جامعة نايف العربية للعلوم الأمنية
Naif Arab University for Security Sciences

Naif Arab University for Security Sciences
Journal of Information Security & Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Overview of Cyberattack on Saudi Organizations

Salem Alelyani *, **Harish Kumar G R**
Department of Computer Science, College of Computer Science, King Khalid University, Abha, Saudi Arabia.

Received 16 Mar. 2018; Accepted 04 May. 2018; Available Online 05 Jun. 2018.

CrossMark

Abstract

The beginning of Twenty first century saw a new dimension of security, the cybersecurity. Developed countries have started exploiting the vulnerabilities of cybersecurity to gain supremacy and influence over the rival countries. Hence, over the past decade, malware, i.e., malicious software, has become a major security threat in regards to the cybersecurity. The Kingdom of Saudi Arabia (KSA) has become a major target of cyber conflicts due to increased economic activity, digital transformation, high rate of technology adoption between citizen and organizations and rise of the oil and gas industry. However, unfortunately, there is a lack of research or scientific investigation of cyberattacks on KSA. This fact motivated us in conducting this work. This paper presents, a case study of attacks on Saudi Organization by malwares. We concentrate on two particular malwares: Shamoon and Ransomware. The timeline of attacks by these malware, also presented, along with their structures and methodologies in order to shield ourselves against similar attacks in the future.

I. Introduction

With the increase in number of connected devices to internet, network and computer attacks are becoming pervasive in today's world. Any computer connected to internet is under threat of viruses, worms or attacks from hackers. These threats or attacks can harm home users, business users, corporate users or entire country's security. Barack Obama, the 44th president of US has stated that [1], the economy of the country depends on cyber security. Thus the need to combat with these computer and network attacks has turn out to be a major issue of concern.

A security threat is a potential cause of unwanted event, which may result in damage to systems or networks. Wireless networks are exposed to various threats and attacks. Out of which malware attacks pose serious threats to the wireless networks exploiting the fundamental limitations of wireless network [2], such as limited energy, dynamism in topology due to mobility and unreliable communication.

In 1988, Morris worm caused $10 to $100 million damage on internet with 60,000 connected computers. Within the period of five years, 4,00,000 computers got affected by Blaster worm. Anti-Spyware in 2011, attacked Windows 9x, 2000, XP, Vista, and Windows7. Due to the rapid growth of consumer demands and advancements in wireless technologies, malware attacks in the internet imposing billions of dollars in repair. In Middle east, the cyberattack was initiated by Stuxnet attack in 2009 on Iranian nuclear facility. With Stuxnet attack, the countries all over the world realized that critical infrastructures

Keywords: *Intrusion Detection System; Machine Learning; Deep Learning, Long Short Term Memory (LSTM); Recurrent Neural Network (RNN), Bi-Directional Recurrent Neural Network (BRNN).*

Production and hosting by NAUSS

* Corresponding Author: Salem Alelyani
Email: s.alelyani@kku.edu.sa

doi: 10.26735/16587790.2018.004

were vulnerable to cyberattacks and that the potential consequences could be devastating [3]. Consequently, in 2011, in Iran and Sudan, as reported by Kaspersky [4], Duqu, a malware, intended to collect data from several targets that could then be used in future cyber-attacks. Flame, another malware, attacked, in 2012, the Iranian oil ministry and national oil company that shared the same design with Stuxnet. Shamoon, another malware, in August 2012, attacked the Saudi Arabia's state oil company Aramco, the world's largest oil producer company, and wiped out data from 30,000 clint computers in the company. RasGas, a Qatar-based gas company RasGas, is second largest producer of Liquid Natural Gas in Qatar was hit by similar malware . The similarity between Shamoon and RasGas malware, implies that these malware were developed by the same developer [5].

In September 2012, to support Iran's nuclear program, a group of hacktivists named 'Parastoo' has conducted a series of attacks on public targets in Israel on 2012 and 2013. In the second half of 2015, ransomware attacks blocked access to users' systems and files and forced users to pay a ransom in order to have the decryption key. In the same year, victims of Duqu 2.0 have been found in several places in the middle east region. Nowadays, Shamoon 2.0 malware is making headlines and new targets in Saudi Arabia are discovered each day [6].

