Hacker leaks 386 million user records from 18 companies for free

By Lawrence Abrams

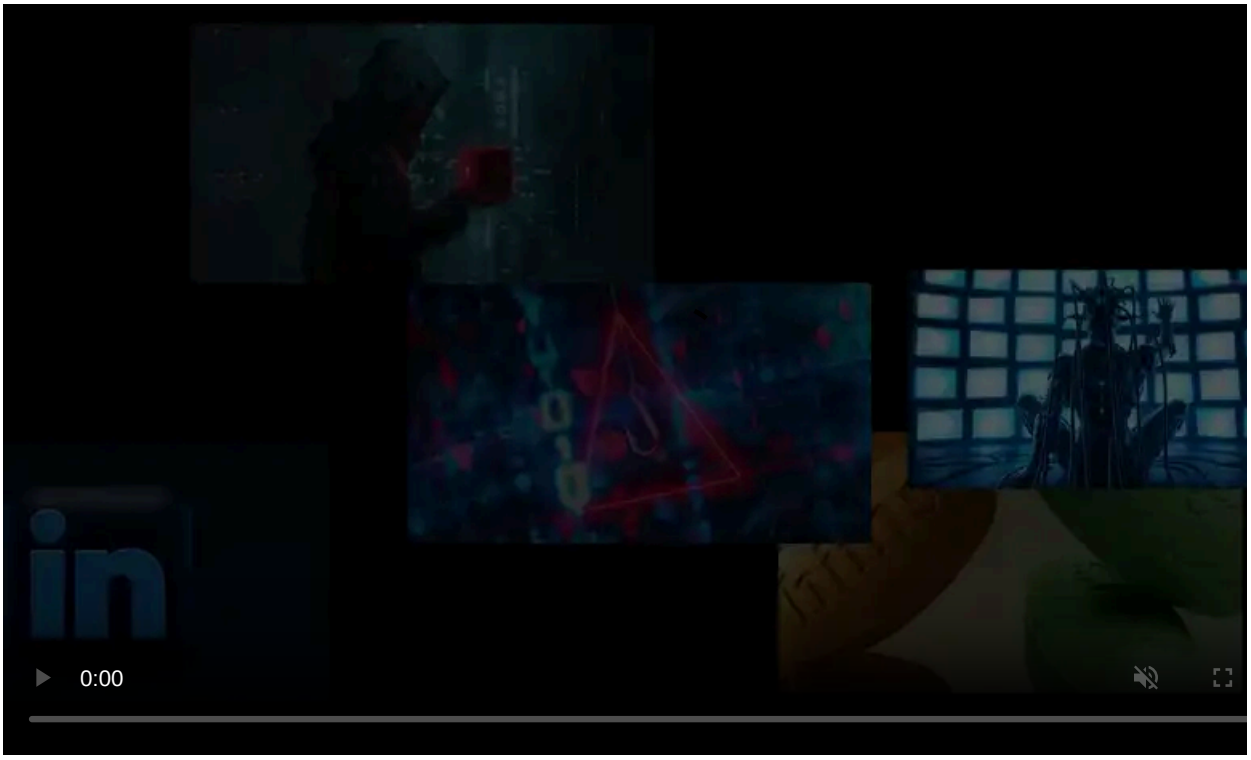
Published: 2020-07-28 · Archived: 2026-04-05 16:19:06 UTC

