Yuqing Zhai

11/06/2024

Recently, millions of tickets from Tickermaster are hacked by hackers using the company's Snowflake account info. This essay will first analyze the scope of attack and the response of from Tickermaster. It will then argue that this breach violates the all CIA triad objectives and that Tickermaster and Snowflake are unethical using virtue ethics. [1, 2, 3, 4]

As noted by Wired, the hacker group called ShinyHunters first gained access to one EPAM worker's computer using leaked information in dark web. Tickermaster stored their user data via Snowflake's application suites, which EPAM provides additional services for. By breaking the computer, the hacker group gained plain username and password to Tickermaster's Snowflake account, therefore leaking all the information in it. The information includes user information like order, mailing, and credit card information. Additionally, ShinyHunter posted a tutorial of recreating the authentic ticket pdf using the leaked info in Tickermaster's database, potentially invalidate millions of tickets. These data are for sales are the dark web now. [1, 2, 3, 4]

After the sales are released on dark web, Ticketmaster filed a report to Security and Exchange Commission. However, there was a delay and denial during the initial breach, and only after sometime did the parent company finally confirms to the data breach, and send a email to all the customer about the scope of leaked information, potential security measure, and a free 1 year license in one security software. [3, 4] In this case, Tickermaster released the information at very late stage when the data is already on sale.

The CIA triad is *Confidentiality*, *Integrity*, and *Availability*. In this case, all of three keys are violated. The leaked information contains personally idenitfiable information of all its users, which break confidentiality. The hacker derived a system that could generate legitimate pdf tickets and duplicate all existing tickets, which compromise the ticketing system. The mass generation of fake tickets could potentially disrupts legitmiate users' access to events, potentially causing denials at venues for legitimate ticket holders, and this breaks availability.

Virtual Ethics judges whether the people is ethical by when they demonstrates virtuous character traits, and these virtues includes *responsibility*, *transparency*, and *foresight*. Tickermaster fails to display any of them. As a company, Tickermaster have the responsbility of properly keeping its user data, yet it failed to do so. As the response to the public, it didn't address the finer details of the attack, and have an delay to their public response, this makes their company lack of transparency. They are also lack of foresight, a multifactor authentication (MFA) could be an easy fix [4], and the hacker will not be able to get into their Snowflake database if they have turned it on. They should have also checked the inner details of the company EPAM

and Snowflake, so they could avoid their reliance in the first place. Therefore, we see that Tickermaster displays the opposite of these virtuous character traits, and is therefore unethical.

Reference

What Actually Happened with Snowflake, Ticketmaster - Risky Business News (6 minute podcast)
Ticketmaster Confirms Data Breach. Here's What to Know. - The New York Times
Taylor Swift Eras Tour - Hacker Leaks 440,000 Tickets, Raises Ransom Demand - MSN
The Ticketmaster Hack Is Becoming a Logistical Nightmare for Fans and Brokers - 404 Media
Hackers Detail How They Allegedly Stole Ticketmaster Data From Snowflake - WIRED