Asian Journal of Engineering and Applied Technology
ISSN: 2249-068X (P) Vol.10 No.2, 2021, pp.25-28

DOI: https://doi.org/10.51983/ajeat-2021.10.2.3057

The Cyber Attack on Saudi Aramco in 2012

Alaa Alsaeed
Lecturer, Management Information Systems, Bowie State University, United States
E-mail: alaa.adnan1990@hotmail.com
(Received 10 June 2021; Revised 27 June 2021; Accepted 20 July 2021; Available online 16 August 2021)

Abstract **- In recent years, information security has become a corporate priority due to the large number of cyber-attacks that happen every day. These attacks could cause a regression in economic growth, which makes corporations another reason to defend their system. This paper provides an introduction to Saudi Aramco as well as an overview of its products. Then, the paper examines the Aramco cyber-attack in 2012. Aramco is a massive company with huge facilities that require powerful policies on security. Aramco should implement a Redundant Array of Independent Disks and Intrusion Detection System and review the log files on the server to protect its servers against attacks.**
Keywords: **Saudi Aramco, Cyber Attack, Shamoon Virus, RAID, IDS, Log Files, Masking Address, Pretty Good Privacy, Contactor Employees**

I. INTRODUCTION

Technology has become an essential part of the development process. Technology is being used in almost all areas, such as business, education, health, and politics. There is no doubt that the use of technology has accelerated the development process and made life easier. Many industries nowadays rely on the Internet to spread and improve their products and services. Most of the benefits gained these days would not exist without computers or the Internet. However, technology can be a threat to companies and other industries. For example, companies might face cyber-attacks that cause damage, and important private data could be stolen.

Cyber-attacks are a big problem for companies:"the Pentagon reports that they receive about 10 million cyber-attacks every day" [5]. In addition, "in 2012 Thomas D'Agostino of the National Nuclear Security Administration says that they face 10 million cyber-attacks daily" [6]. Furthermore, according to Tom Whitehead, "in 2011 the United Kingdom had 44 million cyber-attacks" [10]. Moreover, "the CEO of British Petroleum Bob Dudley, said that BP suffers 50,000 cyber-attacks a day" [8]. Saudi Aramco is one of those energy companies affected by cyber-attacks. In 2012 Saudi Aramco had cyber-attacks from a malware virus called Shamoon. The energy company has remedied the situation and solved the problem after the damage. Cyber-attacks are part of electronic warfare, and they seem to be increasing. Companies must be aware of the risk of cyber-attacks and prepare solutions to prevent future attacks.

II. SAUDI ARAMCO

Saudi Aramco started in 1933 when the Saudi government awarded exploration rights for an oil company - Standard Oil of California (Socal). After repeated failed attempts to identify large oil reserves, the company finally discovered oil in 1938. That happened just before the Second World War. After that, the company changed its name to the Arabian American Oil Company (Aramco). In 1988 Saudi Arabia Oil Company (Saudi Aramco) got its current name. Saudi Aramco is an integrated petroleum and chemical company owned by the Kingdom of Saudi Arabia. It is a global leader in the field of production and exploration, distribution, refining, exploration, and the marketing of oil and gas. Oil reserves in Saudi Aramco number at around 260 billion barrels of oil, and Aramco manages the fourth-largest reserves in the world. In 2013, Aramco produced approximately 9.4 million barrels daily, and the total production for the year was around 3.4 billion barrels. This number is about an eighth of production around the world, so Aramco is one of the biggest oil companies in existence.

They also have oversight of the natural gas reserves of 288.4 trillion standard cubic feet, and they also produced 455.9 million of natural gas liquid. Almost all of the products are exported in each part of the world, but the majority of exported to Asia; in 2013, around 54 percent of crude oil was exported to Asia. Hence, Asian countries are the biggest customers for Aramco. (About Saudi Aramco) Saudi Arabia's government almost completely depends on Aramco for its revenue and budget.

The head office of Aramco is in Dhahran, which is on the east coast of Saudi Arabia, and it has a large workforce with more than 54,000 people from 66 countries. Dhahran has the largest community with more than 10,000 people who around the fifth are working in the headquarters, and it has the finance department, engineering, and materials supply. The workers are friends who enjoy an excellent lifestyle. In addition to that, it has many branches outside Saudi Arabia in Asia and Europe such as the Netherlands and the United Kingdom [1].

