Cyber-attacks on Industrial Control Systems (ICS) and Operational Technology (OT) environments in the water sector over the last twenty years.

secolve
OT SECURITY SOLVED

Head Office Address: Level 2, 11 York Street,
Sydney, NSW 2000

Contact: info@secolve.com
1800 SECOLVE (732 658)

INTRODUCTION

Industrial Control Systems (ICS) and Operational Technology (OT) are essential to critical infrastructure. They are the key to the successful, on-going operation of the equipment and software that control, measure and ensure the availability of the service the vital infrastructure provides. The security of these systems is crucial to ensure availability and up-time as hackers can exploit any vulnerabilities therein. Any breach can also potentially cause serious damage to critical infrastructure and endanger the safety of the population.

Industries that are supported by critical infrastructure include chemical, energy, transportation and water. The water sector, in particular, is essential to the survival of communities and functioning of essential services such as hospitals and manufacturing. The sector also impacts non-essential services like restaurants and movie theatres. Due to the consequences that compromised water infrastructure can bring, its cybersecurity is of primary importance.

Despite the growth in digital transformation, water and other sectors lack adequate cyber security guidelines, specialists and cyber-secure systems to safely guard against cyber threat actors. In fact, the water sector is the third-highest targeted sector for cyber attackers. Many cyberattack incidents in the water sector go undetected, primarily due to the reluctance of the victim to disclose details of the breach. The result of this lack of disclosure is that the cyber security of these infrastructures is often overlooked and undervalued.

The purpose of this paper is to pinpoint the importance of the need for enhanced cybersecurity measures to help to protect the water industry. This paper will cover twenty real-world cyber-attack incidents from the year 2000 to 2020 in the water sector that have been disclosed and will attempt to identify what happened, how it happened and if it was successful. If successful, what was or would have been the impact?

"Despite the growth in digital transformation, water and other sectors lack adequate cyber security guidelines, specialists and cyber-secure systems to guard against cyber actors"

IDENTIFIED CYBER-INCIDENTS IN THE WATER SECTOR

Attack – 1 : 2000 Maroochy Water Services, Australia

What happened

Hunter Watertech Pty Ltd (HWT) is a third-party contracted company responsible for the installation of PDS Compact 500 RTU at 128 sewage pumping stations in Maroochy Shire council in Queensland. PDS Compact 500 RTU enabled the remote control and monitoring of the pumping stations through the utilisation of a SCADA system. In early 2000, a disgruntled employee of HWT managed to gain unauthorised access to the SCADA systems and, over a period of three months, the system started experiencing system faults such as the impairment of pumping capabilities, false alarms, loss of communications as well as the release of millions of gallons of raw sewage into the local environment. In March of 2000, evidence of the intrusion was uncovered by private investigators and on April 23rd of the same year the culprit, Vitek Boden, was apprehended by the police and subsequently sentenced to 2 years in prison and was required to pay $13,111 to the council for the damages caused by the spilt sewage (Hassanzadeh et al., 2020) (Hemsley & E. Fisher, 2018).

How did it happen and was it successful?

The culprit managed to gain unauthorised access to the SCADA system and subsequently acquired control over the pumping stations by taking advantage of the then insecure and often improperly configured radio communications utilised in SCADA systems. The attacker did this by just using a standard laptop and a radio transmitter. This, as well as the inherent vulnerability of the legacy system, was the major contributing factor for the success of the attack (Hemsley & E. Fisher, 2018).

Impact

Millions of gallons of sewage was released into the environment and caused significant damage to the local areas of the spill. The spill polluted a tidal canal after polluting upwards of 500 meters of open drains in a residential area. The spill resulted in the discolouration of creek water, the death of marine life, and scent pollution which severely inconvenienced local residents. The subsequent clean-up of the spill resulted in considerable expenditure by local authorities to fix the damages ("Maroochy Shire Sewage Spill", n.d.).

Attack - 2 : 2003 Virus discovered in SCADA water system, Australia

What happened

In 2003 a water facility in Australia discovered the blaster virus in its water control system, which caused impairments in control system performance as well as errors in the systems database ("Baseline Audit Uncovers Virus in Water Control System", n.d.).

