Security cameras are vulnerable to attacks using infrared light: study

19 September 2017

Ben-Gurion University of the Negev (BGU) researchers have demonstrated that security cameras infected with malware can receive covert signals and leak sensitive information from the very same surveillance devices used to protect facilities.

The method, according to researchers, will work on both professional and home security cameras, and even LED doorbells, which can detect infrared light (IR), not visible to the human eye.

In the new paper, the technique the researchers have dubbed "aIR-Jumper" also enables the creation of bidirectional, covert, optical communication between air-gapped internal networks, which are computers isolated and disconnected from the internet that do not allow for remote access to the organization.

The cyber team led by Dr. Mordechai Guri, head of research and development for BGU's Cyber Security Research Center (CSRC), shows how IR can be used to create a covert communication channel between malware installed on an internal computer network and an attacker located hundreds of yards outside or even miles away with direct line of sight. The attacker can use this channel to send commands and receive response messages.

To transmit sensitive information, the attacker uses the camera's IR-emitting LEDs, which are typically used for night vision. The researchers showed how malware can control the intensity of the IR to communicate with a remote attacker that can receive signals with a simple camera without detection. Then the attacker can record and decode these signals to leak sensitive information.

The researchers shot two videos to highlight their technique. The first video shows an attacker hundreds of yards away sending infrared signals to a camera. The second video shows the camera infected with malware responding to covert signals by exfiltration data, including passwords.

According to Dr. Guri, "Security cameras are unique in that they have 'one leg' inside the organization, connected to the internal networks for security purposes, and 'the other leg' outside the organization, aimed specifically at a nearby public space, providing very convenient optical access from various directions and angles."

Attackers can also use this novel covert channel to communicate with malware inside the organization. An attacker can infiltrate data, transmitting hidden signals via the camera's IR LEDs. Binary data such as command and control (C&C) messages can be hidden in the video stream, recorded by the surveillance cameras, and intercepted and decoded by the malware residing in the network.

"Theoretically, you can send an infrared command to tell a high-security system to simply unlock the gate or front door to your house," Guri says.

More information: aIR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras &

Infrared (IR), arXiv:1709.05742 [cs.CR]
arxiv.org/abs/1709.05742

Provided by American Associates, Ben-Gurion University of the Negev

APA citation: Security cameras are vulnerable to attacks using infrared light: study (2017, September 19) retrieved 18 June 2019 from https://phys.org/news/2017-09-cameras-vulnerable-infrared.html