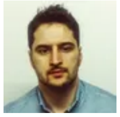
# Round 4: Hacker returns and puts 26Mil user records for sale on the Dark Web

zdnet.com/article/round-4-hacker-returns-and-puts-26mil-user-records-for-sale-on-the-dark-web/

Gnosticplayers returns with new user records, most of which he obtained by hacking companies last month.



Written by Catalin Cimpanu, Contributor on March 17, 2019

A hacker who has previously put up for sale over 840 million user records in the past month, has returned with a fourth round of hacked data that he's selling on a dark web marketplace.

This time, the hacker has put up for sale the data of six companies, totaling 26.42 million user records, for which he's asking 1.2431 bitcoin ($4,940).

The hacker's name is Gnosticplayers, and since February 11 the hacker has put up for sale data for 32 companies in three rounds [stories on Round 1, Round 2, and Round 3] on Dream Market, a dark web marketplace.

Today, the hacker published a new batch of files from six new companies, namely game dev platform GameSalad, Brazilian book store Estante Virtual, online task manager and scheduling apps Coubic and LifeBear, Indonesia e-commerce giant Bukalapak, and Indonesian student career site YouthManual.

| Company | DB size | Breach date | Price | Content |
|---|---|---|---|---|
| GameSalad (game dev platform) | 1.5 Mil | 2019/02 | ฿0.0785 | email, password (SHA1/SHA256), username, IP address |
| Estante Virtual (Brazilian book shop) | 5.45 Mil | 2019/02 | ฿0.2618 | name, username, password (SHA1), address, email, phone number |

| | | | | |
|---|---|---|---|---|
| Coubic (scheduling software) | 1.5 Mil | 2019/02 | ฿0.157 | name, email, password (SHA256) |
| LifeBear (Japanese scheduling app) | 3.86 Mil | 2019/02 | ฿0.2618 | email, password (MD5), username, event details, app settings |
| Bukalapak (Indonesian e-commerce site) | 13 Mil | 2017/07 | ฿0.34 | username, name, email, password hash (SHA512+salt), shopping details, IP adress, other |
| YouthManual.com (Indonesian youth student and career site) | 1.12 Mil | 2019/02 | ฿0.144 | name,email, password hash (SHA1+salt), hobbies, education, other |

Image: ZDNet

*ZDNet* has reached out to the allegedly hacked companies with emails earlier today. It is worth mentioning that many of the companies whose data Gnosticplayers has sold in the previous three rounds have already confirmed breaches.

Coubic returned comment and said it was investigating the breach. So did LifeBear, which admitted that it was "most likely" that it servers got hacked, but the company is still investigating. [*UPDATE: Bukalapak, Coubic and LifeBear have publicly acknowledged the hacks.*]

The difference between Round 4 and the previous three rounds is that five of the six databases Gnosticplayers put up for sale were acquired during hacks that have taken place last month, February 2019.

The hacker said that he put up the data for sale mainly because these companies had failed to protect passwords with strong encryption algorithms like bcrypt.

Most of the hashed passwords the hacker put up for sale today can cracked with various levels of difficulty --but they can be cracked.

"I got upset because I feel no one is learning," the hacker told *ZDNet* in an online chat earlier today. "I just felt upset at this particular moment, because seeing this lack of security in 2019 is making me angry."

In a conversation with *ZDNet* last month, the hacker told us he wanted to hack and put up for sale more than one billion records and then retire and disappear with the money.

But in a conversation today, the hacker says this is not his target anymore, as he learned that other hackers have already achieved the same goal before him.

Gnosticplayers also revealed that not all the data he obtained from hacked companies had been put up for sale. Some companies gave into extortion demands and paid fees so breaches would remain private.

"I came to an agreement with some companies, but the concerned startups won't see their data for sale," he said. " I did it that's why I can't publish the rest of my databases or even name them."

*Article updated with Coubic and LifeBear responses.*

**Data leaks: The most common sources**

### More data breach coverage: