CSCY 1000

July 5, 2023

Professor: Claude Sam-Foh

By: Aman Toor

Breach Scenario Interpretation Report

In October 2021 10 million records were leaked from a streaming service, the platform allowed gaming enthusiasts to stream and broadcast their games well interacting with viewers. The provider named Twitch, was infiltrated by a source code Breach which publicly show cased confidential data and documents including program files which can hinder the provider’s security if used unethically. The breach was responsible for the publication of almost 10 million streamers’ valuable information including income and payments. The following interpretation recaps the Chain of evidence that occurred at the time of the breach including classification of activity and its connection to this course studies.

On October 6th, 2021, 11:18am Twitch admitted to a data breach accruing via social media post on twitter. On the same day an article was published on BBC news website publicizing Twitch TVs confirmation of a massive data breach. Published by David Molloy and Joe Tidy. In the article it stated that the hackers claimed the breach was done by a source code breach. A source code breach is caused by the compromise of a developer or high-level access account being stolen and used by unauthorized personnel. The breacher once accessing the source code discovered data from September 2019 to October 2021. The discovery of this data breach breached Twitch’s confidentiality agreement that they pride them self on for when working with their streamers, the leak of payment and other information compiled was more than 100 GB of storage which is nearly 10 million streamers information. The data which was leaked can be identified as personally identifiable information (PII) and financial information as its connection to payment can connect towards the streamer’s banks, address, email, and possibly phone numbers.

This incident can be categorized into data exfiltration, as during in no point of the breach or in the articles did the hackers use the confidential data against the organization for personal use as a ransomware does. Data exfiltration tends to occur when unauthorized data is accessed and transferred from one computer to another, going back to the possibility of the alleged hackers gaining unauthorized access via a developer account or higher. This method of breaching is also known as modus operandi. It does seem to me to be a denial of service as the amount of the data leaked included sensitive data essential to the automation of the organization’s code. The essential files leaked included the “core config package” which is commonly used for the organization of scripts and codes that can come across errors if the config package isn’t set correctly, possibly leading to a halt of a system or organizations work. Other leaked files included “Devtools”, and “infosec”. Devtools also known as developer tools tend to allow authorized users to access tools that are able to change settings that can be changed well a live version of the program is uploaded and running on active servers. Infosec are tools that are connected to the information security asset part of the organization and its programs and services, possibly allowing which users to be given access and authorization to other files such as Devtools.

Once this incident has been resolved and taken care of by twitch’s developers there is still the matter of their security being questioned in the eyes of the public. The anonymous leaker suggested via a twitter post that there is more to post as he captioned “part one” indicating possibly more information they are holding out with. Though the incident has been entirely delt with, the matter of how strong twitch’s data security needs improvement. The alleged hacker has left a reputational impact on twitch and its confidence of its security it has also left possible firing of developers or possible authorized users once an investigation is done within the company. The financial penalties of this aren’t stated within the article by BBC news but there has left opportunity for other organizations in this category of business, show casing their security to their streamers/broadcasters which can drastically affect twitch’s financial income as streamers may change platforms taking along their viewers. In summary this report provides a breakdown event of the twitch data breach incident of 2021 and the chain of evidence that shows the situation and its work including financial, firing, and reputational impacts.

Works Cited/Reference:

<https://www.bbc.com/news/technology-58817658>

<https://twitter.com/Twitch/status/1445770441176469512?lang=en>