After the aforementioned attacks, we still don't find enough resources investigating these attacks from inside to explain what and how it happened and also very less research papers in this topic exist beside the confidentially of the attacks on governmental and private organizations. This motivated us to conduct a study on cyberattacks on Saudi Arabia, in particular, using malware, namely: Shamoon and Ransomware. This paper is a part of funded study regarding cyberattacks, especially ones involving insider threat.

In the remaining of this paper, we present the attacks on Saudi organization by the malware, i.e., Shamoon and Ransomware. Section 2 presents the timelines of the attacks of these malware including the different versions. Section 3 discusses the structure of Shamoon & Shamoon 2 malware. Ransomware structure is discussed in section 4 and finally in section 5, the methodologies to shield ourselves against these malwares are discussed in details.

II. Attacks on KSA

Saudi Arabia has witnessed series of cyberattacks in the past few years, due to its economic and political positions. Saudi Arabia was attacked by Shamoon, which was originated from Iran as described by US Secretary of Defense Leon [7]. Thus, in order to understand the background of the Saudi attacks, we will start by introducing where it was initiated. The attacks on the middle east was initiated by Stuxnet attack in June 2010 on Iranian nuclear facility and it's believed that the USA built Stuxnet with the support of Israel with the goal of stopping or delaying the Iranian nuclear program. The worm was probably implanted by an insider in the Natanz power plant's network with the use of a compromised USB-drive. This technique enabled the worm to penetrate a network that is normally separated from other networks. A newly published document leaked by Edward Snowden, a former CIA employee, indicates that the NSA feared the same thing and that Iran may already be doing exactly the same. The NSA document from April 2013, published by The Intercept, shows the US intelligence community is worried that Iran has learned from attacks like Stuxnet, Flame and Duqu - all of which were created by the same teams - in order to improve its own capabilities [8].

Following, we present the timeline of the attacks of these malware i.e., Shamoon and its other version and Ransomware.

A. Shamoon

It is a very destructive wiper malware. Wiper is the class name of malwares that wipe out hard drives. Usually, wiped data is not recoverable. Shamoon was the most famous wiper so far. As expected, Iran might have learned from the above mentioned attacks and then replicated the techniques of that attack in a subsequent attack, known later as Shamoon, that targeted Saudi Arabia's oil conglomerate, Saudi Aramco. "Iran's destructive cyberattack against Saudi Aramco in August 2012, during which data was destroyed on tens of thousands of computers, was the first such attack NSA has observed from this adversary," the NSA document states. "Iran, having been a victim of a similar cyberattack against its own oil industry in April 2012, has demonstrated a clear ability

to learn from the capabilities and actions of others." This might indicate that Iran has launched the attack against Saudi company. This conclusion is similar to what investigators have concluded.

Although NSA document doesn't credit the US and its allies for launching the attack, Kaspersky researchers [8], found that it shared some circumstantial hallmarks of the Duqu and Stuxnet attacks, suggesting that Wiper might have been created and unleashed on Iran by the US and/or Israel. Many believe it served as inspiration for Shamoon, a subsequent destructive attack that struck computers belonging to Saudi Aramco in August 2012. The document claims Iran was behind Shamoon. The Shamoon malware wiped data from about 30,000 machines before overwriting the Master Boot Record, preventing machines from rebooting. Researchers said at the time that Shamoon was a copycat attack that mimicked Wiper. The document suggests that such attacks don't just invite counterattacks but also school adversaries on new techniques and tools to use in their counterattacks, allowing them to increase the sophistication of these assaults. Iran, the document states, "has demonstrated a clear ability to learn from the capabilities and actions of others." Thus on KSA, the first attack was by Shamoon 15 August 2012 [7], and the target was Saudi Aramco which was chosen due to deep political conflict between Saudi Arabia and Iran.

