Aramco Cyber Attack

1. Introduce yourself and the purpose of the presentation.
   1. Introduction
      1. Hi, my name is Marco, I am a student at ECU, and this is assessment 3 for IoT OT. In today presentation I am going to analysing the cyber-attack that victimised one of the biggest oil companies in the world. Aramco is a Saudi-Arabian company that in 2012 experienced massive cyber-attack. In fact, as reported from the CNN the company IT system was partially wiped off or destroyed by a virus known by the name of Shamoon which was unknow until that day. This presentation is to outline the facts that have accrued exposing the oil industry giant to a serious risk of collapsing.
2. Provide a high-level overview of the attack using a graphical illustration. The graphic could be as simple as a block-diagram or improved using icons and symbols. You must reproduce it from an existing source.
   1. Find the existing source of a block diagram that overview the Aramco cyber attack
   2. The sh
      1. phishing email attack that an unnamed Saudi Aramco Information Technology employe
      2. e opened, giving the group entry into the company's network around mid-2012
      3. In this step, we penetrated a system of Aramco company by using the hacked systems in several countries and then sent a malicious virus to destroy thirty thousand computers networked in this company. The destruction operations began on Wednesday, Aug 15, 2012 at 11:08 AM (Local time in Saudi Arabia) and will be completed within a few hours.[[21]](https://en.wikipedia.org/wiki/Shamoon#cite_note-22)
      4. normal business was resumed on 25 August 2012.\*//
3. Provide a timeline of tTimeline

   Description automatically generatedhe attack.
   1. Time-line to be applied (find an existing timeline)

day

Reference:

<https://malwiki.org/index.php?title=Shamoon>

<https://www.cleverfiles.com/help/shamoon-malware-analysis.html>

https://www.enisa.europa.eu/publications/info-notes/shamoon-campaigns-with-disttrack

**Slide 1 Introduction**

HI in today presentation I am going to talk about 2021 Saudi Aramco cyber attack

My name is Marco, and this is assessment 2 IoT and OT security

**Slide 2 outline**

This presentation outlines:

* Attack Overview
* Timeline
* Consequences
* How the target was infected?
* Vulnerabilities
* How the OT Systems Affected?
* People and Process

And finally, my own recommendation

**Slide 3 overview**

In 2012 the worst cyber-attack ever seen victimised one of the largest oil enterprises in the world erasing something like 35,000 computers. The massive attack on Saudi Aramco put at risk the ability to supply 10% of the global demand for oil. the first sign of the malware activities was noticed in the morning on **Wednesday** **15 August 2012 During the Ramadan,** when some monitors started flickering, files began to vanish and computers shutdown without a reason. After the attack some desktop displayed an image of a burning U.S flag and a group called “The Cutting Sword of Justice” claim the responsibility for the attack.

**Slide 4 Timeline**

All started early 2012 when the phishing attack was targeted then approximately in July 2012 attackers were able to use a compromised computer as proxy. After that, in August 2012 the first sign of the attack were notices and soon later on August 15th more then 35K Windows based Saudi Aramco PCs being shutting down and being wiped. The same date Saudi Aramco disconnected from the internet.

**Slide 5 consequences**

As a consequence, the company ability to operate was compromise. Saudi Aramco is considered a critical infrastructure as they supply oil and gas for the 10% of the global demand. Even though, the company didn’t stop the global distribution during the attack, the internal demand for oil in Saudi Arabia wasn’t full filled for 17 days. However, the attack damaged more than 35.000 computers causing the company a financial effort to replace all machines. Also, many assets were lost such as :

* customer records and personal information
* email records
* financial records
* marketing plans
* intellectual property

**Slide 6 how the virus infected the target?**

Initially the hackers sent a malicious link via email which was open by a Aramco’s technician. with the fishing attack the attackers were able to obtain right credentials to exploit the system, after that they injected the virus that erased more than three quoter of the files within the system. To be more precise, the malicious link contained a Microsoft office file which trigged a bash shell script that enabled the remote connection between the hackers and the computer interface, after that they started to injecting malwares to escalate privileges on the network.

Once they gained the privileges, a network analysis was conducted to locate the critical systems. After that, the attackers detonated the malware.

The system was infected by a virus called Shamoon. The Shamoon is composed by three different components :

* The Dropper —which was used to create a persistent service on the infected computer .It was made in 32 and 64-bit versions as could attack the system based on the architecture it discovered. Moreover, it copied itself to other computers to spread its malicious code.
* The Wiper —, which was used to overwrite the hard disk’s master boot record (MBR) with an image embedded in the malware. The component enabled user-mode access to the hard disk without using the Window APIs. After the MBR was overwritten, the system was unusable.
* The Reporter as final component established a communication with a command and control server. The attackers control this server and used it to download additional code, change the pre-configured disk-wiping time, and send reports to verify that a particular disk has been destroyed.

**slide 7 Vulnerabilities**

1.2.3 - OT system runs on legacy software that lack of sufficient user and system authentication, data authenticity, or integrity checking futures, which allowed the attackers uncontrolled access to the organization system

4 - systems with default or simple passwords and standard configurations

5 – lack of encryption as the attackers were able to discover username and password

6 – lack of remote access policies which gives the hackers the back door access to the OT network

7 – lack of policies and procedures to approach cyber security

**Slide 8 how were the OT system affected**

The attackers took an advantage of the vulnerabilities and exploited the OT system where they were able to install a persistent bash shell program to gain remote access to the company network, use malware to discover username and password and lunch the wiping attack that destroyed ¾ of the total files. After that the system was unusable.

**Slide 9 People and process**

In the 2012 Aramco cyber attack people process and technologies involved

People- The Aramco technician, which opened the malware.

And process in following order: the phishing attack, Installation of persistent bush shell program, Deployment of software to escalate credential, Network analysis, Deployment of Shamoon virus, Lunch of the wiping attack.

The technologies used were email, Microsoft office, windows, bush shell program, corporate LAN and VPN.

**Slide 10 Recommendation**

My recommendation for the future is to:

* Provide employees with appropriate cyber security training
* Reinforce firewalls on the system
* Perform regular monitoring of network activities
* Setting Remote access restrictions
* Back-up data systems regularly
* Enlarge the cyber security team

Slide 11 References

https://repository.nauss.edu.sa/bitstream/handle/123456789/65730/455-1419-1-PB.pdf?sequence=1&isAllowed=y

**The vulnerabilities exploited on the system were the email in which the attack began, the remote access which was not detected**

What caused the attack? Discuss about vulnerabilities

The system was exploited using a technique called fishing. In the first stage the attackers sent a link via email which was opened by a corporation’s technician. The link enabled the hackers to obtain system credentials that were used to gain remote access to a Saudi Aramco’s computer which was then used as a proxy to infect the entire system with the virus. However. In my opinion the luck of training and the vulnerabilities of the OT system exposed the company to the threat, and all could have been prevented embracing the right measurements.

Slide 6 Recommendation