NEWS
Database leak exposes 3.3 million Hello Kitty fans

Database storing 3.3 million sanriotown.com accounts found online

🐦 📘 in 🅶⁺

CSO | Dec 19, 2015 6:26 PM PT

A database for sanriotown.com, the official online community for Hello Kitty and other Sanrio characters, has been discovered online by researcher Chris Vickery. The database houses 3.3 million accounts and has ties to a number of other Hello Kitty portals.

Vickery contacted Salted Hash and Databreaches.net about the leaked data Saturday evening.

The records exposed include first and last names, birthday (encoded, but easily reversible Vickery said), gender, country of origin, email addresses, unsalted SHA-1 password hashes, password hint questions, their corresponding answers, and other data points that appear to be website related.

MORE ON CSO:Millions of records compromised in these data breaches

Vickery also noted that accounts registered through the fan portals of the following websites were also impacted by this leak: hellokitty.com; hellokitty.com.sg; hellokitty.com.my; hellokitty.in.th; and mymelody.com.

In addition to the primary sanriotown database, two additional backup servers containing mirrored data were also discovered. The earliest logged exposure of this data is November 22, 2015.

In order to prevent identification of the database, Salted Hash is withholding screenshots of the data, IP information, DNS data, and other identifying markers.

Sanrio, as well as the ISP being used to host the database itself, have all been notified. An automated email from the ISP confirmed that the incident notification was logged, but no further details are available.

The Hello Kitty brand is highly popular the world over, to kids and adults, so the immediate concern is that the database might contain the personal information of children.

The recent VTech data breach exposed 11.6 million people, and 6.4 million of them were children. We've asked Sanrio to confirm if there were minors in the database, and the exact count if so. This post will be updated as new information emerges.

In the meantime, it might be wise to take some basic precautions.

If you or your child are registered on sanriotown.com or any of the related domains, it might be best to make sure that you're not using the same password on critical websites, such as those related to financial matters, email, or social media.

In the event that such overlap exists, then you should change your passwords immediately. Moreover, if you use the same hint question and answer across all websites, or related hints and questions, it's a good idea to change those as well.

If the option is available, you should strongly consider using two-factor authentication. Most banks and social media websites offer this feature.

While having sensitive details exposed is bad enough for adults, when the information relates to a child – it's worse. If someone managed to compromise a child's identity, the fraud might not be detected for years, because most parents don't monitor their child's credit record.

Given the way things have been, considering all the data breaches in the last year or two, It might be a good idea to start doing so. Yearly credit reports are free, and victims of identity theft can obtain access to all necessary reports at not cost.

More information is available at Consumer.gov.

Update: Shortly after this article was published, Vickery contacted Salted Hash to report that the passwords were in fact SHA-1 hashes, and not MD5 as he had previously stated.

Steve Ragan — *Senior Staff Writer*

👤 ✉ 𝕏 in g⁺ 🔊

Insider: Free IDC FutureScape webcast: Worldwide security 2016 predictions

💬 **View Comments**

You Might Like