Saudi Aramco (Saudi Arabian Oil Company) is the state owned company responsible for exploration, production, and refining of these reserves. The market value of this oil giant has been estimated at up to $10 trillion USD in some financial journals, making it the world's most valuable company [9]. Threats against Aramco could potentially jeopardize the national security of Saudi Arabia. Therefore, the Kingdom has invested in securing Aramco facilities with an armed force of 33,000 soldiers and 5,000 guards [10]. Despite its vast resources, Aramco, according to reports, took almost two weeks to recover from the damage. Viruses frequently appear on the networks of multinational firms but it is alarming that an attack of this scale was carried out against a company so critical to global energy markets, thus causing significant disruption to the world's largest oil producer [11].

B. Shamoon 2.0

After Shamoon, one of the most mysterious wipers in history, was dormant for four years [12], another version of it show up with new features called Shamoon 2.0. Shamoon 2.0 attacked the KSA first on 17 November 2016, then on 29 November 2016 and finally on 23 January 2017. Apparently, it prompted Saudi Arabia telecom authority to issue a warning for all organizations to be on the alert for a new variant called Shamoon 2. Saudi state-run Al Ekhbariya TV reported that 15 government entities and private organizations had been hit with Shamoon 2. These targeted organizations was various critical and economic sectors in Saudi Arabia. Just like the previous variant, Shamoon 2.0 wiper aims for the mass destruction of systems inside targeted organizations in KSA. Shamoon 2 shares many similarities with the Shamoon, though featuring new tools and techniques. During Shamoon attack, the attackers obtain administrator credentials for the victim's network (Dormant period from 2012 – 2016) [13]. Next, they build a custom wiper (Shamoon 2.0) which leverages these credentials to spread widely inside the organization. Finally, on a predefined date, the wiper activates, rendering the victim's machines completely inoperable. It is worth mentioning that the attacks take place either in the last business day of the week or either a holiday as Lailat al Qadr, the holiest night of the year for Muslims. This is planned to give the malware the time to spread over the network. Also, it should be noted that the final stages of the attacks have their activity completely automated, without the need for communication with the command and control center. Following is the summarize of some of the characteristics of the new wiper attacks, for Shamoon 2.0 in perspective of Shamoon [12].

- Unlike Shamoon, Shamoon 2.0 includes a fully functional ransomware module, in addition to its common wiping functionality.
- Shamoon 2.0 has both 32-bit and 64-bit components.
- Shamoon 2.0 samples do not implement any command and control (C&C) communication. On contrast, first version of Shamoon included a basic C&C functionality that referenced local servers in the victim's network.

- Shamoon 2.0 embeds Arabic-Yemen resource language sections.
- Shamoon 2.0, used the horrific photograph of the body of Alan Kurdi, the three-year old Syrian boy who washed up and drowned in Bodrum, Turkey in September 2015 [14], whereas, the Shamoon had used the picture of a burning American flag.

The common modus operandi of both Shamoon and Shamoon [14], is as follows:

- Same structural component.
- Primarily Saudi targets.
- The time of attack was on a weekend / holiday.
- Destruction oriented attack.
- Politically motivated attack.

C. Ransomware

Mamba Ransomware attacked the KSA on July 2017, and corporate networks inside Saudi Arabia were targeted. Mamba Ransomware appeared in 2016 in USA and was one of the first viruses that encrypt not files, but whole hard drives. It uses a legitimate tool DiskCryptor for full disk encryption. Adversaries gain access to the network of the attacked company and through the aid of Ransomware and encrypts the entire disk and also encrypts the disk partitions. The Mamba Ransomware can only be decrypted by the hackers [15].

III. Structure of Shamoon and Shamoon 2

Shamoon: W32.Disttrack [16], aka Shamoon is a destructive malware that corrupts files on a compromised computer and overwrites the MBR (Master Boot Record) in an effort to render a computer unusable. W32.Disttrack consists of three components and are listed below and also is illustrated in Fig. 1:

Dropper - the main component and source of the original infection. It drops a number of other modules.

Wiper—this module is responsible for the destructive functionality of the threat.

