xLED: Covert Data Exfiltration from Air-gapped Networks via Router LEDs

Researchers

Dr. Mordechai Guri
moti.guri@gmail.com

Boris Zadov
borisza@gmail.com

Andrey Daidakulov
daidakul@post.bgu.ac.il

Prof. Yuval Elovici
elovici@inter.net.il

Publications

M. Guri, B. Zadov, A. Daidakulov, and Y. Elovici, "xLED: Covert Data Exfiltration from Air-Gapped Networks via Router LEDs," 2017. arXiv:1706.01140.

Demo video

https://www.youtube.com/watch?v=mSNt4h7EDKo

Goals

We demonstrate how attackers can covertly leak data (e.g., encryption keys, passwords and files) from highly secure or air-gapped networks via the row of status LEDs that exists in networking equipment such as LAN switches and routers.

Description

Although it is known that some network equipment emanates optical signals correlated with the information being processed by the device ('side-channel'), intentionally controlling the status LEDs to carry any type of data ('covert-channel') has not been previously studied. We show how a malicious code is executed on the LAN switch or router, allowing full control of the status LEDs. Sensitive data can be encoded and modulated over the blinking of the LEDs. The generated signals can then be recorded by various types of remote cameras and optical sensors. We provide the technical background on the internal architecture of switches and routers (at both the hardware and software level) which enables this type of attack. We also present amplitude and frequency based modulation and encoding schemas, along with a simple transmission protocol. We implemented a prototype of an exfiltration malware and present a discuss of its design and implementation. We evaluated this method with a few routers and different types of LEDs. In addition, we tested various receivers including remote cameras, security cameras, smartphone cameras, and optical sensors, and addressed different detection and prevention countermeasures. Our experiment shows that sensitive data can be covertly leaked via the status LEDs of switches and routers at a bit rates of 10 bit/sec to more than 1Kbit/sec per LED.