GSMem: Data Exfiltration from Air-gapped Computers over GSM Frequencies

Researchers

Dr. Mordechai Guri
moti.guri@gmail.com

Assaf Kachlon
assafka@post.bgu.ac.il

Ofer Hasson
hassonofer@gmail.com

Gabi Kedma
gabikedma@hotmail.com

Yisroel Mirsky
yisroel@post.bgu.ac.il

Prof. Yuval Elovici
elovici@inter.net.il

Publications

M. Guri, A. Kachlon, O. Hasson, G. Kedma, Y. Mirsky, and Y. Elovici, "GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies," 24th USENIX Security Symposium, Washington DC, 2016.

Demo video

https://www.youtube.com/watch?v=RChj7Mg3rC4

Goals

Air-gapped networks are isolated, separated both logically and physically from public networks. Although the feasibility of invading such systems has been demonstrated in recent years, exfiltration of data from air-gapped networks is still a challenging task. We present GSMem, a malware that can exfiltrate data through an air-gap over cellular frequencies.

Description

We demonstrate how rogue software on an infected target computer modulates and transmits electromagnetic signals at cellular frequencies by invoking specific memory-related instructions and utilizing the multichannel memory architecture to amplify the transmission. Furthermore, we show that the transmitted signals can be received and demodulated by a rootkit placed in the baseband firmware of a nearby cellular phone. We present crucial design issues, such as signal generation and reception, data modulation, and transmission detection. We implement a prototype of GSMem consisting of a transmitter and a receiver and evaluate its performance and limitations. Our current results demonstrate its efficacy and feasibility, achieving an effective transmission distance of 1-5.5 meters with a standard mobile phone. When using a dedicated, yet affordable hardware receiver, the effective distance reached over 30 meters.