Reporter—this module is responsible for reporting infection information back to the attacker.

The Detailed Description of each component of the Shamoon can be found at the Appendix A.

Shamoon 2.0, on the other hand, has similar capabilities of that of Shamoon, but far more advanced evasive

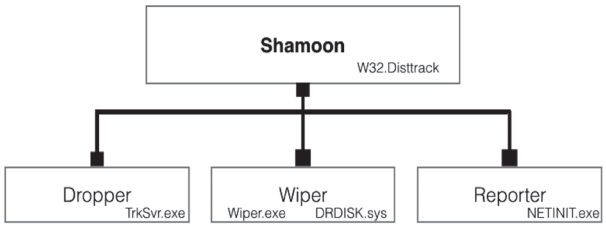

Fig. 1. Shamoon Components.

technologies. The Shamoon 2.0, Just like the previous Shamoon, aims for the mass destruction of systems inside targeted organizations and reuses 90 percent of the code of the Shamoon, but it also comes with "a fully functional ransomware module, in addition to its common wiping functionality [12]", and installs a legitimate-looking driver that changes the infected computer's system date to a random one to "fool the driver's license checks and evaluation period [17]". During the first stage, the attackers obtain administrator credentials for the victim's network. Next, they build a custom wiper (Shamoon 2.0) which leverages these credentials to spread widely inside the organization. Finally, on a predefined date, the wiper activates, rendering the victim's machines completely inoperable. It should be noted that the final stages of the attacks have their activity completely automated, without the need for communication with the command and control center. The Shamoon 2, attempts to spread to other systems on the local network or Active Directory domain of the victim system and overwrites - or wipes - files in hard-coded directories on each system. The malware destroys data and renders the system inoperable, while also attempting worm-like behavior in an attempt to spread the malware to other systems on the network. The samples contain hard-coded domain names, usernames, and passwords, supporting the highly targeted nature of the malware.

IV. Structure on Ransomware

Ransomware: Fig. 2, depicts the logical flow of events for the Mamba Ransomware attack. The malware gains access to an organization's network and uses the psexec utility to execute the ransomware and for each machine in the victim's network, the threat executor generates a password for the DiskCryptor utility [18]. This password is passed via command line arguments to the ransomware

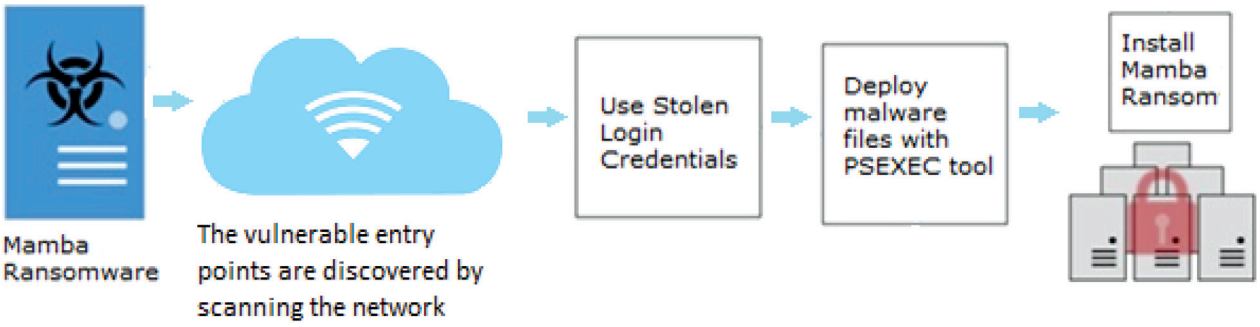

Fig. 2. Logical flow of Events for Mamba Ransomware.

