Lab - Cybersecurity Case Studies

Objectives

Research and analyze cyber security incidents.

Part 1: Conduct search of high profile cyberattacks.

Part 2: Write an analysis of a cyberattack.

Background / Scenario

Governments, businesses, and individual users are increasingly the targets of cyberattacks and experts predict that these attacks are likely to increase in the future. Cybersecurity education is a top international priority as high-profile cyber-security related incidents raise the fear that attacks could threaten the global economy. The Center for Strategic and International Studies estimates that the cost of cybercrime to the global economy is more than $600 billion annually. In this lab, you will study four high profile cyberattacks and be prepared to discuss the who, what, why and how of each attack.

Required Resources

- PC or mobile device with internet access

Instructions

Part 1: Conduct search of high profile cyberattacks.

a. Using your favorite search engine conduct a search for each of the cyberattacks listed below. Your search will likely turn up multiple results ranging from news articles to technical articles.

   - The Stuxnet Virus
   - Marriott data breach
   - United Nations data breach
   - Microsoft customer support database breach
   - Lifelabs data breach

   Note: You can use the web browser in virtual machine installed in a previous lab to research the hack. By using the virtual machine, you may prevent malware from being installed on your computer.

b. Read the articles found from your search in Step 1a and be prepared to discuss and share your research on the who, what, when, where, and why of each attack.

Part 2: Write an analysis of a cyberattack.

Select one of the high-profile cyberattacks from Step 1a and write an analysis of the attack that includes answers to the questions below.

a. Who were the victims of the attacks?

   The Stuxnet attack was aimed primarily at Iran's nuclear facilities, with a particular focus on the Natanz uranium enrichment plant. The virus was carefully programmed to infiltrate and disrupt the automated systems that controlled their industrial processes, causing significant interference with their operations.

b. What technologies and tools were used in the attack?

The Stuxnet worm was a highly sophisticated piece of malware that exploited several previously unknown security flaws, known as zero-day vulnerabilities. One of the key systems it managed to infiltrate was the Siemens SCADA system, which is widely used around the world for controlling and monitoring industrial processes

- Zero-Day Vulnerabilities: Stuxnet exploited multiple zero-day vulnerabilities, which are security flaws in software that were unknown to the developers and had no existing patches.
- Rootkits: The worm used rootkits to hide its presence on infected systems, making it difficult to detect and remove.
- Siemens SCADA System Exploitation: Stuxnet specifically targeted Siemens Supervisory Control and Data Acquisition (SCADA) systems, which are used to control and monitor industrial processes.
- Advanced Encryption: To protect its code and communication, Stuxnet used sophisticated encryption methods, making it harder for security experts to analyze and understand its workings.

c. When did the attack happen within the network?

The Stuxnet attack is believed to have started as early as 2005, but the virus wasn't discovered until 2010. While the exact timeline of its infiltration into the network remains unclear, it's likely that the malware had been operating undetected for several years, quietly carrying out its mission before finally being exposed. The stealthy nature of the attack allowed it to stay hidden and cause damage over a prolonged period without raising suspicion.

d. What systems were targeted?

Stuxnet was a specialized worm created to target Siemens SCADA systems, specifically those running Siemens Step7 software on Windows-operated machines. These systems were responsible for controlling centrifuges used in the process of uranium enrichment. The worm's design allowed it to infiltrate and manipulate the operations of these centrifuges, causing them to malfunction while remaining undetected. Its precision and focus on this particular industrial setup made it a powerful tool in disrupting the targeted nuclear facilities

e. What was the motivation of the attackers in this case? What did they hope to achieve?

The motivation behind creating Stuxnet may have been to cause physical damage to the centrifuges used in uranium enrichment, thereby crippling the country's ability to produce atomic weapons. By targeting and disrupting these critical components, the worm aimed to render the entire process of making nuclear weapons ineffective.

f. What was the outcome of the attack? (stolen data, ransom, system damage, etc.)

Stuxnet caused significant physical damage at the Natanz facility, reportedly putting around 1,000 centrifuges out of operation. This demonstrated that a cyber weapon could indeed cause real-world destruction, leading to heightened awareness and concern over cybersecurity issues. The incident highlighted the potential for digital attacks to have devastating physical consequences, making the need for robust cybersecurity measures more urgent than ever.