FIREDOME

Targeted Hack Hijacks Full Fleet of 11,000 Xiaomi Pet Feeders

In September 2019, the website "hackday" published an article disclosing new vulnerabilities targeting devices running FreeRTOS (ESP8266 espressif), with the author explaining: "We've always wondered when we'd see the first ESP8266 attacks in the wild, and that day has finally come." They had no idea how right they were, as a month later the first attack against an IoT manufacturer using those vulnerabilities was published.

Xiaomi, in collaboration with the company Furrytail, launched a crowdfunding project consisting of an Internet-connected, app-controlled pet feeders, which were sold on Youpin, Xiaomi's official store and Aliexpress. Russian security researcher Anna Prosvetova discovered API and firmware issues that allowed her to **take over all 11,000 deployed Xiaomi FurryTail pet feeders:**

"While studying the feeder API, I discovered some records that run on the screen of any of these devices, as well as ***data on the WiFi networks of the people*** *who bought them." she explained. "After a couple of clicks I was able to feed any dog or cat, although it also has a malicious use, as it is possible to delete the schedules programmed by the user,* ***which would leave the pets without food."***

The vulnerabilities found in Xiaomi's API allows access to the devices without authentication, allowing an attacker to take control of all the online devices and change their feeding programs. In addition, he/she would be able to see the WiFi data transmitted over the networks the devices are connected to.

FreeRTOS, an open-source Internet of Things operating system used by Amazon.com, among others, was recently found to have 13 vulnerabilities. Some of these result in flaws related to remote code execution:

- 4 remote code execution bugs
- 1 denial of service
- 7 information leak
- another security problem which is yet undisclosed

The FreeRTOS kernel is a market-leading real-time operating system (or RTOS), and the de-facto standard solution for microcontrollers and small microprocessors (according to freertos.org). Having those vulnerabilities unpatched or having no proactive security solution to mitigate the unknown ones allows hackers to potentially brick & hijack entire fleets of IoT devices, such as the one mentioned in this article.

The device uses a WIFI chip named ESP8266, which has known vulnerabilities that allow data collection, disabling or bricking the device, DoS attack and could lead to the flashing of malicious firmware that could open a backdoor, install a botnet agent (malware), use it as a spam service or other malicious activities.

What Could Have Been Done To Detect & Mitigate an Attack?

With the Firedome platform, monitoring the fleet with the "eagle's view" approach, an attacker trying to exploit these vulnerabilities and hijack the device base would be detected and blocked. Firedome's Endpoint Protection agent for FreeRTOS (including ESP8266 devices), together with its Cloud AI engine, enables the platform to detect & block suspicious and malicious activities during the entire attack's kill chain:

In the reconnaissance phase of the attack, they scan the internet for the FurryTail devices and their open ports, then it would try to exploit the entire discovered device base using the mentioned vulnerabilities (trying to crash the devices / sniffing network traffic, etc).

The agent blocks the attack before it can get past this phase in the Cyber Kill Chain using the below actions:

1. The platform identifies a new suspicious activity coming in from the attacker's infrastructure (IP / domains)
2. Firedome's Cloud AI assesses the source with its *IoT Threat Intelligence Engine*, enriching knowledge about the threat source
3. The *port scanning* activity is detected and reported
4. These indicators allow the platform to automatically deploy protection rules against the threat source, protecting the fleet before the attacker ever reached them

The platform can also identify abnormal activity across the entire device base's operational behavior, detecting devices that suddenly stop communicating or become unreachable (disconnected), that suffer from network problems (jittering), and that frequently crash and restart. Once this behavior is detected, the running agent can restore the device to a normal safe state by executing its fail-safe feature.

And yes sweet kitten, with Firedome installed, you won't have to starve (due to hacking at least, Firedome can not protect against owners who forget to program your meals)!