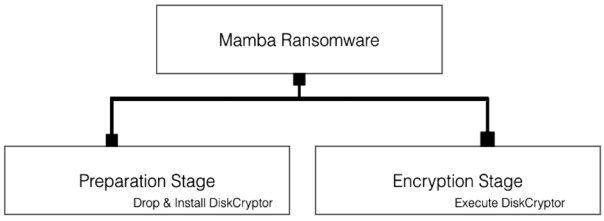

Fig. 3. Mamba Ransomware Components.

dropper. In a nutshell, the malicious activity can be separated into two stages [19] and as shown in the Fig. 3:

1. Preparation Stage.
2. Encryption Stage.

Preparation Stage: In this stage, firstly, a folder in the path "C:\xampp\http" is created, consequently in the new created folder, DiskCryptor components is dropped. Later on the dropped DiskCryptor is Installed. further the system service i.e., Defragment Service is registered and finally the machine is rebooted.

Encryption Stage: In this stage, firstly, Setup bootloader to MBR (Master Boot records) and encrypt disk partitions using DiskCryptor software, consequently Clean up and finally Reboot the machine.

DiskCryptor, is a legitimate utility, used for full disk encryption and Unfortunately, there is no way to decrypt data that has been encrypted using the DiskCryptor utility because this legitimate utility uses strong encryption algorithms. And Mamba ransomware in the preparation stage, drops & install this DiskCryptor, and execute in the encryption stage and thereby encrypting an entire hard drive instead of single files. What makes this kind of ransomware even more alarming is that it isn't made to collect bitcoins [20] from its target but seeks to cause severe destruction. When the Mamba successfully encrypts one's data, there is virtually no way to decrypt the information.

V. Recommended Solutions and Best Practices

A survey about the KSA, reports some of the facts as follows [21]: Administrative passwords are stored in plaintext by > 70% users. The same password has been used over multiple systems, by over 45% of the users. The passwords have been shared by more than 40% of the users. Only 13% users change their passwords once a month.

Based on the above survey statics, following are the recommended solution and best practices [22], [23]. If a discovered threat exploits one or more network services immediately disable and block access to those services until a patch has been applied. Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.

Firewall use should be heavily applied to block all incoming connections from external sources to services that should not be publicly available. By default, you should deny all incoming connections and only allow services you explicitly want publicly accessible. Enforce a strict password policy. Complex passwords make it difficult to crack password files on compromised computers. Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a task. When prompted for a root or UAC password, ensure that the program asking for administration-level access is a legitimate application.

Configure your email server to block or remove emails that contain file attachments which are commonly used to deploy malware. Such attachment types may include but not limited to: .vbs, .bat, .exe, .pif and .scr files. Isolate compromised computers quickly to prevent threats from spreading further. Perform a forensic analysis and restore the computers using trusted media.

Train employees not to open email attachments unless the attachments are expected from an outside source. Moreover, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Ensure that only essential services necessary to server or host functionality are running and that all unnecessary ports are either blocked or disabled until proper patches are applied.

Always maintain firewall capabilities with patch updates for servers that are public facing and accessible via ports 21, 443, 80, and 110. Servers hosting certain services should have only necessary ports open to permit for defined functionality. Shutdown all ports and services within the firewall settings and only open and permit for ports and services within the ingress/egress points which are critical to the functionality of the application or the system. Establish strict password policy adherence to include requirements such as 30-60-day password change, uppercase letters, 2-lowercase letters, 2-special characters, and 14-character minimum. Also, prevention of dictionary passwords is strongly recommended.

Only permit and create administrative access accounts to those that need it. Account permissions should be designated and assigned at the lowest level of need and upgraded on a need-to basis depending on the requirements. Configure anti-virus and SIEMS within a computer infrastructure to monitor and block email attachments from outside sources or unknown parties. Scanning of attachments should occur in the event that execution or deployment of attachment is absolutely necessary.

Develop a strong Incident Response team that has the tools and proper procedures in place that shall be utilized when a compromised asset or event has occurred. This includes segregation of compromised assets from the network infrastructure for containment and forensics purposes.

Regular vulnerability and scanning efforts should be conducted on a weekly or daily basis. This identifies vulnerable systems that need attention or should be patched as per the current policies and procedures set in place by the IT/Operations Department.

