Even DSLR cameras can be easily attacked by ransomware

Ransomware, also known collectively as ransom data encryption software, has become one of the major security threats to all computer systems worldwide in recent years. .

Ransomware, also known collectively as ransom data encryption software, has become one of the major security threats to all computer systems worldwide in recent years. .

Ransomware has caused billions of dollars in damage each year, and the list of victims of this type of malware extends across all areas, from personal computers, businesses, to government agencies and organizations. , public services . In other words, every computer system in the world is at risk of becoming a victim of ransomware.

1. Ransomware (ransomware) is showing signs of explosion worldwide, paying is no longer the most effective option.

Ransomware - data ransom data encryption

But recently, security researchers have even discovered that a seemingly 'irrelevant' device could also be at risk with ransomware: DSLR cameras.

Check Point Software Technologies, one of the most reputable security organizations in the world, recently released a detailed report on how their security researchers can install malware remotely, specifically, this is the software for encrypting extortion, on digital DSLR cameras. In it, Itkin researcher Eyal has discovered that a 'skilled' hacker can easily infect malware through modern digital cameras.

1. No More Ransom - the flag of the war against ransomware

According to Itkin's Eyal, Picture Transfer Protocol, which is commonly used on most digital camera models today, is in fact an ideal tool for hackers. distributing malware. The reason is that this protocol is not authentic and can be used with both WiFi and USB.

In addition, the Check Point report also noted that individuals who own Wi-Fi hotspots that have been infected with malware are mostly unaware, and this Wi-Fi access point may be use as a vector to infect malicious devices connected to it, including desktop computers, laptops, smartphones, tablets, and especially DSLR cameras.

Also in the report, Eyal Itkin released a video showing how to exploit the Canon E0S 80D camera via Wi-Fi and encrypt images on the SD card so that users cannot access them. In addition, the researcher noted that in the future, cameras may become a particularly attractive target for hackers: This device contains an important, extremely suitable data type to used in blackmail activities, that is the image. In a real ransomware attack, hackers will ask victims to pay some money in exchange for decrypting files that have been encrypted by them. This amount is usually not too large and within the victims' range, so most people often choose to pay the ransom to get rid of the inconvenience.

1. The official GandCrab 5.2 decoder was released, ending the bad nightmare called GandCrab Ransomware

Canon E0S 80D can be hacked via Wi-Fi and encoded images on SD card

In a related move, Check Point said it had sent all of the E0S 80D security vulnerability information to Canon since March, and the two parties began to work together to develop the patch to be sent. user. From this incident, it can be seen that not only Canon products but also from all other major camera manufacturers can hide similar security holes, by the mechanism of image transfer between machines DSLR images are often similar.

Last week, Canon issued a security recommendation, asking customers to avoid connecting the camera to unsecured Wi-Fi networks, turning off the camera's network functions when not in use, and at the same time.

Update and install the latest security patches for your device to ensure safety.

1. [Infographic] 7 effective ways to protect businesses from Ransomware

Please update your camera to the latest software version

That is also the general advice that we want to send to readers who own DSLR cameras in general. Please update the device software to the latest version!

You finished reading the article "**Even DSLR cameras can be easily attacked by ransomware**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