How did it happen and was it successful?

The attack was successful. The success of the virus infecting the control system is attributed to the out of date system patches and virus protection software which needed to be updated for more optimal security ("Baseline Audit Uncovers Virus in Water Control System", n.d.).

Impact

While the virus did cause the system to experience performance problems, the overall impact was minimal due to the timing of these problems. If the problems had occurred at a more critical time, the damages would have been more extensive ("Baseline Audit Uncovers Virus in Water Control System", n.d.).

Attack - 3 : 2004 Trojan backdoor in SCADA water system Canada

What happened

In 2004, a Trojan backdoor was discovered in the Human-machine interface (HMI) of a water utilities SCADA system in Canada, during a security audit of the system ("Trojan Backdoor on Water SCADA System", n.d.).

How did it happen and was it successful?

The attack was successful as the Trojan was found in the system. The Trojan is assumed to have infected the HMI due to an operator accessing an email infected with the Trojan through external email websites. The Trojan contained a reverse tunnel which led to an external website that was blocked, as well as a keylogger which was not blocked, utilising Simple Mail Transfer Protocol (SMTP) to transport data recorded by the keylogger. The attack at best can be considered partly successful as the reverse tunnel was blocked and the keylogger was not ("Trojan Backdoor on Water SCADA System", n.d.).

Impact

If the attack had been entirely successful, the back-door Trojan would possibly have allowed attackers to gain complete remote control of the SCADA system's HMI , possibly allowing attackers to interfere with systems operations to remotely cause performance issues ranging from mild to catastrophic ("What is a Trojan Virus?", n.d.). If the reverse tunnel had not been blocked, information about the systems operation methods would be tracked by the keylogger and sent through the reverse tunnel to the outside website into attackers hands, which would give them additional tools and information for remote unauthorised tampering with the system ("What is a Keylogger? | How Hackers Install a Keylogger", n.d.).

Attack - 4 : 2005 Virus found in SCADA devices, Australia

What happened

Staff at a water utility in Australia discovered three types of viruses in one or more SCADA laptop devices during a routine audit of the devices ("Routine Audit of SCADA Laptop Identifies Virus", n.d.).

How did it happen and was it successful?

The attack was successful as the laptop devices were infected with three types of viruses. The viruses managed to infect the laptop because of the lack of staff inclination to bring them in for routine patches and upgrades, hence making the devices more susceptible to the infection ("Routine Audit of SCADA Laptop Identifies Virus", n.d.).

Impact

The impact of the attack was minimal as the fixed computers connected directly to the SCADA network were subjected to routine patches which reduced the vulnerabilities for infection and it was confirmed that the viruses were not inherently harmful to the system. If the viruses were intended to cause harm and both the laptop devices and the fixed SCADA computers were not subject to routine patches, the virus would have likely compromised the SCADA systems. This could have led to the operations of the utility that the system is responsible for experiencing debilitating performance issues ("Routine Audit of SCADA Laptop Identifies Virus", n.d.).

Attack - 5 : 2006 Pennsylvania Water Filtering Plant, United States

What happened

In a water treatment plant in Harrisburg, Pennsylvania, investigations by the FBI discovered that a virus had infected the laptop of an employee of the water plant which was used by attackers situated outside of the United States. The hackers managed to install both spyware and a virus into the water treatment plant's computer system (Hassanzadeh et al., 2020) ("Pennsylvania Water Company Hack", n.d.).

How did it happen and was it successful?

The attackers used the employee's infected device as an initial access point which allowed them to get access to the plant's main computer network. This provided attackers with the opportunity to install malicious software. The attack, therefore, is a success as the attackers did achieve this goal (Hassanzadeh et al., 2020) ("Pennsylvania Water Company Hack", n.d.).

Impact

The objective of the attack was found to be not to cause harm but to gain various emails and information. However, if the scope of this attack had been different and seriously malicious, the methods used had the potential to cause serious harm to the operations of the plant, as attackers can cause various problems to occur such as "altering the concentration levels of disinfectants in potable water", and similar or more disastrous damages ("Pennsylvania Water Company Hack", n.d.).