III. SHAMOON VIRUS

Let's first talk about the history of this virus, in August 2012 there was a virus similar to Shamoon from the way it works, this virus attacked Gas company in Qatar. The worst

day for Aramco Company was On August 15th, 2012 when the attacks take place at 11:08 AM. The virus destroyed and disrupted over 30,000 computers and 2,000 servers. [2].

The Shamoon virus works by focusing on user files, configuration files, and system data, which makes Shamoon more destructive than other viruses. This virus is made specifically for cyber espionage in the energy sector. Aramco was lucky because the day of the attack was an Islamic holiday, so many employees were on vacation and their computers were shut off; otherwise, the damage would have been greater. The impact was less effective.

There were two steps in this attack. The first one has distributed denial of service (DDoS), and obsession for all companies because there is no clear solution or way to prevent such an attack. However, there is a way to minimize the impact: expanding the bandwidth capacity.

The way DDoS works are simple—by dumping a site's stream of data, causing heaviness and traffic in the network. This makes it difficult for users to get information from the system. After this step, the hackers can handle the network, so they can do the next step.

Aramco did not realize that they were under attack; they thought it was normal to have traffic in their network because it had happened many times before.

The second step the hackers considered was the real attack. They spread the virus by breaching some Windows systems in the Aramco network. Shamoon works by scanning the IP range and giving hackers the power to plant the virus in one computer; then the virus can easily spread from one computer to another in the same IP range by using the shared files between the computers.

Shamoon can be timed by hackers, just like a bomb. So the hackers planted the virus and set the time for it to search for all infected files and destroy them by adding false data. During the DDoS attack, Aramco experienced normal activity, but in the second attack, they noticed the system was corrupted, causing a loss of data. Some employees could not access their computers.

The hackers were smart: they caused traffic when they planted the Shamoon virus. DDoS had been used many times with many companies before, so no one can blame or say Aramco could have done better with this attack.

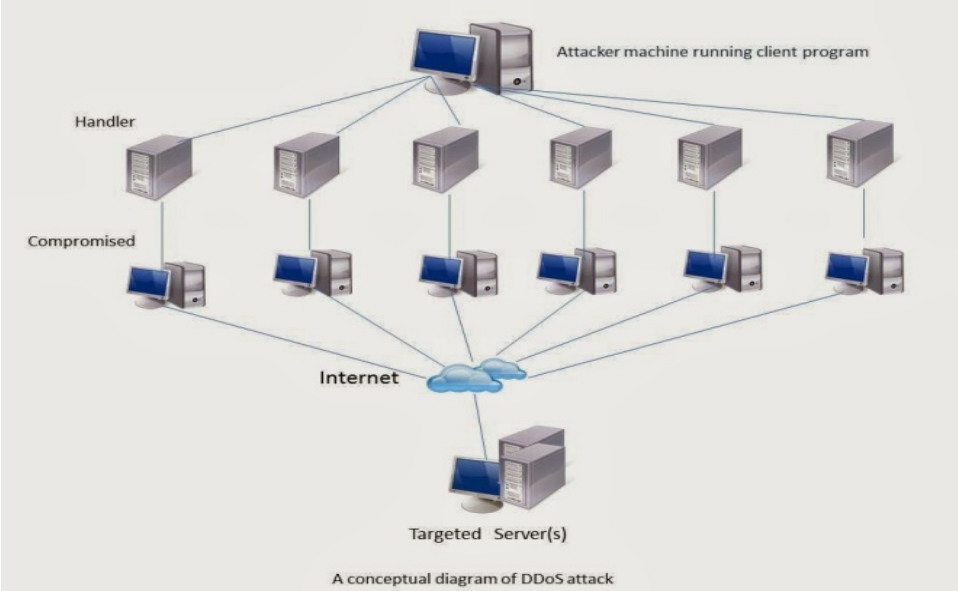

Fig. 1 A conceptual diagram of DDoS attack

IV. RECOMMENDATIONS

Aramco is a massive oil company with huge IT facilities. There are more than 2,000 servers and 30,000 PCs. For that reason, Aramco should put many provisions in place to protect its disk drives on servers, networks, and computers from damage and failure. The recommendations are as follows.