VI. Conclusion

The digital transformation in Saudi Arabia has led to a growth in utilization of internet and technology. Therefore, cyberattacks have increased ever since. In this paper, we took an overview of the perspective of cybersecurity in the Kingdom of Saudi Arabia. We studied, in particular, attacks of Shamoon and Ransomware. We studied the timeline of when the attacks by the malware in KSA had taken place, and who were the targets of these attack. In addition, we studied the structure of these malware. Finally, we concluded with recommendations, solutions and best practice that we believe should be applied and followed as a response to the attacks.

Shamoon Component

Dropper Component: The Dropper component performs the following actions:

- Copies itself to %System%\trksvr.exe
- Drops the following files embedded into resources:
  - A 64-bit version of the dropper component: %System%\trksrv.exe (contained in the “X509” resource).
  - Reporter component: %System%\netinit.exe (contained in the "PKCS7" resource).
  - Wiper component: %System%\[NAME SELECTED FROM LIST].exe (contained in the "PKCS12" resource).
- Copies itself to the following network shares:
  - ADMIN$.
  - C$\\WINDOWS.
  - D$\\WINDOWS.
  - E$\\WINDOWS.
- Creates a task to execute itself
- Creates the following service to start itself whenever Windows starts:
  - Service name: TrkSvr.
  - Display name: Distributed Link Tracking Server.
  - Image path: %System%\trksvr.exe.
  - Wiper Component: The Wiper component includes the following functionality:

- Deletes an existing driver from the following location and overwrites it with another legitimate driver:
  - %System%\drivers\drdisk.sys.
  - The device driver is a clean disk driver that enables user-mode applications to read and write to disk sectors. The driver is used to overwrite the computer's MBR but may be used for legitimate purposes.
  - The file is digitally signed.
- Executes the following commands that collect file names, which will be overwritten and writes them to f1.inf and f2.inf
- Files from the f1.inf and f2.inf will be overwritten with the JPEG image. Overwritten files are thus rendered useless.
- Finally, the component will overwrite the MBR so that the compromised computer can no longer start

Reporter Component: The Reporter component is responsible for sending infection information back to the attacker. The following data is sent to the attacker:

- [DOMAIN]—a domain name.
- [MYDATA]—a number that specifies how many files were overwritten.
- [UID]—the IP address of the compromised computer.
- [STATE]—a random number.

Acknowledgment

The authors would like to thank King Khalid University for funding this research via Institute of Research and Consulting Studies

References

[1] Text: Obama's Remarks on Cybersecurity, May 29, 2009. [Online]. Available: https://www.nytimes.com/2009/05/29/us/politics/29obama.text.html (accessed Sept. 16. 2017).

[2] O. Adebayo, M. A. Mabayoje, A. Mishhra and O. Oluwafemi, "Malware Detection, Supportive Software Agents and Its Classification Schemes," *Int. J. Netw. Secur. & its Appl. (IJNSA)*, vol. 4, no. 6, pp. 33-49, Nov. 2012, doi: 10.5121/ijnsa.2012.4603.

[3] M. Baezner, P. Robin, "Hotspot Analysis: Stuxnet," Cent. Secur. Stud. (CSS), ETH Zürich , Switzerland, Oct. 2017. [Online]. Available: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf

[4] K. Zetter. "Kaspersky Finds New Nation-State Attack - in Its Own Network." June 10, 2015. [Online]. Available: https://www.wired.com/2015/06/kaspersky-finds-new-nation-state-attack-network/ (accessed Apr. 2, 2018).

[5] T. Pattar. "Cyber Attacks in The Middle East." July 29, 2013. [Online]. Available: http://thesigers.com/analysis/2013/7/29/cyber-attacks-in-the-middle-east.html (accessed Dec. 31, 2017).

[6] J. Moubarak, M. Chamoun and E. Filiol, "Comparative study of recent MEA malware phylogeny," in *2017 2nd Int. Conf. Comput. and Commun. Syst. (ICCCS)*, Krakow, pp. 16-20. doi: 10.1109/CCOMS.2017.8075178.

