drinking water.[17] CyOTE analysts assess that some systems likely were temporarily unavailable until they were restarted.

OT Staff, OT Cybersecurity, Engineering, and Support Staff personnel may have been able to observe the results of the temporary loss of availability when trying to control or restart systems.

One observable was identified with the use of the Loss of Availability technique (T0826). This technique is important for investigation as it could be relevant in assessing and responding to the impact. This technique appears late in the attack timeline. Terminating the chain of techniques at this point would likely have minimal influence on preventing any impact; however, rapid response may reduce impact severity and reduce recovery time.

The one observable is assessed to be highly perceivable and is italicized and marked † in Appendix A.

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	OT Staff, OT Cybersecurity, Engineering, Support Staff

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are italicized and marked †

Observables Associated with Transient Cyber Asset Technique (T0864)	
Observable 1	Anomalous Usage of Transient Cyber Asset: Usage of Cellular Device: Usage of Personally Owned Cellular Device: Usage of Remote Service Application: Usage of GoToMyPC Application
Observable 2	Anomalous Usage of Remote Access Service: GoToMyPC: Using Personally Owned Cellular Device
Observable 3†	*Anomalous Access Log Entries on Webapp Service Account: GoToMyPC.com*

Observables Associated with Internet Accessible Device Technique (T0883)	
Observable 1†	*Anomalous Usage of Remote Access Service: GoToMyPC: Using Cellular Device*
Observable 2	Anomalous Network Communications: Over TCP Port 80 (Outbound)
Observable 3	Anomalous Network Communications: Over TCP Port 443 (Bidirectional)
Observable 4†	*Anomalous Network Communications: Over UDP Port 8200 (Bidirectional)*
Observable 5†	*Anomalous Network Communications: Domain Name System (DNS) Requests: Over UDP/TCP Port 53: To Anomalous Domain: *.filestackapi.com*
Observable 6†	*Anomalous Network Communications: Domain Name System (DNS) Requests: Over UDP/TCP Port 53: To Anomalous Domain: api.filepicker.io*
Observable 7†	*Anomalous Network Communications: Domain Name System (DNS) Requests: Over UDP/TCP Port 53: To Anomalous Domain: *.expertcity.com*
Observable 8†	*Anomalous Network Communications: Domain Name System (DNS) Requests: Over UDP/TCP Port 53: To Anomalous Domain: *.getgo.com*
Observable 9†	*Anomalous Network Communications: Domain Name System (DNS) Requests: Over UDP/TCP Port 53: To Anomalous Domain: *.getgoservices.com*
Observable 10†	*Anomalous Network Communications: Domain Name System (DNS) Requests: Over UDP/TCP Port 53: To Anomalous Domain: *.getgoservices.net*
Observable 11†	*Anomalous Network Communications: Domain Name System (DNS) Requests: Over UDP/TCP Port 53: To Anomalous Domain: *.goto-rtc.com*
Observable 12†	*Anomalous Network Communications: Domain Name System (DNS) Requests: Over UDP/TCP Port 53: To Anomalous Domain: *.GoTo.com*
Observable 13†	*Anomalous Network Communications: Domain Name System (DNS) Requests: Over UDP/TCP Port 53: To Anomalous Domain: *.GoToinc.com*
Observable 14†	*Anomalous Network Communications: Domain Name System (DNS) Requests: Over UDP/TCP Port 53: To Anomalous Domain: *.raas.io*
Observable 15†	*Anomalous Network Communications: Domain Name System (DNS) Requests: Over UDP/TCP Port 53: To Anomalous Domain: *.accounts.logme.in*
Observable 16†	*Anomalous Log Entries on Local Host: user/appdata/local/temp/logmeinlogs*
Observable 17†	*Anomalous Access Log Entries on Webapp Service Account: GoToMyPC.com*