A. Redundant Array of Independent Disks (RAID)

RAID is a set of techniques for connecting several hard disk drives to a computer. The primary goal of using RAID is to store data redundantly on several hard disk drives to enable Aramco to retrieve data in case there is deliberate destruction. Common RAID techniques are RAID-0, RAID-1, RAID-3, and RAID-5. We recommend that Aramco apply RAID-1 and RAID-3 because they allow users to store data and duplicate at least two disk drives in case one disk is corrupted. Aramco can get the data from the other disk. RAID-3 works the same as RAID-1; however, RAID-3 has error-checking, which ensures the data is stored on a separate disk. More importantly, error-checking is capable of detecting errors and amending the data if the disk is corrupted.

B. Intrusion Detection System (IDS)

IDS is a software application that inspects a network or a system's activities to prevent malicious activities and reports to the management of a company if there is a policy violation.

The benefits of IDS are as follows

1. It prevents security violations, such as users running applications against Aramco policy.
2. It limits infections, such as Trojan horses or viruses.
3. It detects information leakage, like spyware and unintentional information leakage by Aramco employees.
4. It allows Aramco to find configuration errors, such as systems with inaccurate security settings.
5. It identifies unauthorized clients and servers, such as network scanning tools.

C. Review the Log Files on the Server

Reviewing the log files on the server provides the usability needed to find valuable data about user attitude precisely, rapidly, and cheaply. Reviewing the server log files will help Aramco to gather information about user behavior because the review provides a data source that illustrates what people are doing on Aramco's website. Moreover, logs display what people click on, the pages they view, and how they move from one page to another.

D. Masking Address

A masking address enables Aramco to hide its real identity from unwanted IP sources or third-party applications. For instance, if Aramco had a request from an IP source, a masking address would check on that IP through two lists: a black list and a white list. If the IP existed in the black list, Aramco's address would be hidden, and the source would be referred to another global address. However, if the IP were in the white list, the address would be available.

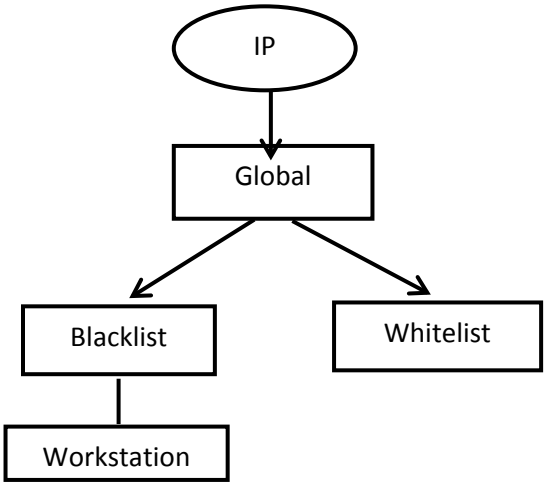

Fig. 2 Masking Address

E. Pretty Good Privacy (PGP)

PGP is a program that is used to encrypt e-mails and send an encrypted digital signature. It is used by individuals and many companies. PGP will help Aramco to secure sending and receiving e-mails, especially internal e-mails between employees. For instance, if an employee wants to send an e-mail to another employee, the sender sends the e-mail by using the recipient's public key, and the recipient should decrypt by using the recipient's private key. The recipient is the only person in world who should have this private key. In this way, sensitive information will be more secure.

