Evolution and Trends of Industrial Control System Cyber Incidents since 2017

Robert Grubbs,[1, 2] Jeremiah Stoddard,[3] Sarah Freeman,[4] Ron Fisher[5]

[1] Senior Cyber Intelligence Analyst, Idaho National Laboratory

[2] Corresponding Author, Robert.Grubbs@INL.gov

[3] Critical Infrastructure Security Analyst, Idaho National Laboratory

[4] Industrial Control Systems Cyber Security Analyst, Idaho National Laboratory

[5] Director of Infrastructure Assurance and Analysis, Idaho National Laboratory

[*see Author Capsule Bios below*]

Abstract

The industrial control systems (ICSs) that manage our critical infrastructure are increasingly converging with corporate networks and the Internet as technology and businesses prioritize digital connectivity. These connections make them more vulnerable and available to malicious cyber actors who traditionally targeted the companies' more public-facing information technology (IT) networks. This paper will review select publicly reported cyber incidents to highlight the continued and growing threat to ICS devices and operational technology (OT) environments. It will summarize the incident and when available, will provide information on the cyber actors, the vulnerabilities they exploited, and any publications the U.S. Government (USG) provided in response. Data belonging to the Department of Homeland Security (DHS) will be used to highlight quantitative trends concerning ICS incidents. This paper builds on "History of Industrial Control System Cyber Incidents" (Hemsley & Fisher 2018), a paper that highlighted select noteworthy threats and incidents to ICS systems up to 2017. This paper will similarly review select incidents occurring after the last previously reviewed incident, Triton/HatMan, December 2017, and will note ICS incident trends including IT/OT convergence and advances in cyber-threat actors' capabilities in observed in the examined incidents.

Keywords: Industrial Control System, Information Technology, Operational Technology, Compromise

doi: 10.18278/jcip.2.2.4

Introduction

Control systems manage and regulate devices or other systems, ranging from simple household appliances such as a refrigerator or air-conditioning unit in a single-family home, to large-scale systems governing public transportation or factory machinery. Industrial control systems (ICSs) are a collection of control systems and their instrumentations used to govern or automate industrial processes and exist in operation technology (OT) environments. ICSs are frequently managed via a Supervisory Control and Data Acquisition (SCADA) system that provides a graphical user interface (GUI) for the operator to perform their duties, including observing the system, receiving and acting upon alarms, or adjusting processes governed by the SCADA. These industrial processes are essential to the critical infrastructure sectors, including but not limited to water and wastewater systems (WWS), energy, fuel, and transportation, which are the backbone of modern conveniences. Whereas the primary benefit of using control systems in consumer devices is convenience, at the corporate and national critical infrastructure level ICS and SCADA systems provide significant cost efficiencies and thus permeate the operation and control of those infrastructures. Table 1 provides an example of how ICS and SCADA are widely utilized in critical infrastructures.

Table 1. Examples of Control Systems in Critical Infrastructures.

Critical Infrastructure	Control Systems/ICS Example(s)
Energy Sector	SCADA and Distributed Control Systems (DCS) used to operate and manage hundreds of thousands of miles of transmission and distribution of power grids and oil and natural gas pipelines; and the complexity of operating and maintaining petroleum refineries.
Water/Wastewater Sector	SCADA used to operate and monitor water treatment, water testing, water quality, and water flows to storage through end use.
Transportation Sector	Control systems are embedded in all modes of transportation (e.g., trucking, automotive, rail, air, water) to efficiently transport goods and people. As movement towards autonomous vehicles continue, this will increase significantly the control systems in automobiles and other transportation equipment.
Public Health	Control systems increasing utilization in medical devices including dialysis equipment, pacemakers, and health monitoring equipment.

Even though the services ICSs provide touch our lives every day, from a cyber-perspective, ICS/SCADA and OT generally receive less attention than the information technology (IT) environments that govern our modern Internet-dependent businesses and lifestyles. As businesses and the technologies that run them become more Internet-connected, many devices and systems that have not traditionally been Internet-connected are coming online, increasing the cyber-footprint for many companies not accustomed to minding cybersecurity best practices.

This paper will examine incidents that either compromised ICSs or disrupted ICS/SCADA operations due to a compromised IT environment, and when available, will note the attack vector and threat type. Some of the attack vectors include ransomware, insider threat, supply chain and brute force attacks, and these incidents were carried out by both cyber-criminal groups and advanced persistent threat (APT) (i.e., nation-state) cyber actors. The incidents covered in this paper do not review every single recorded ICS compromise during the examined timeframe, but rather a selected list. Some of the compromises directly targeted ICS devices, whereas in other incidents, ICS devices were indirectly targeted and affected.

The incidents selected for review are notable for a variety of reasons including, but not limited to: having occurred since 2017 to avoid anything in the Hemsley & Fisher paper, the attack vector used in order to demonstrate the diversity of ways a network or environment can be targeted, the notoriety and amount of media coverage of the event, leading to an expectation it would be covered (e.g., Colonial Pipeline, JBS meat plant, Oldsmar), the amount of publicly available information allowing for comprehensive and verifiable incident review and independent research, or to specifically highlight one facet of the incident, such as how the victim handled the incident publicly (e.g., Volue ASA). Lastly, a few incidents listed were chosen because the company did not make the initial compromise public and only later agreed to be anonymously covered in Cybersecurity and Infrastructure Security Agency (CISA) reporting, highlighting that there are many more incidents than those available on the public Internet.

According to metrics provided by CISA, for the first three quarters of the fiscal year 2021 (FY-21) only 12.6% of victim notifications performed by CISA were to the Energy, Food & Agriculture, Nuclear, Transportation or WWS sectors. Not all of these victim notifications involved an OT compromise, but these sectors are highly reliant upon OT processes. Though IT environments are more frequently targeted by cyber actors, the low percentage of notifications is an indicator many cybersecurity events in OT environments may go unreported and remain unknown to their customers until well after the incident is over.

Timeline of ICS Incidents

This paper timeline starts in 2018, picking up from the previous ICS paper (Hemsley & Fisher 2018) to provide a continuous glimpse of ICS incidents over time. These papers combined provide insights into the increasing level of vulnerabilities and threats to ICS and highlight the growing number of attack vectors available to threat actors.

Table 2 below lists the incidents covered in this paper temporally.

Table 2. ICS Incidents Covered in this Paper.

YEAR	ATTACK TYPE	VICTIM(S)	SUMMARY
2018	Third-party / supply chain	Energy Services Group	Attack on billing software company disrupts a natural gas company
2019	Insider Threat	Unidentified Power Plant	Employee installed ransomware via infected peripheral device
2019	Remote Exploit	sPower	Remote exploit caused Denial-of-Service (DoS) and device restarts
2019	Insider threat	Post Rock Water District, Ellsworth County (KS)	Ex-employee attempted to alter water disinfectant levels using still-valid user credentials
2019	Brute Force	Energy Companies Across Europe and U.S.	APT actors use Kubernetes cluster in brute force attacks
2020	Remote Exploit	Camrosa Water District (CA)	Cyber actors encrypt files, exfiltrate personal information
2020	Word Press vulnerability / watering hole	Florida Water Infrastructure Construction Company	Cyber actors turn legitimate water sector site into a watering hole attack page
2021	Unauthorized Remote Access	San Francisco Bay-area Water Treatment Plant (CA)	Cyber actors use TeamViewer to delete programs used to treat water
2021	Ransomware in the IT environment	Eletrobras & Copel Electric Power Utilities	Ransomware affects operations at two plants; cyber actors exfiltrate sensitive business and network data
2021	Unauthorized Remote Access	Oldsmar (FL) Water Treatment Plant (WTP)	Cyber actors use remote access in attempt to change water chemistry
2021	Unknown ransomware in the OT environment	Nevada-based WWS	Ransomware affects the ICS/SCADA environment
2021	Supply chain	Metropolitan Water District of Southern California (MWD)	China-based APT cyber actors compromise MWD device using Pulse Secure exploit

2021	Ransomware in the IT environment	City of Tulsa (OK)	Ransomware affects city services and customer-facing website
2021	Ryuk ransomware in the IT environment	Volue ASA (Norway)	Ransomware disrupts operations; company lauded for transparency and accountability in public response
2021	Ransomware in the IT environment	Colonial Pipeline	Ransomware disrupts operations on US' largest pipeline
2021	ZuCaNo ransomware in OT environment	Maine-based WWS	Treatment center needed to be run manually until operations returned to normal
2021	Ghost variant ransomware in the OT environment	California-based WWS	Ransomware sat on several SCADA servers for a month until detected

Chronological List of ICS Incidents

Energy Services Group LLC

In March 2018, unidentified cyber actors compromised a software platform developed by Energy Services Group LLC that is used for billing and customer transactions (Lyngaas 2018) The attack on the billing software impacted the Texas-based Energy Transfer Partners LP, a natural gas and propane pipeline company, with more than 71,000 miles of pipelines across 38 states and Canada (Energy Transfer 2018). The attack specifically targeted an Electronic Data Interchange (EDI) for the Eastern Panhandle pipeline serviced by Energy Services Group LLC and caused the system to be taken offline. Taking the system offline did not disrupt the flow of natural gas in the pipeline (Ciscomag 2020).

