Amazon Key delivery driver could knock out security camera, researchers show

November 21 2017, by Matt Day, The Seattle Times

A Seattle-based group of cybersecurity researchers has demonstrated a way to knock Amazon.com's new security camera offline, a capability that could enable malicious delivery drivers for the online retailer's new in-home delivery service to snoop around a house undetected.

Amazon Key, which became available to customers this month, gives Amazon delivery drivers one-time access to a residence to drop off a package. The program, designed to eliminate the theft of packages left outside a home and to open up the potential for remote authorization of other home services, is a test of whether consumers trust Amazon enough to give it access to their front doors.

It relies on two pieces of hardware: a smart lock, and Cloud Cam, which communicates with Amazon's servers to authorize the driver to unlock the door, and then records the delivery, beaming live or recorded video to a smartphone app to give the homeowner peace of mind.

Rhino Security Labs, a security research company, showed that it could exploit a weakness in the Wi-Fi protocol that Cloud Cam and many other devices use to communicate with their routers. A savvy hacker within Wi-Fi range can send a series of "deauthorization" commands to a specific device, temporarily severing its link to the internet.

In the case of Amazon's Cloud Cam, that means the camera would stop recording and sending images to Amazon's servers. A delivery driver who had already received approval to unlock the front door could,

before exiting and locking the door, roam inside without being recorded. Or, as demonstrated in a video posted by Rhino, leave the home and re-enter undetected.

Part of the problem, Rhino CEO Benjamin Caudill said, is that during such internet interruptions, Cloud Cam doesn't immediately go dark or tell the user it is offline. The company's test instead shows that the Cloud Cam smartphone app displays a still frame of the last image the camera saw before losing its connection, which could give the impression the device was functioning properly.

"You can do this multiple times over without any sort of alert or log at all," Caudill said. "Now I, as a bad guy, have blocked the signal and blocked your camera, and, unless you are specifically thinking this is an attack, there's no way for you to verify that this had happened," he said.

Amazon said in a statement that safety and security "are built into every aspect of the service," and reiterated that Amazon Key's delivery drivers, employed by contracting firms, have to pass comprehensive background checks.

"Every delivery is connected to a specific driver, and before we unlock the door for a delivery, Amazon verifies that the correct driver is at the right address, at the intended time," the company said.

Still, Amazon said it planned to issue a software update that will notify customers sooner if the camera goes offline during a delivery.

The company said its initial read on Rhino's findings were that they posed little risk to customers. The Wi-Fi vulnerability cannot unlock the front door, for example, and if a driver does act maliciously, Amazon would have a record of the individual and their vehicle. The company also reiterated the guarantee it offers for home services - a broad pledge

to help make things right if customers file a claim after something goes wrong.

Still, the discovery is a reminder that internet-connected devices like the Cloud Cam can be exploited by bad actors.

Some were skeptical of Amazon Key when it was introduced, raising the prospect of theft, damage to a home or lost pets.

Research firm Morning Consult found that 68 percent of U.S. adults it surveyed said they were not comfortable letting delivery drivers have access to their homes. Young people, the survey found, were most comfortable with the idea, with 33 percent of 18- to 29-year-olds saying they were comfortable with the idea, compared with just 14 percent of those over 65.

Amazon has a generally good reputation for cybersecurity, Caudill said, particularly for its cloud computing arm, Amazon Web Services.

But some in the security community were wary when Amazon Key was announced. "So we kind of set out fairly quickly to provide some tangible details" on the service's security, he said.

Caudill said the issue his team identified could be remedied if Cloud Cam stored video on the device itself if it lost internet connectivity. The camera's video recordings are now stored only on Amazon's servers for 24 hours to 30 days, depending on a customer's subscription plan.

Securing the growing number of internet-connected devices, like security cameras, stoves and garage-door openers, represents the biggest cybersecurity challenge since the advent of smartphones, Caudill said. "I think people are almost constantly taking risks they don't realize, because they think things like this don't happen," he said.