Short Research Paper #1

5.4 million Twitter Accounts On Sale in a Hacking Forum

Jeggo Paolo V. DyCok

School of Cybersecurity, Old Dominion University

CYSE300_29216: Introduction to Cybersecurity

Dr. Joseph Kovacic

January 22, 2023

Information is now more important than ever. The advent of social media technology has given rise to the possible threat to personal data and the importance of security. The social media site Twitter has found itself a victim of a data breach after a post that dumped over 5.4 million user accounts for sale and potentially millions more by exploiting a code. This paper will cover the vulnerabilities that were exploited, who exploited them, the repercussions and steps that could be taken to mitigate the instances of being exploited.

What were the cybersecurity vulnerabilities?

The vulnerability lies in Twitter’s API which was disclosed in HackerOne bug bounty program which allowed people to submit private information such as emails and phone numbers to retrieve Twitter IDs. According to a user named “zhirinovskiy”, the vulnerability bypasses the privacy settings in any individual’s user account, leaking their personal information and allowing bad actors to identify people based on their phone numbers or email addresses. Zhirinovskiy also states that “the bug exists due to the process of authorization used in the android client of Twitter, specifically in the process of checking the duplication of a Twitter account.” (Zhirinovskiy, January 2022)

What threat(s) exploited the vulnerabilities?

Since the leak’s discovery in 2021, it is not clear whether the report on HackerOne was leaked but a website called BleepingComputer was informed that there were multiple bad actors utilizing the bug to steal private information. Although, an owner of a hacking forum named Breached communicated with BleepingComputer, declaring responsibility for leaking 5.4 million users and dumping user records for sale.

What were the repercussions of the incident?

Repercussions of the incident include the possibility of any bad actor with basic coding knowledge exploiting this threat by creating a database that links Twitter usernames to the database. Although, it is not clear whether this information has been exploited already, given the period in which this vulnerability was discovered. In addition to 5.4 million records, there was another 1.4 million Twitter profiles belonging to suspended users that were collected using the API. Speculation from a user named “Loder” explained that Twitter leak could contain more than 17 million records before he was banned from Twitter. Private information obtained from the vulnerability can prove to be fatal to users as bad actors can utilize such data for phishing and other types of frauds.

What cybersecurity measures could have been taken to mitigate the consequences or prevent the incident?

To put it simply, there are plenty of measures that can be taken to mitigate the consequences or prevent the incident. Resources will always be at odds with the demand, but engineers must continue to test for potential vulnerabilities and to inspect for bugs. Twitter has taken good measures in posting the HackerOne bug bounty program because it had led to one user finding out about it and reporting to twitter for fix. Finding vulnerabilities is a tedious process and twitter must employ more penetration testers in order to reduce the instances of information leaks.

Conclusion

Websites often deal with intrusion all the time and Twitter is only one of the victims that were attacked based on the bugs that exist on its APIs. A vulnerability like the one found on Twitter is not a unique situation and it can happen to any company. The larger the information databank, the more prone they are to attacks and exploitation no matter the size of the cybersecurity team and engineers they employ. The implications will always have the capacity to be catastrophic.

Although, it would be best to always practice constant vulnerability scans in order to mitigate the situation. Good response is what a company should always prioritize and a solid framework is what keeps it efficient and effective.

References

Powell, O. (2022, October 5). *5.4 million Twitter accounts reportedly on sale in Hacking Forum*. Cyber Security Hub. Retrieved January 18, 2023, from https://www.cshub.com/attacks/news/54-million-twitter-accounts-reportedly-on-sale-in-hacking-forum

Abrams, L. (2022, November 27). *5.4 million Twitter users' stolen data leaked online - more shared privately*. BleepingComputer. Retrieved January 18, 2023, from https://www.bleepingcomputer.com/news/security/54-million-twitter-users-stolen-data-leaked-online-more-shared-privately/

Twitter disclosed on hackerone: Discoverability by phone... HackerOne. (n.d.). Retrieved January 19, 2023, from https://hackerone.com/reports/1439026