Cyber researchers discover how any network router can covertly leak data

5 June 2017

Credit: CC0 Public Domain

Researchers at the Ben-Gurion University of the Negev (BGU) Cyber Security Research Center (CSRC) have demonstrated for the first time that it is possible to covertly siphon sensitive files, passwords or other critical data from any common router.

In the new paper, the researchers demonstrated how LEDs functionality can be silently overridden by malware they developed (code named "xLED"), which infects firmware in the device. Once the xLED malware infects the network device, it gains full control of the LEDs that flash to indicate status.

Network devices such as routers and local area network switches typically include activity and status LEDs used to monitor traffic activity, alerts and provide status.

According to research leader Dr. Mordechai Guri, the head of research and development at the BGU CSRC, "sensitive data can be encoded and sent via the LED light pulses in various ways. An attacker with access to a remote or local camera, or with a light sensor hidden in the room, can record the LED's activity and decode the signals."

Click here to watch a video of the demonstration and determine what famous book is being leaked via the flickering LED signals of a WIFI router.

"Unlike network traffic that is heavily monitored and controlled by firewalls, this covert channel is currently not monitored, says Dr. Guri. As a result, it enables attackers to leak data while evading firewalls, air-gaps (computers not hooked up to the internet) and other data-leakage prevention methods."

The xLED malware can program the LEDs to flash at very fast speeds - more than 1,000 flickers per second for each LED. Since a typical router or network switch includes six or more status LEDs, the transmission rate can be multiplied significantly to as much as thousands of bits per second. As a result, a significant amount of highly sensitive information can be encoded and leaked over the fast LED signals, which can be received and recorded by a remote camera or light sensor.

The BGU CSRC has a dedicated research program to uncover and demonstrate vulnerabilities of electronic devices. Over the past two years, they have successfully demonstrated how malware can siphon data from computer speakers, headphone jacks, hard drives, and computer fans, as well as 3D printers, smartphones, LED bulbs, and other IoT devices.

Provided by American Associates, Ben-Gurion University of the Negev