Check Point Research shows DSLR camera vulnerabilities

August 13 2019, by Nancy Cohen

A security researcher took advantage of vulnerabilities in a protocol used in digital cameras to infect ransomware into a DSLR camera over a rogue WiFi connection.

Ionut Ilascu in *BleepingComputer* reported on August 11 that flaws were discovered in the implementation of the Picture Transfer Protocol (PTP)

in a Canon camera offering exploit options for attacks. "The final stage of an attack would be a complete takeover of the device, allowing hackers to deploy any kind of malware on the camera."

Eyal Itkin at Israel-based firm Check Point found that the way cameras transfer information – the Picture Transfer Protocol (PTP) – could be exploited. A device such as a laptop uses PTP to ask the camera for pictures and other information such as battery level, and the camera responds with the requested information.

BleepingComputer said Itkin was not only able to build an exploit that worked over both USB and WiFi but also found a way to encrypt files on the camera's storage card, using the same cryptographic functions used for the firmware update process.

Check Point Research issued a video on "Ransomwaring a DSLR camera" that shows an exploit in action purposed for the end results of ransomware installed and the camera locked. Check Point disclosed the vulnerabilities responsibly to Canon. The two companies worked together to fix the issues, said *BleepingComputer*.

Vulnerabilities would allow a takeover of a DSLR camera through both WiFi and USB. Such an infection could, for example, be used for installing a Ransomware and demanding ransom for both the images and the camera itself.

Meanwhile, at Check Point Research, "Say Cheese: Ransomware-ing a DSLR Camera" was the headline in a blog where Eyal Itkin explained the Check Point journey to test if hackers could hit. Itkin posed a question, "Imagine how would you respond if attackers inject ransomware into both your computer and the camera, causing them to hold all of your pictures hostage unless you pay ransom."

He touched upon two potential avenues for attackers: USB – For an attacker that took over your PC, and wants to propagate into your camera; and WiFi – "An attacker can place a rogue WiFi access point at a tourist attraction, to infect your camera."

All in all, Itkin pointed that out: Any "smart" device, in their case a DSLR camera, is susceptible to attacks. However, the "combination of price, sensitive contents and wide-spread consumer audience makes cameras a lucrative target for attackers."

How did the protocol enable an exploit?

"Modern DSLR cameras no longer use film to capture and later reproduce images. Instead, the International Imaging Industry Association devised a standardised protocol to transfer digital images from your camera to your computer. This protocol is called the Picture Transfer Protocol (PTP). Initially focused on image transfer, this protocol now contains dozens of different commands that support anything from taking a live picture to upgrading the camera's firmware," Eital stated.

Simulating attackers, the researchers wanted to find implementation vulnerabilities in the protocol, hoping to leverage them in order to take over the camera. "Such a Remote Code Execution (RCE) scenario will allow attackers to do whatever they want with the camera, and infecting it with Ransomware is only one of many options."

Why single out Canon? They chose to focus on Canon's EOS 80D DSLR camera, as "the largest DSLR maker, controlling more than 50% of the market."The EOS 80D supports both USB and WiFi and Canon has an extensive "modding" community, called Magic Lantern.

One important takeaway, despite using Canon center-stage, is that the

weaknesses do not solely reside with the Canon brand. It is the Picture Transfer Protocol (PTP).

"During our research we found multiple critical vulnerabilities in the Picture Transfer Protocol as implemented by Canon. Although the tested implementation contains many proprietary commands, the protocol is standardized, and is embedded in other cameras. Based on our results, we believe that similar vulnerabilities can be found in the PTP implementations of other vendors as well."

On August 6, Canon issued this statement, regarding the security advisory for Canon digital cameras related to PTP (Picture Transfer Protocol) communication functions and firmware update functions.

"An international team of security researchers has drawn our attention to a vulnerability related to communications via the Picture Transfer Protocol (PTP)...as well as a vulnerability related to firmware updates... Due to these vulnerabilities, the potential exists for third-party attack on the camera if the camera is connected to a PC or mobile device that has been hijacked through an unsecured network. At this point, there have been no confirmed cases of these vulnerabilities being exploited to cause harm, but ... we would like to inform you of the following workarounds for this issue."

Canon then listed its advice:

Ensure the suitability of security-related settings of devices connected to the camera; do not connect the camera to a PC or mobile device in an unsecure network, e.g., free Wi-Fi environment; do not connect the camera to a PC or mobile device potentially exposed to virus infections; disable the camera's network functions when not being used; download the official firmware from Canon's website when performing a camera firmware update; check the website "of the Canon sales company in your

region for the latest information regarding firmware designed to address this issue."