Issued 5/21/18

TeenSafe Leaks Thousands of Kid's Email Addresses and Passwords

TeenSafe advertises itself as a service allowing parents to monitor what their children are doing on smartphones in order to keep them safe. It does this through the use of an iOS or Android app, which allows parents to view the texts, call logs, web history, and location of a phone. The problem is, TeenSafe didn't secure its servers or the data it stored properly. For TeenSafe to work it requires two-factor authentication be turned off on a device, and in the case of an iPhone, for the parent to know a child's Apple ID and password. TeenSafe stores these details for each account on servers hosted by Amazon Web Services and did so without encrypting the data. Two of those servers were not protected properly, which meant anyone could access the information. TeenSafe has been forced to take the servers offline and alert customers whose details were exposed that they may be at risk. It's unclear exactly how many accounts were exposed, but one of the servers contained 10,200 records from the past three months. What leaked includes parent TeenSafe and child Apple ID email addresses, device unique identifiers, and the password associated with each Apple account. ZDNet verified with several parents over iMessage that the leaked data was correct. To be clear, most of the leaked data allows access to the devices of children because that's what was stored to allow parents to gain access to the devices through TeenSafe.