Attack - 6 : 2007 Tehama-Colusa Canal, United States

What happened

A disgruntled former employee at Tehama-Colusa Canal managed to disrupt the automatic operation of water diversion from Sacramento River to local farms by damaging the computer responsible for the operations. Fortunately, manual operation of the canals was not affected (Hassanzadeh et al., 2020).

How did it happen and was it successful?

The attacker managed to conduct this successful attack by using his authority as an electrical supervisor at the Tehama-Colusa Canal Authority to get access to the canal's SCADA computers where he then installed unauthorised software that was responsible for the impairment of the automatic water diversion operation (Hassanzadeh et al., 2020) (McMillan, 2007).

Impact

The attack resulted in the Tehama-Colusa Canal Authority suffering $5000 worth of damages (Hassanzadeh et al., 2020) (McMillan, 2007).

Attack - 7 : 2011 South Houston Water Treatment Plant, United States

What happened

A hacker going by the alias "prof" claimed to have penetrated a water utilities network in South Houston and gained privileged access to the SCADA software that was responsible for the management of a number of water plants in the area. The attacker claimed to have done this to not cause harm but with the goal to highlight the glaring vulnerabilities that exist in similar Industrial Control Systems ("South Houston Water Treatment Plant Hack", n.d.) ("loldhs pr0f", 2011).

How did it happen and was it successful?

The attacker claimed to have cracked an insecure password to gain access to Siemens Simatic HMI software. In their post, they also critiqued the practice of connecting the Human-Machine Interface of SCADA interface to the internet, implying it to be a major vulnerability that contributed to his success ("South Houston Water Treatment Plant Hack", n.d.) ("loldhs pr0f", 2011).

Impact

According to the attacker, the purpose of the attack wasn't to cause harm but instead to showcase glaring vulnerabilities, so no damage was inflicted. However, according to "prof" they had plenty of opportunities in their intrusion to tamper with the settings of the SCADA system such as denying remote access service to people and the shutting down of certain components ("South Houston Water Treatment Plant Hack", n.d.).

Attack - 8 : 2012 Decoy water plant, United States

What happened

A decoy water plant in the US set up for a research project to showcase vulnerabilities in industrial control systems was infiltrated by a Chinese hacker group known as APT1 (Simonite, 2013).

How did it happen and was it successful?

The hacker group APT1 fell for the honey pot set up by the researchers. The hackers in their attack made use of a nondescript Microsoft Word document embedded with malicious software that, when accessed, would compromise the water plant's ICS system. On the attacker's end, this should not be considered a success, as even though they did succeed in infiltrating the decoy water plant, it was a honey pot designed to lure attackers (Simonite, 2013) ("Chinese Hacking Team Caught Taking Over Decoy Water Plant | Information Security Buzz", 2013).

Impact

This attack, as well as the other attacks in the research project, showcased the many vulnerabilities in industrial controls systems and that many groups and individuals such as APT1 have the goal to compromise these systems both partly and fully, with the necessary skills and tools to carry them out. This would spawn severe consequences to infrastructure and citizens if successful attacks are frequent (Simonite, 2013) ("Chinese Hacking Team Caught Taking Over Decoy Water Plant | Information Security Buzz", 2013) (Sterling, 2013).

Attack - 9 : 2013 Bowman Avenue Dam, United States

What happened

In 2013, unauthorised access to the SCADA system of the Bowman Avenue Dam was acquired by Iranian hackers with the assumed goal of reconnaissance, not an intrusion to cause harm (Hassanzadeh et al., 2020) (History).

How did it happen and was it successful?

The attackers were successful in their intrusion. This success is due to the control system of the dam configured in a way that made it directly accessible through the internet. Furthermore, there was lack of security controls to account for this configuration, such as authentication access controls and a firewall. The attackers taking advantage of the previous point also made use of the Google Dorking hacking technique which would allow them to locate vulnerabilities in web applications. The attackers made use of an independent computer connected to the dam's system to facilitate their intrusion (Hassanzadeh et al., 2020) (Hemsley & E. Fisher, 2018).

