Issued 5/11/17

New IoT Malware Spreading Worldwide Infecting Vulnerable Cameras

A brand new IoT malware was discovered spreading like wildfire, infecting over 100,000 Internet-connected cameras already. Called Persirai, the new malware has been working on infecting Chinese-made wireless cameras since April, cyber security company Trend Micro said.

The malware managed to infect so many devices by exploiting flaws in the cameras reported back in March. Then, Pierre Kim, a security researcher, discovered that numerous wireless cameras were affected by a vulnerability that allowed attackers to remotely execute code, making for a highly effective hijack. According to his claim, at least 1,250 camera models produced by a Chinese manufacturer carry the bug, which means there are plenty more cameras that could get hacked. Over the past month, Trend Micro says it noticed a new malware spreading by exploiting those very same products that were affected by the reported vulnerability. According to the company, after running a Shodan search, there are about 120,000 cameras vulnerable to the malware.

The purpose of this malware, it seems, to infect these cameras and form a botnet, much like it always happens with IoT malware. These botnets can be used to carry DDoS attacks in order to force sites offline. So far, the botnet Persirai hasn't been used for any website attacks, but that's mostly because it seems like its creators are still testing the waters. An interesting fact about this malware, Trend Micro notes, is the fact that once it infects a device, it blocks anyone else from exploiting the same vulnerabilities. While it carries a different code, it does borrow some certain functions from Mirai, namely to scan the Internet for new devices to infect.

The name of the manufacturer has not been released and will remain undisclosed until the patch is published. "Since all consumer grade IP cameras I am aware of do not use secure (certificate based) authentication, along with the inordinate number of known vulnerabilities found in such devices, I believe it is just a matter of time before all cameras globally fall prey to such attacks. I also believe the time is very short," said Mike Ahmadi, global director - critical systems security, at Synopsys.