Impact of Cyber Attack on Saudi Aramco

Mohammed. I.alghamdi

College of Computer Science and Information Technology, Department of Engineering and Computer Sciences, Al Baha University, Saudi Arabia
Email address: mialmushilah@bu.edu.sa

Abstract

Saudi Aramco is the world's leading oil producer based in Saudi Arabia. Around 1/10th of oil is exported from this organization to the world. Oil production is the major source of revenue for Saudi Arabia and its economy relies completely on it. The Shamoon virus attacked Saudi Aramco in August 2012. The country receives over 80% to 90% of total revenues from the exports of oil and contributes over 40% of the GDP [8]. Shamoon spread from the company's network and removed all of the hard drives. The company was limited only to office workstations and the software was not affected by the virus, due to which all technical operations could have been affected. It was the most disastrous cyber attack in the history of Saudi Arabia. Around 30,000 workstations had been infected by the virus. This paper also discusses the effects of Ransomware which recently attacked Aramco. Apart from that, we will also discuss some suggestions and security measures to prevent those attacks.

Keywords: Saudi Aramco, oil production, cyber attack, cyber threat, Ransomware, Shamoon, workstations, security measures

1.Introduction

1.1. Background

The oil and gas industry across the world has always been criticized for not investing in cyber security. A ransomware attack hit the Colonial Pipeline in the US recently. Saudi Aramco, the leading oil producer in the world, has reported the leak of its company data from one of the contractors. Now, the files are being used for the extortion of $50 million from the company. Aramco had recently noticed in an email statement that the limited amount of data was leaked indirectly by the third-party contractors. Around 1000 GBs or 1TB of data was being kept by the extortionists, as per reports of Associated Press (AP). It was cited on a page available on the dark web, i.e. a part of the web accessible through some special anonymous tools as an encrypted network.

According to the AP report, the hackers demanded $50 million in cryptocurrency to delete the data. Who is the mastermind of this plot is still not revealed. Experts also believe that the oil and gas sector, including companies owning pipelines, oil wells, and refineries, have not invested in cyber security. It is not the first time a cyber attack has happened in Aramco. The computer network of Aramco was also hit by Shamoon virus back in 2012 [1].

A self-replicating virus, Shamoon, attacked Saudi Aramco's computer network on August 15, 2012 and infected up to 30,000 Windows-based computers. Aramco is the national oil and gas firm of Saudi Arabia. It took over 2 weeks

DOI: 10.5281/zenodo.5172091
Received March 22, 2021 Accepted June 27, 2021

to recover data from the damage because of its vast resources. Viruses usually target the networks of MNCs but that level of critical damage is so alarming against a company for the international energy markets. It led to a huge blow to the largest oil producer in the world.

The random deletion of data from the hard drives of the computer was alleged to be the main function of Shamoon. This didn't cause an explosion, oil spill, or any major destruction in operations of Aramco but it adversely affected business operations and there are chances of loss of some production data and drilling [3]. The virus also spread to other oil and gas networks, including the ones of RasGas [4]. The incident happened after years of alarms about the risk of those attacks targeting major infrastructure.

Washington and Riyadh have always been focused on protecting operations of the oil and gas industry in Saudi Arabia from physical damages over a decade. Even a small disruption of manufacturing units in Eastern Province or any such area would affect oil prices and supplies immediately, followed by knock-on impact for the international economy [5]. After a failed terror attack on the petroleum processing unit in February 2006 at Abqaiq, there have been rising concerns over security at the facilities in Aramco. Though there was no physical damage to the production units of Aramco, Shamoon caused damage to risk assessment of important infrastructure across the world. The impact of the incident was so huge that Leon Panetta, the US Secretary of Defense, described it as a "very sophisticated" virus which caused a huge concern. He commented that only a few countries are capable of handling the impact [2].

The virus attacked the Aramco network and damaged over 30,000 hard drives, keeping them from operating. There was no evidence found about the attempts by the attackers for stealing important data. They haven't disrupted other network devices and did not affect the production of oil and gas. An anonymous group of hackers took responsibility, citing some political explanations [6]. The corporate network of Aramco was disconnected from the web and one or more web servers were shut down to deal with the incident. Despite having a great destruction from this attack, the hackers couldn't stop their production. Aramco supplies around 1/10th of the world's oil. The attack could not disrupt the supply line but it was among the most troublesome cyber attacks conducted against its business operations. The attackers used the Shamoon virus which infected almost all the workstations, causing the organization to halt its internal networks for around a month [7].

