2012 Saudi Aramco Cyberattack - Post Incident Analysis

Incident Summary

Saudi Aramco is one of the largest oil companies in the world and at the time of the attack in 2012, this was one of the largest cyberattacks in history. The malware used is named “Shamoon”, and the type of attack that occurred is classified as a wiper attack that affected around 35,000 computers and devices. A wiper attack deletes all files and data from the affected device resulting in a total loss.

The vector of attack was through an email phishing campaign that a Saudi Aramco employee unwittingly clicked on allowing the hackers to penetrate the network. From the information available, the hackers waited until the holy month of Ramadan to perpetrate the attack which may have given them a strategic advantage due to a reduced number of employees on site.

The group originally attributed to the incident was a group called the “Cutting Sword of Justice” and it claimed to be politically motivated. Later on, it was discovered that nation state threat actors from Iran, APT 33, were likely the real hackers.

The actual damages are not publicly known; however, Saudi Aramco had to revert to fax machines and typewriters to continue business operations in the wake of the attack. They chose to rebuild their computer infrastructure by replacing hard drives, which resulted in a supply chain shortage of hard drives for a period of time due to the large number required. It took five months for the company to go online again.

Recommended Organization Changes

Recommendation 1: Ensure Adequate Staffing Year-Round

Background
The cyber-attack occurred during the Islamic holy month of Ramadan, which is very important to many people who work in this organization. Staffing was lower than normal during the attack, which may have factored into the attack time frame. Backups were not completed for critical drilling data on the day of the attack, which points to a issue in ensuring coverage of critical processes when staff is out of the office.

Recommendation
Inventory processes to determine business risk and plan for employee back-ups or automation where feasible to ensure critical processes continue to run independent of

employee time off.

Recommendation 2: Establish/Reinforce Security Culture

Background
A spear-phishing email was clicked by an Information Technology employee.

Recommendation
Implement a mandatory training process for employees on a periodic basis to ensure each person understands the risk of phishing and other cyber attacks. Supplement employee training with security tools to scan clicked links for malicious websites and payloads.

Recommendation 3: Enhance Security Strategy

Background
Industrial control systems for oil drilling rigs / oil production are separate and have a heavier physical and cybersecurity focus. The Shamoon attack was not able to disable the industrial systems; however, over 30,000 business operations computers were affected. The entire operation is classified as critical infrastructure for not only the nation, but for the global economy and must remain functioning.

Recommendation

Due to the nature of the wiper attack and the amount of infrastructure affected, more focus is needed to secure business operations as oil producers are part of a nation's critical infrastructure. Since it is possible for an infected computer at the business operations level to either (1) infect supply chain companies and (2) be hooked into industrial systems allowing infection with malware if another attack occurs, it is recommended that Saudi Aramco invest in additional cybersecurity infrastructure on the business operations level. Revisit the cybersecurity strategy periodically to ensure history (incident response data, data on other breaches) and emerging threats are considered and policies updated as needed.

Prevention Action Recommendations

1 High Availability, Disaster Recovery, and Physical Protection

Capabilities:

- Data Mirroring/Replication
- Off-site Storage

Rationale:

To prevent the need to revert to paper and fax machine in the event of a wiper attack such as this, replication of data at a secondary site for critical business functions may allow the company to continue services with minimal disruption.

To protect critical data and historical records, ensure there is off-site storage that is not connected to the same network – this will prevent complete loss of data even if the physical infrastructure is damaged.

2 Identity, Authentication, and Access Management

Capabilities:

- Multi-factor authentication

Rationale:

Multi-factor authentication provides an additional layer of verification before allowing a person access to systems. In this case where an IT employee was phished, multi-factor authentication could have prevented the attacker from accessing systems with those credentials. This reduces the potential for successful phishing campaigns in the future.

3 Endpoint, Network, and Device Security

Capabilities:

- Local Administrator Privilege Restrictions
- File Integrity/Change Monitoring

Rationale:

Limiting Local Administrator privileges helps reduce the possibility of malware installation. This type of restriction also protects credentials from being compromised.

File integrity and change monitoring could prevent the proliferation of the malware within the enterprise. In this attack, the malware copied files from one computer to the next. Monitoring will aid in early detection to limit or prevent damages.

Potential Challenges/Roadblocks

- Employee training is only effective if the employee understands the risk and knows what to look for. Even with training, a phishing attack could once again be successful as it only takes one person to click the link or download the attachment.
- Local religious customs may still impact the number of employees available regardless of attempts to moderate time off; outside contractors or other resources must be considered to ensure adequate coverage namely in the IT space.

Conclusion

As one of the larger attacks in history with one of the most debilitating and destructive outcomes, this is a lesson to all to focus on prevention and remediation. While this type of attack is not common, the use of wipers by nation states has appeared to increase over time and it is typically against their purported enemies' infrastructure. The Saudi Aramco incident shows that it can happen and there are nation state threat actors out there who have no issue destroying data for zero monetary benefit.

References

Christopher Bronk & Eneken Tikk-Ringas (2013): The Cyber Attack on Saudi Aramco, Survival: Global Politics and Strategy, 55:2, 81-96

Pagliery, J. (2015, August 5). The inside story of the biggest hack in history. CNN. https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html

Rashid, F. (2015, August 8). Inside The Aftermath Of The Saudi Aramco Breach. Dark Reading. https://www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-aramco-breach