This incident demonstrates the reliance OT systems have on IT infrastructure for many critical infrastructure operations. Even though OT systems may still function correctly, if the owner/operator cannot properly determine usage or billing rates, they may choose to take a service offline. This incident also highlights the supply chain and third-party concerns inherent to OT environments as more of their control systems are regulated by IT systems. While the ICS owner/operator may be secure, their IT partners that manage their data can be compromised which can still lead to service interruptions.

Unidentified Power Plant

Sometime in early 2019 cyber actors convinced a trusted visitor of an unidentified power plant outside of the United States to plug a universal serial bus (USB) mouse into a computer system. The affected computer was a human machine interface (HMI) providing the operator views of the power plant. Once the infected mouse was plugged in, the cyber actors were able to remotely deploy ransomware. The cyber actors did not do any damage to any of the ICSs, despite having access. The power plant paid the ransom but did not get their files back and had to rebuild their network, impacting operations at the plant for three months. The trusted visitor was eventually arrested and charged with knowingly plugging in the infected mouse into an ICS computer in exchange for money (Tomlinson 2020).

This incident highlights how ransomware groups may try to bypass traditional remote, network-based efforts by looking to co-opt insiders. Whether the insider is acting intentionally, as in this case, or is an unsuspecting accomplice, the insider threat posed by trusted visitors or employees of ICS companies remains high and is an appealing choice to cyber-criminals if they have a specific target victim in mind.

sPower

In March 2019, unidentified cyber actors attempted to exploit an Internet-facing firewall, resulting in device restarts, DoS, and periodic loss of view against the Salt Lake City-based solar and wind energy developer sPower for approximately 12 hours. While the power company lost visibility into its network, no actual power outages were reported (Tomlinson 2019). A DoS attack occurs when cyber actors and/or botnets flood the targeted network with enough traffic that it cannot process requests or it crashes, preventing the network from being accessible for legitimate use (CISA 2009). The DoS attack likely targeted a Cisco Adaptive Security Appliance (CASA), an Internet-facing device that functions as a firewall and virtual private network (VPN) that has been associated with numerous vulnerabilities (Behr 2019). The CASA devices have previously been successfully targeted via CVE-2018-0296 and CVE-2018-0101[1] by malicious cyber actors who seek to cause a denial-of-service condition by causing the affected devices to reload unexpectedly (Cimpanu 2018).

[1] CVE-2018-0296: According to Mitre.org, CVE-2019-0296 is a vulnerability in the web interface of the Cisco Adaptive Security Appliance (ASA) could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. It is also possible on certain software releases that the ASA will not reload, but an attacker could view sensitive system information without authentication by using directory traversal techniques. The vulnerability is due to lack of proper input validation of the HTTP URL.

CVE-2018-0101: According to Mitre.org, CVE-2018-1010 is a vulnerability in the Secure Sockets Layer (SSL) VPN functionality of the Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause a reload of the affected system or to remotely execute code. The vulnerability is due to an attempt to double free a region of memory when the webvpn feature is enabled on the Cisco ASA device. An attacker could exploit this vulnerability by sending multiple, crafted XML packets to a webvpn-configured interface on the affected system. An exploit could allow the attacker to execute arbitrary code and obtain full control of the system or cause a reload of the affected device.

This attack, directed against transmission-level assets, is the first of its kind; although this event did not result in disruptions in electricity delivery, it was the largest attack against the U.S. electric sector by affected megawatt (MW) (nearly 20 MW). This incident demonstrated the fragility of IT infrastructure within the OT environment. Manufacturers of OT systems often go to great lengths to ensure the reliability and availability of their technologies, often implementing robust resiliency testing. IT asset resiliency however, for assets deployed within the OT environment, is often overlooked. The disruption of IT can still impact OT functions.

Post Rock Water District, Ellsworth (KS)

In March 2019 a former employee of the Post Rock Water District in Ellsworth County, Kansas allegedly logged into their computer system in an effort to alter the disinfectant levels. The former employee worked for the WWS utility from 2018 until January 2019, and remotely logging in after hours to monitor the facilities computer system was part of his normal work duties. It is likely that the ex-employee successfully logged in after his termination date, using credentials which were not properly revoked at the time of his resignation (O'Donnell & Welch 2021; Morgan 2021). The unauthorized intrusion caused an unplanned shutdown of the plant's processes, affecting the facility's cleaning and disinfecting procedures. It is alleged in the indictment that the former employee logged in with the intention of harming the drinking water treated by the Ellsworth County Rural Water District (ksn.com 2021).

This incident demonstrates the insider threat attack vector that IT and OT companies face, and it was compounded by poor operational security (OPSEC) practices. The mandatory and timely deletion of credentials for exiting employees, and periodic audits comparing valid user credentials to current employees can help diminish this attack vector.

Unidentified Energy Companies in Europe and the U.S.

Beginning in mid-2019 and continuing through early 2021, APT actors targeted unidentified energy companies in Europe and in the United States in a global brute force campaign. The APT actors—Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS), military unit 26165—have been attributed in open-sources by the private sector as APT 28, Fancy Bear, Pawn Storm, Sofacy Group, Sednit, STRONTIUM, Tsar Team, and other names (defense.gov 2021; mitre.org 2021).

The APT actors employed a Kubernetes[2] cluster to conduct brute force at-

[2] A Kubernetes cluster is a set of nodes that run containerized applications. Kubernetes clusters allow containers to run across multiple machines and environments: virtual, physical, cloud-based, and on-premises. Kubernetes containers are not restricted to a specific operating system (OS), unlike virtual machines.

tacks against various targets globally. A significant number of the targeted entities used Microsoft Office 365 cloud services. The actors also targeted other service providers and on-premises email servers using a variety of different protocols. The Kubernetes-enabled brute force attack provided initial access to the victim's networks, allowing access to protected data such as email, and identifying valid account credentials. Using identified account credentials in conjunction with exploiting publicly known vulnerabilities, such as exploiting Microsoft Exchange servers using CVE-2020-0688 and CVE-2020-17144,[3] for remote code execution and further access to target networks is a known tactic, technique and procedure (TTP) for these actors (defense.gov 2021). Once inside the network the actors performed privilege escalation, spread laterally, and installed reGeorg web shells to widen their footprint and secure footholds across the network, allowing the actors remote access beyond the initial intrusion (Hope 2021).

The adoption of sophisticated technology, in this case the Kubernetes cluster, by APT cyber actors helps increase the efficiency of their attack operations. Using a commercially available product has numerous benefits; it saves the actors time and money in developing custom tools; it diversifies and increases the attack vector spectrum, forcing network defenders to account for attacks coming from unexpected or non-traditional technologies, protocols, ports, etc.; and it potentially allows attackers to "hide in plain sight," carrying out their malicious activity under the guise of a product already trusted by network defenders. Kubernetes also enables effective and efficient management of attack servers (e.g., when an actor chooses to introduce new attack tools).

Although Kubernetes is becoming increasingly popular, it is not as well-known as cloud-based solutions for resource management. The adoption of this technology for attack operations alludes to a sophisticated actor interested in computer network operations (CNO) evolution.

Camrosa Water District (CA)

In August 2020, the Camrosa Water District (CA) discovered a cyber-attack resulting in certain devices on its network becoming encrypted. Further investigation, with assistance from a third-party cybersecurity firm, revealed unauthorized access by cyber actors dating back a full year, from August 2019. During that timeframe the cyber actors had access to Camrosa Water District file servers storing personally identifiable information (PII) that included the names and Social Se-

[3] CVE-2020-0688: According to Mitre.org CVE-2020-0688 is a remote code execution vulnerability that exists in Microsoft Exchange software when the software fails to properly handle objects in memory, aka "Microsoft Exchange Memory Corruption Vulnerability."

CVE-2020-17144: According to Mitre.org, CVE-2020-17144 is a Microsoft Exchange Remote Code Execution Vulnerability This CVE ID is unique from CVE-2020-17117, CVE-2020-17132, CVE-2020-17141, CVE-2020-17142.

curity numbers for current and former employees, as well as current and former customers. The current and former customers billing information, including their checking or savings account information, used to pay via an automated clearing house (ACH), may have also been visible to the actors (Stafford 2020).

Camrosa and their third-party cybersecurity partner did not ultimately find any indication the actors viewed or exfiltrated any personal information, but they did offer a free one-year subscription to an identity protection service to everyone potentially impacted (Stafford 2020).

That Camrosa decided to offer the complimentary identity protection service shows how a critical infrastructure asset owner can be impacted financially without its utility services being disrupted or suffering a ransomware attack. The PII of employees and customers that OT-focused businesses house is just as valuable to cyber-criminals as the PII owned by IT companies, and cyber actors may choose to target OT companies, believing them to be easier to exploit than IT companies.

Florida Water Infrastructure Construction Company

In December 2020 unidentified cyber actors, possibly associated with the DarkTeam Store and/or the Tofsee botnet malware, compromised a Florida water infrastructure construction company's website, injecting it with malicious code, to create a watering hole attack page. The malicious code seemed to target water utilities, particularly those in Florida, according to Dragos (Backman 2021). That may simply be due to more Florida-based water utilities needing to visit the Florida-based water infrastructure construction company than water utilities in other states.

