ISSN 2278-5612
Volume 11 Number 5
International Journal of Management and Information Technology

Cyber Attack on Saudi Aramco

Sahar Alshathry

King Saud University

ABSTRACT

Saudi Aramco is the largest oil production company in the entire world. It supplies almost almost 1/10th of the oil in the world. The economy of Saudi Arabia is highly dependent on the production of oil.

Aramco got attacked by a virus named Shamoon on 15th August 2012. It was one of the most disrupting cyber-attack that was carried out against the business. Shamoon had spread from the network of the company and it wiped out the hard drives of the computers. The virus infected almost thirty thousand of workstations during the mid of August .

The paper will discus the impact of the cyber attack on the oil production on Saudi Aramco. In addition, the analysis and the mechanisms that the attackers used to launch the virus. This research explains how Saudi Aramco recovered form the cyber attack.

Indexing terms/Keywords

Aramco,cyber attacks, oil production companies.

INTRODUCTION

The Aramco network of Saudi Arabia got attacked by a virus on 15th August 2012, which damaged almost thirty thousand hard drives of desktop and prevented them from carrying out operations. No evidence was found regarding the attempts made by the attackers for stealing significant information. In addition, none of the other network devices have been disrupted, nor the production of the gas and oil has been impacted. Only one of the anonymous groups of hackers has assumed responsibility and has cited certain political explanations (Andrew, 2014).

As a part of the incident response, Aramco disengaged its corporate network from the Internet and shut down one or more of the internet facing servers of the web. Even though this attack might have caused great destruction to Aramco, the attackers were not able to meet their goals of stopping the operations of production.

AIM OF THE ATTACK

Although the attack on Aramco that supplies almost 1/10th of the oil in the world failed to disrupt the production, it was one of the most disrupting cyber-attack that was carried out against the business. The attack was carried out using a computer virus, which is known as Shamoon that infected all the workstations on 15th August, and the organization had to stop all its major internal networks for less than a month (Holden, 2012).

ECONOMIC IMPACT

The economy of Saudi Arabia is highly dependent on the production of oil. According to the US data, the revenues from the exports of oil account for approximately 80 to 90 percent of the total revenues of Saudi Arabia and more than 40 per cent of the GDP (gross domestic product (Rid, 2013).

Shamoon had spread from the network of the company and it wiped out the hard drives of the computers. Aramco was only restricted to the office computers and it did not have any effect on the software of the systems which might had an effect on all the technical operations.

ANALYSIS

The Saudi Aramco has released restricted information regarding this cyber-attack and the virus was used to conduct it. Most of the security firms have been reviewing a new virus that was discovered on the same date and had capabilities equal to the virus of Aramco. This analysis of the security has revealed major details regarding the virus and the attack. (Bronk and Ringas, 2013).

The attackers gained control of a single computer on the internal network of Aramco, and then they used it as a point of a launching, controlling and commanding center for attack. Even though it is not clear that the hackers have gained control of this computer, this usually can be achieved by pushing the internal goals. An insider could have initiated this attack easily. Both of the attack vectors had higher rates of success.

Gaining greater control of almost one global computer, the attacker costumed a crafted virus that is able to spread from an individual control and command computer, by making use of administrative shares, to almost thirty thousand desktops of Aramco. The attacker triggered the virus in order to destroy greater drive content at a specified time on 15th August and the report on number of the files that have been destroyed. The virus did not appear to have an attempt to steal the contents of files. However, its purpose seemed to be to destroy a lot of systems. (Kumar, 2012).

It has been observed by others that the destructive attacks do not occur frequently. The denial of network service has been an alternative tool for groups that are motivated politically. Furthermore, the attacks, which are motivated politically, might make attempts for copycat attacks on the targeted organizations with new goals of an internal system for disruption

and the destruction of data. The organizations perform well in order to take in to consideration this kind of specific potential threat in the planning management for risk.