Observables Associated with External Remote Services Technique (T0822)	
Observable 1†	*Anomalous Usage of Remote Access Service: GoToMyPC: Using Cellular Device*
Observable 2†	Anomalous Use of Shared Account: Remote Services Application: GoToMyPC Application
Observable 3	Anomalous Network Traffic Associated with Remote Services Application: GoToMyPC Application: Over HTTP TCP Port 80 (Outbound)
Observable 4	Anomalous Network Traffic Associated with Remote Services Application: GoToMyPC Application: Over TCP port 443 (bidirectional)
Observable 5†	*Anomalous Network Traffic Associated with Remote Services Application: GoToMyPC Application: Over TCP port 8200 (unidirectional)*
Observable 6†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: *.filestackapi.com*
Observable 7†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: api.filepicker.io*
Observable 8†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: *.expertcity.com*
Observable 9†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: *.getgo.com*
Observable 10†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: *.getgoservices.com*
Observable 11†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: *.getgoservices.net*
Observable 12†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: *.goto-rtc.com*
Observable 13†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: *.GoTo.com*
Observable 14†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: *.GoToinc.com*
Observable 15†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: *.raas.io*
Observable 16†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: *.accounts.logme.in*
Observable 17†	*Anomalous Log Entries on Local Remote Service Host: GoToMyPC Application: user/appdata/local/temp/logmeinlogs*
Observable 18†	*Anomalous Access Log Entries on Webapp Service Account: GoToMyPC.com*

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1†	*Anomalous Usage of Remote Access Service: GoToMyPC: Using Cellular Device*

Observables Associated with Valid Accounts Technique (T0859)	
Observable 2†	Anomalous Use of Shared Account: Remote Services Application: GoToMyPC Application
Observable 3	Anomalous Network Traffic Associated with Remote Services Application: GoToMyPC Application: Over HTTP/TCP Port 80 (Outbound)
Observable 4	Anomalous Network Traffic Associated with Remote Services Application: GoToMyPC Application: Over TCP port 443 (bidirectional)
Observable 5†	*Anomalous Network Traffic Associated with Remote Services Application: GoToMyPC Application: Over TCP port 8200 (unidirectional)*
Observable 6†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: *.filestackapi.com*
Observable 7†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: api.filepicker.io*
Observable 8†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: *.expertcity.com*
Observable 9†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: *.getgo.com*
Observable 10†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: *.getgoservices.com*
Observable 11†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: *.getgoservices.net*
Observable 12†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: *.goto-rtc.com*
Observable 13†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: *.GoTo.com*
Observable 14†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: *.GoToinc.com*
Observable 15†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: *.raas.io*
Observable 16†	*Anomalous Network Traffic: Domain Name System (DNS) requests: Over UDP/TCP Port 53: To Anomalous Domain: *.accounts.logme.in*
Observable 17†	*Anomalous Log Entries on Local Remote Service Host: GoToMyPC Application: user/appdata/local/temp/logmeinlogs*
Observable 18†	*Anomalous Access Log Entries on Webapp Service Account: GoToMyPC.com*

Observables Associated with Service Stop Technique (T0881)	
Observable 1†	*Anomalous Shutdown of Controlled Processes: Water Treatment Processes: Shutdown of Water Filtration Process*

Observables Associated with Loss of Availability Technique (T0826)	
Observable 1†	*Anomalous Loss of Availability of Controlled Processes: Water Treatment Processes: Shutdown of Water Filtration Process*

APPENDIX B: ARTIFACTS LIBRARY

Artifacts Associated with Transient Cyber Asset (T0864)	
Artifact 1	TFTP Port
Artifact 2	Telnet Traffic
Artifact 3	RDP Traffic Port
Artifact 4	VNC Traffic Port
Artifact 5	SSH Traffic Port
Artifact 6	Network Discover Protocols
Artifact 7	.lnk File
Artifact 8	Media Transfer Protocol (MTP) Connections
Artifact 9	MAC Address
Artifact 10	Picture Transfer Protocol (PTP) Connections
Artifact 11	Mass Storage Class (MSC) Connections
Artifact 12	FTPS Port
Artifact 13	USB Version
Artifact 14	Changes to System Registry SYSTEM\MOUNTEDDEVICES
Artifact 15	USB Model
Artifact 16	DNS Queries Traffic
Artifact 17	USB Make
Artifact 18	HTTP Port
Artifact 19	HTTPS Port
Artifact 20	ARP Connections
Artifact 21	USB Serial Number
Artifact 22	First Time Device Connected
Artifact 23	User Agents
Artifact 24	Honey Pot Logs
Artifact 25	Network Connections with Honeypot
Artifact 26	Security Log Attempt to Access Removable Storage Object Event
Artifact 27	System Log Plug and Play Driver Installed Event
Artifact 28	Plug and Play Log File setupapi.log
Artifact 29	Changes to System Registry SYSTEM\CURRENTCONTROLSET\ENUM\USBSTOR
Artifact 30	Device Disconnected Time
Artifact 31	Drive Letter Creation
Artifact 32	Source IP Address