Saudi Arabia heavily relies on its oil production for its economy. These types of attacks are widely known as "Advanced Persistent Threats (APT)" and they affect the workstations most of the time. The attackers looked for hashes of the passwords of admin accounts and they had "passed the hash" to access greater machines and found greater admin power accounting for hashes of the password. Higher domain levels were accessed by the APT attacks and they accessed the server admin accounts with this method. If they found and passed the hash for hacking, one thing worth noting is that they could not access the Aramco systems. There are also chances that there was effective and better control in the Saudi Aramco, which prevented a more severe level of attack [2].

The Saudi Aramco is the world's leading oil producer and the organization added that it halted the connections of its electronic systems to the outer world to avoid further cyber attacks [8]. The exploration and production of oil was being done separately and they were not affected. The organization assured that the virus cannot affect the partners, customers, and stakeholders and the operations would be functioning well. In addition, Aramco websites were offline and down. Emails sent to the employers were bounced back [6]. This virus came from other sources and attackers would keep doing such attempts. The IT experts had already warned that cyber attacks on the oil and gas industry could disrupt energy supplies, whether they were the attempt of militant groups, hostile governments, or private hackers.

The global sanctions by Iran were the main target of the oil industry and it affected the nuclear program. A lot of cyber attacks affected the organization over the past years. A virus had affected the networks of national oil exporters and the ministry of Iranian oil had led Iran to disconnect its oil control systems for the Kharg Island and other oil facilities. Most of the crude oil was exported from Kharg Island. Iran has some points of attacks on Israel, Britain, and the US. According to the existing and former officials of the US, they have introduced a complex virus to keep Tehran from making nuclear weapons [10].

DOI: 10.5281/zenodo.5172091
Received March 22, 2021 Accepted June 27, 2021

1.2 Literature Reviews [11] presented a case study on Saudi Aramco, the largest oil organization in the world. A severe cyber attack paralyzed the whole operation of the company for several months in 2012. They analyzed the response of the company to that attack along with existing policies to deal with such kinds of attacks. Saudi government, Saudi Aramco's key stakeholder itself, has reacted and responded to this attack. The researchers studied how this response has helped in existing standards for cyber security.

Cyber criminals have primarily targeted the Kingdom of Saudi Arabia (KSA) by causing cyber conflicts due to digital transformation, economic activity, high technology adoption and growth of the oil and gas sector. But there is still a lack of investigation and research on cyber attacks in Saudi Arabia. Due to this reason, [12] conducted a case study on malware attacks on Saudi organizations. They particularly focused on Ransomware and Shamoon and presented the timeline of those attacks, apart from their structures and measures to prevent those attacks.
To be specific, nations have become highly vulnerable which are developed and improving their infrastructure. They rely on their computer networks and technology. [13] briefly discussed and explained some cases of cyber attacks in the United Arab Emirates (UAE), the Kingdom of Saudi Arabia (KSA), and other Muslim countries, the common threats, and possible suggestions for the governments.

1.3 Research Gap

Cyber attacks are not only harmful to business operations, computer networks, productivity and profitability of an organization, but they are also harmful to the economy of the country, especially when the target is a large organization like Saudi Aramco. It has again been targeted by cyber criminals with ransomware, followed by a 2012 attack using a computer virus named "Shamoon." In order to understand modus operandi behind those attacks and find security measures to prevent those attacks, this study fills the gap.

1.4 Research Question

- Why Saudi Arabia is the biggest target of cyber criminals?
- How Shamoon and Ransomware broke into the systems of Saudi Aramco?
- What are the best security practices and recommendations to prevent those attacks?

1.5 Importance of the Study

Being one of the richest countries and major oil exporters in the world, Saudi Arabia has always been on the radar of cyber attackers. It is also observed that the oil and gas industry has not put much emphasis on cyber security. Hence, this study is important to help researchers and policymakers to understand the importance of cyber security and implement some security measures to prevent those attacks in future.

1.6 Research Objectives

- To analyze the increasing cyber attacks on Saudi Arabia
- To understand the structure of most popular virus attacks on Saudi Aramco – Ransomware and Shamoon
- To find out the best practices and solutions to prevent those attacks in future

2. Research Methodology

2.1 Research Method & Design

DOI: 10.5281/zenodo.5172091
Received March 22, 2021 Accepted June 27, 2021

Shamoon was the most popular cyber attack on Saudi Aramco. But there are also other attacks that are worth discussing. The recent Ransomware attack has also cost billions to the companies. Cyber attacks on Saudi Aramco are one of the interesting cases to study because it is the most popular cyber security incident in Saudi Arabia. For this study, we used secondary data from relevant sources.