Impact

Even though the intrusion was a success, the scope of the attack was not to damage the dam control systems but to gather information. Furthermore, the remote-controlled sluice gate could only be operated manually at the time due to being disconnected from the network for maintenance (Hassanzadeh et al., 2020) (Hemsley & E. Fisher, 2018). Had this not been the case – if the attacker's scope had been to cause harm and they could have acquired remote access to the sluice gate, gaining full control over the water flow over the blind brook creek, allowing them to alter the water level of the creek - the attackers hypothetically would have been able to cause a flood in the area (Kutner, 2016).

Attack - 10 : 2014 Five water utilities, United States

What happened

Adam Flanagan was a fired radio frequency engineer of a company responsible for the manufacture of smart meters that had been installed in five water utilities across 3 States. He managed to gain unauthorised access to the protected networks and the utilities and water meters, where through malicious activities he caused the water meters to shut down (Hassanzadeh et al., 2020) ("United States Department of Justice", 2017).

How did it happen and was it successful?

The attack was a success. The attacker managed to acquire unauthorised access by taking advantage of the unchanged default password of the Tower Gateway Base Station (TGB), which communicated with smart water meters to send data received back to the appropriate facilities for billing and monitoring. With this access over a short period, the attacker shut down the TGB, altered the TGB's radio frequency and changed root passwords (Hassanzadeh et al., 2020) (Gallagher, 2017).

Impact

The attack caused inaccuracies in billing data due to the TGB not being able to send back up to date data from the smart water meters. This resulted in water companies affected by this attack to resort to time consuming manual data collections, as well a forensic investigation being commissioned to identify the attacker at Flanagan's former employer's expense (Hassanzadeh et al., 2020) ("United States Department of Justice", 2017).

Attack - 11 : 2016 Undisclosed drinking water utility, United States

What happened

Four out of seven Sixnet BT cellular routers that facilitated wireless monitoring of pumping stations of an undisclosed drinking water company were compromised and used to steal internet bandwidth by attackers that had acquired unauthorised access (Hassanzadeh et al., 2020).

How did it happen and was it successful?

The attack was a success and was executed by the attackers by taking advantage of the hardcoded credential vulnerability present in the routers at the time of the attack, which allowed the attackers to hack into the routers' unchanged factory default password (Hassanzadeh et al., 2020) (Walton, 2017).

Impact

The scope of the attack did not appear to be to harm the water utility's infrastructure but instead to steal internet bandwidth, so no disruption to the utility occurred. However, due to the attack, the water utility did have a massive surge in the amount owed in their monthly cellular bill, which increased from the initial $300 a month to $45,000 then to $53,000 (Hassanzadeh et al., 2020) (Walton, 2017).

Attack - 12 : 2016 Undisclosed utility, United States

What happened

Heavy suspicious activity was identified from the network of the control panel of a pumping station of an undisclosed water facility by a systems administrator. This lead to the realisation a possible cyber-attack was taking place (Hassanzadeh et al., 2020).

How did it happen and was it successful?

The attack appeared to be a success as ICS-CERT did uncover malware artefacts in the network, which they proceeded to reverse engineer in order to identify what was compromised and accessed and the intrusion point of the attack (US Department Of Homeland Security, 2016) (Hassanzadeh et al., 2020).

Impact

Not enough information is available on the impact of this attack. However, since the suspicious network activity did originate from the control panel of a pumping station, the scope of the attack may have been to cripple the pumping station which, if successful, would likely have disrupted the operations of the utility. (Hassanzadeh et al., 2020).

Attack - 13 : 2016 Kemuri Water Company, United States

What happened

A Verizon investigation into the OT-IT systems of a water company referred to as Kemuri, uncovered evidence of unauthorised access attempt by state-sponsored hackers. The attack is believed to have been the reason for the irregular operations of water valves, the irregular alterations of water chemical levels and an effect on production and treatment operations (Hassanzadeh et al., 2020) (Hemsley & E. Fisher, 2018).

How did it happen and was it successful?