Attacks of this kind are commonly known as APT (Advanced Persistent Threats), mostly the workstations have searched for password hashes of the administrative accounts and then they have used a method, “pass the hash” in order gain access to greater machines and search for greater administrative power that accounts for the password hashes. The APT attacks have gained greater access to higher levels of domain and the accounts of server administration by this method. It is important to note that if the attackers have used the method of find and pass the hash for the purpose of attacking, then, they would not succeed at gaining greater access to the systems of Aramco. It is also likely that the Saudi Aramco has greater and effective control, which prevents an attack from obtaining greater access (Bronk and Ringas, 2013).

The response for such incident is not easy as most of the incidents that occur now. Most of the organizations just initiate fixing things in quick manner after the incident. Moreover, a significant well tested incident response plan can usually save the cost of restoration and would result in quick recovery.

Recovery from the Attack

The Saudi Aramco is the biggest oil producer in the world and it resumed its operations on major computer networks after the virus infected almost thirty thousand of workstations during the mid of August. Soon after the cyber-attack on the 15th of August, the organization proclaimed that it reduced its electronic systems from the external world in order to prevent upcoming cyber-attacks. (Rid, 2013).

The production and exploration of oil was not effected as they were operated isolatedly. According to Khalid al-Falih, it has been emphasized and assured that the customers, partners and stakeholders are all unaffected and are functioning reliably. Furthermore, the websites of Aramco went offline after the attack and the company remained down. The emails that were sent to employers in the organization continued to bounce back (Andrew, 2014). An organization said that this virus has originated from outside sources and those who are responsible were to continue their attacks. It was not elaborated. The experts of information technology have warned that the cyber-attacks on the energy infrastructure of the country, whether they have been conducted by hostile governments, militant groups or private hackers, could disrupt the supplies of energy.

Target of the global sanctions of the economy by Iran has a major focus on its oil industry and it has disputed the nuclear program. It has observed a hit from several cyber-attacks in the past years. In the year 2012, a virus that targeted the ministry of Iranian oil and the networks of the national oil company, forced Iran to disengage it systems of control for the oil facilities, which included the Kharg Island. The Kharg Island handles most of the crude exports of the country. Iran has certain attributes of attacks to the United States, Britain and Israel. The former and current officials of the United States told the Reuters that during this year the United States built a complex computer worm in order to prevent Tehran from the completion of the nuclear weapons.

THREAT OF CYBER WARFARE IN GULF STATES

The Gulf energy sector has been increasing in a vulnerable manner due to the cyber-attacks. A rise in the propensity and tensions for the rivals has unleashed the cyber strikes against one another and the energy infrastructure compounded the threats to the international markets of energy, both based on the physical disruption in the supply and injecting extra price volatility in the market of oil (Rid, 2013).

Analysis: Impacts

There has been an isolated cyber-attack on the gulf countries since the early 2000s. The initiation of the hostilities have been traced to the unleashed Stuxnet virus that targeted the enrichment facilities of the Iranian Uranium and it was uncovered in the year 2010.

Iran

Iran has been experiencing certain attacks on their computer networks due to the efforts it made to create enriched uranium for stronger global opposition. The most damaging computer attacks that have been against Iran were initiated during the Presidential period of George W Bush’s and under a program that was named by the Olympic Games, where the US probably worked together with Israel in order to create a malware artifact that was sophisticated enough to disrupt the nuclear enrichment of Iran at the Natanz plant.

President Barack Obama has continued the program, which was uncovered after the virus bolted Natanz facility in Internet in the year 2010. After the attack of Stuxnet, certain other viruses of computers have targeted infrastructure of computers in Iran. In the year 2012, W32 Flame virus had an attack on the National Oil Company of Iran and the Oil Ministry of Iran (Holden, 2012). In order to reduce the number of attacks, the officials of Iran disconnects certain of its major oil terminals from Internet to prevent virus from being spread.

Saudi Arabia

The attack of Shamoon virus on Aramco deleted the information from thirty thousand computers in the company and network servers of the company went offline. With the attacks against the oil facilities of Iran, Shamoon did not disrupt the

production, as the major computer systems of production facilities of Aramco are secured. The officials of the United States believed that Iran was joined to the attacks, even though Tehran has denied any complicity. Iran has assumed to get hold of both the capability and motive to carry out the cyber-attacks, but none of the evidence presented provides an indication of the perpetrator.