2.2 Research Approach

We used a comprehensive exploratory study to understand how Ransomware and Shamoon work and the preventive measures to avoid those attacks to answer the research questions. We also attempted to know the narrative of the event as well as the nature of cybersecurity policies adopted by Aramco. We used several text sources that are available to the public for this study, such as posts by authorized sources, news articles by famous media houses, and press releases by Saudi Arabia government and Aramco, along with the newspaper articles and blogs discussing the attack.

3. Data Analysis

With the rise in the number of digital devices, computer and network attacks have been very pervasive in this day and age. Any connected device in this era is at risk of worms, viruses, or malware attacks. These attacks don't spare business users, home users, companies, or the whole nation's security. According to Barack Obama, cyber security is important for the country's economy. So, it is very important to deal with network and cyber attacks as it has been a major concern [15].

A security threat is the common cause of disasters which damage the networks or systems. Several attacks and threats target wireless networks and malware attacks wreck havoc to those networks due to their basic loopholes [16], such as dynamism in topology because of non-reliable communication and mobility issues, and limited energy. A worm, Morris, cost $10 to $100 million by damaging 60,000 connected workstations in 1988. Another worm, Blaster, attacked 400,000 workstations within 5 years. In 2011, Windows 2000, 9x, Vista, Xp, and Windows 7 computers were affected by AntiSpyware. Malware attacks imposed the damages of billions of dollars due to rapid advances and consumer demands for wireless networks.

3.1. Why Saudi Arabia is the biggest target of cyber criminals?

A range of cyber attacks has been reported in Saudi Arabia over the recent years because of rapid changes in political positions and economic conditions. Shamoon, a computer virus which came from Iran, attacked Saudi Arabia, according to the US Secretary of Defense [2]. Hence, it is important to start from the very beginning to know the major cause of cyber attacks on Saudi Arabia. It all started in the Middle East when Stuxnet attacked a nuclear facility in Iran in 2009. Stuxnet attack was a wakeup call as countries across the world realized the vulnerability of their important infrastructure to cyber attacks and their consequences could be disastrous [17].

A malware, Duqu was spying on several targets in Sudan and Iran that could lead to cyber attacks in future in [18]. In 2012, another malware, Flame, attacked the national oil company and oil ministry in Iran, which was designed like Stuxnet. Next one was the most popular, Shamoon which attacked Saudi Aramco, the world's leading oil producer in Saudi Arabia in 2012 and wiped out information from over 30,000 client computers. This malware also attacked the second largest Liquid Natural Gas producer based in Qatar, RasGas. The developer behind those malwares was the same [19].

A group of hackers ``Parastoo" posed a series of attacks in Israel on public domains for the nuclear program in Iran in 2012 and 2013. The users' access to their files and systems was blocked by ransomware attacks in 2015 and demanded users for ransom in exchange of a decryption key. Duqu 2.0 attacked several areas of the Middle East in the same year. Every day, Shamoon 2.0 is making headlines and several new targets have been found in Saudi

DOI: 10.5281/zenodo.5172091
Received March 22, 2021 Accepted June 27, 2021

Arabia [20]. It appears that digital transformation has led to the wide usage of the internet and digitization in Saudi Arabia, making it the top priority for cyber criminals.

3.2. How Shamoon and Ransomware broke into the systems of Saudi Aramco?

Shamoon was designed in a way that developers could remove files on random workstations in Saudi Aramco. The virus infected the computers and corrupted the files. Then, it overwrites the master boot records of the computers and renders them useless. Shamoon had a dropper module (the source and main part of infection), a reporter module (to send data to the hackers), and a wiper module (to delete data on the computers). The virus could activate at the given time, overwrite files, and showcase a distorted picture of an American flag which is set on fire, after being released from one of the company's workstations on the internal network. It is all done before infected computers could unleash the red signal about its activities [21]. It was also found that physical access to the workstations inside Aramco was required to initiate Shamoon on the network, which leaves a question mark on the internal security of the company [22].

Later on, the volatility of the virus was tested by the "US Computer Emergency Readiness Team" and found that disruption of important systems and loss of intellectual property could be the operational impacts of the highly destructive nature of the "Wiper" module of the virus. As per the number and nature of systems infected, actual impact may vary to the organization [23].