[7] C. Bronk and E. Tikk-Ringas, "The Cyber Attack on Saudi Aramco," *Survival*, vol. 55, no. 2, pp. 81-96, Apr. 2013, doi: 10.1080/00396338.2013.784468.

[8] K. Zetter. "The NSA Acknowledges What We All Feared: Iran Learns From US Cyberattacks." Fab. 10, 2015. [Online]. Available: https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/ (accessed Dec. 31, 2017).

[9] C. Helman. "The World's Biggest Oil Companies." Mar. 19, 2015. [Online]. Available: https://www.forbes.com/sites/christopherhelman/2015/03/19/the-worlds-biggest-oil-and-gas-companies/ (accessed Dec. 31, 2017).

[10] H. Cordesman, *Saudi Arabia: national security in a troubled region*, Washington, D.C., USA: ABC-CLIO, 2009.

[11] B. Acohido, "Why the Shamoon virus looms as destructive threat." May 16, 2013. [Online]. Available: https://www.usatoday.com/story/cybertruth/2013/05/16/shamoon-cyber-warfare-hackers-anti-american/2166147/ (accessed Feb. 6, 2018).

[12] C. Raiu, M. Hasbini, S. Belov and S. Mineev. "From Shamoon to StoneDrill." Mar. 06, 2017. [Online]. Available: https://securelist.com/from-shamoon-to-stonedrill/77725/ (accessed Sept. 14, 2017).

[13] Kaspersky Team. "Double trouble: A pair of wipers in Saudi Arabia." Mar. 06, 2017. [Online]. Available: https://www.kaspersky.com/blog/shamoon-stonedrill/15170/ (accessed Jan. 6, 2018).

[14] P. Darren. "Shamoon malware returns to again wipe Saudi-owned computers." Dec. 02, 2016. [Online]. Available: https://www.theregister.com/2016/12/02/accused_iranian_disk_wiper_returns_to_destroy_saudi_orgs_agencies/ (accessed Jan. 20, 2018).

[15] A. Ivanov and O. Mamedov. "The return of Mamba ransomware." Aug. 09, 2017. [Online]. Available: https://securelist.com/the-return-of-mamba-ransomware/79403/ (accessed Sept. 13, 2017).

[16] A. Johnson. "The Shamoon Attacks." Aug. 16, 2012. [Online]. Available: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=281521ea-2d18-4bf9-9e88-8b1d-

c41cfdb6&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments (accessed Sept. 14, 2017).

[17] M. Mullen. "What Is Destructive Malware?" July 31, 2017. [Online]. Available: https://www.bluvector.io/what-is-destructive-malware/ (accessed Sept. 16, 2017).

[18] A. Gupta. "Samas changes the way a Ransomware operates." March 19, 2016. [Online]. Available: https://news.thewindowsclub.com/samas-ransomware-changes-way-ransomware-operates-82755/ (accessed Jan. 10, 2018).

[19] A. Ivanov and O. Mamedov. "The return of Mamba ransomware." Aug. 09, 2017. [Online]. Available: https://securelist.com/the-return-of-mamba-ransomware/79403/ (accessed Jan. 10, 2018).

[20] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge and E. Kirda, "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks," in *Detection of Intrusions and Malware, and Vulnerability Assessment*, M. Almgren, V. Gulisano and F. Maggi, Ed, Cham, CH: Springer, 2015, pp. 3-24.

[21] G. Paul and Shaunak. "Detailed threat analysis of Shamoon 2.0 Malware." Feb. 05, 2017. [Online]. Available: http://www.vinransomware.com/blog/detailed-threat-analysis-of-shamoon-2-0-malware (accessed Sept. 14, 2017).

[22] C. Mercer. "StoneDrill – Shamoon & Shamoon 2.0 Variant." Mar. 13, 2017. [Online]. Available: https://nsfocusglobal.com/stonedrill-shammon-shammon-2-0-variant/ (accessed Sept. 16, 2017).

[23] S. Gates and C. Mercer. "Shamoon2: Back on the Prowl." Feb. 8, 2017. [Online]. Available: https://nsfocusglobal.com/shamoon-2-back-on-the-prowl/