The attack was a success. This is attributed to attackers taking advantage of the vulnerabilities discovered by Verizon in the outdated computers and systems linked to the water company's valve and flow controls. More specifically, the attackers exploited vulnerabilities in a payment application server that was linked to the valve and flow controls. The valve and flow controls are vital to the control of the Programmable Logic Controllers (PLC) which is responsible for the operation of the water company's water treatment and production facilities (Hassanzadeh et al., 2020) (Hemsley & E. Fisher, 2018).

Impact

The attack resulted in irregular activity in the production and treatment facilities which was the cause of the alteration in water chemical levels and supply recovery speed. The investigation concluded that if the attackers were more capable, the consequences would have been serious to the local residential area (Hassanzadeh et al., 2020) (Hemsley & E. Fisher, 2018).

Attack - 14 : 2016 2017 Dragonfly campaign - Target Europe and North America

What happened

In 2017 the United States Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) issued a joint technical alert warning of a persistent Russian state-sponsored cyber campaign targeting critical sectors in the United States. Specifically, the targets were government entities, manufacturing, aviation, energy, commercial services and the water sector (US Department of Homeland Security, 2018).

How did it happen and was it successful?

Impact

The campaign was successful. The campaign's approach consisted of a multi-stage intrusion campaign where the Russian state-based actors staged multiple different types of attacks, the most prominent being credential collecting network reconnaissance, host-based exploitations, spear-phishing campaigns, watering attacks, and specific targeting of industrial control systems. The attackers divided the victims targeted into two categories, the staged targets and the intended victims. The staged targets were third party vendors with low network security; the network of the third party was then used as a jumping-off point to compromise the networks of their intended victims. In many of these instances, they succeeded in intruding into the core systems in many of these sectors (US Department of Homeland Security, 2018) (Kennedy, 2018).

The campaign affected numerous organisations across multiple critical sectors in the US. The scope of the attack seems to be to reconnaissance of the systems and Industrial Control Systems of these sectors with the possible goal of gathering pertinent information that would allow the attackers to gain control of and sabotage the systems of these sectors (US Department of Homeland Security, 2018) (Kennedy, 2018).

Attack - 15 : 2018 Onslow Water and Sewer Authority, United States

What happened

Opportunist attackers launched persistent attacks against the water utility company Onslow Water and Sewer Authority, at the onset of Hurricane Florence (Hassanzadeh et al., 2020).

How did it happen and was it successful?

The act of attacking the utility when it was most vulnerable was the tactic that helped to ensure the success of the attack. Sophisticated ransomware attacks were initially conducted through a persistent polymorphic malware called EMOTET. However, once security experts appeared to have mitigated the malware it morphed into a more advanced and sophisticated virus known as RYUK (Hassanzadeh et al., 2020) (Hudson, 2018).

Impact

The attack resulted in the encryption of files and databases of the water utility as well as locking access to computers for many employees, in turn limiting the utility's computing power. As a result of these efficiency drops, the timeline for many services of the utility were delayed for several weeks after the attack (Hassanzadeh et al., 2020) (Hudson, 2018).

Attack - 16 : 2018 An undisclosed European water utility, European Union

What happened

Radiflow - a critical infrastructure security firm - in their investigation of suspicious network activity in the SCADA network of a European water utility, identified a crypto-mining malware in the utility's OT systems network (Hassanzadeh et al., 2020).

How did it happen and was it successful?

The attack was successful as the attackers managed to stealthily install the crypto mining malware in the OT systems network and were unidentified for some time. The internet requirement of the cloud-based OT analytics system used by the water utility for remote maintenance of the OT systems facilitated the success of the attack, as it enabled installation of the crypto-mining malware into the network the OT systems. The crypto-mining malware then caused the topology change in the OT network by linking to external IP addresses which lead to the site MinerCircle Monero Pool. The alerts triggered by the topology change were the reason for the attack's detection (Hassanzadeh et al., 2020) ("Detection of a Crypto-Mining Malware Attack at a Water Utility | Radiflow", 2018).

Impact

The crypto miner was responsible for the use of 60% of the utility's bandwidth consumption as well as 40% of the OT network's traffic. This resulted in the degradation of operational resources of the SCADA network of the utility which lead to the risk of operational faults (Hassanzadeh et al., 2020) ("Detection of a Crypto-Mining Malware Attack at a Water Utility | Radiflow", 2018).

