Security researchers find that DSLR cameras are vulnerable to ransomware attack

Ransomware has become a major threat to computer systems in recent years, as high-profile attacks have locked users out of personal computers, hospitals, city governments, and even The Weather Channel. Now, security researchers have discovered that another device that might be at risk: a DSLR camera.

Check Point Software Technologies issued a report today that detailed how its security researchers were able to remotely install malware on a digital DSLR camera. In it, researcher Eyal Itkin found that a hacker can easily plant malware on a digital camera. He says that the standardized Picture Transfer Protocol is an ideal method for delivering malware: it's unauthenticated and can be used with both Wi-Fi and USB. The report notes that individual with an infected Wi-Fi access point could deploy it at a tourist destination to pull off an attack, or infect a user's PC.

cameras could be a particularly juicy target for hackers
In a video, Itkin shows off how he were able to exploit a Canon E0S 80D over Wi-Fi and encrypt the images on the SD card so that the user wouldn't be able to access them. He also notes that cameras could be a particularly juicy target for hackers: they're full of personal images that most people likely won't want to walk away from. In a real ransomware attack, a hacker will typically demand a small amount of money in exchange for the key that will decrypt the files – usually a small enough amount that people would rather just pay to get

rid of the inconvenience.

Check Point says that it disclosed the vulnerability to Canon back in March, and the two began work in May to develop a patch. Last week, Canon issued a security advisory, telling people to avoid using unsecured Wi-Fi networks, to turn off its network functions when it’s not being used, and to update and install a new security patch onto the camera itself. Itkin says that he only worked with a Canon device, but tells *The Verge* that “due to the complexity of the protocol, we do believe that other vendors might be vulnerable as well, however it depends on their respective implementation.”

https://www.theverge.com/2019/8/11/20800979/check-point-canon-eos-80d-dslr-malware-ransomware-cybersecurity