Rustom Ichhaporia

CS Seminar: UNIX/Linux and Cybersecurity

Ms. Pandya

4 May 2020

Interpreting the Cybersecurity News: Tokopedia Data Breach

On May 1st, 2020, an anonymous black hat hacker dumped a file with the personal details of 15 million users who are registered on Tokopedia, which is the largest online store in Indonesia. Though only 15 million were publicly leaked, analysts estimate that a total of 91 million users’ details were compromised by the breach. The hacker is currently selling the expanded database on the dark web for only $5000, but authorities are attempting to remove the posting and apprehend the hacker. The file was posted in a format matching PostgreSQL, an SQL-compliant database management system. The hacker has not been able to identify the passwords of all of the users whose credentials have been leaked because the passwords are still stored as hashes. However, other black hat hackers are undoubtedly working on cracking these hashes, and other sensitive information such as phone numbers, dates of birth, and location details were leaked in plaintext format.

One element making it difficult for the black hat hackers to crack the hashes is the lack of “salt strings.” These are intermediate strings filled with random data that make the one-way hashes more difficult to decode, without knowing the specific contents of the salt string. This will likely give compromised users more time to reset their passwords and attempt to secure their accounts once again. It is unknown whether the hacker themselves has the salt strings and has chosen not to release them, or the hacker was unable to compromise the salt strings entirely in his efforts.

Tokopedia is urgently advising its users to change their passwords to protect their accounts and data as damage control, but significant damage has been done already which exposes the vulnerabilities of even the largest and most secure private corporations’ databases. This incident highlights the importance of cybersecurity both on the personal and enterprise fronts. For individuals, it is a reminder that creating strong passwords and understanding what data companies collect about you are crucial steps to take to protect your money, livelihood, and safety. On a commercial level, this incident serves as a wake-up call to companies with expanding user data bases that have not spent enough money on cybersecurity professionals and infrastructure; these companies can face similar attacks at any time. In a world where the creation and storage of sensitive data is exponentially growing, cybersecurity must remain one of our foremost concerns if we are to adequately tackle the issue of black hat hacking.