Report on

Cyberattacks on US Energy Companies

Prepared for

Prof. Jason Ellis

ENG2575 D494, Technical Writing

New York City College of Technology, CUNY

Prepared by:

Rifat Bhuiyan

Brian Gomes

Ishtiaq Mahmud

Jose Rodriguez

Shuhanul Islam

May 19, 2022

The purpose of this research report is to understand cyberattacks, give insight into instances where cyberattacks targeted US energy companies and talk about the measurements that were taken to mitigate these issues. Based on these precedents provide a recommendation for the most optimal solution.

You can access the websites associated with this report by clicking here.

Table of Contents

Abstract

Cyberattacks have become as commonplace as the Internet itself gets bigger and so many people and infrastructure require the cyber world. Each year, industry reports, media outlets, and academic articles highlight this increased prevalence, spanning both the amount and variety of attacks and cybercrimes. In this report, we seek to further advance discussions on cyberattacks in energy companies, what problem it causes, and possible solutions that can mitigate these issues. In particular, two of the cyberattacks that caused irruptions on the energy companies are an American oil pipeline system called Colonial Pipeline was affected by an immense ransomware attack and the FDI attack on electric grids. To consider the applicability of our findings, we investigate its infrastructural downfall effects, and possible solutions such as Moving target defense, iECPS for reliable smart grids, Ransomware detection by mining API call usage, and Zero Watermarking Algorithm for Software Protection which could have either prevented it or reduced the effects of the attack. In the end, we propose our recommendation for the best possible solution that can be used to prevent these types of Cyberattacks.

1.0 Introduction

In today's world, so many things operate in the digital landscape. From wearable technology, our phones, social media, bank details in the form of digital wallets, automated robots, self-driving cars, and many more are being interconnected in the digital realm. Virtually everyone in almost every place is becoming more and more connected, sharing data, and socializing. Using the digital world as a medium has become the new norm in society. As the world continues to grow exponentially, so does the threat of those who will abuse this medium for their gain. This threat is generally referred to as Cyber Attack. To give a more explicit definition of Cyber Attack, according to OED Oxford Dictionary Cyber Attack means, “the use of information technology to infiltrate or disrupt computer systems; an instance of this” [1]. So using a computer system and its specific coded software to do reconnaissance or even hijack other devices/networks would be what a cyberattack is all about. There are various types of cyber attacks as well like phishing attacks, ransomware, DoS and DDoS Attacks, FDI, and many more that can target and affect various computing systems.

Cyber-attacks have been prominent ever since the creation of the internet. As more people started getting into the internet, so did the attacks. Cyber attacks happen in various places ranging from personal computers, to corporate networks to even large-scale energy infrastructure making them practically immobile. One of the main targets of cyber attacks has been energy infrastructure. The authors of the article ‘Fighting the Fight: Cyber attacks on industrial control systems are increasing. What can you do?’ explains that disrupting critical national infrastructure is an easy way to cause widespread unrest and dissatisfaction among the population. Equally, they can cause major economic damage by attacking high impact targets. They includes, “They know that disrupting critical national infrastructure is an easy way to cause widespread unrest and dissatisfaction among the population. Equally, they can cause major economic damage by attacking high impact targets” [2]. This means Society’s growing dependence on Energy infrastructure and systems has given birth to a new class of cyber-physical threats that may facilitate physical attacks with a cyber-attack, so-called ‘cyberenabled physical attacks’ on critical infrastructure. While the actions of such attacks are virtual, the impact can be physical.

Not only do these cyber attacks cost millions of dollars of loss because of employee time and potential hardware replacement, but also because these issues have been caused, it would have a devastating impact on the health, safety, security, or economic well-being of citizens or the active functioning of governments. After all, most of society’s basic functions need the energy to operate. So if energy infrastructure is down, the given area the energy infrastructure powers won't be able to function properly, therefore, leading to potentially devastating issues as listed. For example, in the latest of many cyber attacks, an energy company in America called Colonial Pipeline was cyber attacked. This incident led to panic and left the company scrambling for gasoline, jet fuel and diesel.

The cyber attacks are so prominent that it is questionable, can they even be mitigated? So much damage has been caused so where's the solution? Here in this report, possible solutions are discussed to prevent and solve the effects of cyber attacks. For example, to practice anti-ransomware features for attacks there have been different methods applied. MTD is a defense mechanism that continuously changes the attack surface to prevent cyberattacks. There's another method called API calls which is a block of code for detection at the early stage of ransomware. Then there's methods such as CPS for energy theft detection, and a watermarking and de-watermarking system which involves encryption and decryption of meter data. All these methods are part of many possible solutions to mitigate future cyber attacks.

