**Lab - Cybersecurity Case Studies**

**Part 1: Conduct search of high profile cyberattacks.**

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.

1. o The Stuxnet Virus

Stuxnet is a malicious computer worm first uncovered in 2010 and thought to have been in development since at least 2005. Stuxnet targets supervisory control and data acquisition systems and is believed to be responsible for causing substantial damage to the nuclear program of Iran.

1. o Marriott data breach

In 2018 Mariott Hotels reservation system Starwood was found to be hacked. Nearly 500 million records of personal information of hotel guests were copied by an unauthorized party.

1. o United Nations data breach

In August 2019, a cyberattack compromised the core infrastructure of the U.N that targeted a known vulnerability in the SharePoint platform. The New Humanitarian news organizations reported the news. Before that, there was no disclosure of the data breach.

1. o Microsoft customer support database breach

[Microsoft said Friday that hackers breached a computer](https://msrc-blog.microsoft.com/2021/06/25/new-nobelium-activity/) used by one of its customer service agents and stole account data they then used to launch "highly targeted" attacks on customers. The company identified the hacking group as Nobelium, the same one behind last year's major SolarWinds breach.

1. o Lifelabs data breach

In December 2019, LifeLabs began notifying patients that its computer systems were hit with a cyberattack that was discovered on November 1. The investigation that followed determined the hack included patients' lab results, some health card information, contact details, emails, login information, and dates of birth.

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.

Chosen attack: Marriot data breach

1. Who were the victims of the attacks?

Marriott International group

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

In the latest incident, a threat actor “used social engineering to trick one associate at a single Marriott hotel into providing access to the associate’s computer,” a Marriott spokesperson said via email. “The threat actor did not gain access to Marriott’s core network.”

1. When did the attack happen within the network?

After suffering one of the worst data breaches on record, Marriott disclosed [another data breach in March 2020](https://news.marriott.com/news/2020/03/31/marriott-international-notifies-guests-of-property-system-incident) that exposed account details on up to 5.2 million guests. This latest incident, though relatively minor, marks a pattern of personal identifiable information breaches with human error at the root.

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

A previous data breach that began in 2014 and went undetected for four years [ultimately impacted 500 million guests](https://www.ciodive.com/news/500m-hit-by-marriott-data-breach-intrusion-undetected-since-2014/543347/).