International Journal of Computer Networks and Communications Security

VOL. 8, NO. 3, March 2020, 26–31
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Cyber-attacks on Saudi Arabia Environment

Rawan Abdulaziz Al-Mulhim[1], Lama Adnan Al-Zamil[2], Fay Mohammed Al-Dossary[3]

[1, 2] Dept. of MIS, College of Business Administration, Imam Abdulrahman Bin Faisal University,
Dammam, Saudi Arabia

[3] Dept. of MIS, College of Business Administration, Imam Abdulrahman Bin Faisal University, Dhahran,
Saudi Arabia

[1]rawanalmulhim@gmail.com, [2]lamaalzamil21@gmail.com, [3]dossary.fai@gmail.com

ABSTRACT

Even though cyber-attacks can't be compared to a nuclear attack but they both pose a serious threat to national and international security. As we witness today cyberwarfare is increasing and Saudi Arabia has become a major target of Cyber-attacks as a result of its economic and digital revolution, high technology adoption and the growth of the gas and oil industry. This paper presents, a case study of the cyber-attacks on the Saudi environment. We focused on two specific malwares Shamoon and Mamba Ransomware. It also explores their methodologies and structure for future defense.

Keywords: *Cyber-attack, malware; middle east, Saudi Arabia, shamoon, shamoon 2.0, Ransomware, Mamba, Diskcryptor.*

1 INTRODUCTION

Kingdom of Saudi Arabia has a great influence on the middleeast because of its political and economic status which makes it vulnerable to cyberattacks. Currently, there is a kind of confidentiality or concealment in the public and private sector since KSA had been prone to cyberattacks multiple times. In specific, two types of malware: Shamoon and Mamba ransomware. [1]
Shamoon malware, as known as disstrack, is destructive data-wiping malware originated to wipe precious data that cannot be recover after being wiped. [2]
Shamoon was generated by Iran, later, it was discovered on the 16th of August 2012, that it was specially created to attack the Saudi Arabian Oil Company. After four years, Shamoon 2.0 another version of it shows up with advanced features to attack KSA at different intervals of time. Its main purpose was to destruct many Saudi companies. [1]
On the other hand, Mamba ransomware is considered a kind of ransomware that attacked KSA and the internal networks and it encrypted the full disk by using legitimate *DiskCryptor* powerful tool. In addition, this tool can use strong encryption algorithms making it impossible to recover the encrypted disks unless there is a decryption key from the ransom author.[3]

2 LITRERATURE REVIEW

From the starting point of the internet, cybercriminals exploit it to launch their attacks on governments and private sectors. Unfortunately, in the most recent years' cybercrimes became easier due to the availability of hacking tools, the availability of the older attack codes, the growing number of black hackers, the existence of vulnerabilities in the systems and so forth. Moreover, cyber-attacks turned out to be more focused on and serious since it moved into organized crimes.

A. Mamba Ransomware

Nowadays cybersecurity specialists define ransomware as any type of malware that infects computers and encrypt their data with highly strong encryption algorithms. Afterward, it demands a ransom from the victim to decrypt the data. the victims are forced to pay the ransom, or else the hacker will corrupt or delete the encrypted files.

Although the private sector and the governments are spending a lot of money to combat this type of cyber threat, they were attacked by one of the major ransomware attacks called Mamba.

Mamba first appeared in 2016 in the United States and it was one of a kind since it encrypts the whole hard drive, not just the files. In July 2017, Saudi Arabia was attacked by Mamba and it targeted the Saudi corporate networks.

Mamba uses a legitimate tool called *Disk-Cryptor* to encrypt the full disk and it can only be decrypted by them.

The attackers obtain access to the company networks through the aiding of ransomware then they encrypt the entire disk and its partitions.

B. Shamoon data-wiping malware

Large oil and gas companies are suffering from highly increasing cyber-attacks and security breaches into their systems and since Saudi Arabia is one of the world’s largest oil and gas providers it was attacked. In August 2012, Shamoon, a data-wiping malware attacked the Saudi Arabian oil company, and it succeeded in wiping around 30,000 computers. Shamoon is attacked because of political conflict between Saudi Arabia and Iran. [3]

It was built to delete and overwrite data in the system and replace it with a corrupted image. It then reports the origin of infested computers back to the system already in the company’s network. It was discovered in 2012 and is a modular virus targeting only 32-bit versions of Microsoft Windows. It was famous due to its very powerful destructive nature of the attack and the cost of recovery related to this was enormous. It spread from one computer to other machine connected through network.