2.0 Problem

2.1 Colonial Pipeline

Background and Context

The latest high-profile cyberattack that stunned America occurred on May 7, 2021, when Colonial Pipeline, “which sends more than 100 million gal. of fuel daily from Houston to New York, was forced to shut down operations after hackers penetrated its computer networks” [3, p. 19]. The company covers approximately 5500 miles and is a major fuel supplier for Southeast and the East Coast. This incident led to panic and left many states “scrambling for gasoline, jet fuel and diesel” [3 p 19].

The FBI traced the attack to a group called DarkSide, “a cybercrime gang based in Eastern Europe that’s notorious for hacking into companies’ systems, encrypting their files and extorting them to pay large ransoms to unlock the data” [3 p 19]. According to DHS Secretary Alejandro Mayorkas, the US government paid almost $350 million dollars in 2020 alone for ransomware attacks. DarkSide also has suspected links to Russia, which is a national security threat. If a war were to break out between America and Russia, this hacking could lead to major implications. Despite this concern, Biden didn’t take action against Russia.

Aspects of the problem

Consequences of the attack spread rapidly and caused a lot of real-world disruption throughout the US energy sector. The 6-day shut down impacted regular gasoline prices, causing an average increase of 4 cents per gallon in affected areas. The high demand for gasoline and spike in prices imposed a strain on household income and reduced spending on other goods and services, slowing economic growth.

Upon discovering the attack, the company started taking some systems offline, “which temporarily stopped all its pipeline operations and affected a number of its IT systems” [4 p 6]. The company “informed the US government, law enforcement, and engaged third-party cyber forensics. Services resumed towards the end of last week, and late on Thursday 13 May it emerged that the organisation had paid a ransom demand of $5m” [4 p 6].The ransom was paid with “75 Bitcoins, of which 63.7 were recovered by the US Department of Justice one month later. The six-day shutdown ended at 5pm on 12 May 2021, however, it took further time to restore supply to gas stations in southern states “[5].

This incident put a spotlight on US’s aging infrastructure. Most of the equipment that are in used today are 40 to 50 years old. Back then, companies only cared about reaching as many people as they can and did not have the foresight on what was to come. However, incidents like this are creating a renowned push for upgrading the infrastructure. Tom Garrubba, CISO of Shared

Assessments said “Numerous agencies, including CISA [the US’s Cybersecurity and Infrastructure Security Agency] have been trumpeting warnings or calls to action to update critical infrastructure for years, and sadly, the time for initial action has long since passed. The evidence is clear: we are under attack by both rogue and state-sponsored organisations, and the cyber community – along with the general public – have taken notice and are getting very worried.” [4 p 7]

2.2 FDI Effect and Remote Control Instance

Background and Context

Due to technological advancement, engineers have been able to come up with ways to remove the physical aspect from different services. The same goes with Energy suppliers who have evolved and now use electric grid systems to wirelessly provide and communicate their equipment to monitor and control remotely. But the same goes for those who use these advancements for all the negative reasons, like cyberattacking. An electric grid as described by the authors of ‘***Analyzing the effects of cyberattacks on distribution system state estimation***’[6], “An electric grid comprises transmission and distribution networks that connect different sources of power generation to consumers across a large geographic area”[6, p. 1]. It is this very technology that allows the electric grid to function the way it does, which means that other technological methods can be used to target the electric grid, making it vulnerable to cyberattacks.

Aspects of the problem

Nowadays, a talented individual or group of talented people could potentially gain control of equipment through the use of technologies to intentionally create complications, like malfunctions that lead to grave incidents. These kinds of attacks are mostly seen in places where heavy machinery is constantly controlled and dealt with. Electric grids are a perfect example of mechanical automatization, they provide a synchronized connection between power providers and customers which allows for the transmission and distribution of energy. Thus making it a perfect target for cyberattacks. As explained by the authors of the article '***Going beyond Cybersecurity Compliance: W.P. and U.C.R.N.T.C.***'[9]. "Electric grid is monitored and controlled by Indus' trial control systems (ICSs), including supervisory control and data acquisition (SCADA) systems and field devices that are cyber vulnerable"[#, p. 48]. The way cyberattacks cause damage to electric suppliers is by false data injection or random data corruption. But there are also instances where cyberattacks gained control over the equipment that is interconnected through the electric grid. The authors of the '***Going beyond Cybersecurity Compliance: W.P. and U.C.R.N.T.C'***[9] article, also denoted as a cybersecurity case study, a malfunction diagnosed by the Florida Power and Light utility company, wherein February 2008; a system disturbance that began with the transmission malfunction of a Bulk electric system (BES), lead to a domino effect of errors.

