Cyberthreats under the Bed

Nir Kshetri, University of North Carolina at Greensboro
Jeffrey Voas, IEEE Fellow

Internet-connected toys provide an often-overlooked avenue for breaching personal data, especially of those most vulnerable. Government and private measures can minimize the risks, but responsibility for monitoring smart toy usage ultimately lies with parents.

According to Juniper Research, the size of the global smart toy market was $5 billion in 2017.[1] Smart toys employ sensors, cameras, microphones, data storage, voice recognition, GPS, and more. These technologies make toys more fun and engaging but also provide more vectors for cyberattacks.

In early 2017, a security vulnerability was discovered in CloudPets, a line of stuffed animals that connect via Bluetooth to a smartphone, enabling parents and children to send voice messages to and from each other from a distance. Exploiting the flaw, hackers were able to access children's personal information, photos, and voice recordings stored in the cloud. According to one security researcher, more than 820,000 user accounts were compromised including 2.2 million voice recordings. At one point, the hacked information was held for ransom.[2,3]

Two years earlier, Hong Kong–based toymaker VTech had experienced an even larger cyberbreach. Through a flaw in its website, hackers obtained access to photos and chat logs from the accounts of more than 6.3 million children in the US, Canada, Europe, Latin America, Australia, and New Zealand.[4,5]

SLOPPY SECURITY

In part due to limited technology budgets, many smart toymakers have weak security and privacy policies.[6,7]

VTech, for instance, had secured its toys' user data with outdated protocols.[8] It's standard practice to hash passcodes—transform them into a different set of digital characters—to make databases more secure. VTech reportedly used the hashing algorithm MD5, whose developer had publicly announced back in June 2012 that it was

0018-9162/18/$33.00 © 2018 IEEE