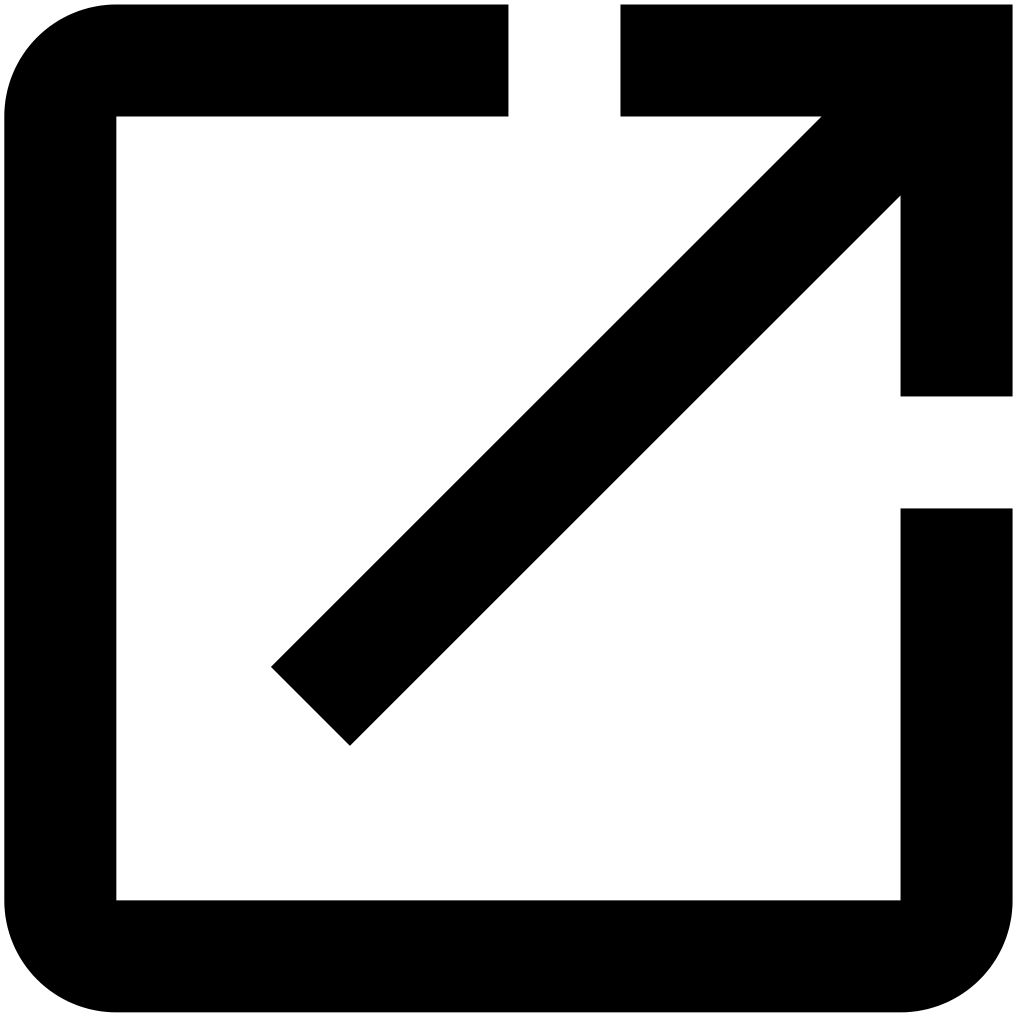
A threat actor is flooding a hacker forum with databases exposing expose over 386 million user records that they claim were stolen from eighteen companies during data breaches.

Since July 21st, a seller of data breaches known as ShinyHunters has begun leaking the databases for free on a hacker forum known for selling and sharing stolen data.

A partial list of databases posted to the forum

ShinyHunters has been involved in or responsible for a wide assortment of data breaches this past year, including Wattpad, Dave, Chatbooks, Promo.com, Mathway, HomeChef, and the breach of Microsoft private GitHub repository.


0:00



Databases stolen in data breaches usually are privately sold first, with prices ranging between $500 (Zoosk) to $100,000 (Wattpad). Once they are no longer profitable, threat actors commonly release them on hacker forums to increase their community reputation.

Of the databases released since July 21st, nine of them were already disclosed in some manner in the past.

The other nine, including Havenly, Indaba Music, Ivoy, Proctoru, Rewards1, Scentbird, and Vakinha, have not been previously disclosed.

The full list of the 18 data breaches are listed below:

Company	User Records	Reported Breach Date	Known?
Appen.com	5.8 Million	N/A	No
Chatbooks.com	15.8 Million	March 26th, 2020	Yes
Dave.com	7 Million	July 2020 *	Yes
Drizly.com	2.4 Million	July 2020 *	No
GGumim.co.kr	2.3 Million	March 2020 *	Yes
Havenly.com	1.3 Million	June 2020 *	No
Hurb.com	20 Million	N/A	Yes
Indabamusic.com	475 Thousand	N/A	No
Ivoy.mx	127 Thousand	N/A	No
Mathway.com	25.8 Million	January 2020 *	Yes
Proctoru.com	444 Thousand	N/A	No
Promo.com	22 Million	July 2020	Yes
Rewards1.com	3 Million	July 2020 *	No
Scentbird.com	5.8 Million	N/A	No
Swvl.com	4 Million	N/A	Yes
TrueFire.com	602 Thousand	N/A	Yes
Vakinha.com.br	4.8 Million	N/A	No
Wattpad	270 Million	June 2020 *	Yes
* Based on threat actor's statements			

From the samples seen of these databases, BleepingComputer has confirmed that the exposed email addresses correspond to accounts on the services.

The combined databases expose over 386 million user records. While a password is not included in every record, for example, promo.com, there is still a massive amount of information being disclosed that threat actors can use.

When BleepingComputer asked ShinyHunters why they dumped all of these databases, we were told that they were leaked for everyone's benefit.

"I just thought: 'I've made enough money now' so I leaked for everyone's benefit."

"Obviously, some people are a little upset because they paid resellers a few days ago, but I don't care," ShinyHunters told BleepingComputer.

Are you a user of the listed services?

BleepingComputer has contacted each of the companies being offered for free by ShinyHunters, but have not heard back from any of them.

This lack of response is common when a data breach is reported, and usually weeks, if not months later, the company will report a data breach.

To be safe, if you are a user of one of the services listed above, I strongly advise you to change your password immediately on the site.

If you use the same password at other sites, you should also change the password at those sites to a unique and strong one that you only use for that site.

Using unique passwords prevents a data breach at one site from affecting you at other websites you use.

To assist you in keeping tracking of unique and strong passwords, I suggest you use a password manager application.

Thx to Cyble for the tip.
