Lab - Cybersecurity Case Studies

Objectives
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**

Stuxnet was a multi-part worm that traveled on USB sticks and spread through Microsoft Windows computers. The virus searched each infected PC for signs of Siemens Step 7 software, which industrial computers serving as PLCs use for automating and monitoring electro-mechanical equipment. After finding a PLC computer, the malware attack updated its code over the internet and began sending damage-inducing instructions to the electro-mechanical equipment the PC controlled. At the same time, the virus sent false feedback to the main controller. Anyone monitoring the equipment would have had no indication of a problem until the equipment began to self-destruct

- **Marriott data breach**

In late 2018, the Marriott hotel chain announced that one of its reservation systems had been compromised, with hundreds of millions of customer records, including credit card and passport numbers, being exfiltrated by the attackers

- **United Nations data breach**

The shocking news emerged that hackers breached the computer networks of the United Nations, it sent shockwaves across the globe. The spokesperson for the U.N Secretary-Generation, Stéphane Dujarric, has confirmed the data breach story on September 9, 2021. The UN hack began with acquisition of an employee username and password from a dark web forum, very likely as part of another data breach. This allowed the attackers to walk in and immediately begin scouting the network and attempting to escalate privileges, with the first incident taking place in April. A number of security researchers have reported seeing the accounts of UN employees listed among large packs of usernames and passwords sold on underground forums, in this case as part of a package going for only $1,000

- **Microsoft customer support database breach**

Microsoft has acknowledged an access misconfiguration where 250 million customer records were exposed on a database without password protection.

The exposed records — including conversations with customers and Microsoft support agents — date from 2005 to December 2019.

The exposed information could raise the risk of tech-support scams targeting Microsoft customers. Scammers might be able to use the information to pretend they’re Microsoft support agents and try to trick customers into sharing their personal information.

- **Lifelabs data breach**

In November of 2019, LifeLabs notified the Office of the Information and Privacy Commissioner of Ontario of a potential cyber attack on their computer systems. A month later, the organization publicly confirmed that they were the subject of a cyber attack on their systems.
The personal information of about 15 million Canadians was extracted by cybercriminals, mainly residents of British Columbia and Ontario. This information included names, addresses, emails, date of birth, national health card numbers from 2016, and earlier. Customer login IDs and passwords appear to have also been exfiltrated in the breach.

Part 2: Write an analysis of a cyberattack.

.
The Stuxnet Virus

a. Who were the victims of the attacks?

While the exact extent of the virus's impact and the number of victims is not publicly known, it is believed to have affected a significant number of computer systems in Iran. The victims of the Stuxnet attack were primarily Iranian entities associated with the nuclear program, including the Natanz facility and other related infrastructure.

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

Zero-Day Exploits: Stuxnet leveraged multiple zero-day vulnerabilities, which are software vulnerabilities that were previously unknown and unpatched at the time of the attack.

Rootkit Techniques: Stuxnet incorporated sophisticated rootkit capabilities to conceal its presence and activities on infected systems.

Propagation Mechanisms: It utilized removable media such as USB drives to infect air-gapped systems, exploiting the AutoRun feature to automatically execute its code upon insertion.

PLC Exploitation: It specifically targeted Siemens Step 7 software and Siemens S7-300 and S7-400 series programmable logic controllers (PLCs).

Code Injection and Modification: Stuxnet employed code injection techniques to insert malicious code into legitimate PLC programs.

Command and Control (C&C) Infrastructure: It used multiple servers and domain names to manage the botnet and issue commands to the infected devices.

Self-Replication and Update Capabilities: Stuxnet had the ability to self-replicate and update itself, allowing it to spread and evolve within the targeted networks.

c. When did the attack happen within the network?

The Stuxnet attack within the target network is believed to have started as early as 2007, with initial infections detected in Iran. However, the full extent of the attack and its propagation within the network became apparent in 2010 when Stuxnet was discovered by cybersecurity researchers. It is important to note that the exact timeline of the attack and its various stages is not publicly disclosed in detail, as it involves classified information related to national security and intelligence operations.

d. What systems were targeted?

The Stuxnet cyberweapon specifically targeted industrial control systems (ICS) used in Iran's nuclear program. More specifically, it focused on compromising and manipulating the Siemens Step 7 software and Siemens S7-300 and S7-400 series programmable logic controllers (PLCs). These systems are commonly used in critical infrastructure and industrial settings to automate and control various processes.

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

The motivation behind the Stuxnet attack is widely believed to be a joint effort by the United States and Israel. The primary objective was to disrupt and delay Iran's nuclear program, specifically targeting the uranium enrichment facilities at Natan.

By targeting the industrial control systems and tampering with the centrifuge operation, the attackers intended to cause physical damage to Iran's uranium enrichment infrastructure. The goal was to slow down or disrupt Iran's progress in developing nuclear capabilities, thereby delaying their nuclear program.

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

Stuxnet successfully compromised the industrial control systems at the Natanz facility, causing disruptions to Iran's uranium enrichment process. The attack resulted in physical damage to centrifuges, leading to operational setbacks and delays in Iran's nuclear program.

The disruption caused by Stuxnet reportedly set back Iran's nuclear program by several months to a year. The exact extent of the setback is not publicly known, as Iran has not provided precise details regarding the impact of Stuxnet on their operations.

The discovery of Stuxnet brought significant attention to the potential impact of cyberattacks on critical infrastructure and industrial control systems. It highlighted the need for enhanced cybersecurity measures, especially in sectors related to national security and essential services