PHYS.ORG

Report: Some top baby monitors lack basic security features

September 2 2015, byBree Fowler

Several of the most popular Internet-connected baby monitors lack basic security features, making them vulnerable to even the most basic hacking attempts, according to a new report from a cybersecurity firm.

The possibility of an unknown person watching their baby's every move is a frightening thought for many parents who have come to rely on the devices to keep an eye on their little ones. In addition, a hacked camera could provide access to other Wi-Fi-enabled devices in a person's home, such as a personal computer or security system.

The research released Wednesday by Boston-based Rapid7 Inc. looks at nine baby monitors made by eight different companies. They range in price from $55 to $260.

The cameras are often mounted over a baby's crib or another place where they spend a large amount of time. They work by filming the child, then sending that video stream to a personal website or an app on a smartphone or tablet. Some of the cameras also feature noise or motion detectors and alert parents when the baby makes a sound or moves.

"There's a certain leap of faith you're taking with your child when you use one of these," says Mark Stanislav, a senior security consultant at Rapid7 and one of the report's authors.

The Rapid7 researchers found serious security problems and design flaws in all of the cameras they tested. Some had hidden, unchangeable passwords, often listed in their manuals or online, that could be used to gain access. In addition, some of the devices didn't encrypt their data streams, or some of their web or mobile features, Stanislav says.

The problems with the cameras highlight the security risks associated with what's become known as the "Internet of things." Homes are becoming increasingly connected, with everything from TVs to slow cookers now featuring Wi-Fi connections. But many consumer devices often don't undergo rigorous security testing and could be easy targets for hackers.

And if a hacker has access to one connected device, he or she could potentially access everything tethered to that home's Wi-Fi network, whether it's a home computer storing personal financial information or a company's computer system that's being accessed by an employee working from home.

In the Rapid7 study, researchers rated the devices' security on a 250-point scale. The scores then received a grade of between "A" and "F." Of those tested, eight received an "F," while one received a "D." All of the camera manufactures were notified of the problems earlier this summer and some have taken steps to fix the problems.

"When one gets an 'F' and one gets a 'D minus,' there isn't an appreciable difference," Stanislav says. "And unlike a laptop where you can install firewalls and antimalware, you can't do that here."

For example, researchers noted that the Phillips In.Sight B120 baby monitor, which retails for about $78, had a direct, unencrypted connection to the Internet. That could allow a hacker watch its video stream online, as well as remotely access the camera itself and change its settings, the report says.

Phillips NV released a statement noting that the model in question has been discontinued. It added that its brand of video baby monitors is now licensed to Gibson Innovations, which is aware of the problems and it working on a software update designed to fix it.

The researchers also tested the iBaby and iBaby M3S, Summer Infant's Summer Baby Zoom WiFi Monitor & Internet Viewing System, Lens Peek-a-View, Gynoii, TRENDnet WiFi Baby Cam TV-IP743SIC, WiFiBaby WFB2015 and Withings WBP01.

Officials for iBaby and Lens Laboratories Inc. didn't immediately respond to requests for comment. A spokesman for Withings said he couldn't immediately comment on the report.

Summer Infant says in a statement saying that it's reviewing the report's findings and will make sure that the needed precautions are taken to protect its customers' security. Gynoii says that it's reaching out to Rapid7 in hopes of fixing the issues with its camera.

TRENDnet notes that physical access to its camera would be needed to exploit its security bug but it has prepared a patch and a software update will be available soon. And WiFiBaby released a statement defending its camera's security, noting that its latest software requires users to set their own unique password when they set up their camera.

Higher camera prices didn't translate to higher levels of security. In fact, the pricier models usually came with more features, which left unsecured could give hackers more ways to potentially access a camera or its video stream, Stanislav says.

In order to protect themselves, consumers should keep an eye out for any camera or mobile application updates. In addition, if parents still want to use a camera that's known to be susceptible to hackers, they should use it sparingly and unplug it when it's not in use, Stanislav says.

Citation: Report: Some top baby monitors lack basic security features (2015, September 2) retrieved 24 April 2024 from https://phys.org/news/2015-09-baby-lack-basic-features.html