The cyber actors possibly exploited a WordPress vulnerability in a plugin used by the WordPress-based site, and inserted malicious code into a website footer, on 20 December 2020. Over the next 58 days, over 1000 computers visited the compromised but otherwise legitimate website. The 1000 plus visitors included municipal water utilities, state and local agencies, various water sector private companies, and legitimate Internet bot and website crawler traffic (Backman 2021).

Notably, a computer on an Oldsmar, FL city-owned network visited the watering hole site on 5 February 2021. This is the same day the Oldsmar water treatment plant (WTP) reported an incident. The Oldsmar city computer visiting the watering hole occurred at 0949ET, after the initial unauthorized login to the Oldsmar WTP, but before a second unauthorized login wherein the cyber actor attempted to alter the water supply. [See below - Oldsmar WTP]

Malicious code reverse-engineered from the watering hole site ultimately pointed to only one other website that had the same unique combination of sophisticated code, a Dark Web site that supplies stolen or illegitimate gift cards and account credentials called DarkTeam Store. However, closer inspection of Dark-

Team Store's website revealed at least part of the site is not a market, but instead a check-in, or command and control (C2), site used for a variant of botnet malware called Tofsee (Backman 2021). It is unclear as of this publication date if DarkTeam Store is associated with the Tofsee botnet, or if its site was compromised by Tofsee and used as botnet infrastructure.

ICS-focused security vendor Dragos noted in a follow-up to their original reporting on the Oldsmar WTP incident that the cyber actor who compromised the site "likely deployed the watering hole on the water infrastructure construction company site to collect legitimate browser data for the purpose of improving the botnet malware's ability to impersonate legitimate web browser activity." In other words, the compromise of the Florida water infrastructure construction company's website was intended to improve a botnet, and not lead to the compromise of the Oldsmar WTP.

Dragos directly contacted Idaho National Laboratory (INL) personnel supporting CISA to initially report its findings, as noted on its blog (Backman 2021). INL and CISA worked to notify several dozen additional water sector entities that visited the watering hole attack page who were identified by Dragos and shared with CISA.

An Unidentified San Francisco Bay-Area WTP

Sometime in January 2021 an unknown cyber actor gained illegitimate access to a San Francisco Bay-area WTP and attempted to stop or alter the treatment of the plant's drinking water. The cyber actor used legitimate credentials from a former plant employee, allowing access to the former employee's TeamViewer account. The TeamViewer account enabled remote access to the plant's computers, where the cyber actor deleted programs used to treat drinking water. The plant discovered the deleted programs the following day and reinstalled them and changed system passwords. There were no subsequent reports of people being sickened by the plant's drinking water (Teague 2021).

The WWS has notable security weaknesses, specifically as it relates to remote management tools and architectures. The lack of centralization for the water sector does provide some measure of security; however, it also means there is no uniform or easily identifiable solution for security. According to the National Rural Water Association, "It's really difficult to apply some kind of uniform cyber-hygiene assessment, given the disparate size and capacity and technical capacity of all the water utilities." The sector cites remote management as a tool that saves time and money, but WWS facilities typically do not have the most comprehensive security standards and cybersecurity personnel in place to ensure they are implemented and maintained correctly from a security perspective (Collier 2021).

Eletrobras and Copel Electric Power Utilities (Brazil)

In late January 2021, two different state-owned electric utilities in Brazil were victims of ransomware attacks. The utilities announced the attacks in early February (Ilascu 2021). Eletrobras is the largest power utility company in South America, generating roughly 40% of Brazil's electrical supply (Thomas 2021). Copel is the largest power utility company in the state of Paraná (estimated population of 11.5 million) (City Population, 2021). Eletrobras also owns Eletronuclear, a subsidiary that operates two nuclear power plants (Ilascu 2021).

The ransomware attacks at both utilities disrupted operations and forced the companies to temporarily suspend some operations. Copel confirmed that it immediately followed security protocols including instructing personnel to stop using its computer systems when it learned of the attack (Ilascu 2021). The Eletrobras network attacked by ransomware was not connected to any Eletrobras OT networks for the nuclear power plants; however, Eletronuclear did suspend the use of some administrative software used by the nuclear power plants (Reuters 2021).

Copel did not publicly disclose the attack, but it was listed in a publicly available filing to the Securities and Exchange Commission (SEC) (Seals 2021). The Darkside ransomware cyber-criminal group claimed responsibility for the Copel attack, claiming to have stolen more than 1,000GB of data. The stolen data included: sensitive infrastructure access information including plaintext passwords; personal details about management and customers; network maps; backup schemes and schedules; as well as Active Directory (AD) data, including user groups and password hashes for all domain users (Ilascu 2021). Eletrobras has not publicly provided any details on the identity of the cyber actors behind the attack, nor has it stated if the cyber actors exfiltrated any data in the attack. However, given the near simultaneous nature of the attacks, it is reasonable to suspect Darkside as being the cyber actors behind the Eletrobras as well (Thomas 2021).

Oldsmar WTP

In February 2021 an unidentified cyber actor (Cyber Actor 1) used unauthorized remote access to view the control systems and attempted to make changes to the water chemistry at the Oldsmar WTP. The cyber actor initially remotely logged into the system around 0800ET. This login was dismissed by a plant employee, who assumed it was normal remote access by an authorized user. Roughly five and half hours later, about 1330ET, Cyber Actor 1 again remotely accessed the plant's control system. This time Cyber Actor 1 again took control of the cursor and began clicking through the plant's controls on the HMI. A plant supervisor working remotely immediately noticed the attempt and reverted the concentration back to the normal amount (Greenberg 2021; Evans 2021; Rasmussen 2021).

Though ultimately unsuccessful, Cyber Actor 1 attempted to alter the water chemistry by increasing the amount of sodium hydroxide, or lye, from 100 parts per million (PPM), to 11,000 PPM. Lye is commonly used in water treatment to control the acidity of the water, but too much can be corrosive to the plant and pipes, and dangerous to humans. Even if the WTP personnel had not noticed the changes, the chemically altered water would not have reached the population the plant serves for another 24 to 36 hours, and automated pH testing safeguards would have caught the change and triggered an alarm, giving the plant plenty of time to stop the water before it reached its customers (Greenberg 2021; Evans 2021; Rasmussen 2021).

Cyber Actor 1 accessed the Oldsmar WTP's network by exploiting an outdated Windows 7 operating system (OS) and poor password security, according to the FBI (Pulse Secure 2021). Though reporting repeatedly indicates Cyber Actor 1 used the TeamViewer tool software—typically used for remote access IT troubleshooting and to share screens—to gain access to the plants control system, this cannot be confirmed according to analysis done by CISA (CISA 2021).

The attack on the WTP described above was almost certainly done independently of the activity described below, despite the coincidence and amount of initial reporting that link the two incidents, according to Dragos in an update to their original report that linked the two incidents (Cyber Defense Magazine 2021).

The WTP attack occurred the same day an Oldsmar city computer visited a website that had been compromised by a cyber actor (Cyber Actor 2) and injected with malicious code. The website hosting the malicious code—now a watering hole attack site—belonged to a Florida water utility contractor site [See above-Florida Water Infrastructure Construction Company], a type of site commonly visited within normal duties for the city. Notably, the 0800ET unauthorized login was prior to the 0949ET visit by an Oldsmar city computer visit to the compromised website, indicating the unauthorized logins were separate cyber actors with separate access vectors (Pulse Secure 2021). The Oldsmar cyber incidents are visually displayed in Figure 1.

Though remote visibility tools are not intended as a security feature, in this instance the shared screen capability may have helped the plant staff discover the unauthorized access, as the employee who first noticed the intrusion became aware when the cursor on his screen began moving strangely around the screen, out of his control. The plant employee noticed it again hours later when Cyber Actor 1 began clicking through the controls.

While remote access and remote management tools are convenient and possibly helped in noticing the intrusion and attempted disruption in this case, they also afford actors the opportunity to disrupt OT operations. Visual tools such as TeamViewer may offer cyber actors who are not familiar with ICS/SCADA programming the ability to disrupt operations more easily than they could relying upon nominal ICS/SCADA skills to deploy their malware or conduct other malicious cyber-operations. This incident highlights the cybersecurity risks associated with remote management of OT devices.

