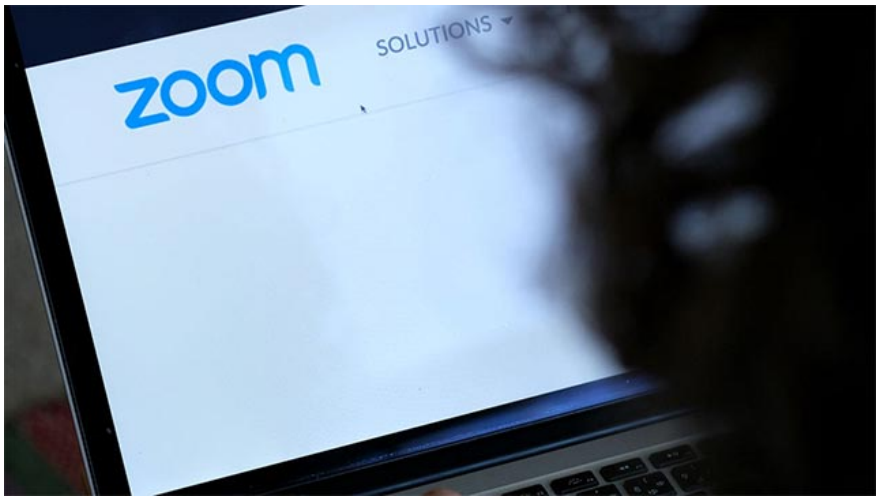
Detected the archive containing data of thousands of Zoom accounts on the dark web forum

Through analysis of experts, this database contains Zoom account login information.

Recently, a group of international cybersecurity experts from security organization IntSights suddenly discovered a database being shared publicly on a dark web forum containing more than 2,300 information. Zoom online conferencing application account has been compromised.

Through analysis of experts, this database contains the Zoom account login information of users who are working in companies in many different fields such as banking, financial consulting, educational institutions. education, health care providers and software providers. Especially among them, there are quite a lot of emails, passwords, meeting IDs, names and host keys.



Learning software and online meeting Zoom

According to initial estimates, this data warehouse is used as a 'material' for credential stuffing attacks. This is a major form of cyberattack using stolen account information, including lists of usernames, email addresses, and corresponding passwords (often obtained from data breaches) for unauthorized access. allow access to user accounts through login requirements. The availability of Zoom accounts can allow an attacker to collect additional data related to the account, using the OpenBullet configuration specifically for Zoom. OpenBullet is a set of web testing tools that can be used to extract and analyze data, to conduct pen tests and more.

In addition, the information stored in this data warehouse can be used to launch denial of service attacks, or simply harass online meeting rooms with the 'Zoombombing' behavior.

At the moment, experts have not been able to pinpoint the exact source of this data warehouse, but it is unlikely that it will be stolen from Zoom's servers.