Alleged Chinese police database hack leaks data of 1 billion

July 6 2022, By ZEN SOO

A police car patrols the street as residents gather nearby, Tuesday, May 31, 2022, in Shanghai. Hackers claim to have obtained a trove of data on 1 billion Chinese from a Shanghai police database in a leak that, if confirmed, could be one of the largest data breaches in history. Credit: AP Photo/Ng Han Guan

Hackers claim to have obtained a trove of data on 1 billion Chinese from

a Shanghai police database in a leak that, if confirmed, could be one of the largest data breaches in history.

In a post on the online hacking forum Breach Forums last week, someone using the handle "ChinaDan" offered to sell nearly 24 terabytes (24 TB) of data including what they claimed was information on 1 billion people and "several billion case records" for 10 Bitcoin, worth about $200,000.

The data purportedly includes information from the Shanghai National Police database including names, addresses, national identification numbers and mobile phone numbers as well as case details.

A sample of data seen by The Associated Press listed names, birthdates, ages and mobile numbers. One person was listed as having been born in "2020," with their age listed as "1," suggesting that information on minors was included in the data obtained in the breach.

The Associated Press could not immediately verify the authenticity of the data samples. Shanghai police did not immediately respond to a request for comment.

The data leak initially sparked discussion on Chinese social media platforms such as Weibo, but censors have since moved to block keyword searches for "Shanghai data leak."

One person said they were skeptical until they managed to verify some of the personal data leaked online by attempting to search for people on Alipay using their personal information.

"Everyone, please be careful in case there are more phone scams in the future!" they said in a Weibo post.

Chinese policemen patrol the bund area, Wednesday, June 1, 2022, in Shanghai. Hackers claim to have obtained a trove of data on 1 billion Chinese from a Shanghai police database in a leak that, if confirmed, could be one of the largest data breaches in history. Credit: AP Photo/Ng Han Guan

Another person commented on Weibo that the leak means everyone is "running naked"—slang used to refer to a lack of privacy—and it's "horrifying."

Experts said the breach, if confirmed, would be the biggest in history.

Kendra Schaefer, a partner for technology at policy research firm Trivium China, said in a tweet that it's "hard to parse truth from the

rumor mill, but can confirm file exists."

Such data leaks are fairly common, according to Michael Gazeley, managing director at Hong Kong-based security firm Network Box.

"There are approximately 12 billion compromised accounts posted on the Dark Web right now. That's more than the total number of people in the world," he said, adding that a majority of data leaks often come from the U.S.

Chester Wisniewski, principal research scientist at cybersecurity firm Sophos, said that the breach is "potentially incredibly embarrassing to the Chinese government," and the political harm would probably outweigh damage to the people whose data was leaked.

Most of the data is similar to what advertising companies that run banner ads would have, he said.

"When you're talking about a billion people's information and it's static information, it's not about where they traveled, who they communicated with or what they were doing, then it becomes very much less interesting," Wisniewski said.

A police officer watch over a road junction with traffic lights, Tuesday, May 31, 2022, in Shanghai. Hackers claim to have obtained a trove of data on 1 billion Chinese from a Shanghai police database in a leak that, if confirmed, could be one of the largest data breaches in history. Credit: AP Photo/Ng Han Guan

Still, once hackers get data and put it online it's impossible to fully remove.

"The information, once it's unleashed, is forever out there," Wisniewski said. "So if someone believes their information was part of this attack, they have to assume it's forever available to anyone and they should be taking precautions to protect themselves."

A major cryptocurrency exchange said it had stepped up verification

procedures to guard against fraud attempts such as using [personal information](#) from the reported hack to take over people's accounts.

Zhao Changpeng, CEO of Binance, a cryptocurrency exchange, said in a tweet Monday that its threat intelligence had detected the sale of "1 billion resident records."

"This has impact on hacker detection/prevention measures, mobile numbers used for account take overs, etc." Zhao wrote in his tweets, before saying that Binance had already stepped up verification measures.

In 2020, a major cyberattack believed to be by Russian hackers compromised several U.S. [federal agencies](#) such as the State Department, the Department of Homeland Security, telecommunications firms and defense contractors.

Last year, over 533 million Facebook users had their data published in a hacking forum after hackers scraped its data due to a vulnerability that has since been patched.