Attack - 17 : 2019 Riviera Beach Water Utility, United States

What happened

Riviera Beach water utility in Florida was subject to severe ransomware attacks. The damage was only resolved after the city council acquiesced to the attacker's monetary demand (Hassanzadeh et al., 2020) (Doris, 2019).

How did it happen and was it successful?

The attack was caused by an employee of the city's police department accessing an email infected with the ransomware. The success of the attack is mostly attributed to the insecure computer network of the city due to lack of updates coupled with outdated hardware, which exposed systems very vulnerable to attacks (Hassanzadeh et al., 2020).

Impact

The attack resulted in the encryption of data and the shutdown of utility operations, especially the control systems of pumping stations, water quality testing facilities and payment processes. The attack also affected the systems of the police department, local government departments and the city council. The city council, against the advice of the Federal Bureau of Investigations and the Department of Homeland Security, acquiesced to the attacker's demands and paid at the time $600,000' worth of bitcoin. Even after paying the attackers the ransom, some encrypted data was still inaccessible (Hassanzadeh et al., 2020) (Doris, 2019).

Attack - 18 : 2019 Fort Collins Loveland Water District, United States

What happened

The Fort Collins Loveland Water District utility was the victim of a ransomware attack affecting some technical data. The attackers demanded a monetary ransom from the district to resolve the situation but were declined (Hassanzadeh et al., 2020).

How did it happen and was it successful?

The attack can be considered successful as the ransomware did infect the utility's systems and encrypt some data. The operation is generally considered as unsuccessful as the district did not pay the ransom and unlocked the data themselves (Hassanzadeh et al., 2020).

Impact

As stated previously, the attack managed to encrypt some technical and customer data but daily operations were not affected. Even though the impact of this attack can be considered relatively minimal, the attack shows more of the damage potential of a ransomware attack on a water utility (Hassanzadeh et al., 2020).

Attack - 19 : 2020 Attack on water infrastructure, Israel

What happened

A large scale coordinated attempted attack on Israel's water infrastructure targeting pumping stations, wastewater treatment facilities and sewage systems was confirmed to have taken place in April by Israel's National Cyber Directorate (Brumfield, 2020) (Kerstein, 2020).

How did it happen and was it successful?

The attack was unsuccessful and was thwarted. The attackers were trying to take advantage of vulnerabilities prevalent in outdated systems and insecure networks that companies use to connect to their systems. As a result, the directorate advised companies to make sure the software of their control systems were up to date. The main goal of the attack appears to be to alter the chlorine levels in the water supply and to confuse sensors to give false readings of the actual chlorine levels to fool the operators (Brumfield, 2020) (Kerstein, 2020) (Press, 2020).

Impact

There was no significant impact as the attack was thwarted. If the attackers had managed to alter the water chlorine level, the consequences would be disastrous as correct water chemical level is a major factor in its safety and if the attackers had succeeded, the local population could have suffered from mild poisoning due to the altered chlorine levels in the water (Brumfield, 2020) (Press, 2020) (Cimpanu, 2020).

Attack - 20 : 2020 Attack on Agricultural water pumps, Israel

What happened

In June 2020, shortly after the previous April Attack on Israel's water infrastructure, there were two more attempted cyber-attacks on Israel's water infrastructure: one against water pumps in Mate Yehuda and the other against agricultural pumps in Galilee (Cimpanu, 2020) (Paganini, 2020).

How did it happen and was it successful?

The attack was not successful as any damage caused to installations was repaired quickly and no harmful consequences occurred due to the attack (Cimpanu, 2020) (Paganini, 2020).

Impact

Two small drainage installations of the agricultural sector where the attacks hit were damaged but were repaired before any real-world damage occurred. If the attack had been successful, Israel's food output may have been negatively affected (Cimpanu, 2020) (Paganini, 2020).

CONCLUSION

Due to a lack of transparency regarding the nature and details of cyber-attacks in this sector, the on-going threats are often underestimated and not given the priority they deserve.