The working of this virus was, once a computer is infected, the virus compiles list of all the files on the system and erase them. Finally, the virus makes the system unusable by overwriting the master boot record of the computer.

The malware was very unique and very powerful. It was used to target the Saudi government by extinguishing the national oil company Saudi Aramco. The attackers cited oppression and the Al-Saud regime as a reason behind the attack. As per a security advisor to Saudi Aramco, it started by sending phishing mail to the employees.

3 METHODE, RESULT AND DISCUSSION

The thing that makes Mamba Ransomware and Shamoon data-wiping malware ideal case to study that is it the only known cyber-security incident threatening Saudi National Security. In this research, we use a variety of publicly accessible sources such as blog posts and newspapers and press releases by Aramco and the government of Saudi Arabia, then we will interpret

A. Shamoon data-wiping malware

The hacker was smart enough to begin an attack on the most valuable company, Saudi Aramco. On this day were more than 55,000 employees have off-day and stayed home to prepare for one of Islam’s holiest nights of the year — Lailat al Qadr “15, August 2012”.[4]

In this day the hacker s Saudi state-owned oil company’s computers, and distribute a computer virus to begin the devastating the data of the computer and he success to erased data on three-quarters of Aramco’s corporate pcs which include necessary documents, spreadsheets, e-mails, files and then replacing all of it with an image of a burning American flag. The purpose of the attack was to cripple the work in Aramco and he success and accomplish the mission. [5]

United States intelligence officials, after what happened, they replay that the real perpetrator was Iran without any supporting evidence due to political conflict between Saudi Arabia and Iran. After all of these, Aramco directly enforces to shut-down the internal network and stop using e-mail and internet access aimed to stop the virus spreading.

The next step that Aramco assigned to researchers at Symantec, a Silicon Valley security company, began analyzing a sample of the virus. Moreover, Aramco asks for a dozen American computer security experts, and they good handle the virus until the expertise arrives.[4]

After investigating they find that the destructive wiper malware is called Shamoon by finding the word embedded in the code. This mechanism it’s called wiper because its wipe out hard drives. [1]

Shamoon was designed to do two things: “replace the data on hard drives with an image of a burning American flag and report the addresses of infected computers.”. [5]

We should mention that security experts analyze the software code and find that the attack involves a company insider that has access to the network and installed the virus by using a USB memory stick that was inserted into a PC.

B. Shamoon 2.0

After the quiescent for four years, a new version of Shamoon shows up with featuring new tools and techniques called *Shamoon 2.0*. *Shamoon 2.0* first attack was discovered in Saudi "first on 17

November 2016, then on 29 November 2016 and finally on 23 January 2017. [1]

Taking caution, the Saudi Arabia telecom authority issues a warning for all organizations to be notified about Shamoon 2. As a result, *Al Ekhbariya TV* shows that 15 government and private organizations had been affected by *Shamoon 2.0. [6]*

The similarity between *Shamoon and Shamoon2.0* is that both of them aim for mass destruction of systems in the targeted organization. Also, it shares many similarities with the 2012 wave with new features.

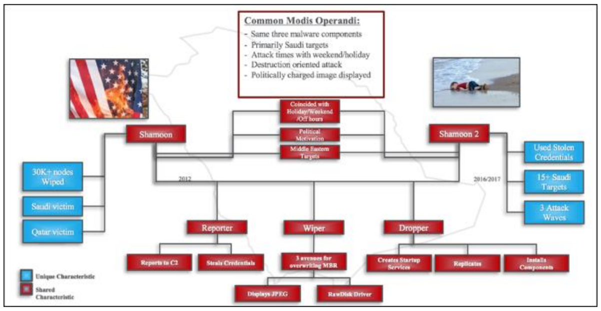


Fig. 1. shamoon and shamon 2.0

The attackers need to obtain administrator credentials for the victim's network as a first stage. Then to spread widely inside the organization its need to build a custom wiper (Shamoon 2.0) that leverages these credentials.

