LED-it-GO: Leaking (a lot of) Data from Air-gapped Computers via the (small) Hard Drive LED

Description

We present a method which allows attackers to covertly leak data from isolated, air-gapped computers. Our method utilizes the hard disk drive (HDD) activity LED which exists in most of today's desktop PCs, laptops and servers. We show that a malware can indirectly control the HDD LED, turning it on and off rapidly (up to 5800 blinks per second), a rate that exceeds the visual perception capabilities of humans. Sensitive information can be encoded and leaked over the LED signals, which can then be received remotely by different kinds of cameras and light sensors. Compared to other LED methods, our method is unique, because it is also covert: The HDD activity LED routinely flickers frequently, and therefore the user may not be suspicious to changes in its activity.

We discuss attack scenarios and present the necessary technical background regarding the HDD LED and its hardware control. We also present various data modulation methods and describe the implementation of a user-level malware that doesn't require a kernel component. We examined the physical characteristics of different colored HDD LEDs (red, blue, and white) and tested different types of receivers: remote cameras, extreme cameras, security cameras, smartphone cameras, drone cameras, and optical sensors. Our experiment shows that sensitive data can be successfully leaked from air-gapped computers via the HDD LED at a maximum bit rate of 4000 bits per second, depending on the type of receiver and its distance from the transmitter. Notably, this speed is 10 times faster than the existing optical covert channels for air-gapped computers. These rates allow fast exfiltration of encryption keys, keystroke logging, and text and binary files. Finally, we also discuss hardware and software countermeasures for such a threat.

Researchers

Dr. Mordechai Guri
moti.guri@gmail.com

Boris Zadov
borisza@gmail.com

Eran Atias
eran_ats@walla.co.il

Prof. Yuval Elovici
elovici@inter.net.il

Publications

M. Guri, B. Zadov, E. Atias, and Y. Elovici, "LED-It-GO: Leaking (a lot) of Data from Air-Gapped Computers via the (small) Hard Drive LED," 2017. arXiv:1702.06715.

Demo Video

https://www.youtube.com/watch?v=4vIu8Id68fc