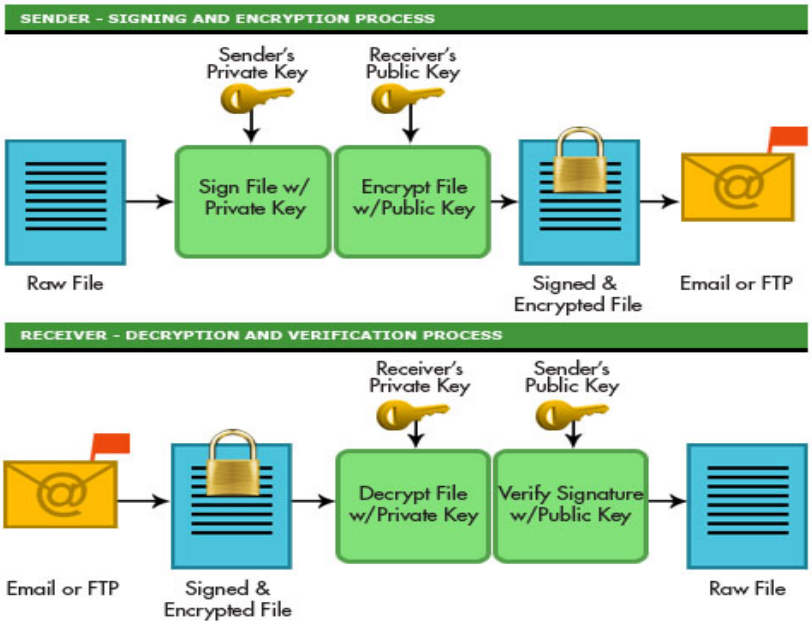

Fig. 3 Explanation of encryption and decryption Emails by using PGP

F. Contractor Employees

Aramco should hire employees from well-known hiring companies in the job market. This hiring company will be responsible for providing qualified contract employees. Aramco should ensure that the hiring company sends employees who fit hiring needs. Additionally, Aramco should require the hiring company to provide a photo of the employees and their full names. When employees arrive to interview, they should provide a photo ID to verify their identities. Aramco should provide a company ID card if the employee is qualified. The contract employee must wear the pass at all times. Aramco should develop a procedure for replacing the contract employee in case of scheduled or emergency absences. Aramco should monitor the contract employees, especially if the contract employees are authorized to work on sensitive systems. Aramco should also investigate employees' backgrounds if their job requires them to work on and access sensitive systems. Aramco should designate noncontract employees to manage contract employees.

V. CONCLUSION

Ultimately, due to the large number of cyber attacks that happen every day, information security is one of the essential corporate priorities. The companies have to keep an eye on their servers and networks continually. They shouldn't ignore the threats because the collapse of the information systems in the company means losing all the company's data, which will disrupt all business processes. Information security experts are continuing to find ways to combat cyber attacks. At the same time, this paper has provided the newest ways that have been innovated, so companies possess high information security, such as RAID, IDS, Log Files, Masking Address, and Pretty Good Privacy. If we cannot combat the cyber attacks that breachers have on our companies, our economy will surely diminish. More research and innovation are needed to maintain the networks and servers while still supporting the information security needs of the companies.

REFERENCES

[1] Aramcooverseas.com. Golf is a Science. [online] Available: http://aramcooverseas.com/en/about-us/about-saudi-aramco, [Accessed 15 January 2022].

[2] B. Christopher and E. Tikk-Ringas, "Survival", *IISS*, 2013. [Online]. Available: http://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-april-may-2013-b2cc/55-2-08-bronk-and-tikk-ringas-e272. [Accessed: 01- Apr- 2013].

[3] "Living in Saudi Arabia", Aramco. [Online]. Available: http://www.aramco.jobs/LivingInSaudiArabia/Communities.aspx. [Accessed: 15- Jan- 2022].

[4] "Denial-of-service attack", Chaininstitute.com, 2013. [Online]. Available: http://chaininstitute.com/?p=1773. [Accessed: 15-Jan-2022].

[5] Z. Fryer-Biggs, "U.S. military goes on cyber offensive", *defense news*, 2012. [Online]. Available: http://www.defensenews.com/article/20120324/DEFREG02/303240001/U-S-Military-Goes-Cyber-Offensive. [Accessed:05- Apr- 2013].

[6] J. Koebler, "U.S. Nukes Face Up to 10 Million Cyber Attacks Daily", us news, 2012. [Online]. Available: http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily. [Accessed: 10- Apr- 2013].

[7] E. Mills, "Saudi Oil firm says 30,000 computers hit by virus", CNET, 2012. [Online]. Available: https://www.cnet.com/tech/ services-and-software/saudi-oil-firm-says-30000-computers-hit-by-virus/. [Accessed: 15- Jan- 2022].

[8] M. Tomaso, "BP fights off up to 50,000 cyber-attacks a day: CEO", *CNBC*, 2013. [Online]. Available: http://www.cnbc.com/id/100529483#. [Accessed: 15- Jan- 2022].

[9] "Photograph of Pretty Good Privacy", *blogspot*. [Online]. Available: http://buyung-belajar.blogspot.com/2012/05/aman-bertukar-data-menggunakan-pgp.html. [Accessed: 15- Jan- 2022].

[10] B. Cosgrove, M. Deacon, B. Brown, A. Lilico, C. Tominey and B. Briggs, "Britain vulnerable from cyber attacks for at least 20 years", The Telegraph, 2013. [Online]. Available: http://www.telegraph.co.uk/news/uknews/law-andorder/9863041/Britain-vulnerable-from-cyber-attacks-for-at-least-20-years.html. [Accessed: 15- Jan- 2022].