Forbes / Security / #CyberSecurity

OCT 23, 2017 @ 10:20 AM 5,517

A Massive Number Of IoT Cameras Are Hackable -- And Now The Next Web Crisis Looms

Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms.

FOLLOW ON FORBES

FULL BIO RECENT POSTS POPULAR POSTS

I cover security and privacy for Forbes. I've been breaking news and writing features on these topics for major publications since 2010. As a freelancer, I worked for The Guardian, Vice Motherboard, Wired and BBC.com, amongst many others. I was named BT Security Journalist of the year in 2012 and 2013 for a range of exclusive articles, and in 2014 was handed Best News Story for a feature on US government harassment of security professionals. I like to hear from hackers who are breaking things for either fun or profit and researchers who've uncovered nasty things on the web. You can email me at TFox-Brewster@forbes.com, or tbthomasbrewster@gmail.com. If you are worried about prying eyes, here's my PGP fingerprint for the Gmail address: 19A0 3F37 B3B7 4C1E C1D1 9AA4 5E37 654C 1660 B817

Hackable CCTV cameras pose a real threat, not just to the devices themselves, but the stability of the web in general. (Photo by Oli Scarff/Getty Images)

Anyone who remembers the Mirai botnet, used to cause widespread internet outages in 2016, might have been forgiven for thinking progress had been made to prevent a similar disaster. But a mysterious botnet, dubbed the "IoT Reaper," has ballooned in recent days by taking advantage of the same vulnerable, internet-connected cameras as Mirai did. And as cybersecurity experts warn the Reaper could be a bigger threat than its forbears, *Forbes* has seen firsthand how hacking a CCTV camera can be used not just for web destruction, but Ocean's 11-style machinations.

In a demonstration hack, Leigh-Anne Galloway, cybersecurity resilience lead at Positive Technologies, abused a flaw in cameras containing code from Chinese manufacturer Dahua. That company's software can be found, and possibly tampered with, in just over 400,000 devices, as shown on the IoT search engine Shodan. In seconds, Galloway's exploit allowed her to quickly switch out the real feed for another. It's not hard to imagine high-tech heists being made significantly easier with such a quick and dirty hack of a CCTV camera.

While the vulnerability was patched with a firmware update back in July, and the US Computer Emergency Response Team put out an alert, Galloway doesn't think many would have updated, as was the case with Mirai.

She also pointed out that updating is a manual process, one that requires the user to find out whether they're vulnerable, before downloading and installing the refreshed software. Unlike with devices from major manufacturers like Apple and Google, users won't be alerted to problems with their cameras, nor is it as simple as clicking a button.

The Reaper

That demonstration took place back in September, long before the emergence of the Reaper, which was brought to light by researchers at Chinese firm Qihoo 360 and Israeli company Check Point on Friday. It dates back to at least September, however.

Rather than trying easy-to-guess default passwords on a large number of digital video recorders (DVRs) to propagate as Mirai did, Reaper fires exploit code at vulnerabilities in similar devices, as well as network video recorders (NVRs), IP cameras and home routers. They include products from D-Link, Netgear and

Linksys, amongst others. Cybersecurity researchers have estimated as many as 2 million devices are vulnerable to the kinds of exploits Reaper has targeted.

The Reaper, which borrowed some code from the Mirai malware, penetrates systems via older weaknesses than the Dahua flaw, but is being updated by its as-yet unknown master and could soon include fresh attacks. "IoT Reaper has the potential to be much more powerful than Mirai," warned Ken Munro, partner at Pen Test Partners, which has been tracking the threats posed by web-connected cameras of late. "IoT Reaper is also a bit simple – I suspect others will refine it shortly and make it even more effective."

Mystery remains around the purpose of the IoT botnet. For now, it's unclear what the Reaper's owners plan to do with their beast. Nor is it known precisely how many bots make up the botnet. "We are currently seeing approximately 30,000 devices participating in this botnet and assume that this is a narrow prism of the network which could be of a much larger scale -- a tenfold will make sense," said Maya Horowitz, threat intelligence group manager at Check Point.

Horowitz said the most obvious use for Reaper would be a distributed denial of service (DDoS) attack, à la Mirai. "Such an attack could either be for the sake of general chaos, or more targeted at a specific country," she added.

Got a tip? Email at TFox-Brewster@forbes.com or tbthomasbrewster@gmail.com for PGP mail. Get me on Signal on +447837496820 or use SecureDrop to tip anyone at Forbes.