Finally, on an assigned date, the wiper will activate automatically without the need for communication with the command and control center, which makes the victim's machines ***completely inoperable***. [7]

It is worth mentioning that the attacker was smart enough to give the malware the time to spread over the network by assigning the malware to spread on special days such as the last business day or the end of the week or even on the governmental holiday as Lailat al Qadr.

C. Shamoon 1.0 & 2.0 structure

Shamoon is a "destructive malware that corrupts files on a compromised computer and overwrites the MBR (Master Boot Record) to convert the computer to be unusable". [8]

Both, Shamoon and Shamoon 2 had similar structure. Listed below the similarities:[9]

- Both had same internal components and comprised of 3 parts:

1. Dropper: It is the main component of Shamoon and Shamoon 2
2. Wiper: It wipes all the data and is most destructive.
3. Reporter: This reports to the hacker about the infection.

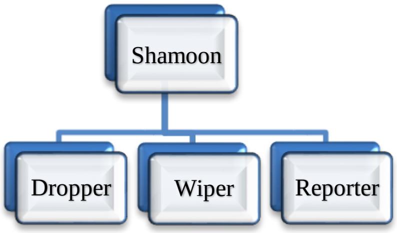


Fig. 2. Shamoon Components

- They both targeted mainly Saudi Organization
  While the Shamoon primarily targeted Saudi Aramco, Shamoon 2 targeted KSA. According to the research, this is done because of political conflict with other countries.

- Attacks using the two were carried out during holiday to get sufficient time for the process.

Shamoon 2 was an improved version of Shamoon, and it uses 90% of the codes from Shamoon. Shamoon was first identified in 2012 whereas, Shamoon 2 was identified in 2016.

There are other differences between the two which are listed in the table below.[1]

Shamoon	*Shamoon 2*
Shamoon has the standard wiping functionality	It included a fully functional ransomware module.
It was released only in 32 bits	It was released in both 32 bit and 64 bits
Shamoon used the picture of burning the American flag	Shamoon 2.0 used the horrific photograph of the body of Alan Kurdi, the three-year-old A Syrian boy who washed up and drowned in Bodrum, Turkey in September 2015

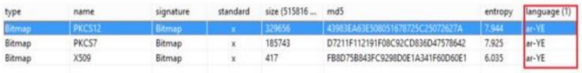
Table 1. Differences between shamoon 1.0 &2.0

A. Techniqual detailes of Shamoon 2.0

In this section, we will describe some technical details and the important details that run the malware. We should mention that, we used the new version which is Shamoon 2.0 hardcoded credentials. During manipulate in the victim's pcs, the main Shamoon 2.0 wiper module is installed through a Windows Batch file with the following content: [7][10]

```
@echo off
set u100=ntertmgr32.exe
set u200=service
set u800=%~dp0
copy /Y "%u800%%u100%"
"%systemroot%\system32\%u100%" start /b
%systemroot%\system32\%u100% %u200%
```

The studies suggesting the attacker might be from Yemen because it appear to have a language ID of "Arabic (Yemen)".



type	name	signature	standard	size (515816 ...	md5	entropy	language (1)
Bitmap	PKCS12	Bitmap	x	329656	43983EA63E508051678725C25072627A	7.944	ar-YE
Bitmap	PKCS7	Bitmap	x	185743	D7211F112191F08C92CD836D47578642	7.925	ar-YE
Bitmap	X509	Bitmap	x	417	FB8D75B843FC9298D0E1A341F60D60E1	6.035	ar-YE

Fig. 3. Language ID

The dropper works as extractor form the *command-and-control communication module* and then wipe components from resources that named *"PKCS7"* and *"PKCS12"*, otherwhile the x86 sample extracts the x64 variant of Disttrack from a resource named "*X509*". [10]

The method of dropper work, first dropper is configured to seek specific offsets within the resource, then read a specified number of bytes after that it is using a specified key its decrypt the contents.

The key exists in the sample as a base64 is an encoded string that the dropper will decode then use each byte of the resulting string to XOR the data obtained from the resource.

The dropper will decode the encoded string which is key exists in the sample as a base64 then use "each byte of the resulting string to XOR the data obtained from the resource". As an additional layer of obfuscation, the dropper will be determining the location of the ciphertext within the resource, after that we will subtracts 14 from the offset value in the sample's configuration.[10]

Table 2: shows the resources within the Disttrack x86 sample, the component it contains, and the values needed to decrypt its contents.