This paper provides twenty real-world case studies of cyber security incidents in the Water and Waste-Water sectors. The incidents in this paper show that many of the factors and vulnerabilities are the same, whether it is outdated hardware, systems and networks or the human factor which include unintentional error by employees or intended sabotage.

This consistency in the type of breaches shows there is a lack of cyber awareness and infrastructure in this sector.

The similarity of cyber attacks in the water sector show the importance of disclosure so that key learnings can prevent future incidents and mitigate cyber threats. Cyber security for the water sector must be a priority as any disruption can have a significant impact on the community.

"The similarity of cyber attacks in the water show the importance of disclosure so that key learnings can prevent future incidents and mitigate cyber threats. Cyber security for the water sector must be a priority as any disruption can have a significant impact on community."

REFERENCES

Baseline Audit Uncovers Virus in Water Control System. Risidata.com. Retrieved 9 September 2020, from https://www.risidata.com/Database/Detail/baseline-audit-uncovers-virus-inwater-control-system.

Brumfield, C. (2020). Attempted cyberattack highlights vulnerability of global water infrastructure. CSO Online. Retrieved 4 September 2020, from https://www.csoonline.com/article/3541837/attempted-cyberattack-highlights-vulnerability-of-global-waterinfrastructure.html.

Cimpanu, C. (2020). Two more cyber-attacks hit Israel's water system. ZDNet. Retrieved 5 September 2020, from https://www.zdnet.com/article/two-more-cyber-attacks-hit-israelswater-system/.

Chinese Hacking Team Caught Taking Over Decoy Water Plant | Information Security Buzz. Information Security Buzz. (2013). Retrieved 9 September 2020, from https://www.informationsecuritybuzz.com/news/chinese-hacking-team-caught-taking-over-decoywater-plant/.

Detection of a Crypto-Mining Malware Attack at a Water Utility | Radiflow. Radiflow.com. (2018). Retrieved 26 September 2020, from https://radiflow.com/case-studies/detection-of-a-cryptomining-malware-attack-at-a-water-utility/.

Doris, T. (2019). Why Riviera Beach agreed to pay a $600,000 ransom payment to regain data access... and will it work? The Palm Beach Post. Retrieved 27 September 2020, from https://www.palmbeachpost.com/news/20190619/why-riviera-beach-agreed-to-pay-600000ransom-payment-to-regain-data-access-and-will-it-work.

Gallagher, S. (2017). Some beers, anger at former employer, and root access add up to a year in prison. arsTechnica. Retrieved 20 September 2020, from https://arstechnica.com/informationtechnology/2017/06/ex-technician-convicted-of-possibly-drunken-attack-on-smart-watermeter-system/.

Germano, J. (2019). Cybersecurity Risk & Responsibility in the Water Sector (p. 6). American

REFERENCES

Water Works Association. Retrieved from https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf

Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, M. (2020). A Review of Cybersecurity Incidents in the Water Sector. Journal Of Environmental Engineering, 146(5), 03120003. https://doi.org/10.1061/(ASCE)EE.1943-7870.0001686
Hemsley, K., & E. Fisher, D. (2018). History of Industrial Control System Cyber Incidents. Idaho National Lab, (2), 4,13,17. https://doi.org/10.2172/1505628

Hudson, J. (2018). CYBER-CRIMINAL Target Critical Utility In Hurricane-Ravaged Area. Onwasa.com. Retrieved 23 September 2020, from https://www.onwasa.com/DocumentCenter/View/3701/Scan-from-2018-10-15-08_08_13-A?bidId.
loldhs pr0f. Pastebin. (2011). Retrieved 18 September 2020, from https://pastebin.com/Wx90LLum.

Kennedy, J. (2018). US officially blames Russia's 'Dragonfly' hackers for attacks on energy grid. siliconrepublic. Retrieved 26 September 2020, from https://www.siliconrepublic.com/enterprise/dragonfly-us-russia-energy-grid-hackers.

Kerstein, B. (2020). Israel Thwarts Major Coordinated Cyber-Attack on Its Water Infrastructure Command and Control Systems. Algemeiner.com. Retrieved 4 September 2020, from https://www.algemeiner.com/2020/04/26/israel-thwarts-major-coordinated-cyber-attack-on-itswater-infrastructure-command-and-control-systems/.

