Hacker Claims Popular Android App Store Breached: Publishes 20 Million User Credentials

Davey Winder Senior Contributor

A popular Android app store with 150 million users has been hacked, claims hacker
GETTY

The stolen records of 20 million users of a popular Android app store have been published online by a hacker who claims to have 19 million more.

Not all app stores are the same. Android users have access to the official Google Play Store, complete with nearly three million (2,870,985) apps available for download. Then there are the manufacturer app stores, of which the best known are probably the Samsung Galaxy Store and the Huawei AppGallery.

Finally, we arrive at the third-party app stores, the ones not pre-installed by the smartphone vendor nor operated by Google. Among the biggest of these, with a claimed global userbase of 150 million and a million apps, is Aptoide. It is Aptoide that would appear to have been breached by a hacker who claims to have stolen 39 million customer records and has published details of 20 million of them, including login emails and hashed passwords, on a popular hacker forum.

A decentralized Android app store

Aptoide was founded in 2011 and has quickly grown thanks to using a decentralized app store model where every user can have their own individually managed app store. The Aptoide app itself is open source and generally well-received, acting as an app discovery platform. It is also thriving, as far as third-party app stores go: one million apps and seven billion downloads are claimed by Aptoide.

Cybersecurity folk, myself included, often warn against the use of third-party app stores because of the potential for

malware distribution. Aptoide, though, has always been keen to emphasize how safe it is. The app description states that "all the apps are checked for viruses, and we perform extra security tests to ensure your Android device is always safe." The Aptoide home page claims that "recent studies prove that Aptoide is the safest Android app store," although I was unable to find any link to those studies. In the research and development section, however, there was mention of the AppSentinel anti-malware system project and a reputation systems knowledge base called

"Using unofficial app stores is basically driving without insurance," Jake Moore, a cybersecurity specialist at ESET, says, "you can do it, but you're not covered when anything goes wrong." The appeal is that they can often offer apps that users want but can't find at the official stores as developers can hit brick walls when it comes to apps being deemed "unacceptable" in some way or other. "Users have to weigh up whether or not it is really worth using such outlets which can so often be used for illicit means," Moore concludes.

Good general advice, but for once, this isn't a story about malware being downloaded from app stores but rather the security of the app store itself.

Aptoide user data published on a hacker forum

On April 19, the Have I Been Pwned (HIBP) database added an entry for Aptoide. This stated that the app store had suffered a data breach and that 20 million customer records had subsequently been shared online in a popular hacker forum. HIBP states the breach date as being April 13 and gives the precise number of compromised accounts as 20,012,235.

Aptoide publishes a 'credentials information' statement

Aptoide issued a statement on April 18, written by Filipa Botelho, head of community marketing. This confirmed only that "the Aptoide database may have been a victim of a hacking attack and a possible database breach." It went on to say that the threat is currently being evaluated and will, if confirmed, take "measures to correct it." In the meantime, however, Aptoide also said that all passwords were encrypted, and no personal data other than the login email address and the encrypted password was contained in the database.

The original reporting at ZDNet on April 17, based on information discovered by Under the Breach, stated that the data published on a popular hacking forum included additional information such as the user's real name, device

details and if provided, date of birth. All of which was contained in a PostgreSQL export file that the reporter had seen. The Aptoide statement, meanwhile, said that users were "never requested for physical addresses, credit card information, telephone numbers, or other personal data." Aptoide has announced that it has now closed the sign-up process at the app store until after a security audit is completed. Once the site is reopened, Aptoide said, "it will be required for you to introduce a new password for security measures."

If you are an Aptoide user and share the same password across sites and services, which is never a good idea, so stop doing that, then you should change those credentials immediately.