Issued 2/23/17

Engineers Exfiltrate Data by Blinking Hard Drives' LEDs

That roll of tape you use to cover the Webcam? Better use some of it on your hard-drive LED, because it can be a data exfiltration vector.

Exfiltration experts from Ben-Gurion University of the Negev's Cyber Security Research Center have added to previous techniques like fan modulation, GSM transmissions, or listening to the RF from USB2 transmissions, have now created malware to control hard drive LEDs. The team led by veteran exfiltrator Mordechai Guri flashes the LED at atound 5,800 on/off cycles per second as a data channel, good enough for 4 Kbps of transmission. That performance also depends on what you use as the receiver: it might be a Digital SLR or high-end security camera (15 bps), a GoPro-level camera (up to 120 bps), a Webcam or Google Glass Explorer (also 15 bps), or a smartphone camera (up to 60 bps).

If you can lay hands on a good photodiode sensor – they're not expensive, the Thorlabs PDA100A they used can be had on eBay for less than US$100 – you'll get around 4 Kbps. In the video below [link], the researchers fitted the detector to a drone, flew it to a window through which the infected disk was visible and started sucking data. Since PCs lack any generic API to control the hard disk LED, the malware from Guri's team takes the direct approach: a small chunk of code to perform reads and writes to the disk, along with a protocol to tell the receiver what it's looking for.