Component	*Resource Name*	*Offset*	*Size*	*Base64 key*
x64 Variant	X509	812-14=798	717312 bytes	5tGLQqku0m02…
Communications	PKCS7	879-14=865	159744	UPi0IzQOAyiL…
Wiper	PKCS12	792-14=778	282112	3Lmqr/nJgzFZ7…

Table 2. resources containing Disstrak components

- 32-bit Shamoon dropper/worm (ntssrvr32.exe)
  The module installs itself as a service named "NtsSrv" and the display name is Microsoft Network Realtime Inspection Service if the malware is running on a 32-bit system.[10]

- 64-bit Shamoon Dropper (ntssrvr64.exe)
  This version is contained within a resource named *"X509"*. Moreover, the dropper has the same functionality as the 32-bit variant. [10]

B. Ransomware structure and execution method

Mamba ransomware *fits into an institute's network and have the privilege to use* PsExec-utility, lightweight telnet (computer-protocol that offers two way cooperative communication compatible for all computers) [12] replacement that lets you perform procedures or activities on other systems and with completely full-interactivity for console applications. [11]

Without having to physically install client-software, in order to implement the ransomware on the targets' network.

This malicious activity in order to be done consists of two fully phases which are they *preparation phase* and *Encryption phase*.

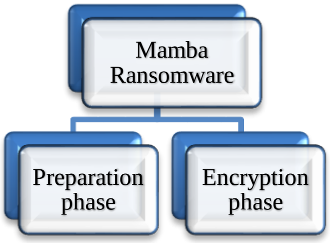


Fig. 4. Mamba Ransomware phases

- **Preparation Phase**

In this phase, the folder is created with special path “C:\xampp\http”, accordingly components of DiskCryptor are dropped. Then, these dropped components are installed. Next, Diskcryptor components will reach out to the system. Eventually, the system will shut-down and start again.

<u>Diskcryptor</u> is consider as a legitimate-utility used for full-disk encryption. Unfortunately, what has been already encrypted by this utility, it is impossible to decrypt because it employs robust encryption algorithms.

- **Encryption Phase**

Firstly, in the encryption phase the bootloader, program that contains or loads the operating system unless the computer is on, to the master boot record (MBR) and encrypt disk divisions by using Diskcryptor software. Therefore, clean up and restart the computer.[13]

Master boot record is a piece of information located at the first division of every hard-disk, and its job is to figure out how and where an operating system is sited, so it is able to be loaded into the computers’ main storage or random-access memory (RAM). [14]

Shortly, ***Mamba ransomware*** drops & installs the DiskCryptor in the preparation phase, and in the encryption phase, DiskCryptor got executed. As a result, it is encrypting the full hard drive rather than single files.

Mamba ransomware is made not only to collect organizations’ data but also to cause harmful disruption and annihilation. And that is why it is considered so dreadful. Besides, when it magnificently encrypts the company’s data, it has been impossible to decrypt it. [1]

4 RECOMMENDATIONS

Since Cybercriminals have a spare number of sophisticated tools as never before, Governments and the private sector need to make these attacks at the minimum and ineffective as possible. Securing the system is like wearing a helmet; you do not realize its importance until you have an accident. The following practices recommended for overcoming future attacks.

They should store a duplicate of their important and valuable data. Since any cyber-attack will become meaningless if they can restore and recover the data after the infection. [15]

Besides, they should always keep their patch levels updated, particularly computers that are accessible through the firewall and host public services as in DNS services, mails, and HTTP.

They should impose strict password policy since complex characters make it harder to crack and is considered to be the front-line defense. Moreover, the Aramco IT department should initiate an alarm system that will alert the IT department once any employee will connect a hard drive to their PCs.

The objective of this system is to ensure the system is sealed up to a certain percentage that protects the system at least from one side. Further, they should provide the users with the lowest level of privilege needed to complete a task and train their employees not to open any email attachment form outsource unless it was expected since they are commonly used to place malware.

Moreover, they should conduct regular scanning of vulnerability on a weekly and daily basis and develop a team to maintain and respond to any incident that may occur with proper tools and procedures. [1]

5 CONCLOUSION

Cyber-Attacks represent a serious threat to Saudi Arabia's environment, and since it is a leader in the energy industry, the cyber-attacks targeting the country have increased evermore and therefore need to be promptly detected. In this paper, we illustrated the details of the most famous malware attacks Shamoon, Shamoon2, and Mamba ransomware. We studied the timeline of when the attacks launched, their methodologies, and structures. In the end, we give some recommendations to prevent these attacks.