Artifacts Associated with Transient Cyber Asset (T0864)	
Artifact 33	Last Time Device Connected
Artifact 34	Device User
Artifact 35	Security Log Failure to Access Removeable Device
Artifact 36	Bytes Received From
Artifact 37	Bytes Sent from System Resource Usage Manager
Artifact 38	FTP Port
Artifact 39	Wireless Transmission

Artifacts Associated with Internet Accessible Device Technique (T0883)	
Artifact 1	Host Registry Entries
Artifact 2	HTTPS Traffic
Artifact 3	Suspicious Connections in Proxy Logs
Artifact 4	Timestamps
Artifact 5	VPN Logoff Events
Artifact 6	Suspicious Connections in Firewall Logs
Artifact 7	VPN Logon Events
Artifact 8	SAP Traffic
Artifact 9	Host Registry Entries HKEY_LOCAL_MACHINE\SYSTEM
Artifact 10	SQL Traffic
Artifact 11	Host Information in External Data Store or Website (SHODAN)
Artifact 12	HTTP 80
Artifact 13	VNC Traffic Port 5800 or
Artifact 14	Dialog Boxes Opened on HMI or
Artifact 15	Application Authentication Events
Artifact 16	Internet Address in Memory Socket Data
Artifact 17	Remote Logins in OS Logs (Windows Event)
Artifact 18	Operational Database Connection to External Addresses
Artifact 19	Industrial Traffic from Internet Address
Artifact 20	Standard Traffic from Internet Address
Artifact 21	Internet Address in Application Logs
Artifact 22	Internet Address in OS Logs
Artifact 23	Internet Address in Command Line Record Data (netstat)

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

Artifacts Associated with Valid Accounts Technique (T0859)	
Artifact 1	Logon Session Creation
Artifact 2	User Account Creation
Artifact 3	Logon Type Entry
Artifact 4	Logon Timestamp

Artifacts Associated with Valid Accounts Technique (T0859)	
Artifact 5	Failed Logons Event
Artifact 6	Successful Logon Event
Artifact 7	System Logs
Artifact 8	Default Credential Use
Artifact 9	Authentication Creation
Artifact 10	Prefetch Files Created After Execution
Artifact 11	Logons
Artifact 12	Application Log
Artifact 13	Domain Permission Requests
Artifact 14	Permission Elevation Requests
Artifact 15	Application Use Times
Artifact 16	Configuration Changes

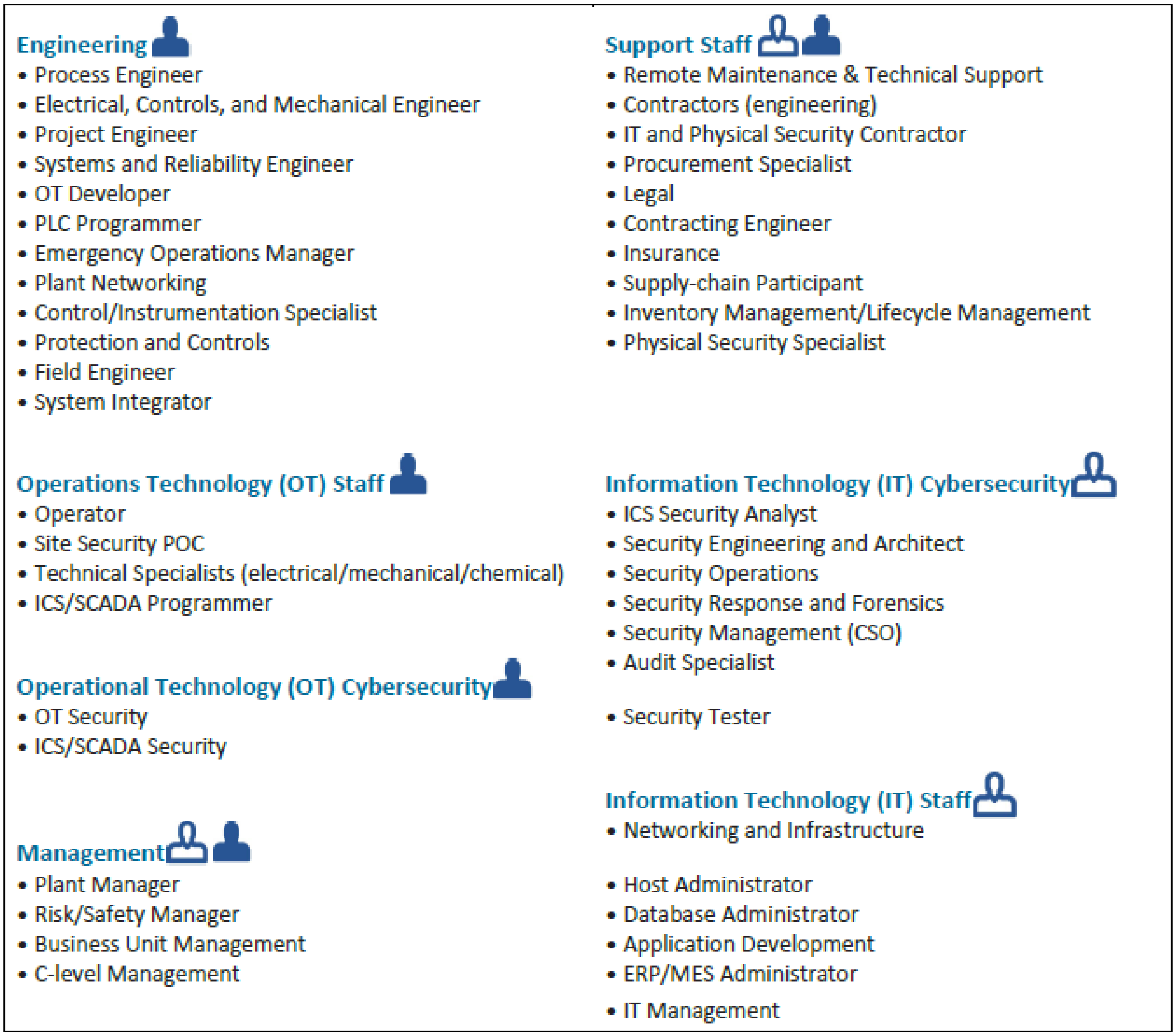
Artifacts Associated with Service Stop Technique (T0881)	
Artifact 1	Internal System Logs
Artifact 2	Alarm Event
Artifact 3	OS API Call
Artifact 4	Application Error Messages
Artifact 5	Process Error Messages
Artifact 6	Application Service Stop
Artifact 7	Registry Change HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES
Artifact 8	OS Service Crash
Artifact 9	System Event Logs
Artifact 10	Application Event Logs
Artifact 11	System Resource Usage Manager Application Usage Change
Artifact 12	Command Line System Argument
Artifact 13	Process Failure

