Hackers sell stolen user data from HomeChef, ChatBooks, and Chronicle

By Ionut Ilascu

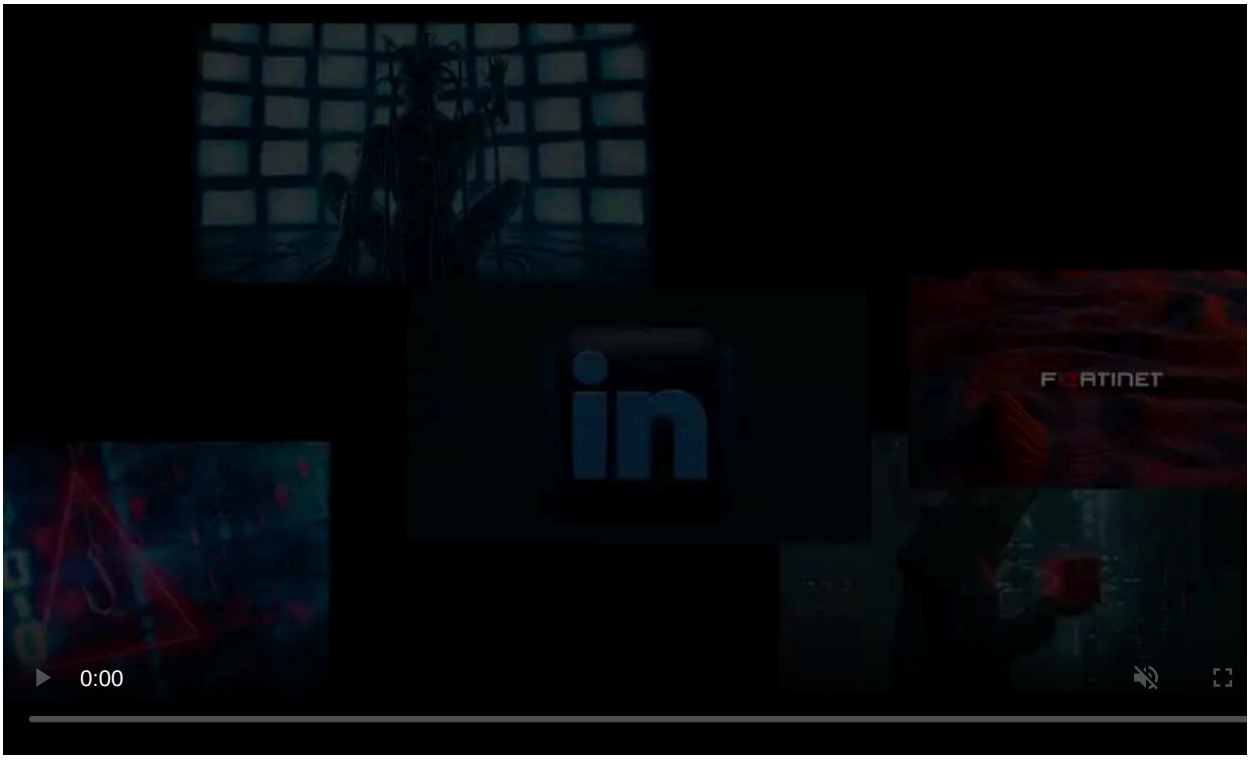
Published: 2020-05-08 · Archived: 2026-04-05 19:08:28 UTC

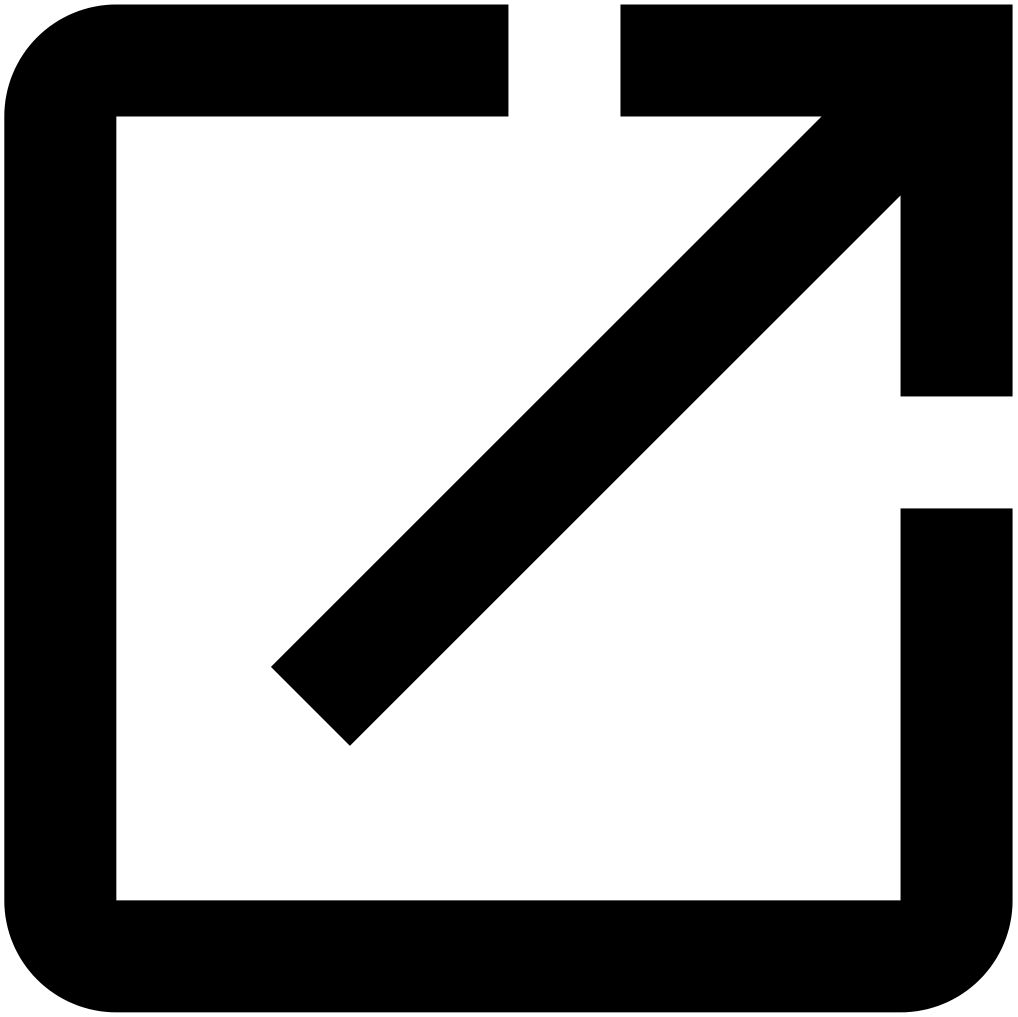
Three more high-profile databases are being offered for sale by the same group claiming the Tokopedia and Unacademy breaches, and the more recently reported theft of Microsoft's private GitHub repositories.

