Botnet Targets Millions of "Smart" and Internet of Things Video Recorders, Thermal Cameras, and Routers

Botnet Targets Millions of "Smart" and Internet of Things Video Recorders, Thermal Cameras, and Routers

by BN Frank
April 23, 2020

All wireless, "Smart" and IoT devices are vulnerable to hacking. This includes medical devices and electric, gas, and water utility smart meters (see 1, 2). The media frequently reports about adults and children being spied on and harassed through baby monitors (see 1, 2) and other home devices (see 1, 2, 3, 4). Cybersecurity experts and even 5G proponents continue to warn against 5G / IoT vulnerability.

From *TechRadar* on one of the most recent threats:

> *dark_nexus has already seen 30 version updates*
>
> *Researchers have identified a new botnet that looks to infect common smart IoT devices like video recorders, thermal cameras and routers.*
>
> *This botnet, known as dark_nexus, is capable of launching a range of various DDoS attacks, spreading multiple malware strains, and can infect devices running on 12 different CPU architectures.*
>
> *According to researchers at Bitdefender, who has been tracking this botnet for the last three months, the botnet*

has already infected over a thousand devices already and is now spreading.

Read full article

Wired Ethernet connections have always been recommended by both security experts AND health experts. **In fact, American Academy of Pediatrics and other health experts have warned for many years that children are especially vulnerable to exposure to wireless – 5G, Bluetooth, cell phone and WiFi radiation.** Despite the warnings, there is still NO safe level that has been scientifically determined for kids or pregnant women.

Research has determined that wireless exposure can cause increased cancer risk (see 1, 2) and much more for humans of all ages and our furry friends. So why risk it when you can go wired instead?

https://youtu.be/lCIAcZov5Hs