Evidences have suggested that Saudi Arabia gained an advantage of the reduction in the output of Iran during the summers of the year 2012 in order to increase exports. The investigation carried out by Saudi Arabia has confirmed that the attack was initiated from the Kingdom and it involves multiple countries, but it has reduced the name of the countries while the investigation is still in progress (Bronk and Ringas, 2013).

Even before the attack on Aramco, Saudi Arabia has been highly concerned with possible breaches and has been focusing on doubling the spending on domestic security during the year 2012 from $7.8 billion to $ 15.4 billion. Riyadh has been focusing on protecting its oil sector from the occurrence of cybercrime.

Qatar

Shamoon attacked RasGas, which occurred only after weeks of the Aramco cyber-attack. The RasGas disturbance was negligible when compared to the servers that were affected in Saudi Arabia and it did not had any effect on the production of natural gas. Qatar was quite proactive for defining its posture of cyber security. It developed a governmental organization in 2004 that focuses on deterring the possible attacks as well as detecting, analyzing and monitoring the cyber threats.

OUTLOOK

An increase in the regional tensions because of the conflict of Gaza, the Iran standoff, Syrian war and the Arab uprising have increased the incentives and the motive that carried out the cyber-attacks. The cyber-attacks utilization that disrupted the nuclear program of Iran has invited a buildup of cyber as the countries that are a part of the region have decided to make investments in the cyber warfare capabilities (Kumar, 2012).

The cyber-attacks have been often viewed as a method that is free of cost to inflict the damages on the rivals as they unlikely to request a traditional military response that bares a greater impact attack. Often, the cyber-attacks are not disclosed in order to avoid the embarrassment. Complicated efforts are made in order to understand the coordinated cyber-attacks to provide an effective counter measure. Identifying the identities of cyber-attacks perpetrators is considered to be a problem due to the difficulties in technology. (Bronk and Ringas, 2013).

CONCLUSION

The growth of the cyber-attacks against energy companies of the Gulf countries would destabilize the complete region and affect the energy markets in the world through a decline in the natural gas and oil supply and an increase in the prices. Even if the cyber-attacks were not successful in disrupting the production of energy, they still have an effect on the global prices of energy, mostly of oil. This increases the volatility of price.

Protecting the operations of petroleum in Saudi Arabia from the physical attacks has been for decades the greater priority for Washington and Riyadh. Even a specific disruption of production in the facilities of the area would have a significant impact on the prices and supplies of oil would influence the international economy. Concerns regarding the security of the facilities of Aramco arose after the failed attacks of terrorist on the petroleum-processing complex at Abqaiq in 2006. Even though, Shamoon did not cause a physical damage to the facilities of production of Aramco, it affected the risk assessment of the global infrastructure.

REFERENCES

1. Bronk C. and Ringas E.T., (2013), “Hack or Attack? Shamoon and the Evolution of Cyber Conflict”, James A. Baker III Institute for Public Policy of Rice University. Accessed on March 24, 2014. Retrieved from: http://bakerinstitute.org/files/641/
2. Holden, (2012), “Cyber Attacks in the Spin Cycle: Saudi Aramco and Shamoon”. Accessed on March 27. Available online at: http://analysisintelligence.com/cyber-defense/narrative-of-a-cyber-attack-saudi-aramco-and-shamoon/
3. James Andrew, (2014), “Cybersecurity and Stability in the Gulf”, Center for Strategic and International Studies. Accessed on March 24, 2014. Retrieved from: https://csis.org/files/publication/140106_Lewis_GulfCybersecurity_Web_0.pdf
4. Mohit Kumar, (2012), Aramco Cyber Attack Intends To Stop Oil Production”. Accessed on March 26, 2014. Retrieved from: http://thehackernews.com/2012/12/aramco-cyber-attacks-intends-to-stop.html
5. Thomas Rid, (2013), “Cyber War Will Not Take Place”, Oxford ; New York : Oxford University Press.