False Data Injection (FDI) consists of introducing false new data into the supervisory control and data acquisition (SCADA) system. This false new data can lead to misrepresenting the status of one or many other components of the electric grid, thus leading those who check the electric grid to mistakenly take the wrong measures. FDI attacks are done in many ways, for example, an attacker can choose to inject the false data in random intervals of quantity and time, or it could be done in a constrained manner. This is very dangerous because the attacker haves' control over what the monitor or operator sees. This is shown by the analysis conducted by the authors of the article '***False Data Injection Impact Analysis in Ai-Based Smart Grid***'[7], where they explain the following, "Our analysis shows that accuracy of model is highly affected even with a slight change in the real data. During the experiment, only 20% of the values of one of the predictors were changed and the accuracy of the model was decreased to 15% on an average. Thus, this result shows that if an attacker has complete knowledge of the profile and gets access to the network, the damages can be catastrophic. For example, expected demand and generation can be highly mismatched and which can result in blackout"[7, p. 4]. This is very impactful. If the expected demand and generation are mismatched, as explained in the article's conclusion, the operator in charge of using this data will most likely take the wrong approach when deciding how much energy to generate as the operator will either increase or decrease the supply of energy. This means that the attackers have indirectly gained control over how much energy is supplied.

An example of a remote controlling cyberattack is found in a simulation of cyberattacks targeted toward one of the equipment components found inside an electric grid, made by the US National Electric Sector Cybersecurity Organization Resource (NESCOR). As the authors of the article '***Model-Base Cybersecurity Assessment with NESCOR Smart Grid Failure Scenarios***' [8]. "The [Distributed Energy Resource (DER)] owner does not change the default password or not set a password for the DER system user interface. A threat agent [. . .] gets access through the user interface and changes the DER settings so that it does not trip off upon low voltage (anti-islanding protection) but continues to supply power during a power system fault"[8, p. 321]. This is an example of an Electric grid part being manipulated by a cyberattack, the result of this attack is later discussed by the same authors which state, "A utility field crew member may be electrocuted"[8, p. 321]. This shows how a breach of the cyberinfrastructure of a mechanical part, can be harmful to the person that operates it.

Another way cyberattacks have branched out is by creating interference that can halt a specific task. As explained before, the authors of the '***Going beyond Cybersecurity Compliance: W.P. and U.C.R.N.T.C'*** article stated that, "transmission system fault led to the loss of approximately 2,300 MW [(Mega Watts)] of load in South Florida. The disturbance further caused the later loss of approximately 4,300 MW of generation within the region and additional load shedding"[9, p. 52]. This goes to show that cybersecurity needs to advance to fully protect our suppliers from the advancement of cyberattacks. These problems are serious and very endangering to us and our suppliers, which is why we must come up with solutions or methods to mitigate the effects of these cyberattacks.

3.0 Solutions

3.1 Context of the Solutions

While we are always proposing new methods to prevent different types of cyberattacks, there are some of the existing methods people talked about. Firstly, we should always just practice just general safe online behavior, a lot of users out there be surprised how many people don't do these things like make sure not to click on attachments or links in emails that you don't know who they're from so only download programs from trusted sites and just kind of avoid shady sites on the Internet in general. The author from Machine Design describes what to consider when developing a security plan in “How to Protect Energy Plants from Cyberattacks”. He states, “As the world of IoT continues to grow, companies will have to adopt multiple layers of protection and backup systems to ensure a secure energy system that can function without interruptions” [10]. This means energy plants need to practice and develop a risk management culture by understanding guidelines. There should be different types of security assessments to understand all kinds of vulnerabilities that might occur, and companies need to choose trusted vendors to utilize advanced cybersecurity technologies.

