Los ataques con ransomware son cada vez más frecuentes a medida que el enfoque de los atacantes ahora se mueve más allá de las computadoras a teléfonos inteligentes y otros dispositivos conectados a Internet.

Los investigadores de seguridad de CheckPoint demostraron lo fácil que resulta para los hackers infectar remotamente una cámara digital DSLR con ransomware y retener fotos y videos privados como rehenes hasta que las víctimas paguen un rescate.

El investigador Eyal Irkin descubrió varias vulnerabilidades de seguridad en el firmware de las cámaras Canon que pueden explotarse por medio de USB y WiFi, lo que permite a los atacantes comprometer y hacerce cargo de la cámara y sus funciones.

Según un aviso de seguridad publicado por Canon, las fallas de seguridad reportadas afectan a las cámaras digitales SLR y EOS-Series, PowerShot SX740 HS, PowerShot SX70 HS y PowerShot G5X Mark II.

> *«Imaginate cómo respondería si los atacantes inyectaran ransomware tanto en su computadora como en la cámara, haciendo que retengan todas sus imágenes como rehenes a menos que se pague un rescate»*, dijo Itkin.

Canon DSLR PTP y vulnerabilidades de firmware

Todas estas vulnerabilidades, enumeradas a continuación, residen en la forma en que Canon implementa el Protocolo de transferencia de imágenes (PTP) en su firmware, un protocolo estándar que las cámaras DSLR modernas utilizan para transferir archivos entre la cámara y la computadora o dispositivos móviles por medio de cable USB o de forma inalámbrica.

Además de la transferencia de archivos, el Protocolo de Transferencia de Imágenes también admite docenas de comandos para manejar de forma remota muchas otras tareas en la cámara, desde tomar fotos en vivo hasta actualizar el firmware de la cámara, muchas de las cuales se encontraron vulnerables.

- CVE-2019-5994: Desbordamiento de búfer en SendObjectInfo
- CVE-2019-5998: Desbordamiento de búfer en NotifyBtStatus
- CVE-2019-5999: Desbordamiento de búfer en BLERequest
- CVE-2019-6000: Desbordamiento de búfer en SendHostInfo
- CVE-2019-6001: Desbordamiento de búfer en SetAdapterBatteryReport
- CVE-2019-5995: Actualización silenciosa de firmware malicioso

Itkin descubrió que las operaciones PTP de Canon no requieren autenticación ni usan cifrado de ninguna forma, lo que permite a los atacantes comprometer la cámara DSLR en los siguientes escenarios:

Vía USB: El malware que ya ha comprometido la PC puede propagarse a su cámara tan pronto como lo conecte a su computadora mediante un cable USB.

Vía WiFI: Un atacante que esté cerca de una cámara réflex digital específica puede configurar un punto de acceso WiFi no autorizado para infectar la cámara.

> *«Esto se puede lograr fácilmente analizando primero la red y luego simulando que el AP tiene el mismo nombre que el que la cámara intenta conectar de forma automática. Una vez que el atacante se encuentra dentro de la misma LAN que la cámara, puede iniciar la explotación»,* explicó Itkin.

Explotación de la falla DSLR de Canon para implementar ransomware por aire

Como prueba de concepto, el investigador explotó con éxito una de estas vulnerabilidades que les permitió impulsar e instalar una actualización de firmware malicioso en una cámara DSLR específica por medio de WiFi, sin que la víctima requiera interacción.

Como se muestra en el video, el firmware malicioso se modificó para encriptar todos los archivos de la cámara y mostrar una demanda de rescate en su pantalla utilizando las

mismas funciones AES incorporadas que Canon utiliza para proteger su firmware.

> *«Hay un comando PTP para una actualización remota de firmware, que requiere cero interacción del usuario. Esto significa que incluso si todas las vulnerabilidades de implementación están parcheadas, un atacante puede infectar la cámara usando un archivo de actualización de firmware malicioso»,* explicó el investigador.

Un verdadero ataque de ransomware de este tipo es una de las mayores amenazas para tus recuerdos, donde los hackers generalmente pueden exigir dinero a cambio de la clave para descifrar las fotos, videos y archivos de audio.

La responsabilidad de los investigadores reportó estas vulnerabilidades a Cannon en marzo de este año. Sin embargo, la compañía actualmente solo ha lanzado un firmware actualizado para el modelo Canon EOS 80D y recomendó a los usuarios de otros modelos afectados que sigan las prácticas básicas de seguridad hasta que los parches para sus dispositivos estén disponibles.

Para obtener más detalles sobre las vulnerabilidades en los modelos de cámara Canon, puede dirigirse al informe de CheckPoint publicado ayer.