According to Seculert, a cyber security organization, Shamoon introduced a two-step process, where hackers first controlled the internal online systems before using them as proxy for the outer "command-and-control" server. Later on, the proxy infected other computers on the same network and let the virus remove all the scraps of other malicious files or lost data from those systems. At the end, the proxy reverted back to the server but this relay was not supposed to work (Seculert, 2008). According to Kaspersky's report, Shamoon had some sloppy errors. One of the experts in the firm Dmitry Tarakanov dismissed the capacity of virus to revert back to its developers. According to him, this module of communication is not effective at all. It is because of an amateurish error made by the creator. Hence, the virus couldn't initiate next programs [25].

Mamba Ransomware attacks the internal network of an organization using PSEXEC tool to initiate the malware in the victim's computer(s) and create a password with thread executor for DiskCryptor tool [26]. Figure 1 features the logical series of events when Mamba Ransomware strikes the network.

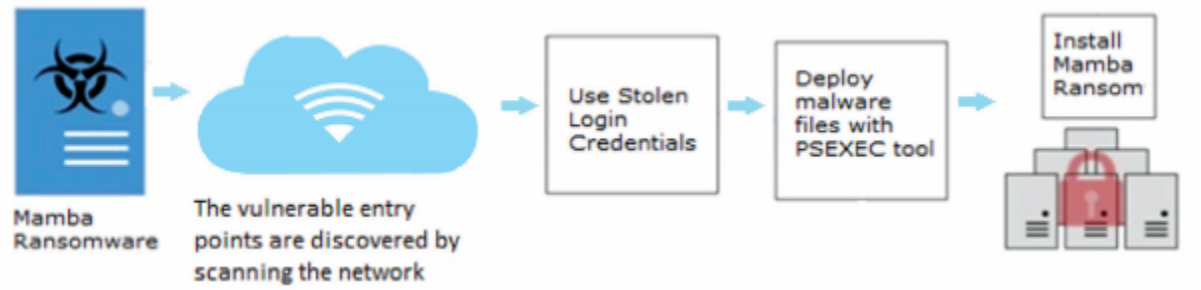

Figure 1 – An Illustration of How Ransomware Attacks (Source: [12])

Command line passes the password to "ransomware dropper". The malware conducts its activities in two different stages [27] & [12].

DOI: 10.5281/zenodo.5172091
Received March 22, 2021 Accepted June 27, 2021

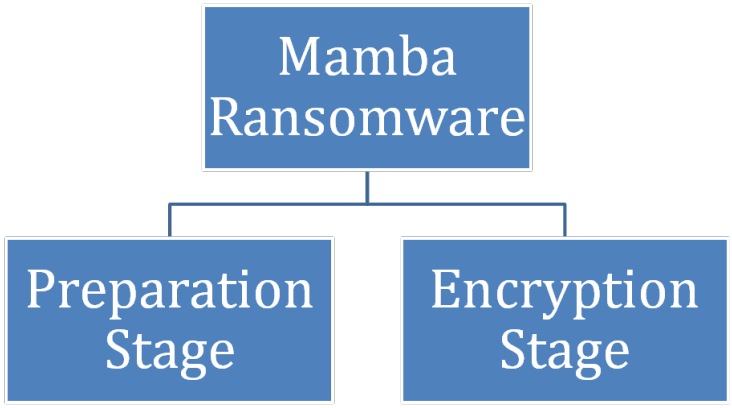

Figure 2 – Components of Mamba Ransomware [12].

Preparation Stage – Ransomware creates a folder in "C:\xampp\http" and drops DiskCryptor elements consequently. It installs this file later on. It registers the "Defragment Service" in the system and reboots the machine.

Encryption Stage - First of all, the attackers load "bootloader" to "Master boot records" or MBR and encrypt the partitions of disk with DiskCryptor. Eventually, they clean up and restart the system.

DiskCryptor – This utility is widely used to encrypt the disk fully. Once the data is encrypted, it leaves no other way to decrypt the data with this utility as strong algorithms are used by this tool. In Preparation, Mamba ransomware simply pastes and installs this utility and executes this tool in the stage of encryption. Later on, the whole hard drive is encrypted rather than single files. This ransomware causes massive destruction to the target, instead of collecting bitcoins [28].