3.2 Different solutions

3.2.1 Moving Target Defense on Ransomware

To practice anti-ransomware features for attacks there have been different methods applied. MTD is a defense mechanism that continuously changes the attack surface to prevent cyberattacks. Protection-based approaches are proposed to prevent attacks by protecting measurements from certain sensors. It is possible to calculate the minimal set of measurements that must be protected from any kind of attack. Detection-based process approaches are another type of countermeasure proposed to detect potential attacks by using several frameworks. The authors of the article, ‘Ransomware protection using the moving target defensive perspective’ discuss their proposed method which can be used to protect files from ransomware. The method of moving target defense works to change the file extensions ransomware attempts to encrypt. Their experiment approach shows that it can protect files with minimal use of a computer and doesn’t need any use of security software as well. There are different types of changes that can be made in the system and they can be characterized into mainly three types which are shuffle, diversity, and redundancy. These works to shuffle different layers of the system, diverse by variating different types of servers, and works to provide more resources by a backup server. The MTD method proposes two phases to be successful as the authors mentioned, “The first phase is creating file extensions and modifying the registry keys. The second phase is changing the file extensions of all target files in a file system” [11]. This means that creating new directory ransomware’s target file won’t work with existing directories and a change of the file extension might lower their motivation to attack as they would need to come up with new techniques which cost more time. They also included, “For example, we can substitute the first 100 bytes of the file’s header with random values” [11]. This explains that the file extension can also increase the cost to attack which will frustrate the attacker’s effort to find target files. This method can be useful if it is researched more as they claim to be successful in 141 cases out of 143.

3.2.2 iECPS for reliable smart grids on FDI

There have been many factors to consider preventing any system from getting attacked with False Data Injection (FDI). There have been methods such as CPS for energy theft detection, and a watermarking and de-watermarking system which involves encryption and decryption of meter data. The authors of the article, ‘Intelligent energy cyber physical systems (iECPS) for reliable smart grid against energy theft and false data injection’ discusses their proposed method which can be used to detect and prevent a FDI attack. The methods work to detect electricity theft on user’s meter while maintaining data consistency. One of the proposed works with the machine learning models as they stated, “This detection and verification system is aimed at accurately identifying electricity thefts carried out by directly hooking on electricity supplies of some other household. The proposed system detects any unanticipated form of malicious attack causing energy theft, while also verifying the suspected attack possibility with the user, through a mailing system” [12]. This describes that the models specify date and time by notifying user through email for verification while detecting suspected theft attack. This would be an ideal solution for the security of Internet of Things (IOT) for energy theft. They also include another system which is watermarking by stating that, “We send the signal through the checker function. The data is checked to be valid by the checker function. We check if the received mean is equal to the mean by calculating the mean on the receiving side. If this stage is passed, it then goes further process of de-watermarking, if not FDI attack took place” [12]. This describes the watermarking is proposed to have improvement in reliability of the smart grid which checks data through transmission channels. This method can be useful for long run as this repeatedly ask for data integrity with proposed algorithms.

3.2.3 Ransomware detection by mining API call usage

The API call is a block of code for detection at the early stage of ransomware. It is challenging to quickly detect unknown malware for the traditional form of antivirus. There are many techniques out in the market, and those techniques do not proactively detect ransomware as soon. Newer the ransomware can encrypt the files in a minute, but the traditional defense system takes more than 48 hours to catch the ransomware. There are two ways to find Malicious software: one is with the static analysis and another with dynamic analysis. The API Call uses the Static analysis because, according to the author of the article, "Detecting malware using dynamic analysis involves monitoring programs as they run for suspicious or malicious behaviors and stopping them. The static analysis does not need the program to execute, instead, it reverse engineers the code and analysis the file" [13]. This meaning is that static analysis is an analysis of the source code, before it executes into the file. On the other hand, dynamic analysis after executing into files observes if that software is malware or not. The API call is used to filter out the most discriminating sets of features so it can be used for classification. Another issue is that others defend systems with the "class imbalance," but API solves this issue by smote technique. A smote process sends features into the basic classifier to get the training data. The first step of the file goes into the preprocessing stage, where static code is used for API calls. Then those API calls are denoted as a binary vector. After that, it uses training data in the classification model to label if the file is ransomware or benign. API functions and the system are other to detect ransomware because API functions and system provide different services to the operating system like network, security, and system service. According to the author, "The patterns of API function calls can provide key information that can be used to detect the movement of software and to represent behaviors of the software. So, analysis on API functions and system calls plays an import role in behaviour analysis of ransomware" [13]. This means that it goes for the pattern to observe the software behavior to find ransomware.

3.2.4 Zero Watermarking Algorithm for Software Protection

Another cyber attack is false data injection for manipulating the data for the measurement, and this has a significant impact on the Smart Grids and the SCADA system. The attacker could attack any region by the network information. According to the author, "The existing traditional watermarking extraction needs to provide real watermark locations. It poses a great threat to the security of watermarks because it cannot ensure whether the watermark locations will be leaked" [14]. It could be prevented by the heuristic algorithm, which will reduce the network information, but even with less information, the attacker can attack. The attatker use the weak point of the security software to inject the data for the manipulation. According to the article 'Zero Watermarking Algorithm for Software Protection', "The algorithm is made up of two constituents: embedding algorithm and extraction algorithm. The algorithm creates a key using a watermark and can retrieve the key of the software even after it gets attacked or tampered. In case software undergoes an attack and tampering is detected, the original code can be restored, causing attack effects to get nullified" [14]. With the zero watermarking algorithms, if an attack happens and the false data gets injected into the system, it could have resorted back to the original.

