Seth Angell & Blake Blackport

Professor Cummings

MIS 534

February 16, 2022

Robinhood

Robinhood made its initial appearance in 2013, breaking onto the scene as a reimagined, mobile-first, stock brokerage experience. They are relatively new compared to other brokers, revolutionizing certain aspects of stock trading. Robinhood launched with commission free stock trading which the industry at large took as a joke. Nowadays though, it has become commonplace, and many other brokerages have followed suit allowing commission free trading themselves. They also made fractional trading, trading fractions of a share, very easy to do. A practice which has quickly become commonplace in the industry.

However, perhaps their most surprising yet obvious advantage, is their heavy emphasis on user friendliness and experience. They were among the first brokerages to have a mobile app for trading, which publicly launched in 2015. From the beginning, Robinhood differentiated themselves by their easy and intuitive user interface for navigating what is traditionally a complex field. Robinhood was, and arguably still is, one of the easiest trading apps to get started with if new to trading. Users with no previous experience at all can likely figure out how to trade by simply downloading their app. Once again, other companies followed suit and now there are many other friendly trading apps, but Robinhood was among the first. These changes get to the core of the company’s ideals, trading in the past was usually exclusive to those with enough money and knowledge to do so. Robinhood places the power in the average people’s hands by giving them a very simple and friendly interface (paying homage to their namesake). You can also start trading on Robinhood with as little as one dollar as they have a minimum account balance of zero dollars and allow fractional trading. As a result, the demographic makeup varies quite heavily from your average stock brokerage.

Robinhood’s breach interestingly includes two different attack vectors, both of which we have covered in class. In a way, for this set up to work the attackers needed to succeed in two disjointed exploitation events. The first vector being the offensive party socially engineered a support technician into disclosing access to a vast collection of user information. However, as far as the threat level of the data leaked, it was mild. The vast majority (around five million) of the victims only had their email leaked. A different smaller portion of two million users (about the population of Nebraska) had their full name leaked, and an exceedingly small portion totaling less than three hundred and twenty people had more extensive information released. (Team, Robinhood)

Given the circumstances, not the worst breach. Due to the age of the internet, email leaks are not entirely uncommon. The popular public data breach notification service haveibeenpwned.com touts right on their website that they have records of almost twelve billion exposed accounts (https://haveibeenpwned.com). What makes the Robinhood data particularly dangerous is the fact that Robinhood itself is a financial trading application. This point leads us into the territory of postulation but based on background research we believe it to be the attackers next steps.

The second exploited attack vector takes place with email addresses of existing accounts in hand. It is believed that the attackers began to pursue a targeted phishing campaign. Phishing campaigns are already relatively successful, with CISCO’s 2021 cybersecurity report attributing ninety percent of data leaks to them (2021 Cyber Security Threat Trends). By gathering the emails of five million confirmed account holders, a more targeted phishing campaign can begin. With the confidence of knowing that every email is or was at some point attached to an account, a phishing campaign which attempts to steal user’s passwords could be very lucrative. If the email looks realistic enough, even an exceedingly small success rate of one percent could return login credentials for fifty thousand stock brokerage accounts.

In response to the attack, Robinhood began work with an external cybersecurity firm by the name of Mandiant. Mandiant’s CTO Charles Carmakal released a statement after the fact stating that their firm had been aware of this threat actor, having encountered them in previous incidents. At the time of that statement (November 9th, 2021), they believed the group was still active and would have the potential to exploit other companies in an equivalent manner. (Robinhood Data Breach Leaves)

While this attack is only truly effective if two parties can be exploited, much of the blame still falls on Robinhood. The leaking of internal user data, no matter how benign, allows their customer base to be targeted and as a result lowers consumer confidence in their data security practices. Their stock price suffered as a result of this breach dropping 3.2 percent pre-market on November eighth when the news was announced (Robinhood Says Hackers Stole). The stock price continues to see negative growth even today, though how much of that is a reflection of this attack would be up to speculation.

Looking at the attack from an elevated level, the hackers utilized pre-texting to socially engineer their way into around 7 million data points of account information. With that information in hand, it is believed that they embarked on a targeted phishing campaign to gather more lucrative data or even potentially funds, from users. The attackers also tried to demand an extortion payment from Robinhood for an undisclosed amount. (Team, Robinhood) It is unknown whether this extortion was actually paid or not. However, it is quite unlikely that it was. The Robinhood attack should be viewed as a cautionary tale into the dangers of even the most innocent data leaks, and the importance of vetting the validity of any requests for account credentials.

**Bibliography**

“2021 Cyber Security Threat Trends- Phishing, Crypto Top the List.” *Resources*, 11 May 2021, https://learn-umbrella.cisco.com/ebook-library/2021-cyber-security-threat-trends-phishing-crypto-top-the-list.

*Have I Been Pwned: Check If Your Email Has Been ...* https://haveibeenpwned.com/.

November 9, 2021. “Robinhood Data Breach Leaves Millions Potentially Vulnerable.” *Channel Futures*, 11 Nov. 2021, https://www.channelfutures.com/mssp-insider/robinhood-data-breach-leaves-millions-potentially-vulnerable.

“Robinhood Says Hackers Stole Data Belonging to 7 Million Customers.” *CBS News*, CBS Interactive, 9 Nov. 2021, https://www.cbsnews.com/news/robinhood-data-breach-security-personal-data-hackers/.

Team, Robinhood. “Robinhood Announces Data Security Incident (Update).” *Under the Hood*, Under the Hood, 16 Nov. 2021, https://blog.robinhood.com/news/2021/11/8/data-security-incident.