Issued 3/15/18

Your Smart Camera may have been Spying on You

At the Kaspersky Security Analyst Summit, researchers from the cybersecurity company said they discovered security flaws with Hanwha Techwin America's surveillance cameras. Vladimir Dashchenko, head of Kaspersky Lab's vulnerability research team, said there were 13 vulnerabilities with the cameras and how they connected online. These vulnerabilities could essentially let an attacker view footage from every Hanwha camera connected online, completely disable the camera, and also use it as a way to get inside your computer's network, Dashchenko said in a briefing with CNET before the announcement. The security flaws could allow an attacker to do whatever he wanted with the camera, the researcher said, including using it to mine for cryptocurrency. The company was originally owned by Samsung until the South Korean tech giant sold it to Hanwha Group in 2015. Kaspersky Lab's researchers looked at Hanwha's PNW SmartCam, which the company released when it was still owned by Samsung. While they tested only that camera, Dashchenko said, the vulnerabilities affected any camera the company made that was connected to its cloud servers. "Within a matter of days, our developers worked diligently to deliver solutions for the vulnerabilities cited by Kaspersky Lab and will provide an upcoming firmware update to remediate the concerns," a Hanwha spokeswoman said. "Remaining potential vulnerabilities are in the process of being fixed now." Hanwha's security cameras were exposed to remote attacks, in which someone could hack them from anywhere in the world, because of how they're hosted on cloud servers online, Dashchenko said. The company suffered from four vulnerabilities on its cloud network, to which all its smart cameras were connected. These cameras were connected to Hanwha's cloud

servers without the protection of a firewall. They also put all their cameras on one cloud server, instead of spreading them apart, Dashchenko said. The majority of smart cameras available are behind firewalls, making Hanwha's vulnerabilities stand out, the researcher said. Once Dashchenko's team broke through the network, it saw nearly 2,000 cameras connected online. There, he was able to access every connected camera, as well as tamper with their footage. He could change what a person was seeing, both in real time and on what was stored. In one attack, Dashchenko said they were able to "clone" a camera, showing one person a completely different camera's surveillance feed. An attacker would also be able to block your camera registration, which each owner has to complete after purchasing the device. "If it's blocked on the cloud, it's just a very pricey toy on your table. It doesn't work," Dashchenko said. The other nine vulnerabilities were on the camera itself. Dashchenko said they were able to exploit these attacks through the cloud, which meant they didn't need to be near the camera at all. Dashchenko's team also found a way to completely destroy the camera, to the point where they couldn't restore it themselves. Any personal information stored on the camera could also be stolen after Kaspersky Lab figured out how to decrypt its files. "If you want to connect your camera to any account, you need to add your username and password," Dashchenko said. "You can extract that from the configuration files of the camera. We found a way to decrypt passwords from its communications." Kaspersky Lab said it reported these vulnerabilities to Hanwha in December and most of them have been fixed.