DOI: 10.5281/zenodo.5172091
Received March 22, 2021 Accepted June 27, 2021

4. Results

According to a survey about the Kingdom of Saudi Arabia, over 70% of users store admin passwords in plain text, and over 45% of users use the same password again and again. In addition, over 40% of users share the same passwords and only 13% change the passwords at least once in a month [29].

Best security practices and recommendations to prevent those attacks

Considering the above statistics, here are some of the recommendations and suggestions to improve security -

- In case a threat has been discovered and it has exploited multiple network services, organizations should block and disable access to the immediate effect until they roll out a security patch. The patch should be up-to-date, especially on workstations which provide public services and can be accessed through firewall, including FTP, HTTP, DNS and mail services.
- Firewall should be used widely for preventing all incoming traffic from outer sources to private services. All incoming connections should be blocked by default and only those services are allowed that should be available in public.
- A strict password policy is a must. Administrators should keep hard-to-guess and strong passwords. They should provide the minimum privileges to the users and programs for finishing the assigned task. It is important to ensure that an authorized application is asking for admin-level access, before giving a UAC or root password.
- Email servers should be set to remove or block emails that have attachments which can be malicious. Those types of attachments may have files with extensions like .bat, .exe, .vbs, .scr, and .pif. Compromised computers should be kept separate immediately to keep threats from passing to the next computer. A forensic analysis must be performed to recover the systems.
- Staff must be warned about those suspicious emails and attachments and they should be instructed to open only authorized emails. In addition, they should scan the software for viruses, which is downloaded externally. Only important services for the host or server should be running and all unused ports must be disabled or blocked without proper patches.
- Passwords must be changed every 30 to 60 days and staff must use the combination of two special characters, two lowercase letters, and uppercase letters, making it to minimum 14 characters. In addition, they should strictly avoid dictionary passwords or common passwords like their name, date of birth, etc.
- Administrative access should be given only to those who need the same. Account permissions must be assigned to the minimum level and upgraded when needed. Antivirus must be set to scan and block emails with suspicious attachments from external sources.
- In case there is a breach, a robust IT response team must be ready with all the tools and procedures, such as separation of infected assets from the network for forensics tests and containment.
- Scans and vulnerability checks must be done on a regular basis. It helps detect any vulnerability in systems that is worth considering and that needs patches according to the latest procedures in the IT department.

5. Conclusion

Cybersecurity is the new edge of security in the 21st century. Developed nations are looking to make the most of loopholes of cyber security to have influence and supremacy against their rival countries. Hence, malicious software or malware has been the primary threat to cyber security over the past decade. Several cases of security attacks and breaches have been reported across the world and high level cyber attacks have been reported that affected national security.

Hacking groups have attacked several organizations like Stuxnet, LuzSec, and others with different levels of risks. These anonymous groups emerged over the years and targeted highly reputed and profiled businesses and organizations. Some attacks were conducted easily and exposed the weaker networks to deal with cyber crimes and some breaches cost heavily to the organizations.

DOI: 10.5281/zenodo.5172091
Received March 22, 2021 Accepted June 27, 2021

The increasing use of technology and dependence on the internet has led to digital transformation in the Kingdom of Saudi Arabia. It has also led to the increasing risk of cyber attacks. This study focused primarily on Ransomware and Shamoon attacks on Saudi Aramco, the leading oil exporter in the world. We also found solutions and recommendations for organizations to prevent those attacks from happening again.