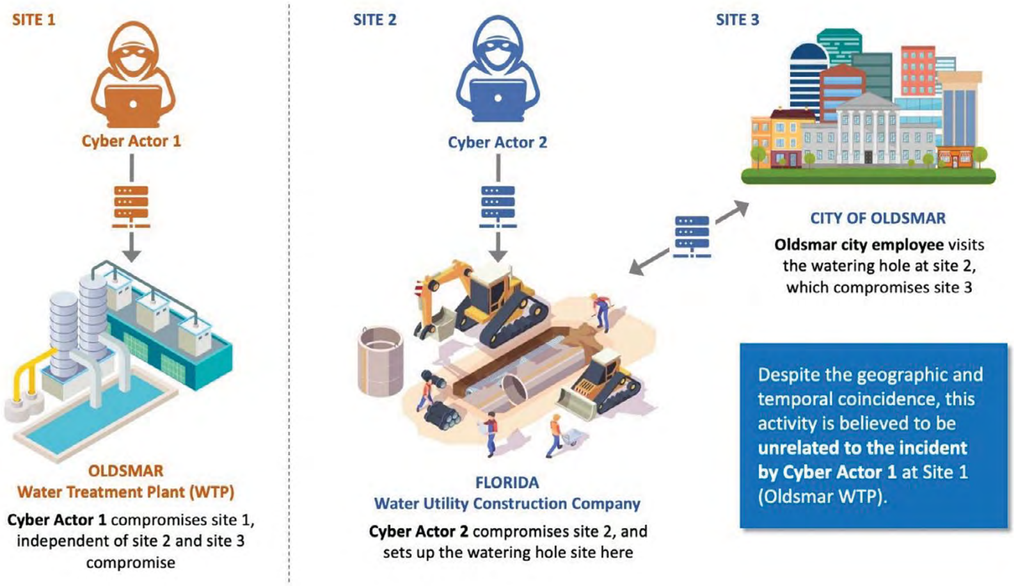
SITE 1
Cyber Actor 1
OLDSMAR
Water Treatment Plant (WTP)
Cyber Actor 1 compromises site 1, independent of site 2 and site 3 compromise
SITE 2
Cyber Actor 2
FLORIDA
Water Utility Construction Company
Cyber Actor 2 compromises site 2, and sets up the watering hole site here
SITE 3
CITY OF OLDSMAR
Oldsmar city employee visits the watering hole at site 2, which compromises site 3
Despite the geographic and temporal coincidence, this activity is believed to be unrelated to the incident by Cyber Actor 1 at Site 1 (Oldsmar WTP).

Figure 1. Oldsmar Cyber Incidents.

Nevada-based WWS Facility

In March 2021 unidentified cyber actors used an unknown ransomware variant against a Nevada WWS facility. The ransomware affected the victim's SCADA system and backup systems. The SDADA system provided visibility and monitoring but was not a full ICS (CISA 2021).

Metropolitan Water District of Southern California (MWD)

Sometime prior to April 2021, China-based APT cyber actors compromised Pulse Secure (since acquired by Ivanti, also known as Ivanti Pulse Secure), a software maker whose Pulse Connect Secure secure sockets layer (SSL) VPN software is used in organizations worldwide. The software allows for secure remote access from any Internet-connected device, including mobile, into corporate resources. The cyber actors identified and exploited previously known Pulse Secure vulnerabilities from 2019 and 2020, as well a new zero-day tracked as CVE-2021-22893 (Cyber Defense 2021). The CVE includes an authentication bypass vulnerability that can allow an unauthenticated user to perform remote arbitrary file execution on the Pulse Connect Secure gateway and has a critical common vulnerability scoring system (CVSS) score, according to the company (Pulse Secure 2021).

The MWD of Southern California was among the most critical and notable victims of the Pulse Secure breach. The MWDSC is the largest wholesale provider of drinking water in the country and its water treatment plants are among the largest in the country (Metropolitan Water District of Southern California 2018). The MWD discovered a compromised Pulse Secure appliance after viewing the alert about APT malicious activity and vulnerability was released by CISA. The WMD immediately took the compromised device offline and believes that none of its systems or processes were affected. The company also did not observe any data exfiltration (Suderman 2021).

The Pulse Secure compromise demonstrates the susceptibility of ICS companies and OT environments to the problems that impact IT environments. The continued targeting of market-leader technology enabling wide-scale exploitation (as also seen in the 2020 SolarWinds and 2021 Microsoft Exchange compromises) (Solar Winds 2021; Osborne 2021) by APT cyber actors can give those actors user credentials and accesses to the company's network that can be leveraged into access into the OT environment and ICSs, without actually compromising the ICS devices themselves. The convergence of the IT and OT environments that can allow a corporate IT compromise to lead to OT impact is a trend that will continue to increase as the lines between those once-separated environments blur.

City of Tulsa Municipal Networks

In late April 2021 cyber actors, likely associated with the cyber-criminal group Conti, installed ransomware on city networks, disrupting the availability of city websites and causing delays to city services. The city became aware of the ransomware in early May when the cyber actors contacted the city via a message on a compromised city server, stated they had compromised the server, provided instructions for paying the ransomware on the dark web along with visual proof of the compromise (Whaley 2021; Canfield 2021; Phillips 2021).

The city claimed to be well prepared for a cyber-incident, with detection systems in place that automatically alerted the IT teams, who immediately started shutting systems down. However, the cyber actors used a well-known TTP and sprung the ransomware during a weekend, when there are fewer people in the office to notice. The timing of the ransomware deployment, when the IT office was minimally staffed, allowed the attack to disrupt services despite the city being prepared, including the ability to obtain police reports, pay utility bills, or have new utilities connected. Residents reported being without water for days after requesting new service. They eventually resorted to manually turning their water services on in their homes themselves (Whaley 2021; Phillips 2021).

The city's chief information officer (CIO) detailed the damage to the media four months after the initial attack, estimating that roughly 40% of the city's 471 servers were damaged or encrypted, as well as 20% of the city's more than 5,000 desktop and laptop computers. The CIO expected a full recovery by October, five months after the attack was discovered. City officials also announced that more than 18,000 exfiltrated files had been made public by the cyber actors but noted nearly all of them were publicly available online police reports and did not contain residents' Social Security numbers or financial information (Canfield 2021). The files may have contained other PII such as name, date of birth, address, and driver's license numbers (Dellinger 2021).

This incident neatly demonstrates how ICS services, such as connections for new utility customers, can be impacted by disruptions to the IT environment even when the OT environment remains unaffected. Nearly all public-serving utility companies have public-facing portals and websites for their customers to request services and pay bills, and when the back end to those portals and sites are compromised, the utility services are also likely to also be impacted.

Volue ASA[4]

On 5 May 2021, Norwegian company Volue ASA "Volue" announced on its corporate website it was the victim of a Ryuk ransomware attack. Volue is a green-energy company providing technology for energy production, trading, distribution, and consumption. The attack limited some front-end customer platforms and encrypted company data. The company stated that all of its data was backed up in cloud storage, and the backup data was not impacted by the ransomware. Forensic analysis showed the Ryuk ransomware only targeted Volue infrastructure and networks and did not seek to spread to or encrypt third-party networks or customer information (Volue 2021; Kovacs 2021).

Upon discovering the ransomware attack, the company immediately deployed its cybersecurity task force and shut down operations and affected applications. The company advised customers to immediately shut off their service, and to change passwords associated with their Volue account. Volue alerted the Norwegian Computer Emergency Response Team (KraftCERT) and shared indicators of compromise (IOCs) with them and allowed KraftCERT to alert other companies that may be at risk, as well as Norwegian law enforcement. Volue also brought in a third-party cybersecurity firm to assist with the recovery (Kovacs 2021; Gjerstad 2021). The company set up a website that provided updates about the incident and the recovery process. The website provided daily updates and webcasts on the recovery efforts, available in both English and Norwegian, and had point of contact (POC) information available for the chief executive officer (CEO) and the chief financial officer (CFO) (Volue 2021). Later, a separate webpage detailed Volue's cybersecurity roadmap, encompassing what it had done to recover from the attack, and what it planned to do in the future to avoid similar attacks (Gjerstad 2021).

[4] ASA: The Norwegian term "Aksjeselskap" is used for a stock-based company. It is usually abbreviated AS. Public companies are called Allmennaksjeselskap (ASA), while companies without limited liability are called Ansvarlig selskap (ANS). https://snl.no/allmennaksjeselskap; https://snl.no/aksjeselskap

Volue's commitment to transparency, ownership and resolution was applauded across the cybersecurity community. Cybersecurity firms, publications and bloggers welcomed how Volue so quickly addressed the attack publicly, kept everyone aware of its actions through clear and concise written and video updates, and provided POC info for key personnel, and not an anonymous hotline or junior employee. The Volue response has been lauded as the model for handling cyber-attacks when they occur (Varghese 2021; Abrams 2021; Mills 2021; James 2021).

Colonial Pipeline

In May 2021 cyber-criminals successfully deployed ransomware onto IT networks belonging to the Colonial Pipeline company. The Colonial Pipeline is the largest refined products pipeline in the U.S., a 5,500-mile pipeline moving more than 100 million gallons of gasoline, diesel fuel and natural gas every day, providing roughly 45% of the fuel consumed on the East Coast, and reaching more than 50 million Americans. The ransomware forced Colonial Pipeline to shut down pipeline operations for several days, leading to fuel shortages causing spikes in gasoline prices, panic buying by consumers and outages at many service stations, mostly across the Southeast. Airline operations were also impacted by the fuel shortages. The attack has been attributed to Darkside, a cyber-criminal group likely operating out of Russia. It is considered the largest publicly disclosed cyber-attack against U.S. critical infrastructure in history (Colonial Pipeline 2021; Greenberg 2021; Kerner 2021).

On 6 May 2021 cyber-criminals logged into a Colonial Pipeline VPN using legitimate credentials belonging to a Colonial Pipeline employee. While the credentials were legitimate, the VPN account was inactive and not meant to be in use, though it still provided access to the network. The employee likely used the same credentials across multiple websites, and the cyber-criminals discovered the password from a separate data breach. It is unknown how the cyber-criminals obtained the VPN username. The VPN did not support multi-factor authentication (MFA) (Culafi 2021; Novinson 2021).