6 FUTURE WORK

Nowadays, technology has become a vital part of all sectors since the considerable development of the Saudi Arabia organization, and the most significant project which is NEOM that will be relay on technology. In this paper, we think as a future work that we should obstacle the attacks by making a new version of the attack such as ‘Shamoon’ with the possible new features that may the attacker think about it. We recommend that a government may make a competition for all cybersecurity's, hackers, and everyone who has an interest in this field in the country. In this competition, they will find the vulnerability and weak spot in the codes. In the second step, they will write and develop the same codes in multiple ways and make multiple versions.

In this case, the new version of the Malicious code will be ready with the solution; as a result, the country will be ready for any attack appear at any time.

7 REFERENCES

[1] S. Alelyani and H. Kumar G R, "Overview of Cyberattack on Saudi Organizations", Journal of Information Security and Cybercrimes Research, vol. 1, 2018. Available: https://journals.nauss.edu.sa/index.php/JISCR/article/view/455. [Accessed 8 October 2019].

[2] R. Stewart, "Shamoon Malware: A brief understanding of the data-wiping malware's attacks | Cyware Hacker News", Cyware, 2019. [Online]. Available: https://cyware.com/news/shamoon-malware-a-brief-understanding-of-the-data-wiping-malwares-attacks-78abf35c. [Accessed: 09- Oct- 2019].

[3] C. Bronk and E. Tikk-Ringas, "Hack or Attack? Shamoon and the Evolution of Cyber Conflict", SSRN Electronic Journal, 2013. Available: 10.2139/ssrn.2270860 [Accessed 17 November 2019].

[4] N. Perlroth, "Cyberattack on Saudi Oil Firm Disquiets U.S.", Nytimes.com, 2012. [Online]. Available: https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html. [Accessed: 10- Oct- 2019].

[5] B. Acohido, "Why the Shamoon virus looms as destructive threat", Usatoday.com, 2013. [Online]. Available: https://www.usatoday.com/story/cybertruth/2013/05/16/shamoon-cyber-warfare-hackers-anti-american/2166147/. [Accessed: 10- Oct- 2019].

[6] القناة السعودية الإخبارية, أخبار البلد: فايروس شمعون يعود من جديد. 2017.

[7] kaspersky, "FROM SHAMOON TO STONEDRILL Wipers attacking Saudi organizations and beyond.", Mohamad Amin Hasbini, 2017.

[8] M. Mullen, "What Is Destructive Malware? |", Bluvector.io, 2017. [Online]. Available: https://www.bluvector.io/what-is-destructive-malware/. [Accessed: 12- Oct- 2019].

[9] S. EMPLOYEE, "The Shamoon Attacks", Symantec Official Blog, 2012.

[10] R. Falcone, "Shamoon 2: Return of the Disttrack Wiper", Unit42, 2016. [Online]. Available: https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/. [Accessed: 14- Oct- 2019].

[11] M. Russinovich, "PsExec - Windows Sysinternals", Docs.microsoft.com, 2016. [Online]. Available: https://docs.microsoft.com/en-us/sysinternals/downloads/psexec. [Accessed: 15- Oct- 2019].

[12] P. Gil, "What Exactly Is Telnet? What Does Telnet Do?", Lifewire, 2019. [Online]. Available: https://www.lifewire.com/what-does-telnet-do-2483642. [Accessed: 20- Oct- 2019].

[13] "What is a bootloader", Cs.tau.ac.il, 2017. [Online]. Available: https://www.cs.tau.ac.il/telux/lin-club_files/linux-boot/slide0002.htm. [Accessed: 25- Oct- 2019].

[14] M. Rouse, "What is Master Boot Record (MBR)? - Definition from WhatIs.com", WhatIs.com, 2019. [Online]. Available: https://whatis.techtarget.com/definition/Master-Boot-Record-MBR. [Accessed: 23- Oct- 2019].

[15] M. Ali, "Is Your Company Ready for a Ransomware Attack?", Harvard Business Review, 2016. [Online]. Available: https://hbr.org/2016/10/is-your-company-ready-for-a-ransomware-attack. [Accessed: 02- Nov- 2019].