References

1. BBC (2021). Hackers reportedly demand $50m from Saudi Aramco over data leak. Retrieved 2 August 2021, from https://www.bbc.com/news/business-57924355
2. Bronk, C., & Tikk-Ringas, E. (2013a). The Cyber Attack on Saudi Aramco. Survival, 55(2), 81–96. doi:10.1080/00396338.2013.784468
3. Roberts, J. (2012). Cyber threats to energy security, as experienced by Saudi Arabia. Platts, November, 27.
4. Tuttle, R. (2012). Virus Shuts RasGas Office Computers, LNG Output Unaffected. Bloomberg.com. Retrieved 2 August 2021, from https://www.bloomberg.com/news/articles/2012-08-30/virus-shuts-rasgas-office-computers-lng-output-unaffected-1-.
5. Shifrinson, J. R. I., & Priebe, M. (2011). A crude threat: The limits of an Iranian missile campaign against Saudi Arabian oil. International Security, 36(1), 167-201.
6. Andrew, J. (2014). Cybersecurity and Stability in the Gulf. Center for Strategic and International Studies. Retrieved from: https://csis.org/files/publication/140106_Lewis_GulfCybersecurity_Web_0.pdf
7. Holden, (2012), "Cyber Attacks in the Spin Cycle: Saudi Aramco and Shamoon". Available online at: http://analysisintelligence.com/cyber-defense/narrative-of-a-cyber-attack-saudi-aramco-andshamoon/.
8. Rid, T. (2013). Cyber war will not take place. Oxford University Press, USA.
9. Bronk, C., & Tikk-Ringas, E. (2013b). Hack or attack? Shamoon and the Evolution of Cyber Conflict.
10. Alshathry, S. (2016). Cyber-attack on saudi aramco. International Journal of Management, 11(5).
11. Dehlawi, Z., & Abokhodair, N. (2013). Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident. In 2013 IEEE International Conference on Intelligence and Security Informatics (pp. 73-75). IEEE.
12. Alelyani, S., & Kumar, H. (2018). Overview of cyberattack on saudi organizations.
13. Basamh, S. S., Qudaih, H., & Ibrahim, J. B. (2014). An overview on cyber security awareness in Muslim countries. International Journal of Information and Communication Technology Research.
14. Basamh, S. S., Qudaih, H., & Ibrahim, J. B. (2014). An overview on cyber security awareness in Muslim countries. International Journal of Information and Communication Technology Research.
15. NY Times (2009). Text: Obama's Remarks on Cyber-Security. Retrieved 3 August 2021, from https://www.nytimes.com/2009/05/29/us/politics/29obama.text.html
16. Adebayo, O. S., Mabayoje, M. A., Mishra, A., & Osho, O. (2012). Malware detection, supportive software agents and its classification schemes.
17. Baezner, M. (2017). Patrice Robin Stuxnet Center for Security Studies (CSS). ETH Zrich.
18. Zetter, K. (2015). Kaspersky Finds New Nation-State Attack-in Its Own Network. The Wired. Available at - https://www.wired.com/2015/06/kaspersky-finds-new-nation-state-attack-network/.
19. Pattar, T. (2013). Cyber Attacks in the Middle East.
20. Moubarak, J., Chamoun, M., & Filiol, E. (2017). Comparative study of recent mea malware phylogeny. In 2017 2nd International Conference on Computer and Communication Systems (ICCCS) (pp. 16-20). IEEE.
21. Perlroth, N. (2012). Connecting the Dots after Cyber attack on Saudi Aramco. New York Times. Available at - http:// bits.blogs.nytimes.com/2012/08/27/ connecting-the-dots-after-cyber attack-on-saudi-aramco/.
22. Digital Dao (2012). Was Iran Responsible for Saudi Aramco's Network Attack?. Available at http://jeffreycarr.blogspot.com/2012/08/was-iran-responsible-for-saudi-aramcos.html.

DOI: 10.5281/zenodo.5172091
Received March 22, 2021 Accepted June 27, 2021

23. Joint Security Awareness Report: JSAR-12-241-01—Shamoon/DistTrack Malware', Industrial Control Systems Cyber Emergency Response Team, 29 August 2012. Available at https://us-cert.cisa.gov/ics/jsar/JSAR-12-241-01B.
24. 'Shamoon, a Two-stage Targeted Attack', Seculert Blog, 16 August 2012, http://blog.seculert.com/2012/08/shamoon-two-stage-targeted-attack.html.
25. Tarakanov, D. (2012). Shamoon The Wiper: Further Details (Part II). Retrieved 4 August 2021, from https://securelist.com/shamoon-the-wiper-further-details-part-ii/57784/
26. Gupta, A. (2016). Samas Changes the Way a Ransomware Operates. TWCN Tech News. Retrieved at - https://news.thewindowsclub.com/samas-ransomware-changes-way-ransomware-operates-82755/.
27. Ivanov, A. & Mamedov, O. (2017). The return of Mamba ransomware. Retrieved 4 August 2021, from https://securelist.com/the-return-of-mamba-ransomware/79403/.
28. Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting the gordian knot: A look under the hood of ransomware attacks. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 3-24). Springer, Cham.
29. Paul, G. & Shaunak (2017). Detailed threat analysis of Shamoon 2.0 Malware - VinRansomware. Retrieved 4 August 2021, from https://www.vinransomware.com/blog/detailed-threat-analysis-of-shamoon-2-0-malware.

DOI: 10.5281/zenodo.5172091
Received March 22, 2021 Accepted June 27, 2021