Artifacts Associated with Loss of Availability Technique (T0826)	
Artifact 1	Process Failure Due to Loss of Required Network or System Dependency
Artifact 2	Unexplained Loss of User Data
Artifact 3	Changes In Network Routing or Usage of Redundant Control System Network Connection Due to Failed Network Path

Artifacts Associated with Loss of Availability Technique (T0826)	
Artifact 4	Significant Reduction or Increase in Network Traffic Due to Malware Propagation of Disappearance of Services
Artifact 5	Significant Logged Usage of Native Crypto Functions or Presence of Import of Crypto Functions in Binaries
Artifact 6	Operator or User Discovery of Encrypted or Inoperable Systems
Artifact 7	File System Modification Artifacts Might Be Associated with The Loss of Availability Might Be Present on Disk
Artifact 8	Unexplained Loss of Application Data

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. District Court – District of Kansas | "Case No. 21-40029-HLT" | https://www.ksn.com/wp-content/uploads/sites/13/2021/03/travnichek-indictment.pdf | 31 March 2021 | Accessed on 4 September 2022 | The source is publicly available information and does not contain classification markings]

[2] [WaterISAC | "(Updated October 21, 2021) Insider Threat – Former Employee Indicted for Unauthorized Computer Access with Intent to Harm a Kansas Public Water District" | https://www.waterisac.org/portal/updated-october-21-2021-insider-threat-%E2%80%93-former-employee-indicted-unauthorized-computer | 21 October 2021 | Accessed on 4 September 2022 | The source is publicly available information and does not contain classification markings]

[3] [U.S. Department of Justice | "Indictment: Kansa Man Indicted for Tampering with a Public Water System" | https://www.justice.gov/usao-ks/pr/indictment-kansas-man-indicted-tampering-public-water-system | 31 March 2021 | Accessed on 4 September 2022 | The source is publicly available information and does not contain classification markings]

[4] [U.S. Department of Justice | "Kansas Man Pleads Guilty to Water Facility Tampering" | https://www.justice.gov/usao-ks/pr/kansas-man-pleads-guilty-water-facility-tampering | 21 October 2021 | Accessed on 4 September 2022 | The source is publicly available information and does not contain classification markings]