Once the cyber-criminals had accessed the VPN, they exfiltrated roughly 100GB of data, deployed their ransomware and left a ransom note on the IT network, demanding 75 Bitcoin (approximately $5 million at the time) in exchange for the files, while threatening to release the information to the public (Wilkie 2021; Robertson and Turton 2021). The cyber-criminals' ransomware locked up numerous corporate systems, including ones used for billing. Colonial Pipeline discovered the ransom note at approximately 0500ET on 7 May 2021. By 0555ET the company began suspending pipeline operations, with the entire pipeline shut down by 0610ET.

The decision to suspend operations was driven by the need to contain the attack and ensure the ransomware did not spread to the OT environment, according to testimony given by the CEO to a Senate committee (Wilkie 2021). Privately, the company also decided to shut down operations due to the billing system being compromised, amidst fears it would not be able to determine how to bill customers, according to people briefed on the matter (Bertrand et al. 2021). The company also had concerns about whether its network backups were also corrupted and would be safe to use (Culafi 2021).

On 7 May 2021 Colonial Pipeline paid a $4.4 million ransom in Bitcoin through a negotiator. The CEO cited the need to have "every tool available . . . to get the pipeline back up and running." The CEO said the decision to pay the ransom was not publicly disclosed at that time due to OPSEC concerns and to avoid providing publicity for the cyber-criminals. The company was initially reported to have been unwilling to pay the ransom. It is unclear if that was incorrect reporting or deliberate misinformation by the company (Wilkie 2021; Walsh 2021).

By 8 May 2021 Colonial Pipeline had begun restoring some services to the pipeline. Colonial Pipeline had contacted the USG, local law enforcement and a third-party cybersecurity firm to assist with the effort. While the main lines remained non-operational, Colonial Pipeline turned on smaller lateral lines connecting terminals and delivery points. By 12 May 2021 Colonial Pipeline initiated the restart of all pipeline operations, though it would take several days for the supply chain to return to normal. Service stations across the Southeast were still without gasoline until at least 18 May 2021. The restoration effort was done in accordance with federal regulations and with support of the USG (Colonial Pipeline 2021; Eaton 2021).

The fallout of the attack continued for Colonial Pipeline even after restoring operations, as the company announced in mid-August that PII for nearly 6,000 people, mostly current and former employees and their families, was included in the initial 100GB data exfiltration. The PII included name, date of birth, Social Security numbers, military and driver's license numbers, and health insurance information (Fung 2021). Colonial Pipeline reached out to the personnel impacted in the PII breach, making them aware of credit monitoring services (Colonial Pipeline 2021).

The Colonial Pipeline incident very publicly, and to a global audience, demonstrated the crippling damage a cyber-attack can cause to a critical infrastructure asset owner and the impact that can have on the public, even when the OT environment is not compromised. Colonial Pipelines' decision to shut down the pipeline affected millions of Americans in their everyday life, from both a convenience and a financial point-of-view. The attack itself reinforces the need for MFA as well as regular network audits, as the VPN was not in use but still provided connectivity. From a best practice's stance, it also highlights the danger of re-using passwords across multiple platforms or websites, and not changing passwords that may have been exposed via separate data breaches.

Maine-based WWS Facility

In July 2021, unidentified cyber actors using remote access targeted and successfully installed ZuCaNo ransomware onto a SCADA computer at a Maine-based WWS facility. The ransomware disrupted the system, resulting in the treatment center needing to be run manually, with more frequent operator rounds. The system was eventually restored using local control (CISA 2021).

ZuCaNo ransomware is a variant of the well-documented Xorist ransomware family, and mitigation and removal techniques are readily available online (Remove Malware 2021). These tutorials and software solutions tend to be catered to IT environments. However, a successful deployment on an OT system may be much harder to manage and require more technical expertise unique to the OT environment, making the mitigation and malware removal more difficult, time-consuming, and expensive for the operator.

California-based WWS Treatment Center

In August 2021 unidentified cyber actors successfully deployed a Ghost variant ransomware onto a California-based WWS treatment center. The ransomware had been in the system for about a month and was not discovered until three SCADA servers displayed a ransomware message (CISA 2021).

Shifts in Cyber-Attacks Requires Shifts in Cyber Policy

Most notable cyber-incidents prior to 2017 have been attributed to a nation-state or specific APT actor and have been handled diplomatically in a reactive manner via sanctions, or individual charges. The legal framework for those diplomatic responses is the Executive Order (E.O.) 13694, enacted April 1, 2015 that "authorized the imposition of sanctions on individuals and entities determined to be responsible for or complicit in malicious cyber-enabled activities that result in enumerated harms that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States." E.O. 13694 was updated with E.O. 13757 that allows for the Department of Treasury's Office of Foreign Assets Control (OFAC) to designate sanctions upon individuals and entities whose conduct meets the criteria set forth in E.O. 13694.

The USG uses that framework to punish nation-state cyber activity, such as in April 2021 when the U.S. Department of Treasury announced broad sanctions across numerous Russian-government affiliated companies following the late-2020 SolarWinds hack, an incident attributed to the Russian Foreign Intelligence Service (SVR) associated APT29/Cozy Bear threat actors. In October 2020 the US Department of Justice charged six members of the Russian state-sponsored Sandworm team (Greenberg 2020). The U.S. Department of Justice has also charged several Iranian and Russian citizens for their involvement with cyber activity related to the Trickbot trojan, and intentions to interfere in the 2020 U.S. Presidential election (Justice 2017), (Justice 2021).

That framework functionally works at the nation-state policy level; however, because it is reactive, the hack has already occurred. In addition, those legal actions are frequently inadequate, with charges being mostly symbolic (assuming Iran and Russia are not likely to extradite their own government and military members), or so long after the incident occurred it is out of the public's mind and the ire is lost. The charges against the Sandworm team came in 2020 but were levied for actions connected to the Ukrainian Christmas blackout of 2015, a Kyiv blackout attack in 2016, the global NotPetya outbreak of 2017 and the Olympic Destroyer malware associated with the 2018 Winter Olympics (Greenberg 2020).

Given that diplomatic and legal responses are negligible and frequently years after the cyber incident, the policy to address malicious cyber activity needs to change too. While the reactive diplomatic response should stay in effect, a proactive U.S.-facing policy framework is necessary to protect U.S. critical infrastructure.

The federal government and U.S. states are moving in that direction. Other E.D.'s including 13800 and 14028 have sought to strengthen the cybersecurity of federal networks, critical infrastructure and the US (CISA n.d.), (CISA n.d.). The National Defense Authorization Act for Fiscal Year 2022 (NDAA) ultimately did not contain a much-debated provision that would have required critical infrastructure owners and operators to report covered cybersecurity incidents to CISA; however, it did contain numerous cybersecurity provisions, including the authorization of the CyberSentry program, focused on the cybersecurity of ICS (Greig 2021).

The NDAA also introduced the Joint Cyber Defense Collaborative (JCDC), in which CISA and its partners—including federal, state, local, tribal, and territorial (SLTT) governments and the public and private sectors—work together to drive down the risk of cyber-attacks. The JDCD is "designed to strengthen the nation's cyber defenses through planning, preparation, and information sharing." It includes cyber operational planning, public and private sector information fusion and analysis, and cybersecurity guidance dissemination to its stakeholders (CISA n.d.). The JCDC will improve upon existing analysis and dissemination vectors, such as the Information Sharing and Analysis Centers (ISACs) and state fusion centers, to ensure more critical infrastructure owners and operators receive the cybersecurity information they need.

The USG has also shifted policy to actively caution U.S. entities that failing to protect their customers information may have legal or financial implications. The December 2021 Log4J vulnerability prompted the Federal Trade Commission (FTC) to demand US companies to update their systems, or potentially face an FTC lawsuit. The FTC referred to their $700 million settlement with Equifax stemming from the 2017 data breach, and specifically highlighted Equifax's failure to patch a known vulnerability in their Log4J warning (FTC 2022). CISA has also issued an Emergency Directive (ED) for Log4J (CISA 2021). ED's serve as mandates to civilian federal agencies, which are legally required to comply.

The shift toward getting U.S. entities to proactively prevent an incident, rather than reactively and punitively punishing foreign nation-state's cyber actors, is a notable change and the preferred action in how the USG should look to apply policy in the cyber space going forward. Increased information sharing between the public and private sector, improved platforms for information dissemination by the USG, and USG programs designed to assist specific sectors such as CyberSentry are good examples of the USG's role in assisting and educating industry on cybersecurity risk to allow industry to create or update cyber-defense plans, incident response plans, and risk models.

Lessons Learned

Many of the incidents covered in this paper highlighted ICS/SCADA operations disrupted by malicious cyber actors who did not actually compromise the OT environment. Several of these incidents' disruptions were caused by ransomware compromising an IT system or network that led to a disruption of the OT environment, or an intentional shutdown of the OT services by the afflicted company. Businesses trying to reduce costs or increase convenience by utilizing technology such as remote management and visibility tools, or billing services connected to both IT and OT environments, has created a hybrid IT/OT environment wherein cyber actors do not need to compromise the OT environment to disrupt ICS/SCADA operations. This shift in business operation tactics has led to cyber actors targeting ICS/SCADA companies and under-funded and under-staffed sectors such as WWS that may not have the resources or staff necessary to defend their networks.

