Hacked CCTV Cameras Used To Launch DDoS

A security firm has warned that Internet-connected devices such as CCTV cameras are being hacked with increasing frequency, allowing them to be taken into botnets and used to carry out attacks.

Such so-called Internet of Things (IoT) devices are prime targets for hackers, in part because their users often have little awareness of security. Once hacked, the devices can be used, for instance, to help carry out Distributed Denial of Service (DDoS) attacks, which draw on large numbers of devices to direct waves of traffic at a target site with the intention of making the target inaccessible.

IoT assault

Internet-connected CCTV cameras are one of the most vulnerable IoT devices, according to security firm Incapsula, due in part to the large number deployed. About 245 million professionally installed surveillance cameras were operating worldwide last year, according to figures from research firm IHS Technology, but Incapsula estimated there are "millions" more that have been set up on an ad-hoc basis.

Research firm IDC anticipates there will be more than 28 billion IoT devices installed by 2020.

Incapsula said it saw a 240 percent increase in malicious traffic on its network in March of last year, most of it originating from compromised CCTV cameras, and more recently the company found that one of its customers was being subjected to a repeated HTTP flood attacks powered by compromised cameras. Incapsula operates a cloud-based security platform.

About 900 cameras were being used to attack an unnamed "large cloud service" with millions of users, Incapsula said.

All of the compromised devices were running embedded Linux with a utilities package called BusyBox, the company said in a blog post. They were infected with ARM malware called (.btce) that specifically scans for devices running BusyBox that are susceptible to password-guessing "dictionary attacks", Incapsula said.

CCTV compromise

In this case, however, such an attack wasn't necessary, since all of the devices involved were accessible using their default login credentials, according to Incapsula. The lack of security meant, unsurprisingly, that the devices involved had, in almost every case, been hacked by several different invdividuals.

"This goes to show just how easy it is to locate and exploit such unsecured devices," wrote Incapsula's Ofer Gayer, Or Wilder and Igal Zeifman in the post.

The cameras involved were spread around the world, with particularly large numbers from India

(169), Latin America and Eastern Europe.

By coincidence, one of the infected devices was located at a shop five minutes from Incapsula's offices, the company said in its blog post. The location of the offices wasn't mentioned, but Gayer's Twitter profile indicates he is based in Israel, where Incapsula operates a Tel Aviv office.

"We were able to meet with the store owners, show them how their CCTV cameras were abused to attack our clients and help them clean the malware from the infected camera's hard drive," wrote Gayer, Wilder and Zeifman. "As we did, we witnessed it coughing out attacking requests up to the very last moment."

The incident illustrates the dangers posed by large numbers of Internet-connected devices for which basic security precautions – such as changing the default access password – haven't been taken, according to Incapsula.

"Whether it is a router, a Wi-Fi access point or a CCTV camera, default factory credentials are there only to be changed upon installation," the company wrote.

A study released in August found that up to 68 percent of IT professionals believe business efficiency requirements are forcing their organisations to adopt IoT devices in spite of the security risks.