Purported data from 200 million Yahoo accounts may be legit

22/09/2016

In August, a dealer in stolen data who goes by the online moniker "Peace"—the person or persons who previously sold data from the accounts of MySpace and LinkedIn users—announced that the results of another "megabreach" were for sale. This time, it's the account information of 200 million Yahoo users. According to a report by Recode's Kara Swisher, Yahoo is preparing to confirm the four-year-old breach, potentially creating problems for the company's planned $4.8 billion acquisition by Verizon.

A previous examination of a sample of the data obtained by Motherboard was inconclusive. There has been a number of other claimed breaches of Yahoo's account data, including a claim of 40 million Yahoo accounts among a total of 272 million alleged stolen credentials reported in May. But that data that may have just as easily been stolen from other sources.

According to a spokesperson at LeakedSource, however, a small sample file of legitimate Yahoo user data exists. But it's not clear whether it's representative of the rest of the data "Peace" has, because no one has been able to look at the full dump yet—"Peace" has offered to sell it for 3 Bitcoin (about $1,860).

"There are two Yahoo files floating around the Internet," LeakedSource told Ars. The first is a "5,000-sample .txt file that's been on the dark web for years." The second, larger file is "an encrypted .zip archive containing 40 text files claiming to be from Yahoo. We have both of them as well as the decryption key for the 40 text files, which we determined to be fake. The first sample, however, may be real and provide enough evidence for Yahoo to begin resetting passwords."

A variety of people with Yahoo accounts, some of whom work at Ars, report they recently received messages when logging in that recommended, but didn't mandate, a password change: