AirHopper: Bridging the Air-gap Between Isolated Networks and Mobile Phones Using Radio Frequencies

Researchers

Dr. Mordechai Guri
moti.guri@gmail.com

Matan Monitz
mmonitz@gmail.com

Gabi Kedma
gabikedma@hotmail.com

Assaf Kachlon
assafka@post.bgu.ac.il

Prof. Yuval Elovici
elovici@inter.net.il

Publications

M. Guri, M. Monitz, and Y. Elovici, "Bridging the Air Gap between Isolated Networks and Mobile Phones in a Practical Cyber-Attack," ACM Transactions on Intelligent Systems and Technology (TIST), Special Issue: Cyber Security, Vol. 8, Issue 4, 2017.

G. Kedma, A. Kachlon and Y. Elovici, "AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies," 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE), Fajardo, PR, 2014.

Demo video

https://www.youtube.com/watch?v=2OzTWiGl1rM&t=20s

Goals

Information is the most critical asset of modern organizations, and accordingly coveted by adversaries. When highly sensitive data is involved, an organization may resort to air-gap isolation, in which there is no networking connection between the inner network and the external world. While infiltrating an air-gapped network has been proven feasible, data exfiltration from an air-gapped network is still considered to be one of the most challenging phases of an advanced cyber-attack. We present 'AirHopper', a bifurcated malware that bridges the air-gap between an isolated network and nearby infected mobile phones using FM signals.

Description

While it is known that software can intentionally create radio emissions from a video display unit, this project was the first time that mobile phones were considered in an attack model as the intended receivers of maliciously crafted radio signals. We examine the 'AirHopper' attack model and its limitations, and discuss implementation considerations such as stealth and modulation methods. We tested AirHopper in an existing workplace at a typical office building and demonstrated how valuable textual and binary data, such as keylogging and files can be exfiltrated from physically isolated computer to mobile phones at a distance of 1-7 meters, with effective bandwidth of 13-60 Bps (Bytes per second).