[5] [CyberScoop | Sean Lyngaas | "Kansas Man Indicted in Connection with 2019 Hack at Water Utility" | https://www.cyberscoop.com/kansas-ellsworth-water-district-hack-travnichek/ | 1 April 2021 | Accessed on 4 September 2022 | The source is publicly available information and does not contain classification markings]

[6] [CyberScoop | Sean Lyngaas | "Kansas Man Indicted in Connection with 2019 Hack at Water Utility" | https://www.cyberscoop.com/kansas-ellsworth-water-district-hack-travnichek/ | 1 April 2021 | Accessed on 4 September 2022 | The source is publicly available information and does not contain classification markings]

[7] [U.S. Department of Justice | "Indictment: Kansa Man Indicted for Tampering with a Public Water System" | https://www.justice.gov/usao-ks/pr/indictment-kansas-man-indicted-tampering-public-water-system | 31 March 2021 | Accessed on 4 September 2022 | The source is publicly available information and does not contain classification markings]

[8] [U.S. District Court – District of Kansas | "Case No. 21-40029-HLT" | https://www.ksn.com/wp-content/uploads/sites/13/2021/03/travnichek-indictment.pdf | 31 March 2021 | Accessed on 4 September 2022 | The source is publicly available information and does not contain classification markings]

[9] [U.S. Department of Justice | "Indictment: Kansa Man Indicted for Tampering with a Public Water System" | https://www.justice.gov/usao-ks/pr/indictment-kansas-man-indicted-tampering-public-water-system | 31 March 2021 | Accessed on 4 September 2022 | The source is publicly available information and does not contain classification markings]

[10] [U.S. District Court – District of Kansas | "Case No. 21-40029-HLT" | https://www.ksn.com/wp-content/uploads/sites/13/2021/03/travnichek-indictment.pdf | 31 March 2021 | Accessed on 4 September 2022 | The source is publicly available information and does not contain classification markings]

[11] [WaterISAC | "(Updated October 21, 2021) Insider Threat – Former Employee Indicted for Unauthorized Computer Access with Intent to Harm a Kansas Public Water District" | https://www.waterisac.org/portal/updated-october-21-2021-insider-threat-%E2%80%93-former-employee-indicted-unauthorized-computer | 21 October 2021 | Accessed on 4 September 2022 | The source is publicly available information and does not contain classification markings]

[12] [WaterISAC | "(Updated October 21, 2021) Insider Threat – Former Employee Indicted for Unauthorized Computer Access with Intent to Harm a Kansas Public Water District" | https://www.waterisac.org/portal/updated-october-21-2021-insider-threat-%E2%80%93-former-employee-indicted-unauthorized-computer | 21 October 2021 | Accessed on 4 September 2022 | The source is publicly available information and does not contain classification markings]

[13] [WaterISAC | "(Updated October 21, 2021) Insider Threat – Former Employee Indicted for Unauthorized Computer Access with Intent to Harm a Kansas Public Water District" | https://www.waterisac.org/portal/updated-october-21-2021-insider-threat-%E2%80%93-former-employee-indicted-unauthorized-computer | 21 October 2021 | Accessed on 4 September 2022 | The source is publicly available information and does not contain classification markings]

[14] [WaterISAC | "(Updated October 21, 2021) Insider Threat – Former Employee Indicted for Unauthorized Computer Access with Intent to Harm a Kansas Public Water District" | https://www.waterisac.org/portal/updated-october-21-2021-insider-threat-%E2%80%93-former-employee-indicted-unauthorized-computer | 21 October 2021 | Accessed on 4 September 2022 | The source is publicly available information and does not contain classification markings]

[15] [U.S. Department of Justice | "Kansas Man Pleads Guilty to Water Facility Tampering" | https://www.justice.gov/usao-ks/pr/kansas-man-pleads-guilty-water-facility-tampering | 21 October 2021 | Accessed on 4 September 2022 | The source is publicly available information and does not contain classification markings]

[16] [U.S. Department of Justice | "Indictment: Kansa Man Indicted for Tampering with a Public Water System" | https://www.justice.gov/usao-ks/pr/indictment-kansas-man-indicted-tampering-public-water-system | 31 March 2021 | Accessed on 4 September 2022 | The source is publicly available information and does not contain classification markings]

[17] [CyberScoop | Sean Lyngaas | "Kansas Man Indicted in Connection with 2019 Hack at Water Utility" | https://www.cyberscoop.com/kansas-ellsworth-water-district-hack-travnichek/ | 1 April 2021 | Accessed on 4 September 2022 | The source is publicly available information and does not contain classification markings]