Going by the name Shiny Hunters, the group is now selling user records from meal kit delivery service HomeChef, from photo print service ChatBooks, and Chronicle.com, a news source for higher education.

Millions of user records for sale

Together, the three databases count user records and passwords from 26 million accounts. The ask prices are between $1,500 and $2,500.


0:00



In a conversation with BleepingComputer, the hackers said that they have more databases from other breached websites. They plan on selling them in the near future.

BleepingComputer was unable to independently confirm if the data that is offered for sale is authentic or not; the past two sales suggest that it is.

Researchers at digital risk protection company ZeroFox caught the posts from the hackers and assess with high confidence that the breaches are legitimate.

With eight million user records, the HomeChef trove is the most expensive. It was advertised today and had not been sold when the researchers saw the hackers' post.

The hackers demand $2,500 for emails, bcrypt-hashed passwords, IP addresses. Although the passwords need to be dehashed to extend the range of illegal activities this database can serve, it still has value.

Personally identifiable information (PII) including phone numbers, zip codes, and partial social security numbers are also present in the sample set from the hackers.

The post for the ChatBooks database was published on May 3 and the asking price is $2,000 for 15 million rows of data. It did not have any buyers through the dark web forum it was advertised on.

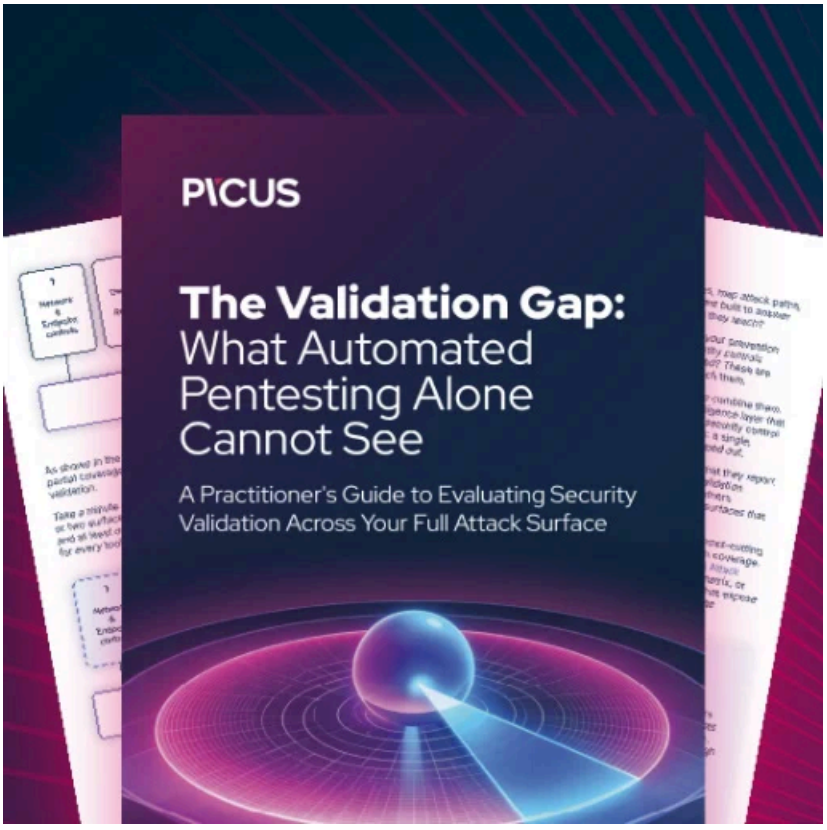
From the sample provided by Shiny Hunters, the database has email addresses, passwords hashed with the SHA-512 function, social media access tokens, and some PII.

With a price tag of $1,500, the data from Chronicle.com is the cheapest. It is also the smallest, with three million user records.

It was posted on May 3 and there are no details about the type of information it contains. Just like with the others, nobody bought it.

The lack of buyers makes it probable that the three databases will soon become available on other markets for lower prices.

"It is likely that this actor will continue to breach companies and post their content for sale," notes ZeroFox Alpha Team in a blog post on Thursday. They add that these tactics proved successful for other hackers and there is no reason this should not work in the case of Shiny Hunters.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/hackers-sell-stolen-user-data-from-homechef-chatbooks-and-chronicle/