Perhaps more critically, this IT/OT merge has also lowered the bar necessary to attack OT environments. Previous well-documented ICS/SCADA disruptions such as Stuxnet, Black Energy or CRASHOVERRIDE were sophisticated pieces of malware specifically targeting ICS/SCADA devices and custom written by well-funded and trained APT cyber actors. The ability to use readily available and cheaply acquired ransomware or malware designed for IT environments to attack an OT environment is a shift in the attack paradigm, opening the opportunity to more cyber actors.

Unlike most IT environments such as a business office where most employees are not working over the weekend and critical updates can be done during that time, many OT environments cannot be turned off for scheduled updates and patching due to the 24/7 nature of the plants and factories running them. This creates an environment rife with outdated and legacy operating systems and software versions full of vulnerabilities. This lack of patching and updates creates a target rich environment for cyber actors looking for vulnerabilities and outdated OSs and software. The 24/7 nature of OT environments and the critical infrastructure that depends upon them has led malicious cyber actors to target these OT environments, assuming the services they provide—water, gas, electricity, etc. —are too important to be down for an extended period of time. ICS/SCADA companies also house valuable PII information that can be leveraged for ransom or sold, just like IT environments. Cyber actors are starting to recognize these factors and targeting ICS/SCADA companies in the same way they have traditionally targeted IT environments.

With actors targeting OT environments with some of the same TTP's used in IT environment attacks, a review of IT best practices can show how they manifest in an OT environment. Table 3 below shows the same list of incidents, with columns added for the likelihood the attack could have been prevented if the victim had been using common IT best practices, with the possible solution for prevention listed if available. The preventability of each incident was scored as "unlikely," "possible," or "likely" per known best practices applicable to the incident. An incident is labeled as "unknown" if a lack of information available makes a judgment impossible.

Table 3. ICS Incidents Covered in this Paper and Potential Mitigation Strategies.

YEAR	VICTIM	THREAT TYPE	PREVENTABLE	POSSIBLE SOLUTION(S) AND COMMENTS
2018	Energy Services Group	Third party / supply chain	Unknown	
2019	Unidentified Power Plant	Insider Threat	Possible	Enhanced insider threat training. IT policy on allowing foreign USB devices into the facility, and allowing them to run on the HMIs.
2019	sPower	Remote Exploit	Unlikely	A review of the firewall hardware and the hardening policies applied.
2019	Post Rock Water District, Ellsworth County (KS)	Insider threat	Likely	Regular audits of current users/employees.

2019	Energy Companies Across Europe and US	Brute Force	Unlikely	Kubernetes as an attack tool was a very new TTP at that time.
2020	Camrosa Water District	Remote Exploit	Unknown	
2020	Florida Water Infrastructure Construction Company	Word Press vulnerability / watering hole	Likely	WordPress is widely known to be commonly targeted, with nearly 3700 CVE entries and nearly 22,000 total vulnerabilities (Mitre, n.d.) (Abela 2021).
2021	San Francisco Bay-area Water Treatment Plant	Unauthorized Remote Access	Likely	Human Resources (HR) and IT should be lockstep in policy that user credentials are revoked / removed the same day an employee exits the company.
2021	Eletrobras & Copel Electric Power Utilities	Ransomware in the IT environment	Unknown	
2021	Oldsmar (FL) Water Treatment Plant	Watering hole attack	Possible	The muddled reporting makes the attack vector unclear. If it was outdated Windows 7 OS and poor password security, as FBI reports, then it likely could have been preventing with Windows 7 OS updates and better password security. See CISA Alert AA21-042a for additional recommendations.
2021	Nevada-based WWS	Unknown ransomware in the OT environment	Unknown	

2021	Metropolitan Water District of Southern California (MWD)	Supply chain	Possible	The actors exploited two known Pulse Secure CVEs, but also used a zero-day. Impossible to judge actors' success with just the zero-day. See CISA Alert AA21-110A for additional information on Ivanti Pulse Connect Secure products.
2021	City of Tulsa (OK)	Ransomware in the IT environment	Unknown	If the actors used Conti ransomware, CISA Alert AA21-265A could have been applied.
2021	Volue ASA (Norway)	Ryuk ransomware in the IT environment	Unknown	
2021	Colonial Pipeline	Ransomware in the IT environment	Likely	The password used was likely discovered in a data breach and used across multiple sites. Better password policy may have prevented that from being successful. The VPN accessed with the credentials did not support MFA. Requiring MFA for the VPN would likely have prevented access. See CISA Alert AA21-131A for additional information.
2021	Maine-based WWS	ZuCaNo ransomware in OT environment	Unknown	See CISA Alert AA21-287A for mitigation recommendations.
2021	California-based WWS	Ghost variant ransomware in the OT environment	Unknown	See Alert AA21-287A for mitigation recommendations.

It is impossible without access to the full forensic reports and proprietary information related to each incident to know if the possible solutions would have prevented the incident. It is also possible the cyber actors have unused exploits or attack vectors available that were unnecessary once they had gained access, that would have worked despite the possible solution. Likewise, perhaps the IT staff of the victim made the intrusion worse with poor incident response techniques or plans, or the decision to take systems offline made by a CEO was too hasty, unnecessarily causing the disruption. However, with the information available, the majority of the incidents are deemed “likely” or “possible” to have been prevented had common best practices for IT environments been in place.

While patching and updating ICS systems can be difficult in the 24/7 environments in which they are often found, it is vital to keep the associated and connected IT environments up to date. Common ICS security recommendations such as ensuring segmentation between IT and OT networks, limiting external connectivity of OT systems and enabling MFA where it is necessary, and establishing user roles and privileges based on work responsibilities, should also be followed. CISA and the Department of Energy maintain comprehensive recommended practices lists and tools for self-evaluating cybersecurity (CISA n.d.) (Defense.gov 2020), (Department of Energy, n.d.). Having an ICS-specific incident response plan is also critical, as unlike an IT network compromise, there are potential threats to life and property that can occur in an OT environment as a result of a cyber compromise (CISA October 2019). No network is invulnerable, but many of the reviewed incidents may have been prevented with better IT and OT cybersecurity policies in place.

Conclusion

ICS incidents continue to be a concern to critical infrastructures. This paper highlighted the increasing trend of how the interconnectivity of devices and services connecting the IT and OT environments and the increasing sophistication of cyber actors, both nation-state (APT) and cyber-criminal, have put many businesses and services that may not consider themselves traditional targets of malicious cyber actors at risk of a cyber-attack. Cyber actors have learned they do not need to compromise the OT environment to disrupt OT services; the convergence of IT and OT has blurred that line. Similarly, cyber actors lacking ICS/SCADA-specific knowledge have realized that an IT intrusion can be just as effective as an OT disruption, lowering the sophistication necessary to target OT environments. This trend has increased the vulnerability to OT systems since both IT and OT exploits can be used to impact OT systems.

Regardless of whether they originate from an IT or OT environment, disruptions of services erode public trust and cause costly outages that ICS/SCADA companies cannot afford. Some ICS/SCADA companies are starting to realize it is not a matter of if, but when, they will be compromised, and are acting accordingly. Investing in cybersecurity, having an OT-specific incident response plan for a compromise, and being transparent and up-front about compromises to the public is the way forward.

Acronyms and Abbreviations

APT	Advanced Persistent Threat
C2	Command and Control
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CNO	Computer Network Operations
CVE	Common Vulnerabilities and Exposures
CVSS	Critical Common Vulnerability Scoring System
DCS	Distributed Control System
DHS	Department of Homeland Security
DoS	Denial of Service
ED	Emergency Directive
E.O.	Executive Order
FTC	Federal Trade Commission
GRU	Russian General Staff Main Intelligence Directorate
GTsSS	85th Main Special Service Center
GUI	Graphical User Interface
HMI	Human Machine Interface
HR	Human Resources
ICS	Industrial Control System
INL	Idaho National Laboratory
IOC	Indicator of Compromise
ISAC	Information Sharing and Analysis Center
IT	Information Technology
MFA	Multi-factor Authentication
MW	Megawatt

MWD	Metropolitan Water District of Southern California
NDAA	National Defense Authorization Act
OPSEC	Operational Security
OS	Operating System
OT	Operational Technology
PII	Personally Identifiable Information
POC	Point of Contact
PPM	Parts Per Million
SCADA	Supervisory Control and Data Acquisition
SLTT	State, Local, Tribal and Territorial
SSL	Secure Sockets Layer
TTP	Tactic, Technique and Procedure
USB	Universal Serial Bus
USG	United States Government
VPN	Virtual Private Network
WTP	Water Treatment Plant
WWS	Water and Wastewater Systems

Robert Grubbs is a Senior Cyber Intelligence Analyst for the Infrastructure Assurance and Analysis division of Idaho National Laboratory (INL). In his current role he provides on-site operational support and intelligence analysis. He has supported the U.S. government for more than 20 years as a federal employee and as a contractor, beginning with four years of college internships with the Department of State. Since graduation he has supported work across the intelligence community (IC) and financial sector in network engineering, network and telecommunications analysis, and cyber intelligence and counterintelligence roles. He has a degree in English with a focus in Technical Writing and Editing from Virginia Polytechnical Institute and State University (Virginia Tech) and is a SANS-certified Certified Forensics Examiner (GCFE).