4.0 Recommendations

In this digital landscape of the world it is tough to overlook our physical insfrastructure which gets weaponized with variant disruptions. However, the tech experts and many other researchers always comes up with new and existing possibilities to secure our systems. In this paper, we talked about different solutions for the ongoing cyber conflicts being created. These are the solutions companies might look towards, and start practicing to have better secure system for future. Within the following outcomes, we decided to endorse two particular solutions which can be more beneficial for each of the cyber problems. Our first proposition for the ransomware attacks would be to use Moving Target Defense (MTD) which approaches to change the attack surface. This would be a valuable to prevent the attacks because as we've seen it is already been experimented in number of occasions and the results have been successful in most cases.

The most effective solution targeting FDI attacks is one proposed by the authors of the article, "***Zero Watermarking Algorithm for Software Protection***". This approach can completely nullify the effects of an FDI attack because it utilizes two algorithms whose duty is to encrypt and retrieve data by creating a key which associates with the watermark, this key is the ultimate measure that can be retrieve by the algorithms at any moment even at the time of an attack. The watermark algorightms is able to recodgnize this and retrieve the original key which can recover the original informatio prior to the False Data injectio Attack. Therefire transforming into the best solution against this issue.

5.0 References

[1] "Cyber-attack, comb. Form," *Oed.com*. [Online]. Available: https://www.oed.com/view/Entry/250879?redirectedFrom=cyber+attack&. [Accessed: 20-May-2022].

[2] D. Alexander, "Fighting the Fight: Cyber attacks on industrial control systems are increasing. What can you do?," *Chem. Eng.*, no. 923, pp. 45–47, 2018.

[3] W. J. Hennigan *et al.*, Eds., *Colonial Pipeline*, vol. 197, no. 19/20. TIME USA, LLC, 2021.

[4] A. Scroxton, "Colonial Pipeline ransomware attack has grave and far-reaching consequences: The ramifications of a major ransomware attack against a US fuel pipeline operator could spread far and wide, with professionals calling for a closer look at the strength of existing security strategies," *Comput. Wkly.*, pp. 4–7, 2021.

[5] S. Corbet and J. W. Goodell, "The reputational contagion effects of ransomware attacks," *Fin. Res. Lett.*, no. 102715, p. 102715, 2022.

[6] G. Saraswat, R. Yang, Y. Liu, and Y. Zhang, "Analyzing the effects of cyberattacks on distribution system state estimation," in *2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2021, pp. 01–05.

[7] S. Tufail, S. Batool, and A. I. Sarwat, "False data injection impact analysis in AI-based smart grid," in *SoutheastCon 2021*, 2021, pp. 01–07.

[8] S. Jauhar *et al.*, “Model-based cybersecurity assessment with NESCOR smart grid failure scenarios,” in *2015 IEEE 21st Pacific Rim International Symposium on Dependable Computing (PRDC)*, 2015, pp. 319–324.

[9] E. Smith, S. Corzine, D. Racey, P. Dunne, C. Hassett, and J. Weiss, “Going beyond cybersecurity compliance: What power and utility companies really need to consider,” *IEEE Comput. Applic. Power*, vol. 14, no. 5, pp. 48–56, 2016.

[10] C. M. Gonzalez, “How to protect energy plants from cyberattacks,” *Mach. Des.*, vol. 90, no. 4, pp. 69–72, 2018.

[11] S. Lee, H. K. Kim, and K. Kim, “Ransomware protection using the moving target defense perspective,” *Comput. Electr. Eng.*, vol. 78, pp. 288–299, 2019.

[12] H. Jain, M. Kumar, and A. M. Joshi, “Intelligent energy cyber physical systems (iECPS) for reliable smart grid against energy theft and false data injection,” *Electr. eng. (Berl., Print)*, vol. 104, no. 1, pp. 331–346, 2022.

[13] S. Sheen and A. Yadav, “Ransomware detection by mining API call usage,” in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2018, pp. 983–987.

[14] C. Iwendi *et al.*, “KeySplitWatermark: Zero watermarking algorithm for software protection against cyber-attacks,” *IEEE Access*, vol. 8, pp. 72650–72660, undefined 2020.