aIR-Jumper: Covert Air-gap Exfiltration/ Infiltration via Security Cameras & Infrared

Researchers

Dr. Mordechai Guri
moti.guri@gmail.com

Dr. Dima Bykhovsky
dmitrby@ac.sce.ac.il

Prof. Yuval Elovici
elovici@inter.net.il

Publications

M. Guri, D. Bykhovsky, and Y. Elovici, "aIR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras & Infrared," 2017. arXiv:1709.05742.

Demo Videos

Infiltration: https://www.youtube.com/watch?v=auoYKSzd0j4

Exfiltration: https://www.youtube.com/watch?v=om5fNqKjj2M

Goals

Infrared (IR) light is invisible to humans, but cameras are optically sensitive to this type of light. We show how attackers can use surveillance cameras and infrared light to establish bi-directional covert communication between the internal networks of organizations and remote attackers. We present two scenarios: exfiltration (leaking data out of the network) and infiltration (sending data into the network).

Description

Exfiltration: Surveillance and security cameras are equipped with IR LEDs, which are used for night vision. In the exfiltration scenario, malware within the organization accesses the surveillance cameras across the local network and controls the IR illumination. Sensitive data such as PIN codes, passwords, and encryption keys are then modulated, encoded, and transmitted over the IR signals.

Infiltration: In an infiltration scenario, an attacker standing in a public area (e.g., in the street) uses IR LEDs to transmit hidden signals to the surveillance camera(s). Binary data such as command and control (C&C) and beacon messages are encoded on top of the IR signals.

The exfiltration and infiltration can be combined to establish bidirectional, 'air-gap' communication between the compromised network and the attacker. We implement a malware prototype and present data modulation schemas and a basic transmission protocol. Our evaluation of the covert channel shows that data can be covertly exfiltrated from an organization at a rate of 20 bit/sec per surveillance camera to a distance of tens of meters away. Data can be covertly infiltrated into an organization at a rate of over 100 bit/sec per surveillance camera from a distance of hundreds of meters to kilometers away.