Jeremiah Stoddard is a Critical Infrastructure Security Analyst for the Infrastructure Assurance and Analysis division of Idaho National Laboratory. In his current role he provides support for efforts on software bill of materials (SBOM) as well as vulnerability disclosure. Mr. Stoddard attended Idaho State University and received a bachelor's degree in History and a Master of Business Administration with an emphasis in cybersecurity. He also graduated from Gonzaga University

School of Law and later received an LLM in National Security & U.S. Foreign Relations Law from The George Washington University Law School.

Sarah Freeman is an Industrial Control Systems (ICS) Cyber Security Analyst for the Cybercore Integration Center at Idaho National Laboratory (INL), where she provides U.S. government partners and private sector entities with actionable cyber threat intelligence, developing innovative security solutions for the critical infrastructure within the U.S. At INL, Sarah pursues innovative threat analysis and cyber defense approaches, most recently Consequence-driven Cyber-informed Engineering (CCE). As Principal Investigator on a laboratory discretionary research project, her current research is focused on new signatures and structured methods for cyber adversary characterization. Following the December 2015 electric grid attacks, Sarah participated in the DOE-sponsored training for Ukrainian asset owners in May 2016. She has also researched the Ukrainian 2015 and 2016 cyber-attacks and the Trisis/Hatman incident.

Ron Fisher, PhD is the Director of Infrastructure Assurance and Analysis (IAA) in the National & Homeland Security (N&HS) directorate at Idaho National Laboratory (INL). He provides over 20 years of critical infrastructure protection experience including serving on President Clinton's Presidential Commission on Critical Infrastructure Protection. Dr. Fisher has worked at INL for eight years, and prior to that, 26 years at Argonne National Laboratory serving as deputy director for the Laboratory's Infrastructure Assurance Center. Dr. Fisher attended Northern Illinois University and received a bachelor's degree in Finance and a Master of Business Administration in finance, economics, and management. He also attended Benedictine University and received a doctorate degree in organizational development.

References

Abela, Robert. (2021, February 10). Statistics Highlight the Biggest Source of WordPress Vulnerabilities. Available from WP WhiteSecurity: https://www.wpwhitesecurity.com/statistics-highlight-main-source-wordpress-vulnerabilities/.

Abrams, Lawrence. (2021, May 17). Ransomware Victim Shows Why Transparency in Attacks Matters. Available from Bleeping Computer: https://www.bleepingcomputer.com/news/security/ransomware-victim-shows-why-transparency-in-attacks-matters/.

Backman, Kent. (2021, May 18). When Intrusions Don't Align: A New Water Watering Hole and Oldsmar. Available from Dragos: https://www.dragos.com/blog/industry-news/a-new-water-watering-hole/.

Behr, Peter. (2019, February 25). Power Lines: The Next 'Green New Deal' Battlefront? Retrieved from E&E News: https://www.eenews.net/stories/1060122295.

Bertrand, Natasha, Evan Perez, Zachary Cohen, Geneva Sands, and Josh Campbell. (2021, May 13). Colonial Pipeline Did Pay Ransom to Hackers, Sources Now Say. Available from CNN: https://edition.cnn.com/2021/05/12/politics/colonial-pipeline-ransomware-payment/index.html.

Canfield, Kevin. (2021, August 14). Ransomware Group Conti Likely Responsible for City's Cyber-attack, Experts Say. Available from Tulsa World: https://tulsaworld.com/news/local/ransomware-group-conti-likely-responsible-for-citys-cyber-attack-experts-say/article_3cad1622-df57-11eb-b3c8-437f9866823f.html.

Cimpanu, Catalin. (2018, February 8). Hackers Pounce on Cisco ASA Flaw (CVE-2018-0101). Retrieved from Bleeping Computer: https://www.bleepingcomputer.com/news/security/hackers-pounce-on-cisco-asa-flaw-cve-2018-0101/.

CISA. (n.d.). Joint Cyber Defense Collaborative. Available from CISA: https://www.cisa.gov/jcdc.

CISA. (n.d.). Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. Available from CISA: https://www.cisa.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure.

CISA. (n.d.). Executive Order on Improving the Nation's Cybersecurity. Available from CISA: https://www.cisa.gov/executive-order-improving-nations-cybersecurity.

CISA. (n.d.). Recommended Practices. Available from CISA: https://www.cisa.gov/uscert/ics/Recommended-Practices.

CISA. (2009, October 6). Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability. Available from CISA: https://www.cisa.gov/uscert/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf.

CISA. (2009, November 4). Understanding Denial-of-Service Attacks. Available from CISA: https://us-cert.cisa.gov/ncas/tips/ST04-015.

CISA. (2021, February 11). AA21-042A – Compromise of Water Treatment Facility. Available from CISA: https://us-cert.cisa.gov/ncas/alerts/aa21-042a.

CISA. (2021, October 14). AA12-287A – Ongoing Cyber Threats to U.S. Water and Wastewater Systems. Available from CISA: https://us-cert.cisa.gov/ncas/alerts/aa21-287a.

CISA. (2021, December 17). Emergency Directive 22-02 Mitigate Apache Log4J Vulnerability. Available from CISA: https://www.cisa.gov/emergency-directive-22-02.

CISOMAG. (2018, April 3). Energy Transfer Partners Reports Cyber Breach. Available from CISOMAG: https://cisomag.eccouncil.org/energy-transfer-partners-reports-cyber-breach/.

City Population (2021, August 28). State of Paraná. Available from City Population: https://www.citypopulation.de/en/brazil/cities/parana/.

Collier, Kevin. (2021, June 17). 50,000 Security Disasters Waiting to Happen: The Problem of America's Water Supplies. Available from NBC News: https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206.

Colonial Pipeline. (2021, May 17). Media Statement Update: Colonial Pipeline System Disruption. Available from Colonial Pipeline: https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption.

Colonial Pipeline. (2021, August 1). Frequently Asked Questions. Available from Colonial Pipeline: https://www.colpipe.com/about-us/faqs.

Colonial Pipeline. (2021, August 13). Available from Document Cloud: https://www.documentcloud.org/documents/21043496-colonial-piepeline-bc-data-breach-notification.

Culafi, Alexander. (2021, June 9). Mandiant: Compromised Colonial Pipeline Password Was Reused. Available from Search Security: https://searchsecurity.techtarget.com/news/252502216/Mandiant-Compromised-Colonial-Pipeline-password-was-reused?.

Cyber Defense Magazine. (2021, April 22). China-linked APT used Pulse Secure VPN Zero-Day to Hack U.S. Defense Contractors. Available from Cyber Defense Magazine.com: https://www.cyberdefensemagazine.com/china-linked-apt/.

Defense.gov. (2020, July 22). NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems. Available from Defense.gov: https://media.defense.gov/2020/Jul/23/2002462846/-

1/-1/1/OT_ADVISORY-DUAL-OFFICIAL-20200722.PDF.

Defense.gov. (2021, July 1). Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments Cybersecurity Advisory. Available from Defense.gov: https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF.

Dellinger, Michael. (2021, June 24). Tulsa Says Ransomware Attackers Accessed, Shared Personal Information. Available from Public Radio Tulsa: https://www.publicradiotulsa.org/post/tulsa-says-ransomware-attackers-accessed-shared-personal-information#stream/0.

Department of Energy. (n.d.). Cybersecurity Capability Maturity Model (C2M2). Available from United States Department of Energy: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

Energy Transfer.com. (2021, November 1). We are Energy. Available from Energy Transfer: https://www.energytransfer.com/about/.

Eaton, Collin. (2021, May 18). Colonial Pipeline Still Moving Fuel Despite Disruptions to Orders System. Available from The Wall Street Journal: https://www.wsj.com/articles/colonial-pipeline-ordering-system-disrupted-but-still-moving-fuel-11621358203.

Evans, Jack. (2021, February 8). Someone Tried to poison Oldsmar's Water Supply During Hack, Sheriff Says. Available from Tampa Bay Times: https://www.tampabay.com/news/pinellas/2021/02/08/someone-tried-to-poison-oldsmars-water-supply-during-hack-sheriff-says/.

FTC. (2022, January 4). FTC Warns Companies to Remediate Log4j Security Vulnerability. Available from US FTC: https://www.ftc.gov/news-events/blogs/techftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability.

Fung, Brian. (2021, August 16). Colonial Pipeline Says Ransomware Attack Also Led to Personal Information Being Stolen. Available from CNN: https://www.cnn.com/2021/08/16/tech/colonial-pipeline-ransomware/index.html.

Gjerstad, Kevin. (2021, September 16). Cybersecurity Roadmap: Volue After the Ransomware Attack. Available from Volue: https://www.volue.com/news/cybersecurity-roadmap-volue.

Greenberg, Andy. (2021, February 8). A Hacker Tried to Poison a Florida City's

Water Supply, Officials Say. Available from Wired: https://www.wired.com/story/oldsmar-florida-water-utility-hack/.

Greenberg, Andy. (2021, May 8). The Colonial Pipeline Hack Is a New Extreme for Ransomware. Available from Wired: https://www.wired.com/story/colonial-pipeline-ransomware-attack/.

