Group Members:

Muhammad Izham Bin Norhamadi (B032020039)

Ahmad Sha Herizam Bin Tahir (B032020009)

Lab 2 Current Cyberattack Scenario

1. Twitch Live Streaming Data Breach (2021)

Date / target the incident take place:
6/10/2021

The target:
Twitch

The damage/malicious activity done:
More than 100GB of leaked data was publicly posted online on 4chan, according to BBC. The leak data including three years of payment information Twitch compensated to gaming live streamer and Twitch source code.

Suspect/criminal who responsible in launching the attack:
Activist Hacker also known as Hacktivist who want to expose Twitch live streamer financial gain from Twitch since they said the community is toxic.

What vulnerabilities/ opportunity that has been exploit by the attacker:
According to Twitch, some data was exposed to the internet due to an error in a Twitch server configuration change that was subsequently accessed by a malicious third party.

Losses involved:
More than 100GB of leaked data posted publicly including Twitch Streamer financial information and Twitch source code.

Your opinion in preventing/mitigating the incident from happening to your organization:
Maintain best security practices, we need to strengthen passwords and stricter data privacy protection. We also need to run vulnerability assessments and annual pentest monthly to make sure organization's security stay on top.

References:

1. https://blog.twitch.tv/en/2021/10/15/updates-on-the-twitch-security-incident/

2. https://www.mitnicksecurity.com/blog/twitch-live-streaming-data-breach-2021

2. Samsung Data and Source Code Leak (2022)

Date of the news:
4/3/2022

Target:
Samsung confidential source code in their server

The damage:

- source code for every Trusted Applet (TA) installed in Samsung's TrustZone environment used for sensitive operations such as hardware cryptography, binary encryption, access control
- algorithms for all biometric unlock operations
- bootloader source code for all recent Samsung devices
- confidential source code from Qualcomm
- source code for Samsung's activation servers
- full source code for technology used for authorizing and authenticating Samsung accounts, including APIs and services

The suspect:
Lapsus$ Group which is also involved in various other recent data breach cases

The vulnerability exploited:
It is unknown how Lapsus$ Group manages to breach Samsung's server, but it may relate to recent discoveries of serious vulnerabilities in the cryptographic design and code structure of the TrustZone Operating System (TZOS) which forms part of the security-sensitive Trusted Execution Environment (TEE) of Galaxy smartphones

The losses:

Almost 190GB of confidential algorithm and source code stolen that can be used to modify Samsung devices and systems

Opinion on preventing the incident:

Any discovered vulnerability in our security environment must be remedied as soon as possible to avoid exploitation and loss of sensitive data

References:

Confirmation of the hack/breach came from Samsung statement to Bloomberg on March 7

1. https://www.forbes.com/sites/daveywinder/2022/03/08/samsung-confirms-massive-galaxy-hack-after-190gb-data-torrent-shared-via-telegram/?sh=136d2516658c
2. https://www.bleepingcomputer.com/news/security/hackers-leak-190gb-of-alleged-samsung-data-source-code/

3. Facebook Data Breach (2021)

Date / target the incident take place:
April, 2021.

The target:
Facebook database.

The damage/malicious activity done:
Over 533 million Facebook users' personal information has been leaked online which is approximately 20% of all accounts. The personal information including Facebook users' phone numbers, Facebook IDs, full names, locations, birthdates, bios, and, in some cases, email addresses even Facebook CEO, Mark Zuckerberg's personal information included as well.

Suspect/criminal who responsible in launching the attack:
Cybercriminal who wants to use leaked personal information to impersonate them to scam someone.

What vulnerabilities/ opportunity that has been exploited by the attacker:
The data has been scraped due to vulnerability that Facebook patched in 2019.

Losses involved:
All the leaked data has been shared online in forum and confidential data now being sold in cloud-based messaging app like Telegram. All of this leaked data can be use to do cybercrime such as Phishing and email fraud.

Your opinion in preventing/mitigating the incident from happening to your organization:
Since the leaked data was from scrap data from two years ago but the information still can be used if the information does not change. So, when an organization is having maintenance and needs to scrap or renew some personal information. This information needs to be paid attention to and needs to be secure to reduce any vulnerability towards this information.

Reference:

1. https://heimdalsecurity.com/blog/everything-you-need-to-know-about-the-2021-facebook-data-breach/

4. Credential-stuffing attack on Tesco database (2020)

Date:
Not specified

Target:
Tesco's Clubcard database

The damage:
Tesco has to re-issue 600,000 compromised Clubcard holders but they are able to detect the fraudulent activity before any real damage is done.

Suspect:

No known suspect was found

The vulnerability exploited:

A database of stolen usernames and passwords from other platforms had been tried out on its websites and may have worked in some cases. This is because many people still use simple passwords or similar login credentials for many different platforms.

Opinion on preventing the incident:
As a user, make use of password manager to lessen the repetitiveness of passwords used on multiple logins. As a website owner, remind user not to use the same password as other platforms

Reference:

https://www.bbc.com/news/technology-51710687

5. Hackers breach US Defense and Tech firms (2021)

Date of the news:
2/12/2021

Target:
US defense, technology companies, and hundreds more US organizations that cover crucial sectors such as defense, health care, energy and transportation

The damage:
Stolen passwords from targeted organizations to gain long-term access to computer systems

Suspect:
Chinese hackers' campaign

The vulnerability exploited:
Organizations that run the same vulnerable software

The losses:
Hacker could try to gain long–term access to computer systems to siphon off key data from US companies

Opinion on preventing the incident:
If an organization that's has a lot of branches uses the same software across all the branches, this software needs to have high priority security. This is because if this software becomes vulnerable and being targeted by hackers, all the organization branches' system is going to break down and can be hacked easily.

Reference:

https://www.wral.com/suspected-chinese-hackers-breach-more-us-defense-and-tech-firms/20013143/