Kutner, M. (2016). A cyberattack on a Westchester County dam has security experts wondering what's next. Newsweek. Retrieved 20 September 2020, from https://www.newsweek.com/ cyber-attack-rye-dam-iran-441940.

Maroochy Shire Sewage Spill. Risidata.com. Retrieved 6 September 2020, from https://www.risidata.com/Database/Detail/maroochy-shire-sewage-spill.

McMillan, R. (2007). Insider charged with hacking California canal system. Computerworld. Retrieved 18 September 2020, from

REFERENCES

https://www.computerworld.com/article/2540235/insidercharged-with-hacking-california-canal-system.html.

National Infrastructure Advisory Council. (2016). Water Sector Resilience Final Report and Recommendations (pp. 1,20). National Infrastructure Advisory Council.

Pennsylvania Water Company Hack. Risidata.com. Retrieved 16 September 2020, from https://www.risidata.com/Database/Detail/pennsylvania_water_company_hack.

Paganini, P. (2020). Two more cyber attacks hit Israel's water facilities in June. Security Affairs. Retrieved 5 September 2020, from https://securityaffairs.co/wordpress/106141/hacking/israel-water-facilities-cyber-attacks.html.

Press, A. (2020). Israeli Cyber Chief: Major Attack on Water Systems Thwarted. Securityweek.com. Retrieved 26 September 2020, from https://www.securityweek.com/israeli-cyber-chiefmajor-attack-water-systems-thwarted.

Routine Audit of SCADA Laptop Identifies Virus. Risidata.com. Retrieved 9 September 2020, from https://www.risidata.com/Database/Detail/routine-audit-of-scada-laptop-identifiesvirus.

Simonite, T. (2013). Chinese Hacking Team Caught Taking Over Decoy Water Plant. MIT Technology Review. Retrieved 10 September 2020, from https://www.technologyreview.com/2013/08/02/15525/chinese-hacking-team-caught-taking-over-decoy-water-plant/.

South Houston Water Treatment Plant Hack. Risidata.com. Retrieved 8 September 2020, from https://www.risidata.com/Database/Detail/south_houston_water_treatment_plant_hack.
Sterling, B. (2013). China China hack hack hardware. WIRED. Retrieved 19 September 2020, from https://www.wired.com/2013/08/china-china-china-hack-hack-hackhardware/.

Trojan Backdoor on Water SCADA System. Risidata.com. Retrieved 8 September 2020, from https://www.risidata.com/Database/Detail/trojan-backdoor-on-water-scada-system.
United States Department of Justice. Justice.gov. (2017). Retrieved 20 September 2020, from https://www.justice.gov/usao-edpa/pr/bala-cynwyd-man-sentenced-prison-hackingcomputers-public-utilities.

REFERENCES

US Department Of Homeland Security. (2018). Alert (TA18-074A) - Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. Cyber Security & Infrastructure Security Agency.

US Department Of Homeland Security. (2016). ICS-CERT MONITOR March/April 2016 (pp. 1-2). ICS-CERT.

Victorian Auditor-General's Office. (2019). Security of Water Infrastructure Control Systems (pp. 7,8,11). Victorian Auditor-General's Office.

What is a Keylogger? | How Hackers Install a Keylogger. Comodo Enterprise. Retrieved 17 September 2020, from https://enterprise.comodo.com/what-is-a-keylogger.php.
What is a Trojan Virus?. www.kaspersky.com.au. Retrieved 17 September 2020, from https://www.kaspersky.com.au/resource-center/threats/trojans.

Walton, B. (2017). Water Utility Cyberattack Rings Up Hefty Data Charges. Circle of Blue. Retrieved 21 September 2020, from https://www.circleofblue.org/2017/water-management/water-utility-cyberattack-rings-hefty-data-charges/.

secolve

OT SECURITY SOLVED

Head Office	Level 2, 11 York Street,
Address:	Sydney, NSW 2000
Contact:	info@secolve.com
	1800 SECOLVE (732 658)