Greenberg, Andry. (2020, October 19). U.S. Indicts Sandworm, Russia's Most Destructive Cyberwar Unit. Available from Wired: https://www.wired.com/story/us-indicts-sandworm-hackers-russia-cyberwar-unit/.

Greig, Jonathan. (2021, December 15). U.S. Senate Passes $768 Billion Defense Bill Without Cyber Incident Reporting Provisions. Available from ZDNet: https://www.zdnet.com/article/us-senate-passes-defense-bill-without-cyber-incident-reporting-provisions/.

Hemsley, Kevin, Fisher, Ron. (2018, December). History of Industrial Control System Cyber Incidents. Available from the Office of Scientific and Technical Information: https://www.osti.gov/servlets/purl/1505628/.

Hope, Alicia. (2021, July 8). NSA and GCHQ Warn That Russian Hackers Frequently Brute Force Passwords at Scale Using Kubernetes Clusters. Available from CPO Magazine.com: https://www.cpomagazine.com/cyber-security/nsa-and-gchq-warn-that-russian-hackers-frequently-brute-force-passwords-at-scale-using-kubernetes-clusters/.

Ilascu, Ionut. (2021, February 5). Eletrobras, Copel Energy Companies Hit by Ransomware Attacks. Available from Bleeping Computer. Available from: https://www.bleepingcomputer.com/news/security/eletrobras-copel-energy-companies-hit-by-ransomware-attacks/.

James, Timothy. (2021, May 17). Ransomware Victim Shows Why Attack Transparency Matters. Available from News Block: https://news-block.com/ransomware-victim-shows-why-attack-transparency-matters/.

Justice. (2017, November 21). Acting Manhattan U.S. Attorney Announces Charges Against Iranian National for Conducting Cyber Attack And $6 Million Extortion Scheme Against HBO. Available from United States Department of Justice: https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-charges-against-iranian-national-conducting.

Justice. (2021, October 28). Russian National Extradited to United States to Face Charges for Alleged Role in Cybercriminal Organization. Available from United

States Department of Justice: https://www.justice.gov/opa/pr/russian-national-extradited-united-states-face-charges-alleged-role-cybercriminal.

Kephart, Tim. (2021, May 19). Report: Oldsmar Water Hack Came After City Computer Visited Compromised Website. Available from ABC Action News: https://www.abcactionnews.com/news/region-pinellas/report-oldsmar-water-hack-came-after-city-computer-visited-compromised-website.

Kerner, Sean M. (2021, July 7). Colonial Pipeline Hack Explained: Everything You Need to Know. Available from What is Tech Target.com: https://whatis.techtarget.com/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

Kovacs, Eduard. (2021, May 13). Green Energy Company Volue Hit by Ransomware. Available from Security Week: https://www.securityweek.com/green-energy-company-volue-hit-ransomware.

KSN.com. (2021, March 13). United States District Court Case No. 21-40029-HLT. Available from KSN.com: https://www.ksn.com/wp-content/uploads/sites/13/2021/03/travnichek-indictment.pdf.

Lyngaas, Sean. (2018, April 3). Major U.S. Pipeline Hit by Cyberattack on Transaction Software. Retrieved from CyberScoop.com: https://www.cyberscoop.com/major-u-s-pipeline-disrupted-cyberattack-transaction-software/.

Malware Remove. (2021, July 7). How to Remove Zucano Ransomware and Restore Files. Available from Remove Malware.com: https://malware-remove.com/blog/how-to-remove-zucano-ransomware-and-restore-files/.

Metropolitan Water District of Southern California. (2018, September 1). Metropolitan's Water Treatment Plants Safeguard Public Health. Available from Metropolitan Water District of Southern California: https://www.mwdh2o.com/media/4360/water-treatment-plants-fact-sheet-final_web.pdf.

Mitre.org (2021, October 18). APT28. Available at Mitre.org: https://attack.mitre.org/groups/G0007/.

Mitre.org (n.d.) WordPress Query. Available at Mitre.org: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=wordpress.

Mills, Matt. (2021, May 19). Why Transparency is Important to Curb Ransomware. Available from ITGIC: https://itigic.com/why-transparency-is-important-to-curb-ransomware/.

Morgan, Lisa. (2021, April 9). Another Cyber Attack Affecting Water Supply. Retrieved from Cyber Security Hub.com: https://www.cshub.com/attacks/articles/another-cyber-attack-affecting-water-supply.

Novinson, Michael. (2021, June 5). Colonial Pipeline Hacked Via Inactive Account Without MFA. Available from CRN: https://www.crn.com/news/security/colonial-pipeline-hacked-via-inactive-account-without-mfa.

O'Donnell-Welch, Lindsey. (2021, April 2). Kansas Water Utility Attack Underscores Security Limitations in Municipalities. Retrieved from Decipher.com: https://duo.com/decipher/kansas-water-utility-attack-underscores-security-limitations-in-municipalities.

Osborne, Charlie. (2021, April 19). Everything You Need to Know About the Microsoft Exchange Server Hack. Available from ZDNet: https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/.

Phillips, Sharon. (2021, July 22). Story Behind the Ransomware Attack on the City of Tulsa." Available from 2 News Oklahoma: https://www.kjrh.com/news/local-news/story-behind-the-ransomware-attack-on-the-city-of-tulsa.

Pulse Secure. (2021, April 1). SA44784 - 2021-04: Out-of-Cycle Advisory: Multiple Vulnerabilities Resolved in Pulse Connect Secure 9.1R11.4. Available from Pulse Secure.net: https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784.

Rasmussen, Jeremy. (2021, April 5). Lessons Learned from Oldsmar Water Plant Hack. Available at Security Today: https://securitytoday.com/articles/2021/04/05/lessons-learned-from-oldsmar-water-plant-hack.aspx.

Reuters. (2021, February 4). Brazil's Eletrobras Says Nuclear Unit Hit with Cyberattack. Available from Reuters: https://www.reuters.com/article/us-eletrobras-cyber/brazils-eletrobras-says-nuclear-unit-hit-with-cyberattack-idUSKBN2A41JN.

Robertson, Jordan and Turton, William. (2021, May 10). Cyber Sleuths Blunted Pipeline Hack, Choked Data Flow to Russia. Available from Bloomberg: https://www.bloomberg.com/news/articles/2021-05-10/cyber-sleuths-blunted-pipeline-hack-choked-data-flow-to-russia?srnd=technology-vp.

Seals, Tara. (2021, February 5). Ransomware Attacks Hit Major Utilities Threat Post. Available from: https://threatpost.com/ransomware-attacks-major-utilities/163687/.

Solar Winds. (2021, April 6). SolarWinds Security Advisory. Available from Solar Winds.com: https://www.solarwinds.com/sa-overview/securityadvisory.

Stafford, Tony. (2020, August 13). Notice of Data Breach. Available from Camrosa Water District.com. https://oag.ca.gov/system/files/Camrosa%20-%20California%20Notification.pdf.

Suderman, Alan. (2021, June 15). MWD Among Targets in Large-Scale Cyber-Espionage Hack Blamed on China. Available from Los Angeles Times: https://www.latimes.com/world-nation/story/2021-06-15/critical-entities-targeted-suspected-chinese-cyber-espionage.

Teague, Courtney. (2021, June 18). FBI Investigating Hacker Attempt to Poison Bay Area Water: Report. (2021, June 18) Available from Patch.com: https://patch.com/california/san-francisco/fbi-investigating-hacker-attempt-poison-bay-area-water-report.

Thomas, Ian. (2021, June 9). The State of Ransomware Attacks across Latin America. Available from Iron Scales: https://ironscales.com/blog/ransomware-latin-america/.

Tomlinson, Kerry. (2019, May 9). What Happened to the U.S. Grid on March 5? Available from Archer: https://archerint.com/what-happened-to-the-us-grid-on-march-5/.

Tomlinson, Kerry. (2020, February 27). Power Plant Reportedly Hit by Mouse Ransomware Attack. Retrieved by Archer: https://archerint.com/power-plant-reportedly-hit-by-mouse-ransomware-attack/.

Varghese, Sam. (2021, May 11). Norwegian Firm Shows How Ransomware Attack Should Be Handled. Available from ITWire: https://itwire.com/security/norwegian-firm-shows-how-ransomware-attack-should-be-handled.html.

Volue.com (2021, July 12). Urgent Updates on the Cyberattack. Available from Volue.com: https://www.volue.com/urgent-updates.

Walsh, Joe. (2021, May 12). Colonial Pipeline Reportedly Won't Pay Hacker Ransom. Available from Forbes: https://www.forbes.com/sites/joewalsh/2021/05/12/colonial-pipeline-reportedly-wont-pay-hacker-ransom/?sh=2eee20e941c3.

Whaley, Sara. (2021, May 10). Ransomware Attack Targets City of Tulsa, Causing Technical Difficulties. Available from Fox News: https://www.fox23.com/news/local/tulsa-city-officials-ransomware-attack-causing-technical-difficulties/R4BXX

HIRVJCYDHUG6VAUFJB4BQ/.

Wilkie, Christina. (2021, June 9). Colonial Pipeline Paid $5 Million Ransom One Day After Cyberattack, CEO Tells Senate. Available from CNBC: https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html.